www.FutureOfFinance.org **THE FUTURE OF FINANCE PROJECT**

A Report on the Future of Finance, Future of Risk, and Future of Quant

'Knight Reconsidered'
Risk, Uncertainty, and, Profit for the Cyber Era

Post-Doctoral Research Thesis on
Finance, Risk, and, Quant Modeling
Beyond the Global Financial Crisis

January 2015

Dr. Yogesh Malhotra
PhD, MSQF, MSNCS, MSCS, MSAcc, MSEco, BE
CEng, CISSP, CISA, CEH, CCP/CDP, CPA (Education)
Who's Who in America®, *Who's Who in the World®*,
Who's Who in Finance & Industry®,
Who's Who in Science & Engineering®
Global Risk Management Network, LLC
757 Warren Road, Cornell Business and
Technology Park, Ithaca, NY 14852-4892
dr.yogesh.malhotra@gmail.com (646) 770-7993
https://www.linkedin.com/in/yogeshmalhotra
http://www.yogeshmalhotra.com/

SUNY POLYTECHNIC INSTITUTE

SUNYIT New York's Public Polytechnic

Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics

MS Network and Computer Security Thesis

On Model Risk Management of Statistical Probability Distributions in Cyber Insurance Modeling

Yogesh Malhotra, PhD

www.yogeshmalhotra.com

Thesis Presented to the

Department of Network and Computer Security

Department of Computer Science

In Partial Fulfillment

of the Requirements for the

Master of Science in Network and Computer Security Degree

SUNY The State University of New York

Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics

MS Network and Computer Security Thesis

Yogesh Malhotra, PhD
www.yogeshmalhotra.com

Declaration

I declare that this thesis is my own work and has not been submitted in any form for another degree or diploma at any university or other institute of tertiary education. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references and sources is included. Information cited from other sources in the text and/or listed references and footnotes/endnotes is acknowledged as the intellectual property of corresponding respective sources. Any trademarks cited are likewise acknowledged as the intellectual property of corresponding respective sources.

Yogesh Malhotra

Yogesh Malhotra, PhD

January 19, 2015

Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics

MS Network and Computer Security Thesis

DEPARTMENT OF NETWORK AND COMPUTER SECURITY
DEPARTMENT OF COMPUTER SCIENCE

Approved and recommended for acceptance as a thesis in partial fulfillment of the requirements for the degree of **Master of Science in Network and Computer Security**.

DATE _____

_____

Prof. Jorge Novillo, PhD, Thesis Chair and Research Advisor

_____

Prof. John Marsh, PhD, Thesis Co-Chair and Research Advisor

_____

Prof. Saumendra Sengupta, PhD, Thesis Co-Chair and Research Advisor

_____

Prof. Kevin Kwiat, PhD, Information Assurance Research Advisor

_____

Prof. Zora Thomova, PhD, Quantitative Finance Research Advisor

_____

Dr. John Bay, PhD, External Reviewer and Cybersecurity Practice Advisor

Preface

Coming from an Engineering background as a Chartered Engineer, I led global Banking & Finance modeling and development projects for largest US and worldwide banks. I also led modeling and implementation projects for the Big-3 IT firm on which hundreds of global Banking & Finance firms relied as a key global financial systems provider. Then, I earned a quantitative double doctorate from a Top-10 PhD Program and subsequently taught as Associate Professor and Assistant Professor of Quantitative Methods at Syracuse University with research focus on quantitative risk modeling. Just before the Global Financial Crisis, my research was surfacing critical questions about the *model risk* inherent in Financial Engineering models. For instance, I made reference to it in an interview by a UK based global management research publisher in 2005.

Those questions were about the compatibility of deterministic and stochastic models of natural sciences with the increasingly non-deterministic, i.e., *uncertain*, sociotechnical post-WWW digitally social networked world. Those questions were also about the capacity of deterministic and stochastic Financial Engineering *risk* models to cope with increasing *uncertainty* characterizing a rapidly and dynamically changing digital world. Those questions led me to post-doctoral research in Quantitative Finance leading to working for top Wall Street investment banks such as JP Morgan Private Bank in midtown Manhattan. My technical and applied hands-on leadership guiding JP Morgan top executives and MDs focused on advancing their advanced Quantitative Finance risk modeling and analytics. I focused on guiding their financial risk modeling beyond quantitative models that had become targets of criticism given association with large-scale financial failures over the span of the Global Financial Crisis.

After concluding those Quantitative Finance projects, I continued to further advance related post-doc research in Computational Finance and Cybersecurity. While conducting research on rapidly increasing Cyber risk in Banking and Finance domains with emergency warnings coming from the White House, US Treasury, Department of Homeland Security, and, Office of Comptroller of Currency, this thesis was born. It was born out of the observation about the specific risk models *blamed* for the Global Financial Crisis which nearly drove US investment banks to extinction. *The same models were now becoming the predominant models of choice by commercial providers for cyber risk and cyber insurance related modeling for estimation of potential cyber risk related financial loss….*

Abstract

Quantitative modeling of cyber risk for cyber insurance modeling is at a nascent stage characterized by sparse empirical research and reliable data. Our current investigation reveals that VaR, short for Value-at-Risk (Jorion, 2006), is the current predominant model of choice for cyber insurance modeling. Model risk related to VaR was a key factor in the Global Financial Crisis given its known limitations in modeling tail risks and systemic risks (Haldane & Nelson, 2012; Malhotra, 2012, 2014[1]). As a result, US Federal Reserve and OCC issued model risk compliance guidance for US financial institutions (US Fed & OCC, 2011). Basel Committee of worldwide central bank supervisors stopped relying on VaR for risk modeling (BCBS, 2013). Given history of model risks associated with VaR, we investigate if current reliance of cyber insurance modeling on VaR entails model risk. We develop qualitative frameworks to benchmark relative levels of tail risks and systemic risks associated with cyber risk vis-à-vis financial risks typically modeled with VaR. Our analysis reveals that cyber risk entails exponentially higher tail risks and systemic risks thus making VaR unfit for reliance as the primary risk model for cyber insurance modeling. We develop specific frameworks of model risk management (Derman, 1996; Morini, 2011) for cyber insurance modeling and demonstrate their empirical application in model risk management. We distinguish between model risks arising from the choice of specific quantitative models from those arising from the choice of quantitative methodologies. We demonstrate how to manage model risks associated with VaR using it with multiple simple and advanced models to cross-check its reliability. We also offer alternative coherent risk measures as better alternatives to VaR and empirically demonstrate their application. To enable further minimization of model risk in cyber insurance modeling we do three more things. First, we analyze the Bayesian quantitative statistical inference methodology as a possible alternative to frequentist classical inference methodology that VaR and advanced models typically rely upon. Second, we analyze the Markov Chain Monte Carlo models and related Gibbs Sampling and Metropolis-Hastings statistical computing algorithms to enable the use of Bayesian methodology. Finally, given increasing uncertainty in cyber risk modeling and management, we develop a framework for enabling Knightian uncertainty management (Knight, 1921) relating it to model risk management.

[1] http://ssrn.com/abstract=2538401

Contributions

To avert the impending national Cyber risk and Cyber-insurance disaster based upon large-scale commercial reliance upon quantitative models with inherent model risks, tail risks, and systemic risks in current form, this dissertation makes the following key contributions.

- First, we develop the first known Cyber-Finance-Trust framework for Cyber insurance modeling to analyze how finance risk entangled with Cyber risk further exacerbates the systemic, interdependent, and correlated character of Cyber risks.
- Second, we develop the first known model risk management framework for Cyber insurance modeling as model risk management has received sparse attention in Cyber risk assessment and Cyber insurance modeling.
- Third, our review of quantitative models in Cyber risk and Cyber insurance modeling develops the first known analysis establishing significant and extreme *model risks*, *tail risks*, and, *systemic risks* related to predominant models in use.
- Fourth, we develop an empirical study of VaR and Bayesian statistical inference methodologies with specific guidance for containing model risks by applying multiple simple and advanced models for cross-checking the reliability of VaR.
- Fifth, we develop an analysis of the Markov Chain Monte Carlo Models, Gibbs Sampling and Metropolis-Hastings statistical computing algorithms for enabling Bayesian statistical inference methodologies to minimize model risk in Cyber risk and Cyber insurance risk modeling for the specific context of cybersecurity.
- Sixth, we develop the first known portfolio theory based framework for Cyber insurance modeling with guidance to minimize model risks, tail risks, and systemic risks inherent in models in commercial Cyber insurance modeling.
- Finally, given increasing role of uncertainty in cyber (and financial) risk modeling and management, we develop a framework for enabling Knightian uncertainty management relating it to model risk management.

Understanding of the developed frameworks and technical models listed above should minimize model risk in the recommended applications based on above contributions.

Acknowledgements

The current thesis marks the culmination of post-doctoral research in computational quantitative risk modeling and risk management. It lasted a bit longer than the PhD earned 17 years ago with doctoral fellowship and scholarship supported research done at the University of Pittsburgh and the Carnegie Mellon University. The current post-doc research advances upon my earlier uncertainty management and quantitative risk modeling research published prior to the Global Financial Crisis of 2008-2009. The latest research spanned multiple organizations and institutions across academia and industry. Research done in Banking & Finance industry included hands-on technical research leadership of leading-edge quantitative risk modeling for $1 trillion funds at Wall Street investment banks such as JP Morgan Bank. Research done across academic programs included Quantitative Finance program at the Fordham University; PRMIA Quantitative Finance and Risk Management program at the Kellogg School of Management; Financial Engineering program at the University of California, Berkeley; and, Computer Science, Network & Computer Security, and Accountancy programs at the SUNY Polytechnic Institute. I acknowledge the contributions of the respective faculties in advancing the current post-doc research program.

I am grateful to Dr. Emanuel Derman, earlier Head of Quantitative Risk Strategies Group at Goldman Sachs who now directs the Financial Engineering program at the Columbia University. His pioneering work on Model Risk Management is the inspiration behind the central and primary focus of this thesis. His personal feedback about my quantitative risk modeling and uncertainty management research over the last two decades is greatly appreciated. In course of two meetings with him in midtown Manhattan, his responses affirmed two key working hypotheses guiding overall focus of my research program. The first hypothesis was about the past (sociotechnical) uncertainty management focus of my research program. The second hypothesis was about the future of quantitative risk modeling (and quantitative finance) which is the central focus of this thesis.

Computational quantitative risk modeling research done for the JP Morgan Private Bank under direct supervision of JP Morgan Global Head of Quantitative Research & Analytics and US Head of Portfolio Management Dr. Georgiy V. Zhikharev served as the key technical background and input for the thesis. I am grateful to him for his mentorship and for the opportunity to serve as hands-on technical leader for leading

his Portfolio Liquidity Assessment Framework Development, and, Portfolio Construction, Optimization & Stress Testing projects. I am also thankful to him for the opportunity to guide and advise his team of Managing Directors, Portfolio Managers, and senior Quants, and, lead his team of Quant analysts for the development of quantitative risk models.

I am grateful for academic support and mentorship of senior professors at the Fordham University Quantitative Finance program as their guidance advanced my research leading to Quantitative Finance leaderships with above Wall Street banks. Dr. James R. Lothian, Topetta Family Chair in Global Financial Markets and Distinguished Professor of Finance was my mentor and advisor for applied macroeconomics modeling. Dr. Paul D. McNelis, Robert Benheim Professor of Economics and Financial Policy, was my mentor and advisor for advanced financial econometrics modeling. Professor Nusret Cakici was my advisor for large-scale data modeling which inspired my interest in financial high frequency econometric modeling. Their support is gratefully acknowledged.

The current thesis on Model Risk Management of Statistical Probability Distributions in Cyber Insurance Modeling was written independently while working on the most recent two Masters in the Computer Science department at the SUNY Polytechnic Institute. For the current thesis, I acknowledge specific contributions of the following SUNY Polytechnic senior faculty members.

First, I am grateful for the unsurpassed and unequalled academic support of **Dr. Jorge Novillo (PhD Mathematics, Lehigh University)**, Professor of Computer Science and former Dean of Information Systems and Engineering Technology. For the current thesis, Dr. Novillo, an academic descendant of Carl Friedrich Gauss (founder of the *Gaussian distribution* known popularly as the *normal distribution* in probability theory), provided unsurpassed academic support. Interestingly, the thesis focused on advancing statistical probabilistic computational quantitative risk modeling and computational quantitative risk management *beyond* the Gaussian distribution. He was the primary MS Network & Computer Security thesis supervisor and advisor; formal advisor for MS Computer Science; supervisor and advisor on multiple MS Network & Computer Security and MS Computer Science independent study courses, project courses, and supervised courses.

Next, I am grateful for the unsurpassed and unequalled academic support of **Dr. John A. Marsh (PhD Physics, Carnegie Mellon University)**, Associate Professor of

Computer Science and Associate VP for Research. He was the MS Network & Computer Security thesis co-supervisor and advisor; formal advisor for MS Network & Computer Security; supervisor and advisor on multiple MS Network & Computer Security and MS Computer Science supervised courses. Most of the technical chapters of the thesis focused specifically on statistical probabilistic models and methodologies of quantitative risk modeling and quantitative risk management were developed in course of the research conducted for independent and supervised courses taken with Dr. Novillo and Dr. Marsh. Multiple other computational quantitative modeling Quantitative Finance and Cryptography papers, some of which are referenced here, were also written while advancing research in course of Computer Science and Network & Computer Security projects done with them.

Next, I am grateful for the academic support of **Dr. Saumendra Sengupta (PhD Physics, University of Waterloo**, home of the Institute for Quantum Computing**)**, Professor of Computer Science. He was the administrative thesis co-chair and sounding board in the initial write-up phase. I thank him for his discussions about his prior PhD research on Bose-Einstein condensate in the context of my nascent interest in Quantum Computing, at one point even contemplating a future PhD in Quantum Computing. His guidance on numerical methods in large scale data modeling furthered my interest in that area based on my recent SAS high frequency econometric large-scale data modeling and market microstructure liquidity modeling research leadership with a top Wall Street investment bank. His guidance on operating systems provided the inspiration to further my interest in hedge fund systematic trading strategies by investigating C++11 concurrency and multi-threading for minimizing latency of high-frequency trading transactions for hedge funds.

Next, I am grateful for the academic support and mentorship of **Dr. Kevin Kwiat, (PhD Computer Engineering, Syracuse University)**, CIV USAF AFMC AFRL/RIGA, Program Manager & Principal Computer Engineer, Air Force Research Laboratory, as Information Assurance Research Advisor and instructor at the SUNY Polytechnic Institute. Given his applied engineering focus, his research and teaching relate scientific high-impact research and applications in most advanced Cybersecurity practices. He was a great inspiration for advancing my computer science and cybersecurity research both as a mentor as well as a computer science and cybersecurity research leader. His work advances information assurance research in multiple collaborations spanning academia, policy, and practice spanning the world. He was the

inspiration for advancing my prior sociotechnical research focus on Claude Shannon's Information Theory[2], originally inspired by Dr. John Holland, the founder of genetic algorithms. He inspired my exploration into coalescing sociotechnical research focus on Claude Shannon's information theory with quantum computing and quantum cryptography leading to my research report presentation titled 'Quantum Computing, Quantum Cryptography, Shannon's Entropy and Next Generation Encryption & Decryption.'

Next, I am grateful for the academic support of **Dr. Zora Thomova, (PhD Mathematics, University of Montreal)**, Chair and Professor of Mathematics, and, Finance Faculty at the SUNY Levin Institute, for serving on the thesis committee as Quantitative Finance Research Advisor. As a professional mathematician whose research, practice, and teaching span applied Math and applied Finance for New York City and Wall Street firms, her insights into securitization of Cyber risk and applications spanning the SME Finance and Banking and Insurance were greatly appreciated.

Last but not the least, I am grateful for the academic support and mentorship of **Dr. John Bay, (PhD Electrical Engineering, Ohio State University)**, for serving as the External Reviewer and Cybersecurity Practice Advisor. As the current Executive Director of the New York State's Cyber Research Institute and having served in prior Senior Executive roles spanning research academia, policy, and practice, including Chief Scientist, Information Directorate, Air Force Research Laboratory, his applied insights and critical reviews of the thesis draft were most highly valued. I am particularly grateful to him for his key contributions at both the initial and final stages of the thesis. Initially, his insights into the global cybersecurity practice were most enlightening in advancing the focus beyond risk prevention to risk control. His perspective from the Cybersecurity national defense perspective seemed to mirror the ongoing transition in global Finance from risk modeling to uncertainty management in Knightian terms. Finally, he provided the most diligent and critical review in helping shape the practical and applied focus of the finished dissertation that greatly benefited

[2] Malhotra, Y., Expert Systems for Knowledge Management: Crossing the Chasm between Information Processing and Sense Making, Expert Systems with Applications: An International Journal, 20(1), 7-16, 2001, WWW: http://www.brint.org/expertsystems.pdf. Cryptology beyond Shannon's Information Theory: Preparing for When the 'Enemy Knows the System' With Technical Focus on Number Field Sieve Cryptanalysis Algorithms for Most Efficient Prime Factorization on Composites, http://www.yogeshmalhotra.com/MalhotraYogesh_CryptanalysisReport.pdf.

from his insights. I am also grateful for his mentorship in introducing my current research program to other senior academics with active research in the Cybersecurity domain.

The current post-doctoral research yielded almost twice as many graduate credits relative to the prior quantitative top-10 PhD double doctorate in IT-Statistics-Quantitative Methods focused on social sciences. It resulted in four new graduate Masters with focus on computational quantitative risk modeling and risk management including MS in Quantitative Finance with Applied Math focus, MS in Network & Computer Security, MS in Computer Science, and MS in Accountancy. Options existed for pursuing additional top-10 PhD either in Economics or in Accountancy with admission offers from both received near the beginning of the current post-doc research. The recent research was however inspired toward greater emphasis on Mathematical Sciences, Computing Sciences, and, Network Sciences to complement prior PhD and subsequent role as Associate Professor and Assistant Professor of Quantitative Methods in IT and Operations Research at Syracuse University. Current natural sciences research focus of my uncertainty management and risk modeling research however builds upon prior social sciences research. Hence, prior faculty colleagues from research academia whose support I would like to acknowledge for prior uncertainty management research conducted in the social sciences tradition before the Global Financial Crisis are listed below.

For speaking invitation to share my research program as well as subsequent invitation to serve as the Fulbright-Queen's University Visiting Research Chair while I served on the faculty at Syracuse University, I am grateful to the Queen's University (Canada). For recognizing my research as an exemplar of serving the public good on the occasion of the above invitation, I am grateful to the then Syracuse University Chancellor and President Dr. Nancy Cantor. For supporting my scholarly, instructional, and applied research as departmental supervisors at Syracuse University Martin J. Whitman School of Management, I am grateful to Dr. Michel Benaroch, Associate Dean for Research & PhD Programs and Professor of Information Systems, and, Dr. Randy Elder, Senior Associate Dean and Professor of Accounting. For supporting my scholarly research and instructional innovation programs as directors of research grant programs in disciplinary areas, I am grateful to Professor of Information Systems Dr. Michel

Benaroch; Professors of Operations Research Fred Easton and Scott Webster; and, Professors of Marketing and Innovation Tridib Mazumdar and David Wilemon. For reviewing manuscripts of my research on quantitative risk and controls modeling subsequently published in top research journals while serving on the faculty at Syracuse University, I am grateful to Professors Jeffrey M. Stanton and Robert Heckman of the Syracuse University School of Information Studies. For invitation to serve on the Syracuse University School of Information Studies PhD committee as external examiner, I am grateful to Professor Ping Zhang. For his role as my PhD thesis chair and advisor, I am grateful to Dr. Dennis Galletta, current Professor of Information Systems & Director of the Doctoral Program at the Katz Graduate School of Business, University of Pittsburgh. For his role as Management Control Systems concentration PhD advisor, I am grateful to Dr. Jacob G. Birnberg, current Robert W. Murphy Jr. Professor of Management Control Systems Emeritus, Business Analytics & Operations at the Katz Graduate School of Business, University of Pittsburgh. For inviting me for PhD research fellowship at the University of Pittsburgh and his role as my MIS major advisor, I am grateful to Dr. William R. King, then University Professor at the Katz Graduate School of Business, University of Pittsburgh.

Table of Contents

List of Tables

List of Figures

Chapter 1.

1.1 Introduction

"The new business model of the Information Age, however, is marked by fundamental, not incremental, change. Businesses can't plan long-term; instead, they must shift to a more flexible 'anticipation-of-surprise' model."

-- Yogesh Malhotra in CIO Magazine interview, September 15, 1999.

"Cyber threats pose one of the gravest national security dangers to the United States. America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet."

-- *Statement by the US President on the Cybersecurity Framework, February 12, 2014*.

"Cyber hacking is a potentially existential threat to our financial markets and can wreak serious havoc on the financial lives of consumers. It is imperative that we move quickly to work together to shore up our lines of defense against these serious risks."

-- *Benjamin M. Lawsky, Superintendent of Financial Services, New York State Department of Financial Services, December 10, 2014, New Cyber Security Examination Process*.

"In our existing environment and at our company, cybersecurity attacks are becoming increasingly complex and more dangerous. The threats are coming in not just from computer hackers trying to take over our systems and steal our data but also from highly coordinated external attacks both directly and via third-party systems (e.g., suppliers, vendors, partners, exchanges, etc.)."

-- *Jamie Dimon, Chairman & CEO, JP Morgan Chase & Co., Annual Letter to Shareholders, April 9, 2014*.

In the wake of the most recent Sony Pictures Entertainment (SPE) hack of December 2014, the Federal Bureau of Investigation (FBI), reiterating the US President, noted that "*cyber threats pose one of the gravest national security dangers*"[3] to the US. Barely three months ago, the data breach at the US financial institution JP Morgan, impacted 76 million of 117 million US

[3] http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

households, and, 7 million small businesses[4]. Given exponentially rising criticality of cyber-attacks, the natural question is how to assess exposure to cyber risks[5].

We define *cyber risk* as *inherent* in all cyber activities including cyber-finance and cyber-economics. Just like the use of any model entails associated *model risk*, similarly use of cyber involves associated cyber risk. In the first known cyber-finance-trust framework relating cyber, finance, and trust domains to elicit the key attributes of cyber risk, we further interpret cyber risk as "risk having consequences affecting the confidentiality, availability, integrity, authentication, non-repudiation, or accessibility of information." Thus, we distinguish cyber risks from (traditional notions of) financial risks (such as market risks, credit risks, liquidity risks, etc.) modeled by VaR in this dissertation.

The above basis of our distinctions and characterization of cyber risk is based upon our analysis discussed further. The key points of such distinctions and characterizations are captured in our following summary statement resulting from our analysis. *Unlike other risks, cyber risk poses a uniquely different set of exposures as it is intertwined with the* ***medium*** *and the* ***message*** *in the increasingly global* ***interconnected***, ***distributed***, *and,* ***networked*** *world of* ***digital communications*** *powered by* ***universal use*** *and* ***reuse*** *of enabling* ***global monocultures*** *of information and communication technologies and* ***standard computing network protocols***.

To avert the impending national cyber risk and cyber-insurance disaster based upon large-scale commercial reliance upon quantitative models with inherent model risks, *tail risks*, and *systemic risks*, this dissertation makes the following key contributions. (*Systemic risk* is the risk of 'spillover' of loss from a specific entity beyond it to other entities resulting in system wide risk. *Tail risk* results from *theoretical* statistical probabilistic distribution assumptions of *normality* about relative *in*frequency of extremely rare but high impact losses in the left tail of the distribution that may not hold in *practice* because of fat tails resulting from high kurtosis.)

- First, we develop the first known cyber-finance-trust framework for cyber insurance modeling to analyze how financial risk entangled with cyber risk further exacerbates the *systemic*, *interdependent*, and *correlated* character of cyber risks.
- Second, we develop the first known model risk management framework for cyber insurance modeling as model risk management has received sparse attention in cyber risk assessment and cyber insurance modeling.

[4] http://www.bloomberg.com/news/2014-10-02/jpmorgan-says-data-breach-affected-76-million-households.html
[5] http://www.yogeshmalhotra.com/cyberrisk.html

- Third, our review of quantitative models in cyber risk and cyber insurance modeling develops the first known analysis establishing significant and extreme *model risks*, *tail risks*, and, *systemic risks* related to predominant models in use.
- Fourth, we develop an empirical study of VaR and Bayesian statistical inference methodologies with specific guidance for containing model risks by applying multiple simple and advanced models for cross-checking the reliability of VaR.
- Fifth, we develop an analysis of the Markov Chain Monte Carlo Models, Gibbs Sampling and Metropolis-Hastings statistical computing algorithms for enabling Bayesian statistical inference methodologies to minimize model risk in cyber risk and cyber insurance risk modeling for the specific context of cybersecurity.
- Sixth, we develop the first known portfolio theory based framework for Cyber insurance modeling with guidance to minimize model risks, tail risks, and systemic risks inherent in models in commercial Cyber insurance modeling.
- Finally, given increasing role of uncertainty in cyber (and financial) risk modeling and management, we develop a framework for enabling Knightian uncertainty management relating it to model risk management.

1.2 Overview of Cyber Risk and Cyber Insurance

Given emergence of cyber risk as a most critical risk, cyber insurance is still a nascent business as studies explore the viability of cyber insurance models. One such recent study (Biener et al., 2015) recognizes the distinct characteristics of cyber risks compared to other operational risks given significant problems resulting from highly interrelated losses, lack of data, and severe information asymmetries. Many definitions of cyber risk at different levels of analyses are reviewed in that study. Given our primary focus on information assurance and cybersecurity, we define cyber risk as "risk having consequences affecting the confidentiality, availability, integrity, authentication, non-repudiation, or accessibility of information." Some descriptions (such as Bodin et al. (2005)) classify the last three aspects, namely, authentication, non-repudiation, and accessibility, as subcomponents of availability. In our view informed by secure encryption protocols, however, the three aspects can exist independently of actual availability; that is why we think there is need to be technically more specific.

Furthermore, in contrast to studies such as Biener et al. (2015), we do not view cyber risk as "operational risk" say as distinct from 'market risk' or 'credit risk.' In our information based view, all networked information based risks including market risks, credit risks, currency risks, interest rate risks, etc., form a subset of cyber risk. In as much as all these risks

are represented in terms of digital information which can be subject to information based manipulation or hacking, they are in fact cyber risks. That being said, our definition is broad as well as consistent with how regulators of insurance and financial markets categorize cyber risk. The only difference is apparently that we are not trying to draw artificial lines with fingers in dry sand. In other words, *if the risk is associated with "cyber" activities, it is cyber risk where "cyber" is short for cyberspace*.

Thus, we define *cyber risk* as *inherent* in all cyber activities including cyber-finance and cyber-economics. Just like use of any model entails associated model risk, similarly use of cyber involves associated cyber risk. The current discussion focuses on the first known cyber-finance-trust framework relating cyber, finance, and trust domains to elicit the key attributes of cyber risk. Based upon our analysis, we interpret cyber risk as "risk having consequences affecting the confidentiality, availability, integrity, authentication, non-repudiation, or accessibility of information." Hence, we distinguish cyber risks from (traditional notions of) financial risks (such as market risks, credit risks, liquidity risks, etc.) in this dissertation.

Our view is both forward-looking as well as a more conservative in its delineation of cyber risks, as our later analysis elucidates how *cyber risks in fact subsumes many other risks*[6]. Our point is all the more relevant given that in the currently nascent cyber insurance industry, some of the early players such as Lloyd's syndicate Aegis London (in global partnership with PwC) already provide coverage for state-sponsored attacks besides other cyber risks. Many of the large corporations, including the largest US financial firms are also cognizant of risks from large-scale sophisticated cyberattacks. Significant cyber insurance coverage for such risks may *yet* be within purview of only deep pockets and deep expertise typically associated with nation state sponsorships.

In our view, the specific (direct or indirect) source of attack is of lesser interest in characterizing the specific attack as compared with the scope, scale, and, impact of the specific attack, which characterize the real risk of expected loss. On the other hand, the source of attack could be important in determining insurance coverage of loss as specific insurance policies do exclude risk and losses attributable to specific sources of cyber risk. That being said, it is critical to note that in the cyber risk realm of the cyber domain, in contrast to (traditional) financial risk realm of the finance domain, it is most challenging to even ascertain the source of cyberattack with certainty. Even in case of the most publicized national cyberattack with

[6] http://www.yogeshmalhotra.com/GriffissCyberspace.html

apparently the most significant economic losses, the security expert and cryptographer Bruce Schneier notes the following about the actual source of the recent SPE attack (Schneier, 2014[7], Zetter, 2014[8]): "However you read it, this sort of evidence is circumstantial at best. It's easy to fake, and it's even easier to interpret it wrong." Categories of sources of cyber risk and as depicted by Biener et al. (2015)[9] are shown in the following Table 1-1.

Table 1-1. Categories of Cyber Risk Consistent with CERT, Basel II, and Solvency II

Category	Description	Elements
Subcategory 1: actions of people		
1.1 Inadvertent	unintentional actions taken without malicious or harmful intent	mistakes, errors, omissions
1.2 Deliberate	actions taken intentionally and with intent to do harm	fraud, sabotage, theft, and vandalism
1.3 Inaction	lack of action or failure to act in a given situation	lack of appropriate skills, knowledge, guidance, and availability of personnel to take action
Subcategory 2: systems and technology failures		
2.1 Hardware	risks traceable to failures in physical equipment	failure due to capacity, performance, maintenance, and obsolescence
2.2 Software	risks stemming from software assets of all types, including programs, applications, and operating systems	compatibility, configuration management, change control, security settings, coding practices, and testing
2.3 Systems	failures of integrated systems to perform as expected	design, specifications, integration, and complexity
Subcategory 3: failed internal processes		
3.1 Process design and/or execution	failures of processes to achieve their desired outcomes due to poor process design or execution	process flow, process documentation, roles and responsibilities, notifications and alerts, information flow, escalation of issues, service level agreements, and task hand-off
3.2 Process controls	inadequate controls on the operation of the process	status monitoring, metrics, periodic review, and process ownership
3.3 Supporting processes	failure of organizational supporting processes to deliver the appropriate resources	staffing, accounting, training and development, and procurement
Subcategory 4: external events		
4.1 Catastrophes	events, both natural and of human origin, over which the organization has no control and that can occur without notice	weather event, fire, flood, earthquake, unrest
4.2 Legal issues	risk arising from legal issues	regulatory compliance, legislation, and litigation
4.3 Business issues	risks arising from changes in the business environment of the organization	supplier failure, market conditions, and economic conditions
4.4 Service dependencies	risks arising from the organization's dependence on external parties	utilities, emergency services, fuel, and transportation

[7] http://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/?single_page=true

[8] http://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/

[9] http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf

The above categories of sources of cyber risk are originally from the CERT taxonomy of operational cyber risks by Cebula & Young (2010) [10] and Cebula et al. (2014)[11]. They are compatible with the financial capitalization standards for global banks such as Basel II and Solvency II. A forward-looking view of cyber insurance is available in more recent new cyber insurance products that offer property damage, bodily injury, environmental pollution and cyber terrorism wrapped around existing policies. One example of such cyber insurance coverage provider is Aegis London[12] whose offering in partnership with PwC is inspired by the view that cyberattacks will be the 'new normal' in 2015 with an increase in destructive attacks linked to on-going global conflicts.

Table 1-2. Categories of Cyber Risk Consistent with CERT, Basel II, and Solvency II

Coverage	Cause of cyber loss	Insured losses
Panel A: Third Party		
Privacy Liability	- Disclosure of confidential information collected or handled by the firm or under its care, custody, or control (e.g., due to negligence, intentional acts, loss, theft by employees)	- Legal liability (also defense and claims expenses (fines), regulatory defense costs) - Vicarious liability (when control of information is outsourced) - Crisis control (e.g., cost of notifying stakeholders, investigations, forensic and public relations expenses)
Network Security Liability	- Unintentional insertion of computer viruses causing damage to a third party - Damage to systems of a third party resulting from unauthorized access of the insured - Disturbance of authorized access by clients - Misappropriation of intellectual property	- Cost resulting from reinstatement - Cost resulting from legal proceeding
Intellectual Property and Media breaches	- Breach of software, trademark and media exposures (libel, etc.)	- Legal liability (also defense and claims expenses (fines), regulatory defense costs)
Panel B: First Party		
Crisis Management	- All hostile attacks on information and technology assets	- Costs from specialized service provider to reinstate reputation - Cost for notification of stakeholders and continuous monitoring (e.g., credit card usage)
Business Interruption	- Denial-of-service attack - Hacking	- Cost resulting from reinstatement - Loss of profit
Data Asset Protection	- Information assets are changed, corrupted, or destroyed by a computer attack - Damage or destruction of other intangible assets (e.g., software applications)	- Cost resulting from reinstatement and replacement of data - Cost resulting from reinstatement and replacement of intellectual property (e.g., software)
Cyber Extortion	- Extortion to release or transfer information or technology assets such as sensitive data - Extortion to change, damage, or destroy information or technology assets - Extortion to disturb or disrupt services	- Cost of extortion payment - Cost related to avoid extortion (investigative costs)

[10] http://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf
[11] http://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf
[12] http://www.cirmagazine.com/cir/Aegis-London-launches-Cyber-Resilience-plus.php

A rearview perspective of cyber insurance policies in existence is available in review of the cyber insurance practices by Biener et al. (2015)[13] and illustrated in Table 1-2. On the demand side, the recent academic presentation titled 'Cybersecurity Investment Optimization with Risk: Insights for Resource Allocation' by a researcher at the University of Massachusetts Amherst pegs cybersecurity investments reaching $120Bn by 2017 growing 11% annually[14]. The cyber risk investment framework composed of Attacks, Assets, and Countermeasures proposed by that research is shown in Table 1-3.

Table 1-3. Cyber Risk Investment Framework of Attacks, Assets, and Countermeasures

ATTACKS	COUNTERMEASURES
Basic attacks:	*Detective countermeasures:*
Keyloggers and spyware	Anti-virus software
Backdoor or command control	Anti-spyware software
Unauthorized access via weak access control lists	Content monitoring
Unauthorized access via stolen credentials	Forensic tools
Physical theft of assets	Intrusion detection system software
Brutal force attack	Log management software
Advanced attacks:	
Abuse of system access/privileges	*Preventive countermeasures:*
Violation of acceptable use and other policies	Biometrics
Phishing	Data loss prevention
Packet sniffer	Encryption
Pretexting	Firewall
ASSETS	Intrusion prevention system
Non-confidential assets:	Public key infrastructure
Point of sale server	Server-based access control list
Network devices	Static account logins/passwords
Database server	Specialized wireless security
End-user system	Smart cards and other one-time tokens
Mobile devices	Virtualization-specific tools
Confidential assets:	Vulnerability/patch management
Customer personal information	Virtual private network
Payment card information	
Off-line data	

Data for cyber risk losses is sparse given its negligible mention in SEC public filings as cyber risk compliance requirements leave such reporting to individual firms' judgment about materiality. Most such loss data as discussed further in our analyses is often underreported and hence may lead to underassessment of cyber risk by a wide margin. Based on estimated S&P 500's intellectual property between $600Bn and $1.2Tn and considering large-scale

[13] http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf
[14] http://www.acscenter.org/news-events/solak_20140919_presentation.pdf

government projects such as the $323 billion development cost of US F-35, the consulting firm McKinsey & Company concludes that $9Tn to $21Tn of economic-value creation is subject to cyber risk exposure in next 5 to 7 years[15,16]. Such reports acknowledge that it may be difficult to put a precise number on such losses. It is so given that most large firms tend to not report them in public financial disclosures as they are deemed 'not material'. The schism becomes all the more apparent when the investigations by law enforcement agencies determine specific large-value cyber-attack losses in case of the same firms not reporting any 'material' losses. Given the nascent and dynamic nature of cyber risk and cyber insurance modeling and underwriting industry, standardization of products, coverage, and terminology is sparse. As a result, cyber insurance underwriting is often highly customized and client specific.

Our analysis establishes that if left unchecked and uncontrolled, large-scale commercial reliance upon quantitative models with inherent model risks, tail risks, and systemic shall lead to an impending national cyber risk and cyber-insurance disasters. Those disasters may be similar to those encountered during the financial crisis wherein the US Federal Government had to save AIG as the insurer of financial risks undertaken by big banks[17].

The current thesis in our knowledge is the first attempt to *recognize the impending cyber insurance crisis* as well as *provide a solution by helping steer cyber risk assessment and cyber insurance modeling practice away from that crisis* by *judicious applications of model risk management related to the relevant quantitative models*. Our analysis that established VaR as the current predominant model of choice in applied practice. Such commercial users of cyber risk assessment and cyber insurance modeling can substantially benefit from the answers to the following questions that we provide to help them better recognize and manage model risk.

(a) How is VaR exactly applied in its native empirical real world context of measuring portfolio loss by real world financial trading desks using VaR models as explained further in Chapter 5?
(b) What are the most critical limitations of VaR that are known in the finance domain related to model risks, tail risks, and systemic risks related to VaR as explained further in Chapters 3, 4, 5, and 7?

[15] http://www.mckinsey.com/client_service/public_sector/latest_thinking/mckinsey_on_government/can_you_hack_it
[16] http://www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_cyberattacks
[17] http://www.wsj.com/articles/SB122156561931242905

(c) How are the critical model risks, tail risks, and, systemic risks related to VaR even *all the more relevant* to the cyber domain and cyber risk assessment and cyber insurance modeling VaR as explained further in Chapters 3, 4, and 7?
(d) How cyber domain's exponentially greater interconnectedness, interdependence, and correlations in case of cyber risks contribute to the above risks related to VaR as explained further in Chapters 2 and 4?
(e) How can cyber risk assessment and cyber insurance modeling applications and practices minimize the above model risks, tail risks, and systemic risks of VaR as explained further in Chapters 3, 4, 5, and 7?
(f) What alternative models can cyber risk assessment and cyber insurance modeling applications use to further minimize the above model risks, tail risks, and systemic risks as explained further in Chapters 5, 6, and 7?

The outline of the subsequent chapters is as follows. **Chapter 2** develops the first known cyber-finance-trust framework to analyze how global financial risk intertwined with global cyber risk further exacerbates the *systemic*, *interdependent*, and *correlated* character of cyber risks. **Chapter 3** develops the first known systematic basis for analysis of model risk management for cyber risk and cyber insurance as model risk management has received sparse attention in cyber risk and cyber insurance related contexts. **Chapter 4** develops the first known analysis establishing significant and extreme model risk and *tail risk* based on a review of the quantitative models in predominant commercial application and use for cyber risk and cyber insurance modeling. **Chapter 5** develops a baseline empirical study of similar quantitative models with specific guidance for containing model risks related to above quantitative models and model risks associated with related statistical inference methodologies. **Chapter 6** develops an analysis of the statistical computing algorithms that can be used for enabling statistical inference methodologies for containing model risk in cyber risk and cyber insurance modeling for the specific context of cybersecurity. **Chapter 7** develops alternative quantitative models for cyber risk and cyber insurance modeling to minimize model risks, tail risks, and systemic risks inherent in currently predominant models in commercial cyber risk and cyber insurance modeling. **Chapter 8** develops a framework for enabling Knightian uncertainty management relating it to model risk management given increasing uncertainty related to risk modeling of cyber risk.

Chapter 2.

The Trust Troika: Cyber-Finance-Trust

> "Security exists to facilitate trust. Trust is the goal, and security is how we enable it."
> -- Bruce Schneier on Trust in The Browser interview, February 23, 2012.

2.1 The Cyber-Finance-Trust Framework for Cyber Insurance

In the current chapter, we develop the first known cyber-finance-trust framework for cyber insurance modeling to analyze how financial risk entangled with cyber risk further exacerbates the *systemic*, *interdependent*, and *correlated* character of cyber risks.

Having reviewed the big picture of the cyber insurance industry, we next review the macroeconomic context of most recent cyber risk trends and developments. Given recent developments in the cyber domain, the following discussion outlines three key interrelated contexts that define cyber risk. The first context is that of cyber war 'games' and economic value creation, exchange, destruction, and transfer. The *cyber* context frames cyber risk and cyberattacks as *economic games* that influence *economic value* of the specific entity at the given unit of analysis such as nation, firm, or individual. The second context is that of trust relationships that underlie and facilitate interactions and exchanges in both finance and cyber domains. The *trust* context frames the contrast between the finance and cyber domains as well as the inter-relationships between the two domains. Within the cyber domain of *trust relationships*, every entity is a plausible target, accessory, or a source of attack. This context is also applicable at the various units of analyses, such as nation, firm, and individual.

The third context is that of *finance* (and economics) in which the economic costs of cyber risks, cyberattacks, 'wins', and 'losses' are accounted for. In the finance context, financial markets at different levels of analyses serve as *scoreboards* of *economic value*. In the context of economic *games* that influence economic value as discussed above, we define *score* as a relative indicator of economic value. We use the term 'relative' to signify the critical importance of score as a proxy for economic value (such as of profits, assets, liquidity, solvency). Trust is the common linchpin around which the cyber and finance domains revolve as all their underlying interactions, exchanges, and relationships are based on trust. Trust about some economic

utility or *value* (such as inherent in a digital message and/or a digital medium) translates into trust in the context of cyber risk such as apparent in most social engineering attacks.

Examples include perception of some economic utility that underlies the motivation to click that poisoned link, or open that poisoned attachment, etc. In the intertwined troika, cyber-finance-trust, the three (cyber, finance, and rust) together define cyber risk and its economic assessment in terms of models such as Value-at-Risk (VaR). It is in the application of the specific economic risk assessment models such as VaR that model risk and model risk management need to be applied.

2.2 Cyber *Games* and *Economic Value* Creation and Destruction

Lloyd's of London insurer AEGIS London in partnership with PwC recently launched a new cyber insurance product bundling property damage, bodily injury, environmental pollution and cyber terrorism with existing policies. In aftermath of the recent Sony cyberattack, they consider cyberattacks as the 'new normal with most such attacks by groups linked to geopolitical tension. Examples they note include former USSR or contested regions, such as the South China Sea. They expect that organizations will be caught-up in the fallout of "hybrid warfare – facing both physical and cyberattacks" [18]. Even though they note Sony as a recent example, such cyberattacks because of their very nature will most severely impact most information intensive firms and industries.

Banking and Finance industry is one such example given that most of its products and services, processes, as well as channels of distribution and consumption are all digital (Malhotra, 2014)[19]. Given common and shared platforms, hardware, software, exchanges, and networks across many of the players in the industry, there is a greater probability of correlated cyber risk. Related examples include FIX (Financial Information eXchange) and FAST (FIX Adapted for STreaming) protocols that form the backbone of buy- and sell-side trading or SWIFT (Society for Worldwide Interbank Financial Telecommunication) protocol that forms the backbone of worldwide banking transactions and messaging.

The US President on signing the 'Executive Order 13636—Improving Critical Infrastructure Cybersecurity'[20] observed that: "Now our enemies are also seeking the ability to

[18] http://www.cirmagazine.com/cir/Aegis-London-launches-Cyber-Resilience-plus.php
[19] http://www.brint.org/WhyKMSFail.pdf
[20] http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

sabotage our power grid, our financial institutions, and our air traffic control systems." These critical national information infrastructures[21] form the backbone of the national economy and economic value creation, exchange, and transfer. Hence, cyberattacks and related cyber risks have clear and present implications for the economic value creation, exchange, and transfer as well as economic destruction at all units of analysis. Shareholders and investors in publicly held firms, for instance, have to contend with market fraud such as insider trading and problems with financial reporting that threaten the integrity of financial markets in normal course[22]. Given increasing criticality of cyberattacks, now they also have to contend with cyber risk that threatens economic value creation, exchange, and transfer[23,24]. While releasing the recent Executive Order sanctioning North Korean government officials for the cyber-attack on SPE, the US President noted[25] "We take seriously North Korea's attack that aimed to create destructive financial effects on a U.S. company and to threaten artists and other individuals with the goal of restricting their right to free expression."

A Bloomberg report also highlights the critical significance of *data as an economic asset* whose *destruction* is considered a distinguishing characteristic of the most recent cyberattack on Sony Pictures Entertainment (SPE)[26]: "The hacking of Sony's computer system was different because it wasn't simply an attempt to disrupt traffic, spy or steal information, but to *destroy data on a foreign network*, according to the official, who asked for anonymity to discuss internal administration debates." Prior statement of the Department of Justice also focused on the economic destruction aspects of the SPE cyberattack[27]: "We are deeply concerned about the destructive nature of this attack on a private sector entity and the ordinary citizens who worked there. Though the FBI has seen a wide variety and increasing number of cyber intrusions, the destructive nature of this attack, coupled with its coercive nature, sets it apart. North Korea's actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves. The FBI takes seriously any attempt—whether through cyberenabled means, threats of violence, or otherwise—to undermine the *economic and social prosperity* of our citizens."

[21] http://www.brint.org/nii/
[22] http://www.cnbc.com/id/102306053.
[23] http://www.wired.com/2015/01/bitstamp-offline/
[24] http://www.wired.com/2014/03/bitcoin-exchange/
[25] http://www.bloomberg.com/news/2015-01-03/u-s-sanctions-seen-as-warning-to-nations-backing-cyber-attacks.html
[26] http://www.bloomberg.com/news/2015-01-03/u-s-sanctions-seen-as-warning-to-nations-backing-cyber-attacks.html
[27] http://www.nytimes.com/aponline/2014/12/19/arts/ap-us-sony-hack.html

The narrative of the MarketWatch report of December 31, 2014, describes the extent of damage from the cyber-attack[28]: "The day after Sony Pictures employees discovered that company email was unusable following a cyberattack, senior executives came up with an old-style communication network: a phone tree, in which updates on the hack were relayed from person to person. With computers down during Thanksgiving week, the Sony Corp. studio's 6,000 employees were forced to improvise, with cellphones, Gmail accounts and notepads. The payroll department dug up an old machine to cut paychecks manually. Before long, the studio unearthed a cache of BlackBerrys, which still worked because they send and receive email via their own servers. Sony Entertainment Chief Executive Michael Lynton told a meeting of senior executives that hackers hadn't simply stolen data. They had erased it, rendering the entire computer system unusable." That combination of damages in terms of stolen credentials, erased hard drives, and leaked documents is described by the cybersecurity company FireEye Inc. as unprecedented in the history of corporate cyberhacks.

The SPE cyberattack is a watershed event in that it will lead to fundamental rethinking about what represents an 'act of war' justifying military response from a national security point of view especially in case of a cyberattack resulting in damage or destruction of data. What is described as the most devastating attack on a US company, by some technically didn't meet the criteria defining such an act of cyberwar. The NATO's Tallinn Manual[29] defines act of cyberwar justifying military response as "a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or *damage or destruction to objects*." Hence, *damage to and destruction of data* in this specific instance was used to define the cyberattack as an act of the adversary state aggression setting a precedent for the future.

The case for bridging the existing *schism* between treatment of *physical* and the *virtual/digital* assets is made by a former NSA research scientist and CEO of the cybersecurity firm Immunity in a Marketwatch report[30]. The report shares his observation that while the attack "doesn't meet the threshold for a response by our military," it should still be viewed as an act of war. He notes that (emphasis added): "We need to change the way we think about cyberattacks. In many cases, these aren't 'crimes' — they're acts of war. A *nonkinetic* attack (i.e., destructive malware, destructive computer network attack) that causes just as much damage

[28] http://www.marketwatch.com/story/sony-hack-behind-the-scenes-as-the-crisis-unfolded-2014-12-31
[29] http://www.knowledgecommons.in/wp-content/uploads/2014/03/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf
[30] http://www.marketwatch.com/story/sony-hack-behind-the-scenes-as-the-crisis-unfolded-2014-12-31

as a *kinetic* attack (i.e., a missile or bomb) should be viewed at the same level of urgency and need for US government/military response." His next point seems to span the prior difference in treatment of *physical* assets such as buildings versus *virtual/digital* assets such as data: "there should at least be firm diplomatic repercussions for these types of attacks. After all, what would we have done if they'd blown up the buildings at Sony Pictures but not caused any casualties? That is the context these attacks need to be put in."

The recent cyberattack on Sony has brought national and global visibility of the financial economic dimensions of global cyberwarfare at probably an unprecedented level. However, it should not be *really* a surprise as 'cyberwarfare is underway all of the time.' That is exactly what the Atlantic Council Board Director Wesley Clark said at an event hosted by Washington, D.C. think tank. A FierceGovernmentIT report of October 13, 2014, notes quoting the former four-star Army general who served as NATO supreme allied commander in Europe that[31]: "Cyberwarfare is not something theoretical or reserved for conflict in the distant future, but happening continuously right now… We're doing it all of the time. So is everybody else; because, I hate to say this, you can't wait 'til the next war to discover what the enemy's cyber vulnerabilities are and what his nodes are."

The above report further notes that US DoD has made cyber reconnaissance a standard tool recently, however it has had cyber offensive techniques for quite some time. In July 2011, the US DoD acknowledged its willingness to use cyber offensive capabilities while unveiling its strategy for operating in cyberspace. However, it has had cyber offensive capabilities including the ability of incapacitating an adversary country's power grids as early as 1994, as he observed at that event. Clark also shared that other countries such as China had the capability to disable another nation's complete national critical information infrastructure including banking, railroads, airlines, sewage, water and electric power since 1999 as published in a report by their military leadership.

2.3 In *Trust Relationships*, Every Entity a Plausible Target

The second context is that of trust relationships that underlie and facilitate interactions and exchanges between different parties in both finance and cyber domains. The *trust* context frames the contrast between the finance and cyber domains as well as the inter-relationships

[31] http://www.fiercegovernmentit.com/story/cyberwarfare-underway-all-time-says-former-nato-supreme-allied-commander/2014-10-13

between the two domains. As observed in our introduction to this chapter, within the cyber domain of *trust relationships*, every entity is a plausible target, accessory, or a source of attack. This context is also applicable at the various units of analyses, such as nation, firm, and individual. Unlike finance, in cyber domain, trust relationship not only underlie the interactions and exchanges (*messages*) between the transacting parties, but they also underlie the infrastructure (*medium*) enabling those interactions.

Hence, it was noted earlier, that *unlike other risks, cyber risk poses a uniquely different set of exposures as it is intertwined with the* ***medium*** *and the* ***message*** *in the increasingly* ***digital world of networked communications***. While in case of cyber risk exposure through spear phishing and whaling, the exposure is through the specific users (decisions to click on a link, for example) reading the *message*. However, the *more significant and latent cyber risk is in the inherent and potential vulnerabilities* in the enabling *medium* such as the underlying operating system or networking software. For instance, the *vulnerabilities inherent in the medium can be exploited resulting in cyber risk regardless of the user's actions or inactions*. That was the case with the cyber risk exposure and the impact of the cyberattack on the employees in the recent Sony hack as observed by Schneier who observed that[32]: "These are people who did nothing wrong. They didn't click on phishing links, or use dumb passwords (or even if they did, they didn't cause this)." This will be the most fundamental distinction representing the most critical challenge of assessing, controlling, and managing cyber risk in contrast to all other kinds of risks. *Cyber risk is most critical compared to all other information based risks in cyberspace because it is inherent not only in the messages but also in the enabling medium*.

From *trust computing* perspective, every component of software, hardware, firmware, or networks that interacts with any other upstream or downstream second-party or third-party provider, vendor, or contractor is vulnerable and exposed. An example of what is feasible was evident in a Wireshark protocol analyzer online forum where it was observed that creating cyber risk exposure for the worldwide base of the most popular operating system for instance required poisoning of one critical upgrade that everyone *trusts*. Given known infiltration and compromises through spear phishing and whaling at the most senior echelons of world governments and global firms, no one is safe including heads of governments and heads of corporate firms.

[32] https://www.schneier.com/blog/archives/2014/12/comments_on_the.html

Once compromised, any such *trusted* user regardless of the status on the respective hierarchy can become the channel of *contagion* that can compromise the complete *network of trust* as well as all other *trusted* users on those networks. Taking the process a step further beyond inter-enterprise focus to intra-enterprise focus, any compromised *trusted* network can become the channel for infiltration of the *trusting* network. Hence, across diverse networks, any entity or device trusting any other network which can be compromised can become potentially vulnerable and after being compromised becomes a *carrier* that can result in other devices being compromised. Once compromised, the exposed network, device, and/or entity serves as a channel for transfer of economic value or destruction of economic value in the online cyber war game.

As in the case of Sony, although the headline on the national state sponsored cyber-attack on a global firm of another nation state apparently received most attention, other alternative threats and scenarios cannot be ruled out. A key challenge is determining the real identity of the device or the network as the source of attack by tracking it precisely across the various intermediaries, *willing or unwilling*, *knowing or unknowing*, involved in the attack. A more complex and convoluted challenge is knowing even if the *authorized* users or *owners* of those specific devices or networks actively participated in the attack or even knew about the attack before or when it was launched. In case of the recent cyberattack on Sony, the hackers routed their attack through computers all over the world one of which, in Bolivia, had been used by the same group to hack targets in South Korea. "But that computer, as well as others in Poland, Italy, Thailand, Singapore, Cyprus and the United States, were all freely available to anyone to use, which opens the list of suspects to anyone with an Internet connection and basic hacking skills."[33]

Regardless, from the above analysis, it follows that *everyone is a potential target, potential accessory, or even a potential source of attack, even when they are unwilling or unknowing participants in any given attack or a 'network of attacks'*. Merely detaching oneself with an air gap from all networks and devices does not necessarily preclude an actor as a potential target, accessory, or, source of attack, not considering RF signals. As long as the agent or device can communicate with, i.e. pass on a digital message to, other agents or devices who are not detached or who can communicate with other agents or devices, it could be plausibly a

[33] http://bits.blogs.nytimes.com/2014/12/24/new-study-adds-to-skepticism-among-security-experts-that-north-korea-was-behind-sony-hack/?_r=0

potential target, accessory, and even a source of attack. This was the exact case of the Stuxnet virus/worm, perhaps the most known example of infection of an air-gapped system[34].

Our above analysis of exponentially increasing *Distrust* in the context of the cyberspace enabling protocols originally designed on the *fundamental premise* of *trust* underlies the most unique nature of cyber risk as compared with all other risks. The implicit message communicated by the Trojan horse shown in Fig. 2-1 on the cover of the above Information Security survey course book is about the arrival of the 'Zero Trust' digital era[35] (Forrester, 2013). Hence, our above posited model of 'every entity being a potential Trojan horse' is consistent with the new 'zero trust' model of cybersecurity.

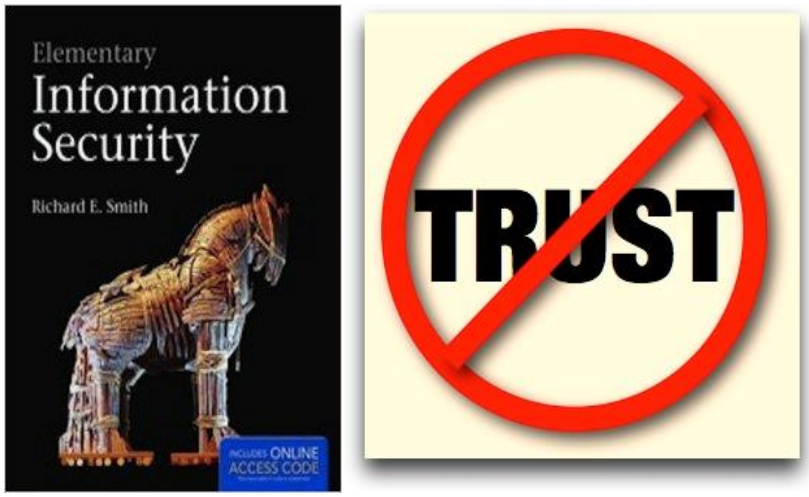


Fig. 2-1. Every Entity, Device, Network, Actor, or, Agent: A Potential 'Trojan Horse'? Hence, No 'Default Trust'

The whitepaper by Palo Alto Networks notes that: "Zero Trust is an alternative security model that addresses the shortcomings of failing perimeter-centric strategies by removing the assumption of trust[36]. With Zero Trust there is no default trust for any entity—including users, devices, applications, and packets—regardless of what it is and its location on or relative to the corporate network." Given the above observations, the 'cybersecurity world is at a cross roads in its evolution' contemplating the switch to 'Zero Trust' (Evans 2014)[37]. Defense-in-Depth based traditional 'perimeter based' security has been rendered less effective by increasing

[34] http://www.wired.com/2014/12/hacker-lexicon-air-gap/
[35] http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03038usen/WGL03038USEN.PDF
[36] http://www.cio.co.uk/cmsdata/whitepapers/3531107/Palo_Alto_-_Getting_started_with_a_zero_trust_approach.pdf
[37] http://www.computerworld.com/article/2476276/security0/the-importance-of-zero-trust-and-an-adaptive-perimeter-in-cyber-fortifications.html

sophistication, scale, and frequency of cyber-crime and adoption of new, disruptive technologies such as social, mobile, and cloud.

For example, the Internet-of-Things opens up a whole new set of vectors of cyber risks and potential cyberattacks. Zero trust approach, relying upon trusting no-one consistent with the above analysis, assumes that the traditional perimeter based security *will* be breached, including all defense-in-depth security layers, and hence valuable data and assets need to be protected from inside-out. Zero-trust approach would therefore include advanced data protection such as encryption, data cloaking, data masking for all critical data assets, both at-rest and in-transmission. It can be deployed in addition to 'adaptive perimeter' approach to minimize the attack surface vulnerable to more sophisticated cyber-attacks. Examples of adaptive perimeter include using application wrapping to encrypt data-in-motion from mobile app across the cyberspace and connecting authenticated mobile users into secure communities of interest, and, wrapping applications on the mobile devices.

The key point of the above discussion is that cyber risk is characterized by 'zero trust' and 'every entity can be a potential Trojan horse' traits. Given its key features of 'zero trust,' in addition to related features of extremely high interconnectedness, interdependence, and correlated-ness, cyber risk is quite unlike most financial risks. Not only is it different from financial risks modeled using VaR, in fact, it is much more riskier in terms of the specific risk characteristics that VaR is already known to be deficient in modeling.

2.4 Financial Markets as *Scoreboards* of *Economic Value*

The above analysis elucidated the *cyber* context of *economic games* that influence *economic value* and the *trust* context that frames the contrast between the finance and cyber domains as well as the inter-relationships between the two. The third inter-related context if that of *finance* (and economics) in which the economic costs of cyber risks, cyberattacks, 'wins', and 'losses' are *counted* and *accounted* for. In those counting and accounting contexts, financial markets at different levels of analyses serve as *scoreboards* of *economic value*. For *cyber finance* (*information based finance*), or, *virtual finance* (whenever the interface is digital and not physical) – which is pretty much most of post-WWW contemporary finance of this century – all products (and services), processes, and channels (of production, distribution, and consumption) are increasingly more or less information-based, digital, cyber, and virtual.

Hence, for most purposes of *actual* production, processing, and distribution, *finance is more or less same as cyber* given that almost all of its risks are cyber risks. Financial market risks, credit risks, and operational risks typical focus at the level of specific business processes and functions. However, in case of finance particularly, all such processes as well as related products, services, and distribution and consumption channels are cyber-based. Hence, each of them is vulnerable to manipulation or hacking of data at rest and in motion. Therefore, it isn't surprising that leading Banking firms such as Goldman Sachs consider themselves more to be a Technology firm rather than an old school Banking firm[38]. The key difference between the cyber and finance domains may be considered in terms of the *score-keeping* function which still seems to be the domain of finance and associated accountants, analysts, bankers, investors, hedge fund managers, and, financiers – human, virtual, or, (increasingly) cyber. There are automated score-keeping aspects such as credit-card and loan authorizations, however under the purview of human or artificial agents, those notions still seem to be the purview of finance.

Our prior analysis defined all activities of economic creation, destruction, transfer, or exchange at all levels of analysis – including nations, firms, groups, or individuals – as economic games of finance. When these economic activities are enabled by cyber, we call them *cyber games of finance* in the cyber-finance-trust contexts. We also defined the score-keeping function of finance and noted that scores are relative indicators of economic value. We use the term 'relative' to signify the critical importance of score as a proxy for economic value (such as of profits, assets, liquidity, solvency). Such scores of the cyber game of finance are evident in global and national economic indicators, stock prices of public firms, assets under management (AUM) for hedge funds, and, net worth of ultra-wealthy individuals including *Fortune 500* and *Forbes 400*.

As fates and fortunes of many other entities, groups, and individuals depend upon the above deep-pocketed entities such as through livelihoods, pension funds, retirement portfolios, university endowments, etc., they may also be receptacles of the trickle-down *scores*. It is important to understand the notion of score-keeping particularly as it may relate to individual firms and ultra-wealthy individuals. Many of their individual economic scores are greater than the GDP of many of the world's countries. In fact, many of the world's largest firms and governments rely upon their investments for their *scores* such as enterprise stock and bond asset valuations and sovereign credit rankings. Hence, we need to recognize that even

[38] http://dealbook.nytimes.com/2014/11/13/goldman-sachs-recasts-its-reputation-to-woo-tech-talent/

though some of the Top-3 billionaires get major headlines for influencing scores of firms and financial markets, many of the largest firms and nations rely for their scores upon many who may not be in the *Forbes 100*.

In the cyber context, the trust relationships are through the interactions of the *message* and the *medium* as discussed earlier. In contrast, in the finance context, the trust relationships are through the interactions of *economic scores* and economic well-being. It follows that the fortunes, stock prices, and sovereign risk rankings of respective firms and nations are intertwined and entangled with the fortunes of the specific investors, creditors, and stockholders generally. It can also be deduced that the fortunes of hundreds of millions of others who are reliant upon the respective firms, institutions, and governments for their livelihoods and sustenance are also entangled with those entities. In the digital information-based view of the troika of cyber-finance-trust, the complex interweaving web of entangled *economic* '*trust relationships*' often inter-relates and corresponds to the *cyber* '*trust relationships*.'

This *interacting web of cyber and economic trust relationships* is relevant to examining and understanding the diverse vectors of potential cyber threats and cyber-attacks, as well as potential targets, accessories and sources of cyberattacks. It is within the above context of financial score-keeping, that Value-at-Risk (VaR) is of interest as a statistical model and methodology of assessment of economic risk of expected loss. It is also within the above context of troika of cyber-finance-trust, we analyze the adoption of the VaR model used in finance domain in the cyber domain for assessment of economic risk of expected loss. To distinguish the application of VaR in the two domains, we shall call the former financial risk, and the latter cyber Risk. Such assessment of risk is relevant to both cyber risk assessment as well as cyber insurance modeling. Prudent risk assessment, measurement, and modeling requires prudent public data about suck risks which is simply not available. The specific reasons attributable to 'non material' cyber risk public filings for sparseness of relevant cyberattack and cyber loss public data is discussed in the next section.

2.5 Finance-Cyber Interact with No Cyber Risk Score in Filings

The U.S. Securities and Exchange Commission (SEC) Division of Corporation Finance (Corp Fin) issued its 'guidance' on October 13, 2011, for publicly-traded corporations about disclosure obligations relating to cybersecurity risks and cyber incidents observing that

(emphasis added)[39]: "Although *no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents*, a number of disclosure requirements *may* impose an obligation on registrants to disclose such risks and incidents. In addition, *material information* regarding cybersecurity risks and cyber incidents is *required to be disclosed when necessary* in order to make other required disclosures, in light of the circumstances under which they are made, not misleading."

The guidance did *not* modify or create any new SEC rules or regulations, rather it discussed how publicly-traded US corporations, both domestic and foreign, *might* consider cybersecurity matters when preparing financial disclosures in periodic SEC reports and registration statements. In an Oct. 15, 2013, speech to the National Association of Corporate Directors Leadership, the SEC head reiterated the materiality standard that governs disclosures about *costs of such attacks* (emphasis added)[40]: "even in the absence of a line item requirement… *Depending on the severity and impact* of the cybersecurity attacks, *disclosure is either required or not*."

A San Francisco law firm's interpretation of the SEC guidance is notable in this respect (emphasis added)[41]: "The disclosure guidance implicitly assumes that *all or most companies face cybersecurity risks* and possibly even that *all or most companies have been attacked*, as the guidance advises that companies "*should not present risks that could apply to any issuer* (of public stock)," refers to *disclosing "successful" or "material" attacks rather than all attacks*, and states that companies should "*avoid generic risk factor disclosure*." Corp Fin, noted above, stated that the *guidance reflects only its views on cybersecurity disclosures*, that *it is not a rule, regulation or statement of the SEC*, and that *the commission has neither approved nor disapproved the guidance*."

The SEC hosted a roundtable on 'Cybersecurity Issues and Challenges'[42] on March 26, 2014 with the following key messages: *Board of Directors' Involvement*: Cybersecurity is a threat that necessitates the involvement of every level of a company, especially the board of directors, but exactly how that responsibility should be allocated and the level of necessary expertise may depend on the industry and other considerations. *Public Dis*closure: Companies must disclose cybersecurity threats and incidents, but when and how is currently unclear even despite that security breach notification laws have existed in the USA since 2002 starting with

[39] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
[40] http://www.sec.gov/News/Speech/Detail/Speech/1370539878806
[41] http://www.mofo.com/files/Uploads/Images/131014-SEC-Continues-to-Target-Cybersecurity-Disclosures.pdf
[42] http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml

the California data security breach notification law SB 1386[43]. *Information Sharing*: Sharing information among companies and with the government is essential in preventing cyberattacks and the government can help by defining the legal protections covering such information and by giving the private sector the appropriate clearances for access to classified information. *Preparation*: Companies must be prepared to defend against and respond to cyberattacks on a timely basis. Adequate preparation includes performing tests and risk assessments daily, quarterly, and annually and developing playbooks defining response plans for breaches. *Government Guidelines*: Government guidance on disclosure and standards that can be implemented by companies to prevent cyberattacks are helpful, but *prescriptive rules are not beneficial, given the changing and dynamic landscape of cybersecurity and the likelihood of having outdated rules*.

However, given lack of specific rules, regulations, or compliance requirements except for the discretionary assessment of 'materiality,' the scores that are most pertinent to cyber risk and cyber insurance modeling are simply not accessible to public as they are not available in any public database. Such scarcity of financial loss disclosure exists even while investors and shareholders as well as public officials have been pressing SEC for requiring such cyber risk disclosures[44]. Such scarcity of available and reliable data on cyber risks further hampers objective and reliable quantification of cyber risk and modeling of cyber risk and cyber insurance. Despite absence of data to test any model, VaR model from finance has emerged as the predominant model being used for commercial cyber risk and cyber insurance offerings. The specifics of the above insight based on original research are discussed further in Chapter 4 which also focuses on the Review of Quantitative Models in Cyber Risk and Cyber Insurance.

2.6 Using VaR to Model Financial Risk and Cyber Risk

Given our focus on *interacting web of cyber and economic trust relationships*, and *scorekeeping* of *economic value*, potential 'value at risk', *literally*, seems a plausible measure of risk assessment. One such commonly used *technical* – as contrasted from *literal* – measure of risk assessment used in Finance and Banking industry is called 'Value at Risk' or in short 'VaR.' Two points of distinction about VaR are important. First, the *technical* notion of VaR must be distinguished from *literal* notion of 'value at risk.' Both terms are used in the cyber

[43] http://oag.ca.gov/ecrime/databreach/reporting
[44] http://www.forbes.com/sites/ciocentral/2013/05/15/how-to-prepare-for-when-the-sec-comes-asking-about-cybersecurity-risk/

risk and cyber insurance literature by well-regarded organizations. Attention to detail is hence necessary which specific notion they are referring to. The literal notion can literally mean anything as it is up to the specific interpretation of the specific firm. The technical notion of VaR is what we focus upon given its increasingly prominent and central role in the nascent cyber risk assessment and cyber insurance modeling industry. Further, the statistical technical notion of VaR (with small case 'a') as used in our analysis must also be differentiated from statistical technical notion of VAR (with capital case 'a') which stands for 'Vector Autoregressive Models' outside the scope of our current discussion.

VaR is essentially a point estimate measure of risk used for assessing various types of financial risks such as market risk, credit risk, and (increasingly) operational risk. To understand the philosophical, methodological, statistical significance of a model such as VaR when it is *transplanted* from finance to cyber domain, it is *critical* to understand the *compatibility* of contexts across the two domains. If the transplant of a model is done without ensuring compatibility of contexts within the bounds of measurement model, the *model* is bound to fail. Such risk of failures of a model when it fails given that its underlying assumptions, boundaries, and limitations are not compatible with its application is called *model risk*. Ensuring that the application of the model is consistent and compatible with the assumptions, boundaries, and limitations of the model is called *model risk management*.

The focus of the current thesis is on model risk management of VaR in cyber risk and cyber insurance modeling. Model risk management of VaR is important given its emerging and growing role as the prominent model being applied for cyber risk and cyber insurance modeling. Model risk management of VaR is also *critically important* given what many attribute to its central and key role in the Global Financial Crisis of 2007-2009[45,46]. The specific reasons for the critical failure of VaR Models include its limitations in not factoring in *systemic risks*, i.e., risks resulting from interdependencies and correlations between the risks that are *components* in computing the *aggregate* risk[47].

The above matters of critical concern are even more critical in the context of cyber risk as compared to financial risk given that *systemic risks*, i.e., risks resulting from interdependencies and correlations, are *much more extreme* as discussed further in our analysis.

[45] http://www.futuresmag.com/2010/11/30/var-number-killed-us
[46] https://books.google.com/books?isbn=1118171543
[47] http://www.ft.com/cms/s/0/b8713aba-a102-11e1-aac1-00144feabdc0.html

Hence, application of VaR *models* (as distinguished from its extensions discussed later which are denote as VaR *methodology*) will result in significant model risk in cyber risk and cyber insurance modeling. More importantly, given the interdependencies and correlations characterizing cyber risk, *given its intrinsic nature*, these model risks of VaR will be of much more extreme levels than even in finance.

The next chapter introduces and explains the concepts of Model Risk and Model Risk Management to set the background for subsequent chapters on alleviating model risk of using VaR for cyber risk and cyber insurance modeling.

Chapter 3.

Model Risks and Model Risk Management

> "This reliance on models to handle risk carries its own risks."
> -- Emanuel Derman, Quantitative Strategies Research Notes, Goldman Sachs, April 1996.

3.1 Model Risk Management Framework for Cyber Insurance

In the current chapter, we develop the first known model risk management framework for cyber insurance modeling as model risk management has received sparse attention in cyber risk assessment and cyber insurance modeling.

We start with an overview of what model risk means and what is model risk management from the perspective of finance. Our motivation in doing so for cyber risk and cyber insurance modeling is twofold. First, cyber risk and cyber insurance modeling are currently predominantly reliant upon financial risk models such as VaR for cyber risk assessment. Hence, we need context-sensitive understanding of such models being adopted for assessment of cyber risk. Second, VaR model has been the subject of intense criticism regarding its neglect of systemic risk arising from interdependent and correlated risks. Hence, in the context of cyber risk which is characterized by high level of interdependent and correlated risks, it is all the more critical to examine how to manage model risk of VaR. We need to develop context-sensitive understanding of model risk management from two related perspectives.

The first perspective is that of financial practice as leading firms and domain experts have pioneered the leading industrywide model risk management practices. The second perspective is of financial regulators who have promulgated model risk management compliance requirements for the financial firms after the Financial Crisis. Following analysis accomplishes the above stated objectives. For applying practical understanding about model risk management to cyber insurance modeling, we analyze the model risk management

practice pioneered at Quantitative Research group of Goldman Sachs[48]. For applying practical understanding from a regulatory standpoint, we analyze the model risk management compliance guidance of the US Federal Reserve and the Office of Comptroller of Currency[49,50].

3.2 Model Risk Management and Uncertainty Management

Within finance, it is relevant to understand the Model Risk Management practice from the firm and the modeler who may be considered its pioneers. Dr. Emanuel Derman[51] was the Head of Quantitative Risk Strategies Group at Goldman Sachs before leading the Financial Engineering program at the Columbia University. In his research note published in April 1996 while at Goldman Sachs, he characterizes Model Risk as "assumptions and risks involved in using models" for financial securities valuations observing that "reliance on models to handle risk carries its own risks.[52]" In the specification of a model, the objects of concern are causally related and that relationship of cause and effect is presumed to be stable while applying the model. In contrast to the domain of natural sciences such as Physics, in sociotechnical contexts such as financial markets and cyber risk management, often the cause-effect variables may themselves reflect human 'expectations' such as expected risk and expected return, not realized quantities[53]. Models about future valuation scenarios require the modeler to translate one's thought and intuitions about independent variables into specific numerical values reflecting dollar figures. Such dollar figures could be 'profits' (Knight (1921)) of the pre-cyber era and 'scores' as we define in this dissertation for the era of cyber games of finance.

The 'overwhelming unknown' as Derman calls it in models applied in sociotechnical fields such as finance (and more so for cyber, as we analyze in this dissertation) is *uncertainty*. His comment, like others (such as Morini (2011), Haldane & Nelson[54] (2012)) underscores the critical *disconnect* between *what is often modeled* and *what needs to be really managed*. All of them explicitly relate to the most crucial distinction originally made by Knight (1921) between the *theory* of risk modeling and related *practice* of risk management. The critical unknown variable of interest in finance (and more so in cyber) is *uncertainty*; however, the variable that most

[48] http://www.emanuelderman.com/media/gs-model_risk.pdf
[49] http://www.federalreserve.gov/bankinforeg/srletters/sr1107a1.pdf
[50] http://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf
[51] http://books.google.com/books/about/My_Life_as_a_Quant.html?id=GJdhjA9fTQMC
[52] http://www.emanuelderman.com/media/gs-model_risk.pdf
[53] https://books.google.com/books?id=lke_cwM4wm8C
[54] http://www.bankofengland.co.uk/publications/Documents/speeches/2012/speech582.pdf

often actually gets estimated using quantitative models (based on classical statistical inference methodologies) is *risk*. That is the underlying basis for Derman's key point above that *all* models (including VaR) entail model risk and hence *must* rely upon model risk management. The distinction between risk and uncertainty is most crucial and is attributed to the economist Frank Knight (Knight 1921). Knight was one of the founders of the Chicago School who taught multiple (future) Nobel laureate economists.

Knight outlined the following important distinction between uncertainty and risk (Knight 1921, p. 9): "Uncertainty must be taken in a sense radically distinct from the familiar notion of Risk, from which it has never been properly separated.... The essential fact is that 'risk' means in some cases a quantity susceptible of measurement, while at other times it is something distinctly not of this character; and there are far-reaching and crucial differences in the bearings of the phenomena depending on which of the two is really present and operating.... It will appear that a measurable uncertainty, or 'risk' proper, as we shall use the term, is so far different from an unmeasurable one that it is not in effect an uncertainty at all." Furthermore, he noted (p. 9, emphasis added): "We shall accordingly restrict the term 'uncertainty' to cases of the non-quantitative type. *It is this 'true' uncertainty, and not risk, as has been argued, which forms the basis of a valid theory of profit and accounts for the divergence between actual and theoretical competition.*"

Therein lies Knight's emphasis of his distinction between the practice of (non-quantitative) risk management relying upon 'true' uncertainty and the theory of (quantitative) risk modeling of 'theoretical competition' relying upon 'measurable uncertainty', i.e., risk[55]. Both Derman[56] and Morini (2011) recognize and relate to the above distinction between true uncertainty and measurable uncertainty as does Malhotra (2004)[57]. Consistently, all three evidently relate to Knight's distinction between "'objective' and subjective 'probability'" (Knight 1921, p. 121) in terms of 'risk modeling' and 'uncertainty management' respectively in their research papers.

[55] http://www.yogeshmalhotra.com/blackswans.html
[56] http://www.emanuelderman.com/media/gs-model_risk.pdf
[57] In contrast to Derman and Morini who as quantitative modelers who became fascinated by uncertainty management, Malhotra as scholar-practitioner of uncertainty management became fascinated by quantitative modeling. He also distinguishes theory from practice in his research focused on 'anticipation of surprise' in contrast to 'historical prediction.'

3.3 Model Risk Management at Goldman Extended to Cyber

Given the entangled Web of trust relationships that determine cyber risk, one may argue that the cyber domain is not only much more uncertain but also more dynamic than finance. In finance models, variables may also include people's opinions. In cyber, however, given intensity and velocity of social and other information flows and resultant impact, not only actors' opinions but also their actions (such as in social engineering, as a target, accessory, attacker, or carrier) are variables. Often major cyberattacks are known months or years after they are initiated in contrast to the real-time ticker of the Financial markets data feeds where speed of (high-frequency) competition is in the order of microseconds and nanoseconds. Hence, the cyber domain which is more or less covert, as compared with finance domain, has not only to deal with an even greater 'overwhelming unknown' of *uncertainty* (as any actor, agent, device, or network could be or become a potential threat), but also another 'overwhelming unknown' of *complexity* given the worldwide entanglement of the troika of cyber-finance-trust relationships described earlier.

Some perspective of the uncertainty in finance compared with uncertainty in cyber may be evident in Sony's recent debacle being described as the first cyber-attack of its kind. One senior executive at Sony earlier estimated the firm's cyber risk in low double-digit millions, whereas the actual loss assessment within few short weeks of the cyberattack is to the tune of $200-$300 million[58]. Extending Derman's comparison of the world of natural sciences to sociotechnical domains such as financial markets and cyber risk can perhaps help illustrate this point.

Since Nov. 24, 2014, when the news surfaced about the hack of unprecedented scale and scope that shut all networks and devices at Sony Pictures specifically, and Sony Corporation, despite reported loss of $300 million, Sony's financial stock seems to be tracking the main market indices quite well while seemingly doing even better than its competitive rival Panasonic as seen in Fig. 3-1. The loss estimate of the relatively smaller subsidiary Sony Pictures ($10 billion annual sales) of the Sony holding company ($80 billion annual sales) from the cyberattack is perhaps miniscule compared with the parent's loss estimate forecast of $2.15

[58] http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/05/why-its-so-hard-to-calculate-the-cost-of-the-sony-pictures-hack/

billion of Sep. 17, 2014, for the year. Furthermore, the above hacked entity, SPE, had Cyber insurance coverage of $60 million from Marsh[59].

Fig. 3-1. Sony Corporation (SNE) Stock Performance just after the Cyberattack

Derman contrasts the world of natural sciences such as Physics with the socio-technical world to underscore the relatively much higher uncertainty that is characteristic of socio-technical domains such as finance. Most can predictably forecast a man-made satellite's position with high precision. However, uncertainty is inherent in predicting a stock price which no one expects to forecast with much precision at all. Compared to the financial market though, uncertainty in cyberattack loss estimates seems even much higher[60]. For instance, the cyberattack loss from an earlier hack that the Sony corporation encountered in 2011 on its PSN Playstation® Network was estimated at $171 million in a Wired[61] report of May 23rd and estimated to cost a 'Billion-Dollar' repair bill in a prior Wall Street Journal[62] report of May 6th.

Another point that Derman raises is the intimate knowledge of the domain needed by modelers for application of the respective model such as VaR. In finance, they need intimate knowledge such as specific times during which specific securities trade, relevant trading rules, settlement conventions, etc. In contrast, however, the *Cyber (attack) domain defies any such rules*

[59] http://www.propertycasualty360.com/2014/12/18/sony-pictures-holds-60-million-cyber-policy-with-m
[60] http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/05/why-its-so-hard-to-calculate-the-cost-of-the-sony-pictures-hack/
[61] http://www.wired.com/2011/05/sony-psn-hack-losses/
[62] http://www.wsj.com/articles/SB10001424052748703859304576307664174667924

and conventions which all attackers adhere to or play by. Rather, it is a round-the-clock increasingly sophisticated global meta-market composed of worldwide open markets such as the Absolute Zero-Day™ Exploit Exchange operated by the once world's most wanted hacker Kevin Mitnick as well as underground exploit markets that sell software such as used in Sony's recent attack.

A critical point that Derman notes is that *even the finest model is just a model*, and *not the real thing*. In that respect, cyber risk assessment and cyber insurance models should represent as naturally as possible the essential variables of the systems and their inter-relationships to allow assessment of cause and effect. Such models can only do few important things really well, hence it is critical to ensure that they focus on the most appropriate and important things for the task at hand. Specifically, in a sociotechnical domain such as finance, and more so in case of cyber, given the predominant role of social engineering in the most critical and damaging cyberattacks, *it may be more damaging to apply a model that really doesn't apply than realizing that there isn't one*[63].

Besides the predominant role of social engineering in cyberattacks to which the most valuable assets and resources have been found to be susceptible, there are additional concerns that may contribute to model risk. Such concerns include besides using a model that is clearly not applicable, missing key variables, incorrect assumptions about certainty (deterministic) vs. uncertainty (stochastic), incorrect dynamics in terms of applicable statistical distributions, incorrect assumptions or missing critical assumptions about the variable inter-relationships, context-sensitivity of the model thus making it valid only in specific contexts, theoretically precise model hindered in applicability when real world doesn't match theoretical logic or assumptions, incorrect estimation of underlying data, and, instability of theoretical assumptions in dynamic real world contexts.

Unless careful testing is done to ensure that analytic solution to the model behaves consistently for all reasonable parameters, even though the model is correct, it may yet have an incorrect solution. Hence, in the case of cyber risk and cyber insurance models, given sparse and unreliable available data makes it much more challenging to test or empirically validate current models, VaR as well as others. However, key characteristics that define the fundamental assumptions, boundaries, and limitations of scope as in the case of VaR applied to finance domain as well as cyber domain can provide valuable insights. In case of complex

[63] http://www.emanuelderman.com/media/gs-model_risk.pdf

models which may be correct, greater probability of inappropriate use contributes to model risk. Hence, cyber risk attacks that lead to losses with high variance may need to be modeled with different parameters than those that lead to losses with low variance. Therefore for best results, users knowledgeable about the model, the solution, as well as what can go wrong with it need to *test the model with different parameters as well as different methods* to determine the methods and parameters for which convergence of findings is achieved. As models are sophisticated programs integrated with backend databases, frontend user interfaces, live data feeds, and, data entry screen inputs, their end result is only good as their weakest link.

Similarly, model risk can result from using different sampling duration windows for computing future estimates of independent variables from historical data. Model risk is thus influenced by the specific domain, the model's applicability, underlying mathematical and numerical analysis of its solution, computer programming and software engineering of its implementation, and, the communication and translation across various inter-linkages connecting the integrated components[64]. When the above tasks are split between users, modelers, and programmers, it may be desirable to have them work together in close-knit teams that know what can go wrong and test the model as well its boundaries and assumptions. Simpler cases of complex models should be tested first with analytical solutions before scaling them as complex models can go wrong if complexity obfuscates the error in the simpler part of the model. Even small discrepancies should be paid attention to as they may lead to large errors. The importance of graphical user interfaces needs to be underscored as often displays of graphical information can help determine or pinpoint model errors. To ensure rigorous testing before they are used at large scale, models need to be diffused gradually from original developers to testers to users to clients so that most kinks are resolved before they are applied in large scale use.

3.4 Model Risk Management Compliance Guidance for Banks

On April 4, 2011, the Board of Governors of the US Federal Reserve System and the US Office of the Comptroller of the Currency published the Supervisory Guidance on Model Risk Management[65,66]. That guidance requires compliance of Banking and Finance firms and provides broad guidance on both model risk and model risk management. Presented below

[64] http://www.emanuelderman.com/media/gs-model_risk.pdf
[65] http://www.federalreserve.gov/bankinforeg/srletters/sr1107a1.pdf
[66] http://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf

are the key points from that document followed by the US finance industry for assessing and managing model risk of models such as VaR. The US Fed and OCC guidance specifies model risk in terms of "potential indirect costs of relying on models, such as the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused." Further: "Those consequences should be addressed by active management of model risk."

Consistently, JP Morgan, one of the world's largest bank based on AUM, defines *model risk* as follows: "Model Risk arises from the potential adverse consequences of making decisions based on incorrect or misused model outputs and reports, leading to financial loss, poor business decision making, or reputational damage." Many such financial institutions have Model Risk Groups such as the above bank which notes that it: "is responsible for conducting model validation to help identify, measure, and mitigate Model Risk. The objective is to ensure that models are used appropriately in the business context and that model users are aware of the models' strengths and limitations and how these can impact their decisions."

Given the emphasis on model validation evident in the above bank's model risk management practice note, the US Fed and OCC guidance further observe that (emphasis added): "Rigorous *model validation* plays a critical role in model risk management; however, *sound development*, *implementation*, and *use of models* are also vital elements. Furthermore, model risk management encompasses *governance and control mechanisms* such as board and senior management oversight, policies and procedures, controls and compliance, and an *appropriate incentive and organizational structure*."

US Fed and OCC guidance refer to *model* as: "a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates… (consisting of) three components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information." The guidance also includes "quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature." The guidance, not unlike the prior banking practice notes acknowledges that models are "simplified representations" of real-world relationships among observed characteristics, values, and events. Simplification is inevitable, given inherent complexity of relationships and to focus

attention on specific aspects that are most important for a given application. Model quality attributes such as precision and accuracy are relevant to future forecasts whereas attributes such as discriminatory power are relevant to relative rank ordering of risk. Regardless, there is imperative need of knowing the boundaries of model's capabilities as well as limitations given its simplifications and assumptions such as in case of VaR.

US Fed and OCC guidance defines *model risk* as: "the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports (which) can lead to financial loss, poor business and strategic decision making, or damage to a bank's reputation." This definition shows consistency of the prior definition used by JP Morgan. Model risk may occur because of two reasons: because of fundamental errors and because of incorrect or inappropriate use. For instance, our focus on application of VaR in the context of cyber risk assessment primarily focuses on the second reason. It is for its incorrect and inappropriate use as a point estimate measure of average risk which doesn't really specify *how much maximum loss can occur* for which other models discussed later are more appropriate.

In addition, previously mentioned limitations of VaR such as its neglect of systemic risks, interdependent risks, and correlated risks (that together characterize the cyber domain) further compounded the problems resulting from its *underestimation* of actual risk of loss [67]: "VaR played a key negative role in the 2008 credit crisis, by severely underestimating the danger from toxic mortgage products and by allowing banks to enjoy excessive levels of leverage on their trading positions… Recognising all this, the Basel Committee for Banking Supervision, which had enthusiastically adopted VaR since 1995, has been busy at work disowning the model and tweaking the bank capital formula. Just a few weeks ago, Basel announced that it no longer wants to keep using VaR." However, as subsequent developments since then establish, given sparse if any *global industry standard* alternatives quantitative risk *methodology* alternatives, VaR *methodology* (distinct from the VaR *model* currently predominant in cyber insurance commercial applications) continues as the foundation for inspiring most recent quantitative risk modeling advancements in both theory and applied practice. [68,69]

[67] http://lexicon.ft.com/Term?term=value-at-risk-_-VaR
[68] http://yogeshmalhotra.com/BayesianVsVARToModelRiskManagement.pdf
[69] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2538401

The US Fed and OCC guidance notes that factors contributing to higher model risk typically include greater complexity of the model, greater uncertainty about inputs and assumptions, as well as broader use which may result in larger potential impact. Fundamental errors resulting in inaccurate outputs may result from errors in application of theory, choice of sample, selection of inputs and estimation, incorrect assumptions, and, information systems implementations. Errors in use occur if a model is used outside the environment for which it was designed or in ways not consistent with the original intent such as when it is applied to new products or markets, or inadvertently as market conditions or changes in targeted behavior. All such errors result in model risk. Aggregate model risk that is relevant to systemic risk in finance as well as to cyber risk is another key concern. *Such errors can also occur if VaR model that neglects systemic risk, interdependent risks, and correlated risks is applied to assessment of cyber risks that are in fact much more extremely systemic, interdependent and correlated than are risks related to different financial assets or financial institutions*.

Particularly in a network of interacting nodes, it depends upon interaction and dependencies among respective models; reliance on common assumptions, data, or methodologies; and factors adversely affecting several models at the same time. The guidance specifies that model risk management be accomplished by "effective challenge" of models which it interprets as "critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes." In summary, model risk management includes robust model development, implementation, and use; a sound model validation process; and, governance resulting in an effective framework for communication of model limitations and assumptions.

Advancing beyond the analysis of model risk and model risk management, the next chapter further elaborates on the factors underlying high model risk of extant cyber risk assessment and cyber insurance models in commercial use. Besides their predominant reliance upon VaR which is a matter of concern for reasons already discussed, unreliable and sparse cyberattack loss data hinders empirical validation of analytical results. Multiple factors contributing to the unique nature of cyber risk making it much different from market risk and credit risk contribute to its relative much higher riskiness. Given the application of imprecise and perhaps inadequate model, unreliable and sparse empirical testing, model risk and hence model risk management are all the more critical in the case of current cyber risk and cyber insurance models and measures being applied in commercial practice. The next chapter's focus is on the above exogenous and endogenous factors that exacerbate model risk in case of the

cyber domain, the predominant risk models applied in current cyber risk and cyber insurance modeling in academic research and applied practice, and related model risk management concerns.

Chapter 4.

Cyber Insurance and Cyber Risk Models

> "I was concerned about inconsistencies in disclosures, investor confusion, and the fact that many corporate leaders did not fully recognize the relationship between their companies' cybersecurity measures and financial success."
> -- John D. Rockefeller IV, Chairman, United States Senate Committee on Commerce, Science, and Transportation in letter to the Chairwoman, U.S. Securities and Exchange Commission, April 9, 2013.

4.1 Review of Quantitative Models in Cyber Risk Insurance

In the current chapter, our review of quantitative models in cyber risk and cyber insurance modeling develops the **first known analysis establishing significant and extreme *model risks*, *tail risks*, and, *systemic risks*** related to predominant models in use.

Developing upon analysis of model risks and model risk management and how they apply to cyber risk and cyber insurance modeling, this chapter further elaborates upon factors contributing to those model risks. Our analysis reveals that besides their predominant reliance upon VaR despite its known limitations relevant to cyber risk modeling, availability of adequate and reliable public data further hampers empirical testing of analytical solutions. Besides endogenous concerns related to appropriate application and use of models, exogenous factors characterizing the cyber domain and associated cyber risks further make their modeling and testing challenging. Those exogenous factors further exacerbate the concerns about model risk management.

Following analysis further elaborates upon the above concerns while observing the relatively greater level of riskiness (in terms of *uncertainty* and *complexity*) of cyber risk relative to other (financial) risk types modeled using similar quantitative finance risk models. A review of such models being applied for cyber risk and cyber insurance modeling in academic research and practice indicates VaR as the predominant model of choice. Specific VaR models in cyber insurance modeling are examined and their model risks analyzed. The next section delves into the factors that contribute paucity of reliable data for empirical testing of analytical models being applied in cyber risk assessment and cyber insurance modeling.

4.2 No Material Disclosures of Cyber Risks in Public Filings

The US 'Executive Order -- Improving Critical Infrastructure Cybersecurity'[70] of February 12, 2013, described cyber threat to the nation's critical infrastructure as "one of the most serious national security challenges." In wake of the recent Sony hack, Department of Justice and FBI also noted that "cyber threats pose one of the gravest national security dangers" to the United States. *Yet, we see negligible disclosures of cyberattack related losses in public filings.* SEC's lack of rules or regulations about reporting cyberattacks related losses except for the *optional* guidance which it "neither approves nor disapproves"[71] seems to explain why companies don't disclose losses from cyberattacks. The companies don't do so because they are not *required* to do so. In prior discussion about SEC's *guidance*, it was also observed that the discretionary application of *materiality* about specific cyberattack losses is left to the discretion of respective firms. The *Treasury & Risk* report of July 15, 2013, 'Putting a Price Tag on Cyber Crimes'[72], observes that cyberattacks have become *so common*, they are becoming *less material*.

As noted by the prior head of SEC's Office of Internet Enforcement and U.S. advisory cybersecurity leader at PwC, (emphasis added) "*Everybody's getting breached*. *With most companies, it's not a matter of if, but when, they get a data breach*," he said. "*The quantitative materiality of a data breach I do believe is deteriorating*." He also noted that while it may be very hard to quantify the damages, "It may also be the case that companies *do not necessarily want to disclose* the full impact of an IT theft." He contrasted the challenge of quantification of costs of compromise of very sensitive information or intellectual property (as in the case of SPE hack) relative to easier to quantify costs. Example of such easily *quantifiable costs* are costs of incidents in which credit card numbers or other personal information is stolen, costs that include the *expense of any remediation*, such as offering credit monitoring to customers. Consistently, cybersecurity survey firm Ponemon Institute Founder Larry Ponemon observed that "We basically know that *companies don't measure these things*" as they're not captured in any of the financial metrics that companies use for financial reporting of their performance.

In other words, publicly-traded US firms rely totally on their *experienced human judgment* and discretion to determine 'materiality' of loss from cyberattacks. Also, as observed above, a

[70] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[71] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
[72] http://www.treasuryandrisk.com/2013/07/15/putting-a-price-tag-on-cyber-crimes

data breach may be deemed *not quantitatively material* as *everyone else is getting breached*. SEC notes that "Materiality concerns the significance of an item to users of a registrant's financial statements. A matter is 'material' if there is a substantial likelihood that a reasonable person would consider it important.[73]" In its Statement of Financial Accounting Concepts No. 2, the FASB stated the essence of the concept of materiality as follows[74]: "The omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item."

The Financial Accounting Standards Board (FASB), which sets accounting standards for public companies, has rejected promulgating quantitative materiality guides thus leaving it to 'experienced human judgment' for determination of materiality. In April, 2013, Sen. Jay Rockefeller wrote to the SEC Chairman that while companies' reporting had improved since the SEC released its guidance, "Investors deserve to know whether companies are effectively addressing their cyber security risks — just as investors should know whether companies are managing their financial and operational risks... Formal guidance from the SEC on this issue will be a strong signal to the market that companies need to take their cyber security efforts seriously… The disclosures are generally still insufficient for investors to discern the true costs and benefits of companies' cybersecurity policies."[75]

Given above observations about regulatory compliance and critical need thereof, the following disconnects about cyberattack losses between what U.S. companies are reporting to their shareholders and what they are sharing with the policy makers may seem understandable. The *Treasury & Risk* report of April 4, 2013 'Disconnect on Cost of Cyberattacks'[76], notes that retired [retired] Army General Keith Alexander, head of U.S. Cyber Command and the National Security Agency, called cybercrime "the greatest transfer of wealth in history." Similarly, Rep. Michael Rogers, a Michigan Republican who leads the House Intelligence Committee, had said foreign intruders "are stealing literally billions" of dollars from companies. On a related note, the study of May 2014 titled 'The Rising Strategic

[73] http://www.sec.gov/interps/account/sab99.htm
[74] http://www.sec.gov/interps/account/sabcodet1.htm
[75] http://www.forbes.com/sites/ciocentral/2013/05/15/how-to-prepare-for-when-the-sec-comes-asking-about-cybersecurity-risk/
[76] http://m.treasuryandrisk.com/2013/04/04/disconnect-on-cost-of-cyberattacks

Risks of Cyberattacks'[77] by the consulting firm McKinsey concluded that over the next five to seven years, $9 trillion to $21 trillion of economic-value creation, worldwide, depends on the robustness of the cybersecurity environment. Figure 4-1 based on a Bloomberg report provides a summary perspective of negligible 'material' filings about cyberattacks losses (Strohm et al., 2013)[78].

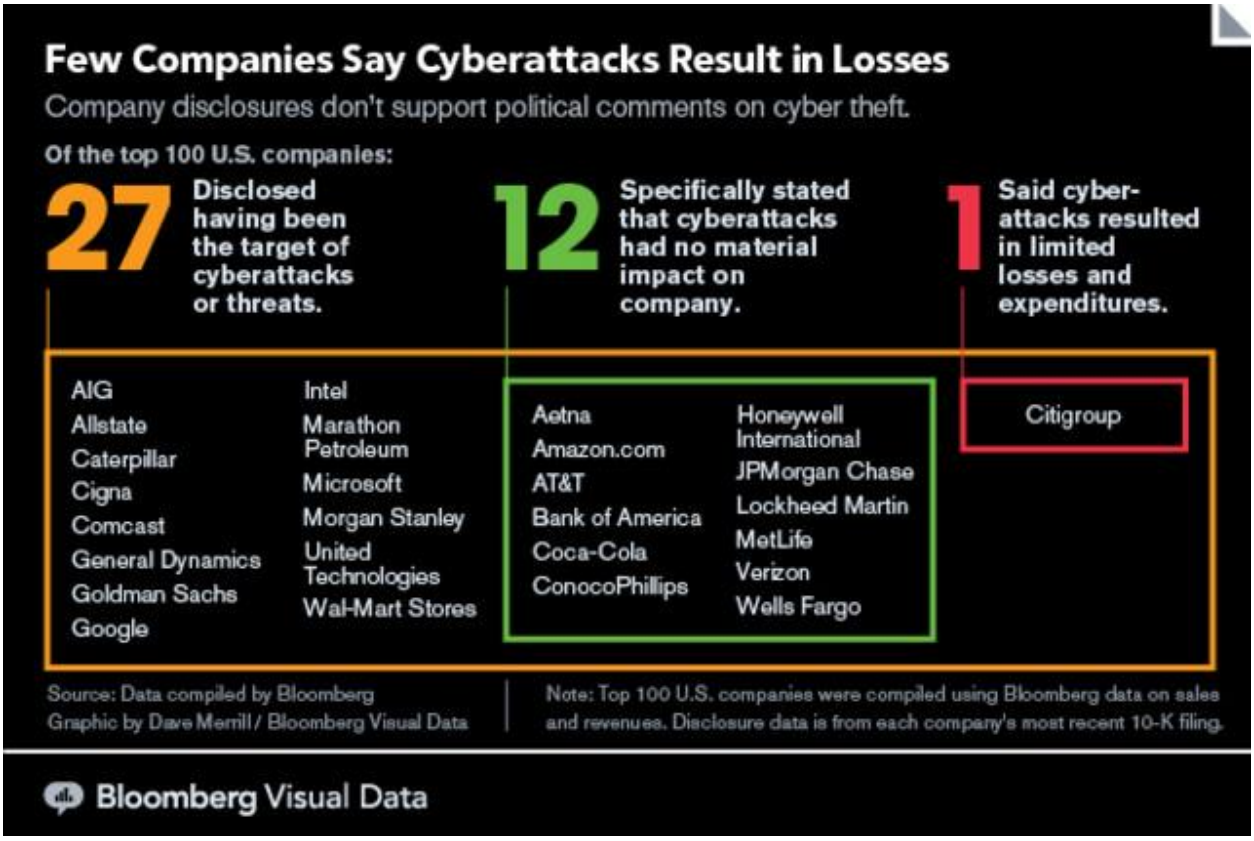


Fig. 4-1. Less than 4% Companies Report Materiality of Cyber Attack Losses

Also, almost all of the top 100 U.S. companies by revenue stated in most recent financial annual reports that they rely on technology that may be vulnerable to security breaches, theft of proprietary data and disrupted operations. Yet, almost none of them reported "material" effects of cyberattacks on their financial performance or financial projections. Even firms whose cyberattacks have been reported in public press mostly reported no "material" effects in SEC filings of financial statements. ConocoPhillips, reported to have been breached by China-based hackers beginning in 2009, said in its 2012 annual report no cyber breaches "had a

[77] http://www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_cyberattacks
[78] http://www.bloomberg.com/news/2013-04-04/cyberattacks-abound-yet-companies-tell-sec-losses-are-few.html

material effect." Coca-Cola was told by the FBI that hackers broke into its computers to steal related files prior to its aborted $2.4 billion bid for China Huiyan Juice Group in 2009. Without mentioning the incident in SEC filings, the company noted that it's "information systems are a target of attacks," and the disruptions "to date have not had a material effect on our business, financial condition or results of operations." Dow Chemical which declared in prepared testimony in a Senate hearing that it was "regularly" attacked "from sources that are advanced, persistent and targeting our intellectual property" made only passing reference to cyber threats in its annual report in the same quarter, putting the risks on par with severe weather events[79].

Absence of public data about the costs of cyberattacks as well as the unwillingness of public firms to report about it given needed regulatory compliance could make the task of finding valid models for assessing costs of cyber insurance all the more challenging. Furthermore given implicit and explicit acknowledgement by regulators and firms being regulated that cyber risk and cybersecurity are fast evolving domains, any specific model validated in one context may require rethinking in another context given dynamics of the fast evolving context. Above observations makes it all the more important to consider all models as tentative and very approximate representations of a fast changing reality. In sum, regardless of the model applied, model risk management is all the more crucial in case of cyber insurance modeling to ensure that it maps on to the most critical and material aspects of the relevant context and the overall framework of cyber risk management.

4.3 Cyber Risk Insurance Riskier than other Risks Types

Before 2000, negligible commercial demand existed for cyber insurance given infancy of WWW, always 'active' and live systems were few; tools, capabilities, and expertise of cyberattacks were limited, and, software installation and upgrades were primarily done offline using floppy drives. Rapid growth of e-Business with related DDOS attacks in 2000 resulted in earlier interest in cyber insurance coverage. Subsequently, consumer data privacy and security related federal regulations such as Graham-Leach-Bliley Act (GLBA) for financial firms and Health Insurance Portability and Accountability Act (HIPAA) have furthered interest in seeking coverage from related liability claims. In 2002-2003, insurance companies specifically started excluding 'intangible' data from general commercial property and liability policies

[79] http://www.bloomberg.com/news/2013-04-04/cyberattacks-abound-yet-companies-tell-sec-losses-are-few.html

covering 'tangible' physical assets. Hence started era of underwriting coverage based on stand-alone specialized policies with firms such as AIG providing cyber insurance coverage for specific markets such as tailoring it to financial services organizations[80].

From an economic perspective, insurance firms have tackled the key problems of economic risk, namely *asymmetric information*, *adverse selection* and *moral hazard*, long before underwriting cyber insurance (Akerlof, 1970). *Asymmetric information* implies that the firm being provided insurance coverage and the insurance underwriting firm providing coverage don't have similar access to information. Given the key role of 'experienced human judgment', materiality may also be interpreted and applied differently by the above two parties. Given the nature of cyber risks and their measurement and reporting discussed earlier, insurance firms face the asymmetric information problem both before and after underwriting or selling coverage to a firm. The risk *to* the insurance firm in providing cyber insurance coverage gets compounded by the *adverse selection* problem given the 'pooled' nature of risks of all underwritten client firms in its portfolio. An insurance firm can remain in business and profitable as long as the proportion of high risk clients is minuscule compared with low risk clients relative to the premium charge.

Client firms exposed to higher risk of cyberattack related loss – because of the intrinsic nature of business, intentionally risky choices or simple neglect, or exposure to high risk dynamic environment – cost more to the insurance underwriter. Adverse selection occurs when the insurance firms underwrites more high risk clients at a given premium which is optimally targeted for lower risk clients. The problem of adverse selection may also occur after the insurance coverage starts as a covered client may choose to take greater risks or become negligent given the fact it is already covered. The last problem of the covered client choosing to pursue high risk behavior given the fact it is covered is called the problem of *moral hazard* (Hölmstrom, 1979).

Conversely, if on purchase of the insurance coverage, the covered client firm takes extra precautions and invests in further reducing risk, that could alleviate the moral hazard problem. Involving much greater levels of asymmetric information, adverse selection, and moral hazard, cyber risks are quite different from risks to tangibles such as commercial property *as well as* intangibles such as financial securities (Baer, 2007). Additionally, scarcity of

[80] http://www.aig.com/CyberEdge_3171_417963.html

reinsurance providers for cyber insurance firms further contributes to inherent risks in cyber insurance coverage as there is no one to backstop losses if a cyber insurance provider defaults.

4.4 Sociotechnical Makes Model Risk More Critical for Cyber

Prior discussion mentioned the two key *intrinsic* characteristics of cyber risk in the networked context that distinguish it from other known risk types. Related to underlying information and communication technologies (ICT), these two intrinsic characteristics are: (i) cyber risks are *interdependent*, and, (ii) cyber risks are *correlated* as seen in Fig. 4-2. The difference between correlation and interdependence is in the fact that *correlation* doesn't imply *causation*, i.e., interdependence. Additionally, in the context of economics of security, interdependence in the above schematic results from externalities in security decisions. Such interdependence resulting from economic externalities is distinguished from statistical correlation (without reference to cause and effect) as well as statistical dependence (with reference to cause and effect). As shown in Fig. 4-2, the above risks follow from the very intrinsic characteristics of the underlying information and communication technology infrastructures.

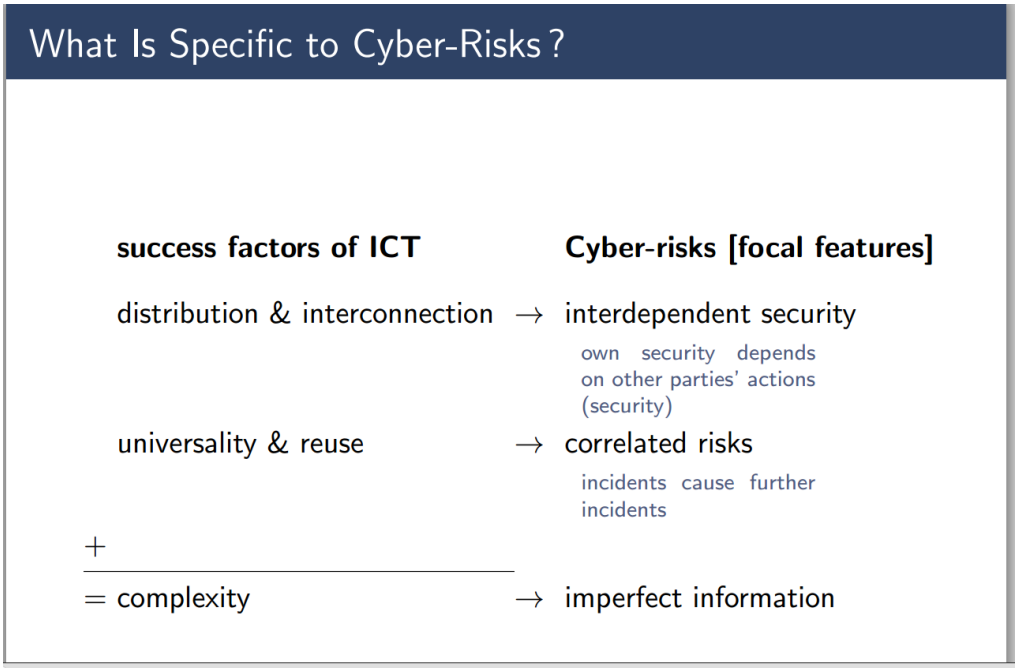


Fig. 4-2. Cyber Risks are intrinsically Interdependent and Correlated

Source: Modeling Cyber-Insurance towards a Unifying Framework[81]
November 10 - 11, 2010, TRUST Workshop at Stanford University

Specifically, success of underlying information and communication technology is determined by its networked interconnections and distribution networks – greater the networked interconnections and wider the distribution networks, more successful the related information and communication technology. Networked interconnections and distribution networks also characterize the interconnectedness and thus *interdependence* of the networked nodes. Secondly, the flip side is that the interconnection and distribution of related cyber risks in the networked context when compromised by an adversary results in *correlated* cyber risks.

To remain viable, insurance underwriters must maintain a large enough portfolio of insured firms representing risks that are *independent* and *uncorrelated*. *The model risk management concern is of central significance given that most statistical models of cyber risk and cyber insurance assessment critically depend on the above two key premises about covered risks: they should be independent and they should not be correlated*. However, unlike insurance of other tangibles and intangibles, *in case of cyber insurance, risks are interdependent* ***and*** *correlated*. According to *Financial Times* report of April 27, 2014, 'Diversity Is the Way to Avoid Cyber Collapse'[82], "what is worrying is the potential for a global *systemwide IT failure occurring simultaneously across many organisations* – a "*correlated loss*" event that affects a vast number of companies, or an entire sector. As businesses get more interconnected, this type of threat becomes a real possibility."

The finance domain has had its own share of globally "correlated loss" resulting from model risk that remained unheeded until after it had already played key role in creating the Global Financial Crisis. That model risk was attributable to the Gaussian copula (Li, 2000)[83] model (joint distribution of random variables used in finance for the estimation of the probability of correlated defaults) which "will go down in history as instrumental in causing the unfathomable losses that brought the world financial system to its knees."[84] That 'formula' was at the center of bundling of hundreds or even thousands of mortgages into pools of

[81] http://weis2010.econinfosec.org/papers/session5/weis2010_boehme_pres.pdf
[82] http://www.ft.com/cms/s/0/7fc4e282-bfcf-11e3-b6e8-00144feabdc0.html
[83] http://stevereads.com/papers_to_read/on_default_correlation-_a_copula_function_approach.pdf
[84] http://archive.wired.com/techbiz/it/magazine/17-03/wp_quant

collateralized debt obligations, or CDOs. Those CDOs modeled the probability of 'correlated' defaults of mortgages in the pool not based on actual empirical data on mortgage defaults (which was sparse just like the current cyber risk loss data) but instead used historical prices from credit default swaps (CDS) market. The implied assumption was that CDS markets price default risk accurately. Given prolific use of the model, which experts cautioned was not suitable for valuation or risk management, the CDS market rapidly grew from $920Bn in 2001 to $62Tn by end of 2007, and, simultaneously, CDO market grew from $275Bn in 2000 to $4.7Tn in 2006[85].

The point that we are trying to highlight in current section is that extremely sociotechnical nature of cyber (cyberspace of globally networked humans is as sociotechnical as any social system can be) endows it with inherent attributes very high tail risk and systemic risk. The stark parallels of the *extreme tail risk* discussed in case of VaR being applied for cyber risk and cyber insurance and the above model at the center of the Global Financial Crisis are apparent. As defined earlier, tail risk results from theoretical statistical probabilistic distribution assumptions of Gaussian normality about the relative infrequency of extremely rare but extremely high impact losses that may not hold in practice. Extreme tail risk results from fundamentally strong deviations from the underlying assumption of statistically normal distribution thus resulting in fat left tails characterizing high kurtosis.

For example, risk doesn't vanish in financial securitization or modeling[86]: "*In finance, you can never reduce risk outright; you can only try to set up a market in which people who don't want risk sell it to those who do.* But in the CDO market, people used the Gaussian copula model to convince themselves they didn't have any risk at all, when in fact they just didn't have any risk 99 percent of the time. The other 1 percent of the time they blew up. *Those explosions may have been rare, but they could destroy all previous gains, and then some*." When the mortgage boom ended abruptly and home values started falling across the country, default correlations jumped while the model accounted for less than ten years for which the CDS existed during which home prices had been simply going up and default correlations were low. Similar scenario, *however much more extreme*, can be contemplated in the case of cyber risks going forward into future given above parallels *and* unique nature of cyber risks.

[85] http://archive.wired.com/techbiz/it/magazine/17-03/wp_quant?currentPage=all
[86] http://archive.wired.com/techbiz/it/magazine/17-03/wp_quant?currentPage=all

As apparent, cyber risks, given their *highly interconnected, distributed, networked, and, universal contexts* and being *embedded in the medium and the message,* unlike most other insured risks, are most highly *interdependent* as well as most highly *correlated*. One reason for such risks is the *monoculture*[8788,,89] in *installed operating systems* such as Microsoft Windows[9091,92,93], Apple iOS[94,95,96], Android[97,98], and *more importantly software enabling underlying network and security protocols*. National and global scale cyber risk exposures and vulnerabilities are being continuously detected and exploited with ongoing continuous patching and upgrades of *active* applications such as Java and Flash, and, *as well as related network layer protocols* with no respite in sight. Use of similar operating systems, software, hardware, and, perhaps *most importantly reliance upon the same universal network protocol layers* such as SSL/TLS represent critical vulnerabilities in the context of cyber risk and cyber insurance.

The last point about network protocols is perhaps most critical *as network layer protocols represent the 'most universal' of all interconnected, distributed, and, networked capabilities as well as potential vulnerabilities exposed to potential exploits*. That point is also critical given that the *notion of monoculture itself is transitioning* from *vendor specific monoculture* to *monoculture of universal and global infrastructure enabling technologies* underlying *all* or *most* of those systems.[99] As a result of such national and global computing and communication information technology monocultures, "a large part of today's computing technology suffers from the same weak spots and bugs. Consequently, worms and viruses can systematically exploit these vulnerabilities and thus *epidemically cause huge damage* by *attacking all computers in a network almost at the same time*." [100,101,102]

---

[87] http://www.whitehouse.gov/files/documents/cyber/IEEE%20-%20IT%20Monoculture.pdf
[88] http://www.cs.sjsu.edu/faculty/stamp/DRM/DRM%20papers/CACMmono.pdf
[89] https://securityledger.com/2014/04/heartbleed-technology-monocultures-second-act/
[90] http://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication
[91] http://www.csoonline.com/article/2865215/operating-system-security/google-unveils-windows-8-1-vulnerability-releases-sample-code.html
[92] http://www.tripwire.com/state-of-security/incident-detection/microsoft-windows-zero-day-exploit-sandworm-used-in-cyber-espionage-cve-2014-4114/
[93] http://securityintelligence.com/ibm-x-force-researcher-finds-significant-vulnerability-in-microsoft-windows/
[94] http://www.zdnet.com/article/apple-ios-7-1-patches-41-vulnerabilities/
[95] https://www.us-cert.gov/ncas/alerts/TA14-317A
[96] https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html
[97] https://www.blackhat.com/docs/us-14/materials/us-14-Forristal-Android-FakeID-Vulnerability-Walkthrough.pdf
[98] http://www.zdnet.com/article/half-of-all-android-devices-still-vulnerable-to-privacy-disaster-browser-bug/
[99] https://securityledger.com/2014/04/heartbleed-technology-monocultures-second-act/
[100] http://infosecon.net/workshop/pdf/15.pdf
[101] https://securityledger.com/2014/03/sohowned-300k-home-routers-hacked/

Our research findings and concern about the criticality of transition of monoculture from vendor-specific platforms to *universal global digital communication network protocols* are shared by others. Dan Geer, the Chief Security Officer at In-Q-Tel, the CIA's venture capital arm, who co-authored the influential report titled 'CyberInsecurity: The Cost of Monopoly'[103] with co-authors such as Bruce Schneier, recently wrote about similar transition of monoculture[104]: "The critical infrastructure's monoculture question was once centered on Microsoft Windows. No more. The critical infrastructure's monoculture problem, and hence its exposure to common model risk, is now small devices and the chips which run them. As the monocultures build, they do so in ever more pervasive, ever smaller packages, in ever less noticeable roles."

The problem of increasingly wider impact of transitioning (from vendor specific to underlying universal network protocol specific) of monoculture is in things such as world pervasive Internet-of-Things on top of *universal* protocols such as SSL/TLS that have *universal* vulnerabilities resulting in wholescale exploitation (CVE-2014-0160[105]) such as in the case of Heartbleed[106,107,108] (which allows a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys) or more recently in case of POODLE[109] (CVE-2014-3566[110]) (which allows an attacker to decrypt and extract information from inside an encrypted transaction for SSL 3.0 with CBC mode encryption).

In addition to above technological concerns, the economic *free rider* problem that compounds the risks related to cyber security as a 'common public good' further contributes to the externality and extremity of cyber risks relative to other insured risks. Specifically, incentives to invest in cyber security at the intra-enterprise level and (more commonly) to invest in cyber security of network backbones enabling all cyber activities at the inter-enterprise level are perverse. At the intra-enterprise level, specific divisions recognizing that they are exposed to 'lateral' attacks launched by adversary using another division's

---

[102] https://www.fireeye.com/blog/threat-research/2014/08/ssl-vulnerabilities-who-listens-when-android-applications-talk.html
[103] http://cryptome.org/cyberinsecurity.htm
[104] http://www.lawfareblog.com/2014/04/heartbleed-as-metaphor/
[105] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
[106] https://www.us-cert.gov/ncas/alerts/TA14-098A
[107] http://business.financialpost.com/2014/04/12/heartbleed-bug-highlights-banks-severe-cyber-security-headaches/
[108] https://www.schneier.com/blog/archives/2014/04/heartbleed.html
[109] http://krebsonsecurity.com/2014/12/poodle-bug-returns-bites-big-bank-sites/
[110] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566

infrastructure, may question if their own cybersecurity investment does them any good. At the inter-enterprise level, specific firms recognizing that their private benefits from investing in cyber security of 'public goods' such as network security protocols are lesser than the social benefits, have until recently chosen not to invest in them despite being subjects of cyberattacks from related vulnerabilities[111]. This has occurred despite the fact that *network layer protocols represent the most universal of all capabilities as well as potential vulnerabilities exposed to potential exploits and are being increasingly used most frequently and persistently for cyber-attacks*.

In recent global cyber-attacks as in the case of 'heart-bleed' bug, the underlying protocol on which everyone relied was developed and maintained by a couple of 'volunteer' scientists on the side[112]. That attack had brought into scrutiny the nature of 'open source' software and its reliability as a 'public good.' It apparently also motivated some of the more visible players to start publicly investing in such 'public goods' on which all commercial firms and governments relied upon as a free public good. The stark economics of profit-seeking entities using the open source software for commercial gain and the 'starving' volunteers developing and maintaining it came to surface with the heart-bleed exposure. Firms and organizations including Cisco, Google, Amazon, and Federal Bureau of Investigation had relied upon OpenSSL code in which the bug was found.

"What makes Heartbleed so dangerous, security experts say, is the so-called OpenSSL code it compromised. That code is just one of many maintained by the open-source community. But it plays a critical role in making our computers and mobile devices safe to use... OpenSSL code has been picked up by companies like Amazon, Facebook, Netflix and Yahoo and used to secure the websites of government agencies like the F.B.I. and Canada's tax agency. It is baked into Pentagon weapons systems, devices like Android smartphones, Cisco desktop phones and home Wi-Fi routers. [113]" However, "firms don't maintain OpenSSL code because they don't profit directly from it, even though it is integrated into their products, and governments don't feel political pain when the code has problems. [114]"

Another reason for greater riskiness of cyber risks is the *intensely technical/human nature of cyberspace*, making it *more susceptible and vulnerable to social engineering risk*. As compared with financial risks or insurance risks related to financial securities and commercial property,

[111] http://mashable.com/2014/04/14/heartbleed-open-source/
[112] http://www.nytimes.com/2014/04/19/technology/heartbleed-highlights-a-contradiction-in-the-web.html
[113] http://www.nytimes.com/2014/04/19/technology/heartbleed-highlights-a-contradiction-in-the-web.html
[114] http://www.nytimes.com/2014/04/19/technology/heartbleed-highlights-a-contradiction-in-the-web.html

social engineering risks are multiple times higher in case of cyber risks. When the two problems of universal reliance upon most universal public good such as network layer protocols and the social engineering problem of exploitation of related vulnerabilities in those protocols are crossed over, we get the current era of exponentially increasing cyber risk[115]. Overwhelming interactions resulting from the intrinsic nature of 'systems' (systems are systems because they are interdependent) make most complex systems, natural and social, behave in non-normal ways. Such violation of statistical normality results from interdependence of observations which fundamentally violates underlying central limit theorem and thus results in fat tails[116]. Furthermore, "Introducing human behaviour is likely to make for stronger interactions within the system, further fattening the tail." [117]

Similar vulnerabilities in universally used software, hardware, and networks – and related network layer protocols at all levels – exploited by similar social engineering schemes using botnets or otherwise escalate cyberattacks causing global 'spikes' in the frequency of related cyber risks. The above observations raise questions about the claims of 'materiality' filed in SEC filings about the similarity of cyber risks being similar to risks related to weather. While earthquakes, tsunamis or tornadoes don't strike anywhere and everywhere at the same time, global cyberattacks can! If the cyber risk is to be assessed and insured analogous to such natural catastrophes, then *catastrophe modeling* taking into account extreme risks is needed.

When such cyberattacks are used for dropping malware or ransomware at a global scale exploiting vulnerable server or client software systems, as they impact hundreds or thousands of users, we get highly correlated and interdependent cyberattacks. Examples of attacks resulting from missing upgrade paths such as in the case of SOHO routers[118] and in case of MS-Windows XP used for worldwide banking ATMs[119] also represent related examples. Recent example of 6,000 employees at SPE knocked off their computer and e-mail systems is another smaller scale firm level example. Correlation and interdependence of cyber-attacks result is significant percentage of the 'pool' of insured 'low risk' and 'high risk' client firms becoming high risk at the same time. The resulting misfortune of the insurance firm challenged to cover such interdependent and correlated cyber risks will be a replay of story of

[115] See for instance, http://www.infosecurity-magazine.com/news/android-malware-rockets-300x-in-2/
[116] http://www.bankofengland.co.uk/publications/Documents/speeches/2012/speech582.pdf
[117] Introducing human behaviour is likely to make for stronger interactions within the system, further fattening the tail.
[118] http://arstechnica.com/security/2014/03/hackers-hijack-300000-plus-wireless-routers-make-malicious-changes/
[119] http://www.computerworld.com/article/2488842/financial-it/most-atms-will-remain-on-windows-xp-after-microsoft-pulls-plug-on-os-support.html

the insurance firm AIG. During Financial Crisis, AIG had to cover claims by multiple insured firms such as Goldman Sachs when and needed US government support for its survival[120].

The above discussion about the intrinsic characteristics of cyber risk is of central importance to understanding what really cyber risk is and how it is quite different from financial risks typically modeled by VaR. The most critical point that is important to recognize is the fact that intrinsic nature of cyber risk in terms of above characteristics results in exponentially higher tail risks *as well as* systemic risks. However, as a modeling tool for assessing financial risks, VaR has had the most disastrous track record as it was not designed to assess such systemic risks and tail risks. Therefore, using VaR for assessing cyber risk assessment and modeling cyber insurance even though it is perhaps the most unfit (and therefore misleading) model to do so is literally asking for disaster. Again, our criticism is not of VaR, but of the misuse and abuse of VaR such as in the context of cyber risk modeling given that doing so totally violates and contradicts the assumptions, logic, and boundaries of the VaR model (Malhotra, 2014).

4.5 Cyber Risk and Cyber Insurance Modeling in Practice

Our above analysis established two key points: (i) cyber risk is exponentially greater in real terms of scale of global and national impact as compared with traditional risks such as financial risks or property risks, and, (ii) hence there is critical need for model risk management in case of cyber risk modeling even more so than for financial risks or property risks. Developing on the above analysis, the following discussion focus is on the most predominantly used models for cyber risk and cyber insurance modeling found in our research. Incidentally, the quantitative models that are found to be currently most popular for commercial applications in cyber insurance modeling for financial assessment of cyber risk loss are characterized by extremely high model risks, systemic risks, and, tail risks.

A review of extant cyber risk and cyber insurance models was undertaken with specific focus on quantitative and financial modeling of cyber risk and cyber insurance. A brief overview of the models observed in applied practice follows. It must however be observed that given paucity of available and reliable public financial data, most models in this domain are at relatively early stages. Even though availability of public data is anticipated to facilitate empirical testing and validation of analytical form of such models, yet the domain of cyber risk and cyber insurance is dynamic and evolving. With increasing concerns of the general public

[120] http://www.bloomberg.com/apps/news?pid=newsarchive&sid=ax3yON_uNe7I

voiced by their representatives, shareholders are asking for better visibility into dollar-figure cyber risk assessments of firms. Firms are hesitant to share information beyond standard press releases given materiality standards of SEC discussed earlier. Firms and regulators such as SEC are both cognizant about not providing too much specific information so as not to abet and aid the adversaries which may further escalate the cyber risks. Our research focused on a broad spectrum of all available quantitative models for risk assessment and modeling in the nascent domain of 'quantification' of cyber risk and cyber insurance. Our research on cyber risk and cyber insurance modeling shows that the most prominent model being applied by most key players across diverse business economic and technology sectors is 'Value-at-Risk' model also called VaR for short.

4.6 VaR Models in Use for Cyber Risk Insurance Modeling

Our analysis of all available quantitative models of cyber risk assessment and cyber insurance modeling found a few recent empirical studies as well as several interesting applications in practice. Given that cyber risk assessment and cyber insurance modeling are fast-evolving domains, most models being applied are at a nascent stage. We also found several other academic and theoretical studies that were not directly related to cyber risk loss assessment and cyber insurance modeling in our specific context. Given our specific focus on the real world application of quantitative finance models in the newly emerging domain of cyber risk assessment and cyber insurance modeling, we focus here on a representative sample of those application-focused studies and applications. We first review representative academic research studies in this domain, thereafter we review specific examples of commercial applications by the industry leading players in the US cyber insurance industry.

4.6.1 Catastrophe Modeling of Tail Risks Using EVT with VaR

One early empirical studies on quantitative modeling of cyber risk and cyber insurance is the 2014 study titled Insurability of 'Cyber Risk: An Empirical Analysis'[121] published by the Institute of Insurance Economics at the University of St. Gallen. That study deployed VaR and TVaR (Tail Value at Risk) models for cyber risk assessment within the overall framework of *Extreme Value Theory* (*EVT*)[122,123] for estimating the loss severity distribution for the tail risk.

[121] http://www.palgrave-journals.com/gpp/journal/v40/n1/abs/gpp201419a.html
[122] http://www.casact.org/library/studynotes/embrechts_extremevalue.pdf
[123] http://www.unige.ch/ses/dsec/static/gilli/evtrm/GilliKelleziCE.pdf

While VaR measures Maximum Loss Not Exceeded with a Certain Probability, T-VaR measures Expected Loss if Tail Event Occurs. This study is an example of *catastrophe ('cat') modeling* mentioned earlier which uses EVT with its focus on extreme losses resulting from rare or random events. It estimated the loss severity distribution using a spliced distribution approach: the exponential generalized Pareto distribution (GPD) model to model exceedances over a defined threshold. EVT uses two kinds of models for modeling extreme values: generalized extreme value (GEV) models for modeling block maxima/minima models; and, GPD for modeling peaks-over-thresholds (POT) models. GPD is a family of continuous probability distributions often used to model the tails of another distribution and is specified by thee parameters: location, scale, and shape. Losses above the predefined threshold are modeled by a GPD, while losses below the threshold are modeled with an exponential distribution, Weibull distribution, Gamma distribution, or lognormal distribution[124]. The above study tested empirical data using all four distributions for the body of the distribution. Having modeled the spliced distribution, it used a VaR estimator to determine estimated loss of severity distribution finding empirical VaR close to modeled VaR.

4.6.2 Portfolio Modeling of Risk Optimization Using MVO with CVaR

In finance, VaR modeling is typically done in the context of *Mean Variance Optimization* (*MVO*) [125]of a portfolio of assets. Hence, it seems intuitive to situate the computation of cyber risk assessment models based upon VaR within overarching *Portfolio Construction and Optimization Models*. Analogous to financial asset portfolio models, cyber risk portfolio models will instead focus on construction and optimization of a portfolio of risks. This approach seems consistent with the risk management frameworks that are typically used for characterizing the cyber risks in cybersecurity related Information Assurance frameworks. The initial concept of one such portfolio model of risks is available in a recent article titled 'Measuring and Optimizing Cybersecurity Investments: A Quantitative Portfolio Approach' (Zhuo & Solak, 2014)[126] and related presentation titled 'Cybersecurity Investment Optimization

[124] These parametric statistical distributions are used in catastrophic risk modeling such as in this case modeling the tail risk exceeding the specified threshold because of rare and random events. Poisson distribution is often used to model rare and random events (e.g., earthquake occurrence), Pareto distribution is used to estimate the flood frequency or fire loss, and lognormal distribution is often used to track the earthquake motion, or Tornado path.

[125] Markowitz, H.M. (March 1952). "Portfolio Selection". The Journal of Finance 7 (1): 77–91.

[126] "Measuring and Optimizing Cybersecurity Investments: A Quantitative Portfolio Approach," with S. Solak. Proceedings of IIE Annual Conference 2014, May 31-June 3, Montreal, Canada.

with Risk: Insights for Resource Allocation' (Solak 2014)[127]. The general portfolio modeling of cyber risks depends on measuring returns from cybersecurity investments, defining uncertainty around those returns, while taking into consideration continuous evolving dynamics of the cyber environment.

Based on the Information Assurance CIA troika of *confidentiality*, *integrity*, and *availability*, a taxonomy (presented earlier) is used for classifying assets such as *confidential assets* and *non-confidential assets*. Cyber*attacks* correspond to all types of threats to information systems of a firm and are distinguished using a taxonomy classifying them as *basic attacks* and *advanced attacks*. Cybersecurity *countermeasures* are the set of security measures used to protect the assets against cyberattacks and are distinguished into *preventive* and *detective* countermeasures. In the context of cyber risk assessment, the risk portfolio's return on investment is computed in terms of *effectiveness in reducing expected loss*. An organization's cyber risk strategy determining how much to invest in each countermeasure depends on distribution of the potential *losses* over basic and advanced attacks as well as the *effectiveness* of each type of countermeasure on these attack categories. Combined effect of countermeasures is then determined by the difference between Losses without countermeasures and Losses reduced with countermeasures. Definition and measurement of risk in cyber risk optimization setting is challenging as discussed earlier. However, reduction of variance around expected losses to minimize the likelihood of extremely high losses is a realistic assumption. *Conditional Value at Risk* (*CVaR*) is used as a measure in optimizing investments in the Portfolio Model. CVaR is defined as the expected loss that will be incurred if the realized losses lie in some given percentile of the total loss distribution.

4.6.3 'CyberV@R: A Model to Compute Dollar Value at Risk of Loss to Cyber Attack'

The above titled presentation at FloCon 2013[128] organized by CERT uses VaR for constructing risk models that can provide relative comparison of economic costs of a cyberattack. The basic premise of this framework is that CIOs face the challenge of safeguarding their enterprise cyber infrastructure from breaches that could lead to 'catastrophic economic losses.' Hence, this framework seems a good candidate for the 'cat' or 'catastrophic' risk assessment models based on EVT discussed above. However, the framework presents the use of ordinary VaR model (without any specific mention of tail risks

[127] http://www.acscenter.org/news-events/solak_20140919_presentation.pdf
[128] http://www.cert.org/flocon/2013/presentations/ulrich-james-cybervar.pdf

or EVT) for the cyber risk loss computation. In their framework, "a VaR model answers the question 'what is the amount of money $X, such that the odds of losing more than $X , over time window T , fall below some threshold of probability P?' We call this the 'P-percent VaR.'" Their model is based on the standard VaR model that doesn't tail risk into consideration (e.g. Christoffersen 2012) and answers the question: What loss is such that it will only be exceeded p.100% of the time in the next T trading days? It is called "p-percent VaR." For example, 1% VaR is the maximal loss that can be suffered on the current portfolio with 99% confidence. In other words, loss worse than VaR should occur only one in 100. VaR is often defined in dollars as $VaR, hence $VaR loss is implicitly defined from probability of getting an even larger loss as in: Pr ($Loss > $VaR) = p. By definition, (1 – p).100% of the time, $Loss will be smaller than the VaR. SANS Security Trend Line note of Sep. 23, 2014, titled 'It Always Costs Less to Avoid a Breach Than to Suffer One' (Pescatore, 2014)[129] illustrates how CyberVaR application would assess how much it would have cost Home Depot to avoid its well-publicized breach[130]. However, that illustration doesn't really show how VaR modeling is applied beyond the assumption of a dollar figure of a $500 million potential liability somehow associated with a "value at risk of $246,000,000."

4.6.4 Other Key Examples of VaR Models in Commercial Cyber Insurance Modeling

As noted earlier, our literature research on models used for cyber risk and cyber insurance assessment shows that the most prominent model being applied by most key players across diverse business economic and technology sectors is 'Value-at-Risk' model called VaR for short. Above two academic empirical studies seem to be in the small minority that seem cognizant and cautious about using regular VaR models for cyber risk and cyber insurance modeling. Like the commercial CyberV@R (also, known as CyberVaR) model above, many of the commercial models of cyber risk and cyber insurance seem to rely upon the regular VaR model. One notable exception at a concept level that seems to be aligned with the portfolio model of one of the above two academic studies is that of Aon Risk Solutions presentation of May 10th, 2012, on Integrated Approach to Operational Risk. It refers to its proprietary source of external data called OpBase for developing scenarios and estimated exposures which are then classified into Expected Loss (left body of the statistical distribution of cyberattack losses), Unexpected Loss (right body of the statistical distribution of expected

[129] http://www.sans.org/security-trends/2014/09/23/simple-math-it-always-costs-less-to-avoid-a-breach-than-to-suffer-one

[130] http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571

losses), and Catastrophic Loss (right tail of the statistical distribution). Summary of other examples from the research indicating use of regular VaR and similar models follows.

Network Risk Assessment Tool (NRAT) model[131] published in the IAnewsletter Vol 11 No 1 Spring 2008 (of the DoD Information Analysis Centers) uses a framework containing the likelihood of an adverse event and the severity of that event to determine reduction in 'value at risk' based upon deployment of specific protection strategy. Autumn 2011 report titled 'Can You Hack It? Managing the Cybersecurity Challenge[132] from the McKinsey & Company Consulting firm's Government proposes a "value at risk" framework and related taxonomy for assessment of cyber risks. They "value at risk analysis" seems to focus on the dollar-figure impact of specific cyberattacks without any specific link to the technical statistical VaR models or methodologies. They do note that their "value at risk" is a combination of three elements: the attacker's capability, the asset's vulnerability, and the relative financial and nonfinancial costs of the attack. Similarly a World Economic Forum titled 'Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience' prepared by Deloitte focuses on "values at risk" without specifying their technical or statistical nature[133]. A presentation of Sep. 19-20, 2011, by Visa at the 'Securing the Enterprise from a Dangerous World' mentions 'Enterprise Value at Risk' in its focus on 'Cyber Security Measures within the context of ABC-based Balanced Scorecard analysis'. A presentation titled 'Cyber Risk in the Financial System through the Stakeholder Lens'[134] of 2011 lists the example of multi-level security deployment for the Philadelphia Stock Exchange in terms of Value-at-Risk corresponding to Economic Value and Brand Integrity Value.

The 2013 Society of Actuaries (SOA) Valuation Actuary Symposium session of 23rd September 2013 titled 'ASOP-46 Risk Evaluation in Enterprise Risk Management'[135] (ERM) and its 'Case Study: Emerging Risk Analysis Cybersecurity Risk' classify cyber risk as an emerging risk defined in terms of Actuarial Standard of Practice (ASOP) as "New or evolving risks that may be difficult to manage since their likelihood, impact, timing or interdependency with other risks are highly uncertain." While observing industry experience data, firm's own historical incidence data, deterministic scenarios, and, Monte Carlo simulations as possible avenues for quantification of cyber risk, it acknowledged lack of any standard methodologies.

[131] http://iac.dtic.mil/iatac/download/Vol11_No1.pdf
[132] http://www.mckinsey.com/client_service/public_sector/latest_thinking/mckinsey_on_government/can_you_hack_it
[133] http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf
[134] http://www.theprobitygroup.com/The_Probity_Group/CyberRiskInTheFinancialSystem.pdf
[135] http://www.actuarialstandardsboard.org/pdf/asop046_165.pdf

Related presentation titled 'Risk Evaluation in Enterprise Risk Management' in the same symposium specified VaR and T-VaR as recommended ERM risk evaluation methodologies while observing the caveat about not relying upon assumptions of normality. It distinguished VaR and T-VaR in the following terms. *VaR*: '*The amount of loss not to be exceeded with a certain probability in a given time frame; typically expressed as a percent of capital.' T-VaR: 'The expected amount of loss if the VaR loss threshold is exceeded.'* It specified VaR and T-VaR as potential ERM risk assessment methodologies without any specific illustration of their application to cyber risk. World Economic Forum agenda note of Nov. 13th, 2013, by the consulting firm Wipro observed that[136]: "Wipro's approach for quantification of cyber risk is based on the concept of Value-at-Risk (VaR), which measures the potential loss in value of a risky asset or portfolio over a defined period for a given confidence interval. This VaR sums up the risk in dollar terms, which helps to communicate the likely impact of cyber risk in a language that is familiar to the senior management and helps them make their risk management decisions."

At an organizational level focus on uncertainty management and risk modeling, the notion of enterprise risk management (ERM) guides most firms. "The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.[137]" The June 2014 report titled 'Insurance Modernization Stakeholder Analysis Risk'[138] from the Big-4 management consulting firm PwC considers cyber risk within the overall enterprise risk framework ERM. It notes about the use of VaR that: "Realizing ERM's promise requires more than just complex economic capital and value at risk (VAR) models. It requires confidence in these models and an understanding of their key assumptions and limitations. This confidence and understanding need to be pervasive – from risk, finance and actuarial personnel themselves, through line of business leadership, up to senior management and the Board of Directors." Their perspective about model risk

[136] https://agenda.weforum.org/2013/11/how-to-measure-cyber-risk/
[137] http://www.coso.org/documents/coso_erm_executivesummary.pdf
[138] http://www.pwc.com/us/en/insurance/publications/assets/pwc-insurance-risk.pdf

management for balancing risk and uncertainty is consistent with the current dissertation and prior related research and analysis (Malhotra 2014[139], Malhotra 2012[140]).

The report titled 'Clear and Present Danger: The Pressing Need to Address Cyber Risk Requires its Better Understanding and Adequate Quantification'[141] in *Financier Worldwide* magazine of August 2014 underscores that even though cyber risk continues to grow, it remains underestimated. The report notes that even in terms of regulatory compliance such as HIPAA, large number of US companies are either non-compliant, or, even unaware about compliance requirements. The report noted use of VaR like risk measures adapted to specific context of cyber risk such as Value at Cyber Risk (VaCR) or Marginal Value at Cyber Risk (MVaCR) unless the degree of uncertainty gets too high to make those measures unusable. Presentation titled 'A Practical Guide to Getting Your Hands around Cyber Risk'[142] at Aegis 2014 Policyholders' Conference shows application of VaR using a Threats-Vulnerabilities-Consequences matrix. Based upon their identification of (1) threats, (2) vulnerabilities, (3) affected assets, (4) range of consequences, and (5) current mitigation strategies, they quantify the minimum / most likely / maximum impacts based on primary and secondary costs and use estimation of frequency / likelihood of specific adverse incidents. Based upon those inputs, they developed a loss distribution for all cyber risks using a product of Poisson Distribution[143] (Frequency) and a Pert Distribution[144] (Impact).

4.7 Significant VaR Model Risk for Cyber Insurance Modeling

Regular VaR refers to the plain baseline VaR *model* to distinguish it from the VaR *methodology* (Malhotra 2014[145]) underlying more advanced models including EVT, GARCH, etc. that overcome many of the limitations of VaR. Reliance of many of the commercial industry players in cyber risk and cyber insurance on regular VaR seems to result from their apparent lack of recognition or acknowledgement of the most fundamental limitations and caveats of

[139] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2538401
[140] http://yogeshmalhotra.com/MarkovChainMonteCarloModels.pdf
[141] http://www.financierworldwide.com/clear-and-present-danger-the-pressing-need-to-address-cyber-risk-requires-its-better-understanding-and-adequate-quantification/
[142] https://www.aegislink.com/content/dam/aegislink/resources/presentations/public/2014/2014_07-29_07-31/Hands_Around_Cyber_Risk_link.pdf
[143] The Poisson distribution expresses the probability of a given number of events occurring in a fixed interval of time.
[144] The PERT distribution is a special case of the beta distribution that takes three parameters: a minimum, maximum, and most likely (mode).
[145] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2538401

regular VaR. Limitations inherent in regular VaR as a risk measurement have prompted books on it such as *The Number That Killed Us: A Story of Modern Banking, Flawed Mathematics, and a Big Financial Crisis* (Wiley, 2011). *The obvious caveat is that the ordinary VaR model doesn't account for the extreme risk in the tails which could lead to 'catastrophic economic losses.'* Furthermore, the problem with ordinary VaR which is all the more critical in case of cyber risk assessment is that VaR is *not* a systemic risk measure. *This point is all the more crucial given that the lack of independence and correlations across diverse cyber risks as well as entities subject to cyber risks discussed earlier can result in significant systemic risk that VaR doesn't account for.* In fact, the above key issues, in addition to the limitations of VaR in not accounting for non-linear and non-normal statistical distributions have been primary shortcomings of VaR for which it has faced intense criticism.

As apparent from the above analysis of nascent cyber risk assessment and cyber insurance modeling, these applications and practices are predominantly reliant upon the VaR model. Based upon recognized limitation of VaR in terms of model risks, tail risks, and systemic risks, one comes away with the unsettling conclusion that given very high interdependence and correlations characterizing cyber risks, application of VaR for cyber risk assessment and cyber insurance is fraught with peril. Based upon the details available in publicly available sources on the applications of VaR in cyber risk assessment and cyber insurance modeling, it appears that VaR is being adopted as a 'black box' in this domain. Our analysis of those applications presented earlier, that most of those commercial practice applications of VaR in cyber risk assessment and cyber insurance modeling did not consider model risks, tail risks, or systemic risks at all. Furthermore, what is even more alarming is the fact that such 'blackbox' reliance upon VaR (or any other model for that matter) is the strongest indicator of model risk calling to attention the most critical need for model risk management.

Our analysis established that if left unchecked and uncontrolled, large-scale commercial reliance upon quantitative models with inherent model risks, tail risks, and systemic risks in current form is expected to lead to impending national cyber risk and cyber-insurance disaster. How can such impending national cyber risk and cyber-insurance modeling disaster be pre-empted and prevented? What can be possibly done to alleviate and minimize the model risk of what looks like unknowing and unquestioning appropriation of VaR model from finance into cyber risk assessment and cyber insurance modeling? This thesis in our knowledge is the first attempt to *recognize the impending cyber insurance crisis* as well as *provide a solution by*

helping steer cyber risk assessment and cyber insurance modeling practice away from that crisis by *judicious applications of model risk management related to the relevant quantitative models*.

Applications such as CyberVaR (also denoted as CyberV@R) presented at the CERT conference share the rationale for adopting the methodology based upon their notion of 'Proof of concept: Risk models in finance' in following terms[146,147]: "In finance, trading desks maintain Value at Risk (VaR) models for measuring portfolio loss exposure…" asking 'Can we do something similar for cyber?' and 'Yes: if we map from finance to cyber.' Many other applications of VaR in cyber risk assessment and cyber insurance some of which we reviewed earlier are based upon similar implicit or explicit logic and assumptions.

The focus of our in-depth qualitative analysis in the current section based on state-of-art research and practice in cyber risk assessment and cyber insurance modeling was on 'what exactly is cyber risk.' Before modeling any risk, it is most critical to understand what exactly it is in terms of its most critical risk related attributes as explicitly delineated in prior focus on model risk management. Based on the related insights, commercial applications of cyber risk assessment and cyber insurance modeling can substantially benefit from answers to the following questions. It is worth reiterating those questions (listed earlier in the first chapter on Introduction) at the current mid-point of the dissertation. Continuing to answer these questions will help modelers and users better recognize and manage model risk:

(a) How is VaR exactly applied in its native empirical real world context of measuring portfolio loss by real world financial trading desks using VaR models as we explain further in Chapter 5?
(b) What are the most critical limitations of VaR that are known in the finance domain related to model risks, tail risks, and systemic risks related to VaR as explained earlier in Chapters 3 and 4, and discussed further in Chapters 5 and 7?
(c) How are the critical model risks, tail risks, and, systemic risks related to VaR even *all the more relevant* to the cyber domain and cyber risk assessment and cyber insurance modeling VaR as explained earlier in Chapters 3 and 4, and discussed further in Chapter 7?

[146] http://www.cert.org/flocon/2013/presentations/ulrich-james-cybervar.pdf
[147] http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_51300.pdf

(d) How cyber domain's exponentially greater interconnectedness, interdependence, and correlations in case of cyber risks contribute to the above risks related to VaR as explained earlier in Chapters 2 and 4?
(e) How can cyber risk assessment and cyber insurance modeling applications and practices minimize the above model risks, tail risks, and systemic risks of VaR as explained earlier in Chapters 3 and 4, and discussed further in Chapters 5 and 7?
(f) What alternative models can cyber risk assessment and cyber insurance modeling applications use to further minimize the above model risks, tail risks, and systemic risks of VaR as explained further in Chapters 5, 6, and 7?

Our prior analyses and discussion in the current chapter as well as the prior chapters in this dissertation already focused on helping applied practice of cyber risk assessment and cyber insurance modeling develop actionable knowledge about concerns (b) through (e) listed above. The next chapter focuses on helping them understand (a) How is VaR exactly applied in its native empirical real world context of measuring portfolio loss by real world financial trading desks using VaR models? Subsequent two chapters help them understand (f): What alternative models can cyber risk assessment and cyber insurance modeling applications use to further minimize the above model risks, tail risks, and systemic risks?

The discussion until the current mid-point of the dissertation has been grounded in theoretical foundations of statistics and probability of quantitative risk modeling, and, cutting-edge research and practice of cyber risk assessment and cyber insurance modeling. Our stated goal of the dissertation is: "To avert the impending national Cyber risk and Cyber-insurance disaster based upon large-scale commercial reliance upon quantitative models with inherent model risks, tail risks, and systemic risks in current form." Consistent with the specific objective, our in-depth qualitative analysis with real world case studies and examples has hopefully helped you develop the critical financial intuition and insight about the specific (cyber, financial, trust) risks and related contrasts and inter-relationships we are dealing with. Such financial insight and intuition is most critical to model risk management of any risk model as underscored by the pioneer of model risk management we introduced to you earlier (Derman, 2014[148]; Derman, 1996[149]; Derman, 2009[150]). As noted in the introduction, intuitive understanding of the above qualitative frameworks is most essential for appropriate use of the

[148] http://www.emanuelderman.com/writing/entry/speech-at-commencement-2014-to-berkeley-mse-grads
[149] http://www.emanuelderman.com/media/gs-model_risk.pdf
[150] http://www.emanuelderman.com/media/Fischer_Black_by_Derman_Bloomberg_2009.pdf

technical models that we discuss in some more depth in the next half of the dissertation. This should help minimize the model risk in applying the frameworks we discussed earlier and the technical models we discuss further.

Chapter 5.

Empirical VaR and Bayesian Modeling

> "VaR is just one of multiple measures of risk we use to assess overall risk in the organization."
>
> – CFO of Morgan Stanley in Financial Times interview, October 18, 2012

5.1 Empirical Study of VaR and Bayesian Inference

In the current chapter, we develop an empirical study of VaR and Bayesian statistical inference methodologies with specific guidance for containing model risks by applying multiple simple and advanced models for cross-checking the reliability of VaR models. In addition to managing model risk of the model, we also focus on managing model risk of the methodology by offering an analysis of the Bayesian statistical inference methodology. The Bayesian methodology is anticipated to overcome many of the known model risks of the classical statistical inference methodology, also known as the frequentist methodology and the null hypothesis significance testing methodology. In doing so we also clarify the ambiguity that sometimes practitioners encounter in distinguishing between the above two model risks, the first related to the model and the second related to the methodology.

In aftermath of the Financial Crisis, some risk management practitioners advocate wider adoption of Bayesian inference to *replace* Value-at-Risk (VaR) models for minimizing risk failures (Borison & Hamm, 2010). They claim reliance of Bayesian inference on *subjective judgment*, the *key limitation* of Bayesian methodology as underscored by statisticians (Kass & Raftery, 1995; Kruschke, 2011; Lynch, 2007), as the most significant *advantage* compared with VaR (Christoffersen, 2012). Despite its well-known limitations, *just like all other quantitative models* (Derman, 1996; Morini, 2011), VaR – (mostly) non-Bayesian *and* (increasingly) Bayesian – continues to be a key methodological foundation of risk management *and* regulation related risk modeling practices in global finance (Danielsson et al., 2014; Zangari, 1996). Bayesian inference modeling and VaR modeling frameworks are outlined to facilitate *model risk management*

(Derman, 1996; Morini, 2011; US Fed & OCC, 2011) for minimizing risk of *any* model – Bayesian, VaR, *or* Bayesian VaR. VaR frameworks are empirically applied for hedge fund risk modeling (Darbyshire & Hampton, 2012, 2014) of a multi-asset fund of funds portfolio of a large Wall Street investment bank. Multiple risk models and measures with transparent assumptions to cross-validate convergent findings across multiple levels of risk analysis are examined for empirical model risk management.

5.2 Distinguishing VaR Model vs. Bayesian Methodology

In aftermath of the Global Financial Crisis (GFC) of 2008-2009, critical analyses of financial risk management failures and the role of quantitative models such as Value-at-Risk (VaR) continue unabated (Danielsson et al., 2014; US Senate, 2013). *How to Manage Risk (After Risk Management Has Failed)* (Borison & Hamm, 2010) in *Sloan Management Review* is one such article addressed to risk management executives, decision-makers, and modelers. Its authors' *Bayesian vs. VaR* argument advocates for wider adoption of Bayesian inference to *replace* Value-at-Risk (VaR) models. Their central message is that choosing Bayesian *instead of* VaR models would minimize risk management failures *because of* the key role of 'subjective judgment' in the Bayesian methodology. They specifically assert that *if* Bayesian inference had been used in financial risk management practice *instead of* VaR, *then* risk management failures of GFC would have been minimal. Their basis for choosing Bayesian over VaR is *subjective judgment* which has its advantages, it is however a *key limitation* as recognized by Bayesian statisticians (Kruschke, 2011; Lynch, 2007). Further, since before GFC, *both* non-Bayesian and Bayesian VaR models have been used in financial risk management practice (Danielsson et al., 2014; Hull & White, 1998; Venkataraman, 1997; Zangari, 1996). Hence, the *Bayesian vs. VaR* dilemma needs to be resolved in order to minimize model *specification* and *estimation* errors in risk modeling (Boucher et al., 2014).

Current research contributes to congruent theme of improving financial risk management practices focused on model risk management. The key problem of model risk in any risk model such as VaR results from the fact that risk cannot be measured, but must be estimated using a statistical model (Boucher et al., 2014; Danielsson et al., 2014) . Hence, model risk occurs because a statistical model is used for risk estimation: *model use entails model risk* (Derman, 1996; Morini, 2011). Using range of different

plausible models which can be robustly discriminated between, the disagreement between their range of readings is a succinct measure of model risk (Danielsson et al., 2014). We apply this notion of model risk and model risk management methodology empirically in course of fund-of-funds portfolio construction and optimization for a top Wall Street investment bank which we discuss here.

VaR, originally popularized by JP Morgan, introduced quantitative rigor to fathom multi-dimensional complexity of risk with a simple and easy to implement measure (Hull & White, 1998; Jackson et al., 1998). It became the "de facto industry standard" for risk management practices among financial institutions as well as their regulators (Simons, 1996). Despite its well-known limitations (e.g. (Berkowitz et al., 2011; Berkowitz & O'Brien, 2002)) *just like all other quantitative models* (Derman, 1996; Morini, 2011), VaR – (mostly) non-Bayesian *and* (increasingly) Bayesian – remains the "methodological common root" of finance risk modeling underlying risk management *and* regulation (Danielsson et al., 2014). It is therefore important to advance beyond the *Bayesian vs. VaR* dilemma to focus on *model risk management* for *all* models – including *Bayesian*, *VaR*, *and*, *Bayesian VaR* – as that is what really matters (Derman, 1996; Morini, 2011; US Fed & OCC, 2011). Hence, the contributions of this paper are as follows.

First, we modulate the 'silver bullet' expectations about 'replacing' VaR with Bayesian models with realities of computational statistical modeling. Specifically, we inform the *Baysian vs. VaR* debate by outlining analytical frameworks of Bayesian inference (based on (Kruschke, 2011)) and VaR (based on (Darbyshire & Hampton, 2012, 2014)). Bayesian statistical inference methodology is anticipated to overcome known limitations of frequentist, also known as null hypothesis significance testing (NHST), statistical inference methodology. Modeling of 'Bayesian priors' – referred by some as 'subjective judgment' – remains a key challenge and limitation of Bayesian methodology. Feasibility as well as precision and accuracy of Bayesian modeling depend on computational statistical algorithms such as Markov Chain Monte Carlo (MCMC) which are themselves reliant upon exponential computing powers (Kruschke, 2011; Lynch, 2007). Such computing power accessibility is becoming available in recent years for mainstream use which explains recent re-emergence of applied interest in Bayesian inference.

Second, we resolve the *Bayesian vs. VaR* dilemma by providing analytical frameworks of Bayesian inference modeling and VaR modeling and advance beyond to empirical model risk management. Related discussion elucidates the central concern of model risk management which is relevant to *every* model – including *Bayesian*, *VaR*, *and*, *Bayesian VaR* – and necessary for minimizing modeling related risk management failures by minimizing model risk. Our current choice of empirical methodology and risk modeling framework is based upon the contextual domain and related current real world practice for risk modeling for multi-asset portfolio hedge funds. Our empirical focus on risk modeling and VaR frameworks for construction and optimization of fund-of-funds portfolio helps fathom the multi-dimensional complexity of financial risk modeling. We empirically examine multiple risk models and measures to cross-validate convergent findings across various levels of risk analysis as one such method of model risk management by applying VaR using classical methodology.

The outline of the chapter is as follows. In next section we discuss the analytical framework of the Bayesian statistical inference methodology as a viable contender for the classical frequentist methodologies of statistical inference. Next we discuss the quantitative risk modeling frameworks including VaR that are relevant to the contextual domain and related current real world practice for risk modeling of multi-asset portfolio hedge funds. Subsequent section presents the empirical context that applies the risk modeling frameworks including VaR in multi-asset portfolio hedge fund risk modeling for a half-trillion dollar fund-of-funds portfolio comprised of diverse equity, currency, commodity, alternative investments, and, hedge fund asset classes. Empirical findings in the next section illustrate the use of multiple risk measures and models at various levels of analysis to find convergence across the observations. The final section concludes our discussion outlining limitations and directions for future research.

5.3 Bayesian Modeling

To align expectations of practice with the challenges of computational statistical modeling inherent in Bayesian modeling, we outline the following analytical framework. The proposed framework aims to facilitate Bayesian estimation of parameter values, prediction of data values, and model comparison (based on

(Kruschke, 2011)). Our synthesis advances beyond the ambiguity of the *Bayesian vs. VaR* dilemma by clarifying central concerns that characterize Bayesian modeling. First, the role of 'subjective judgment' known more formally as 'Bayesian priors' is recognized as key challenge and limitation of Bayesian inference by its strongest critics and proponents alike (Kruschke, 2011; Lynch, 2007). Second, statistical computational complexity necessary for realizing *more sophisticated* Bayesian inference even when overcome at much expense may not necessarily result in more accurate or precise model. *Hence, regardless of models being used, VaR or Bayesian, model risk management is necessary for minimizing risk management failures.* Readers informed by this framework should be wiser in considering the prescriptive advice about 'replacing VaR models with Bayesian' (Borison & Hamm, 2010). Those new to Bayesian statistical inference probabilistic modeling may find Appendix 5-1 Bayesian Inference: Probability Background relevant.

5.3.1 Bayes' Rule

Bayes' rule is based on *conditional probability*, the probability of one event given that we know that the other event is true. *Conjoint probability* is the probability of two outcome events occurring together when considering a conjunction of the two events. Given conjoint events x and y, *total* probability of occurrence of a *specific value* of x *regardless of* the probability of *any value* for y is called *marginal probability* of x. M*arginal probability* of a *specific value of x* regardless of any value of y equals sum of all *conjoint probabilities* p(x, y) for the *specific value of x*.

Marginal probability of x = $p(x) = \sum_y \; p(x,y)$ when x and y are discrete,

$p(x) = \int_y \; dy \; p(x,y)$ when x and y are continuous.

Above process is called *marginalizing over y* or *integrating out the variable y* (Kruschke, 2011).

Probability of a specific outcome of y given known outcome of x could differ from its probability if outcome of x is not known. Conditional probability of event y is then limited *by* the conjoint probability of x and y for that specific value of y given the specific value of x (for all values of y). Conditional probability of y given x denoted as

$p(y|x)$ equals the conjoint probability of x and y divided by the sum of conjoint probabilities for the specific value of x over all values of y where $p(y,x) = p(x,y)$.

$p(y|\boldsymbol{x}) = \frac{p(y,x)}{\sum_{\boldsymbol{y}} p(y,x)} = \frac{p(y,x)}{p(\boldsymbol{x})}$, $p(x|y) = \frac{p(x,y)}{\sum_x p(x,y)} = \frac{p(x,y)}{p(y)}$ given discrete x and y,

$p(y|x) = \frac{p(y,x)}{\int_y dy\, p(y,x)} = \frac{p(y,x)}{p(x)}$, $p(x|y) = \frac{p(x,y)}{\int_x dx\ p(x,y)} = \frac{p(x,y)}{p(y)}$ given continuous x and y.

In summary, (Conditional Probability = Conjoint Probability / Marginal Probability), which can also be expressed as (Conjoint Probability = Conditional Probability * Marginal Probability). From above expressions, it also follows that: $p(x,y) = p(y|x)p(x) = p(x|y)\,p(y)$.

$p(x|y)$ should *not* be interpreted as denoting temporal order implying that y precedes x. It only implies limiting the calculations of probability to a particular subset of possible events: among all events with value y, $p(x|y)$ of them also have value x (Kruschke, 2011). When two events x and y have no influence on each other, they are called *independent events*.

When value of y has no influence on value of x, in general, $p(y|x) = p(y) = \frac{p(y,x)}{p(x)}$.

Likewise,

when value of x has no influence on value of y, in general, $p(x|y) = p(x) = \frac{p(x,y)}{p(y)}$.

Hence for two independent events x and y, conjoint probability $p(x,y)$ equals the product of marginal probabilities $p(x)$ *and* $p(y)$. Symmetrically, when $p(x,y) = p(x)\,p(y)$ for all values of x and y, then $p(x|y) = p(x)$ and $p(y|x) = p(y)$. Both expressions specify *independence of attributes*. The relationship between $p(x|y)$ and $p(y|x)$ called ***Bayes' Rule*** is derived as follows.

From above expressions, $p(y|x)p(x) = p(y,x)$, and, $p(x|y)p(y) = p(x,y)$

=> $p(y|x)p(x) = p(x|y)p(y)$

=> $\boldsymbol{p(y|x)} = \frac{\boldsymbol{p(x|y)p(y)}}{\boldsymbol{p(x)}}$ **(1)** => $\boldsymbol{p(y|x)} = \frac{\boldsymbol{p(x|y)p(y)}}{\sum_{\boldsymbol{y}} \boldsymbol{p(x,y)}} \Leftrightarrow \frac{p(x|y)p(y)}{\int_y dy\ p(x,y)}$

As noted earlier, marginal probability of x is $p(x) = \sum_y p(x,y)$ when x and y are discrete, and, $p(x) = \int_y dy\ p(x,y)$ when x and y are continuous. As $\boldsymbol{p(x,y)= p(x|y)p(y)}$, it follows:

$$\Rightarrow \boldsymbol{p(y|x)} = \frac{\boldsymbol{p(x \mid y)p(y)}}{\sum_{\boldsymbol{y}} \boldsymbol{p(x \mid y)p(y)}} \quad \textbf{(2)}$$

Above two expressions (1) and (2) called the Bayes' Rule are at the core of Bayesian Inference.

Bayes' Rule holds when x and y are independent as well as when x and y are not independent.

5.3.2 Key Objectives of Bayesian Inference

Pre-existing beliefs about different possible values of a parameter before taking into account some particular set of observations are called *prior beliefs* or simply *priors*. The modified beliefs resulting from taking the particular set of data or observations into account are called *posterior beliefs*. *Even though the terms prior and posterior may seem to suggest historical or temporal ordering, in fact it is not the case* (Kruschke, 2011). Prior simply means the probability distribution of beliefs held *without including* a particular set of data. In contrast, posterior simply means the probability distribution of beliefs held *after including*, i.e., after taking into consideration that particular set of data. Bayesian inference transforms prior beliefs into posterior beliefs. Statistical inference based on data observations typically fulfills one of the following three goals: *estimation of parameter values*, *prediction of data values*, and *model comparison*.

Estimation of parameter values is used to determine the probability distribution of beliefs in different possible values of a parameter. For a random process, underlying true parameter is not known and hence related beliefs are uncertain; therefore posterior beliefs about that parameter are an estimate. Data can result in modification of beliefs given that specific probabilities assigned to different values of the parameter may change. Degree of belief in some possible values of a parameter may increase resulting in corresponding decrease in other possible values. Hence, such reassignment of probabilities across different possible parameter values is called estimation of parameter values as it results in shifting of beliefs across those values (Kruschke, 2011).

Prediction of data values means inferring values of data other than that we have already considered based upon current beliefs. Again, prediction means inferring value of data that is not included based on data that has already been included *regardless of the actual temporal relationship* between the two (Kruschke, 2011). Bayesian prediction is based upon taking weighted average of predictions based on respective beliefs, specifically taking a summated weighted average of each possible value of unknown data and the respective (believed) probability of occurrence of the specific value. *Model selection*, also known as *model comparison*, is based upon choosing the model which can generate the observed data with greater likelihood. Bayesian inference can help determine exactly how much more to believe the selected model than those not selected and intrinsically adjusts for model complexity. Complex models, being more flexible, will fit the data better as well as fit random noise better than simpler models (Kruschke, 2011).

5.3.3 Bayes' Rule Applied to Models and Data

In context of application to models and data, a key application of Bayes' Rule is in assessment of conditional probabilities of observed data values and related model parameter values. Its crucial application is in determining the probability of a model when given a set of data. The model itself provides the probability of the data, given specific parameter values and the model structure. Specifically, Bayes' Rule helps to get from the *probability of the data, given the model* to the *probability of the model, given the data*.

Having observed some data, Bayes' Rule is then applied to determine strength of our beliefs across competing parameter values in a model, and, also to determine strength of our beliefs across competing models. Beliefs held prior to the observation of data are called prior beliefs or *priors*. Observed data may modify those priors and result in posterior beliefs or *posteriors*. Again, the notion of "historical data" (Borison & Hamm, 2010) needs to be interpreted carefully especially in the context of Bayesian analysis. *Even though the terms 'prior' and 'posterior' may seem to suggest historical or temporal ordering, in fact it is not the case* (Kruschke, 2011).

Prior simply means the probability distribution of beliefs held *without including* a particular set of data. In contrast, posterior simply means the probability distribution of beliefs held *after including*, i.e., after taking into consideration that particular set of data. Bayesian inference transforms prior beliefs into posterior beliefs thus helping us make

inference from data to uncertain beliefs. Uncertainty in beliefs results from differing likelihood of diverse possibilities. By helping precisely determine likelihood of diverse possibilities, statistical inference models help precisely define such uncertainty with precise numerical bounds. This is particularly useful with increasing variance in data and increasing uncertainty in beliefs.

Data denotes the observable sample statistic observed for a process to estimate corresponding parameter of the process which cannot be directly observed. The first set of assumptions about the process that generates probabilistic observable data outcomes for the unobservable parameter is the *model of observable events*. The second set of assumptions about our beliefs regarding the likelihood of different levels of the specific process parameter is the *model of our beliefs*. Bayes' rule can be visualized spatially (Kruschke, 2011) in terms of events x listed in i rows R_i and events y listed in intersecting j columns C_j wherein any specific intersection of the two is the conjoint probability $p(R_i, C_j) = p(R_i|C_j)\ p(C_j) = p(C_j|R_i)\ p(R_i)$. Then, normalization of probabilities in row R_i by dividing conjoint probabilities by $p(R_i)$ yields the following.

$$p(C_j \mid R_i) = \frac{p(C_j, R_i)}{p(R_i)} = \frac{p(R_i \mid C_j)p(C_j)}{p(R_i)} \qquad \textbf{(1a)}$$

$$p(R_i|C_j) = \frac{p(R_i, C_j)}{p(C_j)} = \frac{p(C_j \mid R_i)\ p(R_i)}{p(C_j)} = \frac{p(C_j \mid R_i)\ p(R_i)}{\sum_i p(C_j \mid R_i)\ p(R_i)} \qquad \textbf{(2a)}$$

Applying Bayes' Rule in spatial representation to data values D_i in rows and intersecting column parameter values θ_i, we get the following expressions about the Bayesian inference for *model given data*. The following expressions are based upon the earlier observation that conjoint probability equals the product of conditional probability and marginal probability. The first expression is that of the posterior for which we need to avoid the computation of large complex integral in the denominator for ease of computation.

$$\boldsymbol{p(\theta_j \mid D_i)} = \frac{p(\theta_j, D_i)}{p(D_i)} = \frac{\boldsymbol{p(D_i \mid \theta_j)\, p(\theta_j)}}{\boldsymbol{p(D_i)}} \qquad \textbf{(1 b)}$$

$$p(D_i \mid \theta_j) = \frac{p(D_i, \theta_j)}{p(\theta_j)} = \frac{p(\theta_j \mid D_i)\, p(D_i)}{p(\theta_j)} = \frac{p(\theta_j \mid D_i)\, p(D_i)}{\sum_i p(\theta_j \mid D_i)\, p(D_i)} \qquad \textbf{(2 b)}$$

Bayes Rule helps us determine how strongly we believe in the model given the data. It helps us get from the probability of the data given the model $p(D_i \mid \theta_j)$ to probability of the

model given the data $p(\theta_j \mid D_i)$ (Kruschke 2011). Writing expression (1b) as follows helps clarify the Bayesian analysis notation.

$p(\theta_j \mid D_i) = \frac{p(D_i \mid \theta_j)\, p(\theta_j)}{p(D_i)}$ i.e. $Posterior = \frac{Likelihood * Prior}{Evidence}$ where

Posterior $p(\theta_j|D_i)$ denotes strength of our belief in parameter θ_j when data D_i is considered.

Prior $p(\theta_j)$ denotes strength of our belief in parameter θ_j without considering data D_i.

Likelihood $p(D_i|\theta_j)$ denotes probability that data D_i could be generated by model with parameter θ_j.

Evidence $p(D_i)$ denotes probability of the data according to the model.

For Likelihood $p(D_i|\theta_j)$, θ that maximizes its value is called the Maximum Likelihood Estimate of θ. Evidence is used here as in machine learning and equals the numerical sum across all possible parameter values weighted by respective strength of the belief in those parameter values. Hence,

$$p(D_i) = \sum_\theta p(D_i, \theta_j) = \int_\theta d\theta\ p(D_i|\theta_j)\ p(\theta_j) \quad .$$

Because parameter value θ_i makes sense only in context of the respective model, it helps to make the specific model explicit.

$p(\theta_j \mid D_i, M) = \frac{p(D_i \mid \theta_j,\ M)\, p(\theta_j \mid M)}{p(D_i \mid M)}$. Correspondingly $p(D_i \mid M) =$

$\int_\theta d\theta\ p(D_i \mid \theta_j,\ M)\ p(\theta_j \mid M)$.

Above assessment of the strength of (posterior) beliefs given data for a specific model can be extended to the case of comparison of strength of belief in two different models M_1 and M_2 given observed data.

$p(M_1 \mid D_i) = p(M_1, D_i) / p(D_i) = p(D_i|M_1)\ p(M_1) / p(D_i)$ and

$p(M_2 \mid D_i) = p(M_2, D_i) / p(D_i) = p(D_i|M_2)\ p(M_2) / p(D_i)$.

Equating the ratios of LHS and RHS above, we get,

$\frac{p(M_1 \mid D_i)}{p(M_2 \mid D_i)} = \frac{p(D_i|M_1)\, p(M_1)}{p(D_i|M_2)\; p(M_2)}$ where the ratio of evidence terms $\frac{p(D_i|M_1)}{p(D_i|M_2)}$ is called the ***Bayes' Factor***.

Hence, for comparison of $M_1$and M_2, ratio of posterior beliefs equals Bayes' Factor times the ratio of priors.

5.4 What Makes Bayesian Inference Challenging

Beyond estimation of model parameters, Bayesian methodology is far more flexible in evaluating model fit and comparing models, producing parameters samples not directly estimated within the model, handling missing data, while capturing greater uncertainty than the classical approach in prediction and forecasting (Lynch, 2007). *It is however recommended to think of sophistication and complexity of models as a two-edged sword. Simple models are always preferred if they help understanding the assumptions and limits of their scope which helps in managing model risk. Complex and sophisticated models may increase the model risk if they obfuscate such understanding and clarity* (Kruschke, 2011). Bayesian modeling can help to the extent given that it automatically accounts for model complexity when assessing the strength of belief in any given model. Let's consider the case wherein for estimation of parameter values a simple model with a few parameter values is compared with one containing many parameter values.

Given that the same probability is spread out over a larger number of values, the simpler model is favored as it shows greater posterior values for the lesser parameter values. However, the complex model may be favored when the observed data do not fit the simpler model. In any case, the model comparison simply tells about the *relative evidence* for each model and makes sense in the context of *relative comparison*. *Regardless of which model seems relatively superior, it may still not be a good model of the data, but the least worse of the models that are compared* (Kruschke, 2011).

The evidence $p(D_i)$ and $p(D_i \mid M)$ involve a complex integral over a possibly high dimension parameter space $\theta_j \in \Theta$. Such complex integration over high dimension parameter space is the principal inferential operation in Bayesian analysis as compared to optimization in classical inference. *Evaluation of such complex integrals over high dimensional parameter space poses major challenge for actual use of Bayesian analysis. All three*

goals of Bayesian inference depend upon the solution of the evidence term which is in the denominator of Bayes' formula (Kruschke, 2011).

Few methods have been typically used to overcome the problems such as those noted above that severely constrain the application of Bayesian analysis. The first method involves using prior and posterior distributions of the same form, i.e., satisfying the condition of *conjugacy*. In other words, the functional forms of distributions $p(D_i|\theta_j)$ and $p(\theta_j)$ combine so that the posterior distribution has same form as prior distribution (e.g. both are normal distributions), then $p(\theta_j)$ is called the *conjugate prior* for $p(D_i|\theta_j)$. Another pure analytical method involves approximation of the actual functions with easier to compute alternatives while demonstrating their reasonableness. Third method involves numerical approximation of the difficult-to-compute integral by approximating the continuous function θ_j as a sum over a fine grid of discrete θ_j values.

Such grid approximation is based upon approximating the integral by summation of discrete intervals across the grid. Instead of treating θ_j as a continuous function with associated *probability densities*, it uses discrete finite values of θ_j and aggregates respective *probability masses* as shown below.

$$p(D_i \mid M) = \int_\theta d\theta\, p(D_i \mid \theta_j,\ M)\ p(\theta_j \mid M) \quad \approx \quad \sum_\theta p(D_i \mid \theta_j,\ M)\, p(\theta_j \mid M)$$

The above grid approximation method is limited to cases where the number of parameters is relatively very small. *For instance, considering a model which may have say, eight parameters, each having a thousand values, the eight-dimensional parameter space contains (1E3)E8 i.e. 1E24 combinations of parameter values which is a computationally complex problem to solve*. Markov Chain Monte Carlo (MCMC) numerical techniques (Gelfand & Smith, 1990; Malhotra, 2014) that work by simulating a discrete time Markov chain on high dimension parameter space $\theta_j \in \Theta$ by using statistical computing algorithms provide a relatively recent breakthrough for making Bayesian analysis feasible for solving high dimensionality problems. MCMC use Monte Carlo simulations to approximate the true posterior probability density $p(\theta_j|D_i)$ by constructing Markov chains whose steady state distribution matches $p(\theta_j|D_i)$. The samples returned by the MCMC methods of simulation based inference can be assumed as random draws from $p(\theta_j|D_i)$. *Only with availability of MCMC statistical computing algorithms such as Metropolis Hastings algorithm and Gibbs Sampling algorithm and faster inexpensive computing power has Bayesian inference*

become feasible lately for mainstream use for doing high dimension parameter space analyses (Gelfand & Smith, 1990; Malhotra, 2014).

5.5 'Subjective Judgment' Limitation of Bayesian Inference

A key limitation of Bayesian inference is often attributed to the choice of the appropriate and reasonable prior distribution. For all parameters, proper priors have to be used in order to avoid possible non-integrability of the posterior parameter distribution which would make the Bayesian model selection rather questionable (Kass & Raftery, 1995). Choice of suitable priors is generally a 'contentious issue' (Miazhynskaia et al., 2003): "One wants the priors to reflect one's believes about parameter values and at the same time to use non-informative (flat) priors that does not favor particular values of the parameter over other values." To avoid the "subjectivity" criticism of Bayesian approach as in choice of 'subjective' priors when contrasted from the classical approach, many Bayesian analyses have used uniform, reference, or otherwise 'non-informative' priors (Lynch, 2007). This has lessened the use of priors as a distinguishing characteristic of Bayesian analyses even though most Bayesian analyses specifically attempt to minimize the effect of the prior such as by excluding the 'burn in' period. It may be however argued that explicit priors should be used because prior beliefs influence rational inference from data because new data modifies beliefs from what they were prior to the new data.

However, it must be recognized that prior beliefs are ***not*** *capricious and idiosyncratic and unknowable* but based on publicly agreed facts and theories and admissible by a skeptical scientific audience (Kruschke, 2011). Hence, it must be emphasized that Bayesian analysis doesn't *ipso facto* imply reliance upon *ad hoc and subjective personal judgment* but is rather based upon use of *priors that are agreeable to a skeptical audience* (Kruschke, 2011). In case of disagreement about two sets of priors, either each can be used to conduct separate analysis and then robustness of posterior assessed w.r.t. changes in prior or they can be mixed into joint prior with posterior reflecting the uncertainty in the prior.

The above synthesis of a Bayesian analytical modeling framework is intended to clarify prescriptive advice about 'replacing VaR with Bayesian models' for its actual execution in applied practice. It is important to recognize three key points from the above discussion. First, Bayesian and VaR models cannot and should not be treated as

mutually exclusive alternatives in risk modeling for minimizing risk management failures given existence of non-Bayesian VaR, Bayesian VaR, as well as risk models other than VaR. Second, Bayesian approach, even though more sophisticated statistically, comes at much computational expense and does not necessarily ensure more precise or accurate model. Third, but most importantly, regardless of using Bayesian approach with *or* without VaR, model risk management is necessary in all cases for mitigating risk management failures.

5.6 Value at Risk (VaR) Modeling

The following discussion focus is on VaR and ES models most widely used in hedge fund risk modeling practice (Darbyshire & Hampton, 2012, 2014; J.P. Morgan, 2008). These risk models are used for empirical analysis as described in the next section. Other sophisticated risk management models which share the "methodological common root" of VaR (Danielsson et al., 2014) are reviewed in the concluding discussion of the current section.

5.6.1 Key Concept of Value-at-Risk

For a given portfolio of assets, Value at Risk (VaR) quantifies how much at most can be lost with a given probability over a specific time horizon. Value-at-Risk denotes the worst expected loss over a given time horizon at a given confidence level under normal market conditions (J.P. Morgan, 2008). VaR provides a single number summarizing the firm's exposure to market risk and the likelihood of an unfavorable move in the portfolio's positions. It also provides a predictive tool to prevent portfolio managers from exceeding risk tolerances defined in the portfolio policies. It can be measured at the portfolio, sector, asset class, and security levels. VaR is just an *estimate* and not a uniquely defined value (J.P. Morgan, 2008). Unlike, Expected Shortfall discussed later, VaR does not provide any information on losses that exceed its value, i.e., VaR is *not* the 'worst case scenario'(J.P. Morgan, 2008).

95% VaR level was defined by the popular Riskmetrics methodology of JP Morgan. 99% VaR level had been the Basel committee's market risk regulatory criterion until 2013 when they proposed replacing it with 97.5% ES in Basel III which is to be implemented sometime until 2019 as of the time of writing. In case of a hedge fund (or a

fund of funds), assumptions about hedge fund portfolio returns following a normal distribution and being affected by linear market forces are called the normality and linearity assumptions. The normal distribution of hedge fund returns can be described by just two parameters, mean μ and standard deviation σ.

Assuming normal distribution ($X \sim N(\mu, \sigma^2) = N(0, 1)$) for monthly returns and a c% confidence level, where $c = 100(1 - \alpha)$, c% VaR implies that the worst estimated portfolio loss for the next month is no more than $z_\alpha\sigma$, i.e. z_α standard deviations below the mean μ. For c% = 95% and corresponding critical value $z_\alpha = -1.645$, $VaR_c = VaR_{1-\alpha}$ implies 95% probability of portfolio loss not exceeding 1.645σ, i.e., 5% probability of portfolio loss worse than 1.645σ. Similarly, for c% = 99% and corresponding critical value $z_\alpha = -2.2326$, $VaR_c = VaR_{1-\alpha}$ implies 99% probability of portfolio loss not exceeding 2.2326σ, i.e. 1% probability of portfolio loss worse than 2.2326σ. VaR *does not* specify the *amount of loss* expected in excess of VaR for the respective time period, but only specifies that there is only α% probability (i.e., event occurrences out of 100) resulting in loss of at least $z_\alpha\sigma$.

5.6.2 Traditional methods for estimating VaR

Hedge fund industry traditional methods for estimation of VaR for funds-of-funds risk management practices include the following (Darbyshire & Hampton, 2012, 2014; J.P. Morgan, 2008): i. Historical Simulation, ii. Parametric Method, and, iii. Monte Carlo Simulation.

While Historical Simulation is based upon actual data, Parametric Method uses the data only for generating the necessary parameters for specifying the distribution, and Monte Carlo generates data using simulation. Each of the three methods is different in terms of how it defines distribution of losses and has its advantages and limitations as discussed below.

i) Historical Simulation based VaR

Historical simulation relies upon the past data of returns based upon the assumption that historic monthly returns are an accurate representation of future returns with no specific assumptions about the return distribution. The data set of historical monthly % returns needs to be adequately large to calculate for each historical

% return a corresponding simulated P&L value by multiplying the % return with the index AuM. The simulated P&L values are then sorted in order of decreasing losses and increasing profits so that the highest loss is on the top and highest profit on the bottom. For each simulated P&L value, an associated cumulative weight is computed based upon total number of data points starting from the highest profit on the bottom for which the cumulative weight is simply the inverse of the number of data points. That value is incremented for each subsequent lower value of profit (or higher value of loss) with lowest profit (or highest loss) accumulating a final cumulative weight of 100%.

The P&L value corresponding to c% confidence level value of the cumulative weights, where c% could be based upon interpolation between the adjacent P&L cumulative weights, is the estimated VaR for the specific confidence interval represented as VaR_c. Its key feature is that it is independent of any assumptions about the underlying statistical distribution or related parameters and is thus non-parametric in nature. Its advantages are the following: it is easy to calculate, easy to understand, does not assume normal distribution, not as data intensive as Monte Carlo, and can be applied to various time periods (J.P. Morgan, 2008). However, historical returns may not be an accurate representation of the future returns. Hence, its disadvantage lie in its assumption that historical correlations will repeat (J.P. Morgan, 2008).

ii) Parametric Method based VaR

For a portfolio of N risky assets, the portfolio variance is given by the expression: $\sigma_p^2 = W^T \sum W$ where W^T is the matrix transpose of W, the vector of individual asset class weights w_i, and, $\sum$, the variance-covariance matrix of the individual assets w_1 thru w_n:

$$\sum = \begin{pmatrix} \sigma_{11} & \sigma_{12} & \cdots & \sigma_{1n} \\ \sigma_{21} & \sigma_{22} & \vdots & \sigma_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{n1} & \sigma_{n2} & \vdots & \sigma_{nn} \end{pmatrix}$$

For portfolio standard deviation $\sigma_p = (W^T \sum W)^{1/2}$, estimated VaR is computed as follows:

$VaR_c = VaR_{1-\alpha} = Pz_\alpha \sigma_p$ where P is the market value of the portfolio. The vector of individual asset weights w_i is derived through the solution of the mean-variance optimization (Markowitz, 1952) for achieving a desired level of portfolio expected return for corresponding level of portfolio risk. The portfolio of weighted assets optimized to yield *minimum variance* (i.e. risk) for a higher expected portfolio return

needs to be rebalanced through computation of new weights as market conditions and risk conditions evolve while considering transaction costs involved in such rebalancing. The mean-variance optimization problem can be stated in terms of a target expected portfolio return r* as: min σ_p^2 = min $W^T \sum W$ s.t. $W^T R = r^*$, $\sum_i^N w_i = 1$ where R is the vector of mean returns of assets in a fully invested portfolio with respective returns elements corresponding to weights in the vector W of individual asset weights w_i. If short selling is not allowed, then additional constraint of $w_i \geq 0$ can be added.

The portfolio variance listed above follows from the following expressions:

$$\sigma_p^2 = \sum_{i=1}^{N} \sum_{j=1}^{N} w_i \, w_j \sigma_i \sigma_j \rho_{ij} \quad \Rightarrow \quad \sigma_p^2 = \sum_{i=1}^{N} \sum_{j=1}^{N} w_i \, w_j \sigma_{ij} \quad \Rightarrow \quad \sigma_p^2 = W^T \sum W$$

Parametric approach is mathematically simple and intuitive to understand and implement using matrices. Hence, its advantages include the following: it is easy to calculate, easy to understand, has minimal data requirements, and can be applied to various time periods (J.P. Morgan, 2008). Parametric methods suffer from the limitations inherent in the *normality* and *linearity* assumptions about portfolio returns being normally distributed and linear relationships assumed between risk variables. They rely upon strong assumptions about statistical parametric return distributions in terms of mean μ and standard deviation σ such as of the independent and identically distributed (iid) random variables of N (0, 1) normal distribution. Such assumptions of normality are clearly oversimplifications particularly for portfolios of hedge funds and funds of funds for which extensions of traditional VaR methods are discussed later.

Furthermore, linear relationships of parametric methods are oversimplifications for portfolios employing sophisticated trading strategies based upon derivatives such as options that have non-linear risk-return characteristics. Therefore, such estimates are not as accurate when asset portfolio consists of non-linear instruments such as in case of specific hedge fund strategies. Hence, disadvantages of parametric VaR include assumption of normality, difficulty of estimating correlations in complex portfolios, and lesser accuracy for non-linear securities such as MBS (J.P. Morgan, 2008).

iii) Monte Carlo Simulation based VaR

Monte Carlo (MC) methods based VaR is based on the premise that the portfolio returns can be characterized by a *stochastic* model typically based upon a *non-deterministic* component. Such a component introduces some degree of uncertainty or

randomness in the data generating process (DGP) by use of random number generators. Simulation based upon a specific mathematical stochastic model over thousands or millions of trials generate corresponding time-based *paths* that series of portfolio returns are probabilistically likely to follow over a certain time period. Each of those trials results in a terminal value for the portfolio return (or P&L) at the end of the simulated time period. Just as in the case of Historical Simulation discussed earlier, VaR_c at a specific confidence interval c is estimated from the simulated P&L distribution by sorting the P&L values and computing P&L value corresponding to c% confidence level value by interpolation between adjacent P&L cumulative weights as needed.

Consistent with prior discussion on Bayesian inference, the stochastic model is driven by the μ and σ of the asset returns distribution based upon historical data *as well as* inclusion of a degree of subjective knowledge based upon market experience in the model as necessary. MC methods are robust and probabilistically strong and are excellent for building and understanding non-linearity associated with use of derivatives in multi-asset portfolios. Such subjective knowledge based MC models are "extensively used throughout the financial markets" and are a "much used technique for estimating VaR within the hedge fund community" (Darbyshire & Hampton, 2012, 2014). Hence, incorporation of 'subjective judgments' into the model and flexibility of choosing the appropriate stochastic DGP are the strong points of MC methods based VaR models. MC methods being mathematically complex and challenging are most demanding of computational resources.

When dealing with intrinsic complexities of specific multi-asset portfolio strategy with derivatives, they can become mathematically challenging and computationally expensive to implement. Markov Chain Monte Carlo (MCMC) algorithms (Gelfand & Smith, 1990; Malhotra, 2014) are often used in such cases for portfolio modeling especially in case of Bayesian inference models. Advantages of Monte Carlo VaR thus include their ability to use any return distribution or asset correlation and greatest suitability for non-linear assets while disadvantages include requirements of too many assumptions and extensive computing power and time (J.P. Morgan, 2008).

In addition to the traditional VaR methods, portfolio managers also run *stress tests* for testing sensitivity of the models to magnified values of parameters and risk factors to allow for extreme or adverse events that could result in catastrophic losses. From portfolio optimization perspective, stress testing also includes sensitivity analysis

that shocks one or several risk factors by a relative small change such as +/- 5 basis points and revalues the portfolio to ascertain the sensitivity of the portfolio to the small change in one or several risk factors (J.P. Morgan, 2008). Similarly, they may also run *scenario analyses* using historical data and associated parameters to test for comparability with high turbulence market events such as the market crash of 1987 and the financial crisis of 2008.

iv) Modified VaR

The normality assumption is the greatest drawback of the above traditional VaR approaches despite use of stress testing and scenario analysis practices. Particularly, hedge fund and fund-of-funds returns are characterized by negative skew and excess positive kurtosis resulting in asymmetric return distributions with fat tails. Hence, extensions of traditional VaR methods have been proposed to address better estimation and specification of market risk for such portfolios. Contemporary extensions of VaR models are based upon explicit consideration of the standardized third (skew) and fourth (kurtosis) central moments of the returns distribution. In addition, they are also focused on the left tails of the returns distribution wherein most of the extreme losses are concentrated. The concept of Modified VaR is based upon the Modified Sharpe Ratio (MSR) wherein the denominator of Sharpe ratio is modified to account for the higher (third and fourth) moments of the returns distribution.

Sharpe ratio which is a measure of risk-free rate per unit of risk, risk being measured in terms of portfolio's standard deviation, is modified by using the Cornish-Fisher expansion (Cornish & Fisher, 1937) to get the MSR. Cornish-Fisher expansion transformation helps transform a standard Gaussian random variable $z_\propto$ into a non-Gaussian z_{cf} random variable as follows:

$$z_\propto \approx N(0,1) \qquad E(z_\propto) = 0 \qquad E(z_\propto^2) = 1 \qquad E(z_\propto^3) = 0 \qquad E(z_\propto^4) = 3$$

$$z_{cf} \approx z_\propto + (z_\propto^2 - 1)\frac{S}{6} + (z_\propto^3 - 3z_\propto)\frac{K}{24} - (2z_\propto^3 - 5z_\propto)\frac{S^2}{36}$$

where sample skew is given by: $S = \frac{n}{(n-1)(n-2)} \sum_{i=1}^{n} \left(\frac{x_i - \bar{x}}{s}\right)^3$

and sample excess kurtosis by: $K = \left[\frac{n(n+1)}{(n-1)(n-2)(n-3)} \sum_{i=1}^{n} \left(\frac{x_i - \bar{x}}{s}\right)^4\right] - \frac{3(n-1)^2}{(n-2)(n-3)}$.

The portfolio Modified VaR is then given by $MVaR_c = MVaR_{1-\alpha} = \mu - z_{cf}\,\sigma_p$

and Modified Sharpe Ratio is given by $\text{MSR} = \frac{R_P - R_F}{\text{MVaR}_{1-\alpha}}$

where R_P is the annualized return and R_F is the annualized risk-free rate computed using T-bill as a proxy.

The above expression for Modified VaR $\text{MVaR}_{1-\alpha}$ represents a more accurate estimate of VaR at a c% confidence level, where c = 100(1 – α), μ = mean of the portfolio returns, and z_α = critical value from the normal distribution for the specific confidence interval.

A limitation of the Modified VaR relates to higher confidence intervals (e.g. 99%) leading further into the left tail of the distribution and to inaccurate results. Another limitation is unreliability of MVaR in case of highly skewed and fat-tailed returns or P&L distributions.

5.7 Expected Shortfall (Expected Tail Risk, T-VaR)

In addition to the non-normality and non-linearity related limitations of traditional VaR methodologies, VaR has additional limitation of not being a *coherent risk measure* (Artzner et al., 1999). A risk measure R (such as VaR) that is a *coherent risk measure* should satisfy *all* four following axioms for a random loss L.

- Subadditivity (diversification) $R\ (L_1 + L_2) \leq\ R\ (L_1)\ +\ R(L_2)$
    - Risk of portfolio of two assets should not be greater than the sum of risk of individual assets
- Positive homogeneity (scaling) $R\ (\lambda L) = \lambda R(L)$, for every $\lambda\ > 0$
    - Increasing size of portfolio by λ-times should increase risk by a multiple of $\lambda\ ceteris\ paribus$
- Monotonicity $R\ (L_1) < R(L_2)$ if $L_1 < L_2$
    - Higher risk is associated with higher loss and lesser risk with lesser loss, i.e., more +ve returns
- Transition property $R\ (L + a) < R\ (L) - a$
    - Adding cash or risk-free asset of value a should reduce risk by an equivalent amount a.

As VaR doesn't satisfy the first axiom of subadditivity, an alternative measure called Expected Shortfall was developed (Tasche, 2002). Expected Shortfall (ES) also

known as Expected Tail Risk, Tail VaR (T-VaR for short), and, Conditional VaR is the average of all the losses greater than (conditionally to going beyond VaR) VaR specified with the same confidence interval that VaR was estimated (J.P. Morgan, 2008). For example, if VaR is calculated at a 99% confidence level, ES averages the worst 1% losses. As the conditional expectation of loss conditional on its value exceeding VaR, ES is a coherent measure as it is subadditive unlike VaR. ES represents expected value (average) of the severity of losses beyond the VaR confidence threshold as these losses are important to regulators. A risk manager strictly relying upon VaR as the only risk measure may avoid losses within the confidence level while increasing the losses beyond the VaR level which are more severe and thus require the regulators or deposit insurers to backstop such losses. In addition, ES mitigates the disadvantages of VaR that result from the choice of a single confidence level and its impact on risk management decisions particularly as they relate to extreme events.

Mathematically, ES as the conditional expectation of loss conditional on its value exceeding VaR_c is described as: $ES_{1-\alpha} = E[L|L > VaR_{1-\alpha}]$ where $ES_{1-\alpha}$ is estimated ES at confidence level c for a loss distribution continuous in α. ES is the *average* loss in the distribution area beyond VaR in the extreme left-tail i.e. average of all VaRs from level α up to 1.

$$ES_\alpha \equiv \frac{1}{1-\alpha}\int_\alpha^1 VaR_c(L)dc$$

where, L = a random loss with distribution function F_L, $\propto \epsilon (0,1)$ = confidence level close to 1.

It is important to recognize that ES gives only 'Expected' value that is the average value of risk in the left tail if the related VaR confidence level is exceeded. Hence, even though ES is a more conservative estimate than VaR, it is only the average or 'expected' loss in the left tail beyond VaR α. The actual loss (and related risk), however, could be more extreme than the average of the left tail risk. Hence, ES does not provide any information about the severity of loss by which VaR is exceeded. For more precise tail risk analysis of extreme events, Extreme Value Theory techniques (Embrechts et al., 1999; Gumbel, 2004; Pickands III, 1975) such as Block Maxima and Peaks over Threshold represent more sophisticated techniques but (just as in case of Bayesian inference) computationally and mathematically demanding alternatives which

are often constrained by lack of adequate representative data for extreme events in case of hedge fund distributions thus leading to broad confidence intervals and weak significance estimates.

5.8 Bayesian VaRs beyond 'Bayesian vs. VaR' Dichotomy

Expected Shortfall overcomes classical problems of risk modeling associated with VaR while offering parsimony and transparency for lesser complexity and computational requirements. However, it must be reiterated that VaR and Bayesian modeling cannot be considered a dichotomy. Just like other statistical inference techniques available in both frequentist null hypothesis significance testing (NHST) and Bayesian statistical inference methodologies, VaR modeling continues to be used with both methodologies. For instance, the quasi-Bayesian and Bayesian versions of VaR have been referenced and applied in Banking & Finance practice since the years preceding the Global Financial Crisis (Hull & White, 1998; Venkataraman, 1997; Zangari, 1996). That being said, it is important to observe that both statistical inference paradigms, NHST *as well as* Bayesian, are moving away from point-estimates toward range based-estimates.

In Bayesian VaR approaches, point estimates for parameters are substituted by distributions of parameters reflecting prior knowledge about the various parameter values with posterior distribution of parameters used for further analysis (Aussenegg & Miazhynskaia, 2006; Hoogerheide & van Dijk, 2008). Hence, there are both non-parametric modeling methods such as historical simulation (discussed earlier), and adjusted historical simulation and parametric modeling methods such as Bayesian, quasi-maximum likelihood (QML) and bootstrap methods for various types of GARCH modeling and analysis. Increasing interest in sophisticated Bayesian VaR models and extensions is evident in research literatures (Aussenegg & Miazhynskaia, 2006; Casarin et al., 2013; Danielsson et al., 2014; Hoogerheide & van Dijk, 2008; Meucci, 2009; Miazhynskaia et al., 2003; Osiewalski & Pajor, 2010).

5.9 Data and Empirical Research Design

Empirical focus was on quantitative risk modeling of a half-trillion dollar fund-of-funds asset portfolio for a top Wall Street investment bank. Monthly returns over a 21-year period from January 1991 until December 2011 for 12 different asset classes

comprising the portfolio were modeled in addition to market benchmark S&P 500 index (SPY). The specific (symbol:) asset classes included: (i) RIY: Developed Large Equity (proxy: Russell Developed Large Cap Index), (ii) RTY: Developed Small Equity (proxy: Russell Developed Small Cap Index), (iii) MXEF: Emerging Market Equity (proxy: MSCI Emerging Markets Index), (iv) LPX50TR: Listed Private Equity (proxy: LPX50 Listed Private Equity Index), (v) DJUBS: Various Commodities (proxy: DJ-UBS Commodity Index), (vi) USTW$: Major Currencies (proxy: Trade Weighted US Dollar Index: Major Currencies), (vii) HFRIEDI: Event Driven Hedge Fund (proxy: HFRI Event - Driven Index), (viii) HFRIEHI: Equity Hedge Fund (proxy: HFRI Equity Hedge (Total) Index), (ix) HFRIMAI: Merger Arbitrage Hedge Fund (proxy: HFRI ED: Merger Arbitrage Index), (x) HFRIMI: Macro Strategy Hedge Fund (proxy: HFRI Macro (Total) Index), (xi) HFRIRVA: Relative Value Hedge Fund (proxy: HFRI Relative Value (Total) Index), (xii) HFRIFOF: Fund of Funds Hedge Fund (proxy: HFRI Fund of Funds Index). All portfolio values, indexes, and returns were measured in US-Dollars (USD).

As noted, the key problem of model risk in any risk model such as VaR results from the fact that risk cannot be measured, but must be estimated using a statistical model (Danielsson et al., 2014) . In other words, model risk occurs because a statistical model is used for estimation of risk: *use of a model in itself entails model risk* (Derman, 1996; Morini, 2011). Consistent with industry practice guidelines, we used a range of different plausible risk models used in hedge fund risk modeling and analysis practice which can be robustly discriminated between, so that the disagreement between their range of readings could help us succinctly assess model risk (Danielsson et al., 2014). Given our focus of quantitative risk modeling on fund-of-funds multi-asset portfolio construction and optimization, we applied standard practices used in the industry for risk modeling of hedge funds and funds-of-funds.

Statistical analysis of the various asset classes included basic performance plots such as *Value-Added Monthly Index* (*VAMI*) and Histograms; Probability Distributions and Probability Distribution Functions; Normality Tests including Distribution, Normal Q-Q Plot, and Jarque-Bera Normality Test; First Four Moment of Distributions with Skewness and Excess Kurtosis analyzed using both Distributions and Numeric Representations; Regression Plots for finding relationship between each fund asset class and the benchmark market index.

We used Risk-Adjusted Return Metrics applied in standard hedge fund risk modeling practice. These included risk models for Tracking Error, M1/M2 ratio of annualized first and second moments of distributions, Sharpe Ratio, Modified Sharpe Ratio, Sortino Ratio, Drawdown Ratio, Information Ratio, M-Squared Metric, Treynor Ratio, and, Jensen's Alpha. Those new to standard hedge fund risk modeling practice will find the industry specific interpretations and application details in Appendix 5-2 Hedge Fund Industry Risk-Adjusted Return Metrics relevant.

We used VAMI for tracking the comparative performance of different funds within the fund-of-funds. VAMI is an index of fund performance of a hypothetical $100 or $1000 investment in the specific asset class based on reinvestment of periodic returns. The focus of VAMI is on comparative assessment of risk in terms of draw-down, worst monthly draw-down, worst peak-to-valley-drawdown across different funds and fund managers (National Futures Association, 2013). Details about use of VAMI for risk assessment of funds are available in Appendix 5-3 Value Added Monthly Index (VAMI) Method.

VaR modeling for portfolio construction and portfolio optimization was done using Historical Simulation, Parametric Method, and Monte Carlo Simulation. Modified VaR was done using Modified Sharpe Ratio. Expected Shortfall was modeled to overcome the known limitations of VaR as a coherent risk measure. In addition to stressing of return to risk ratios for the various asset classes by modifying the assumptions, the portfolio was also stress tested using sensitivity analysis tests including use of equal weights for all asset classes, minimizing variance, maximizing return, and targeting a specific return. Portfolio modeling with the Returns Maximizing portfolio was examined for volatility and chosen for further advanced analysis using VaR, CVAR, ARCH/GARCH, and EVT.

5.10 Empirical Results

In this section, we discuss the main findings of market risk modeling of a half-trillion dollar fund-of-funds asset portfolio for a top Wall Street investment bank, 21-year monthly returns of 12 different asset classes. The two tracking error measures, quadratic standard deviation (SD) and linear mean absolute deviations (MAD), for each asset class are shown in Table 5-1. HFRIMAI tracks the S&P index most closely, whereas MXEF tracks S&P index least closely.

Table 5-1. Tracking Errors Relative to S&P Index for Various Asset Classes

Tracking Error	RIY	RTY	MXEF	LPX50TR	DJUBS	USTW$	HFRIEDI	HFRIEHI	HFRIMAI	HFRIMI	HFRIRVA	HFRIFOF
Quadratic (SD)	0.0599	0.0689	0.0814	0.0796	0.0625	0.0476	0.0461	0.0492	0.0432	0.0501	0.0439	0.0461
Linear (MAD)	0.0462	0.0526	0.0627	0.0572	0.0484	0.0366	0.0357	0.0385	0.0334	0.0401	0.0338	0.0358

Basic performance plots shown in Table 5-2 for each asset include historical performance in terms of Returns (RoR%); VAMI; and, histogram of monthly returns.

Table 5-2. Performance Plots: Returns, VAMI, Histogram for Asset Classes

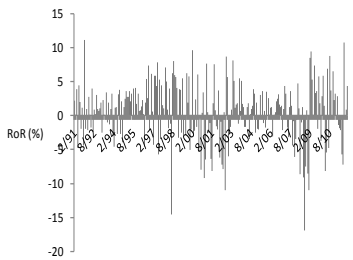
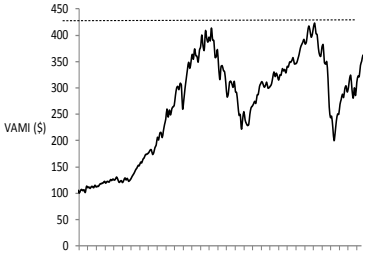
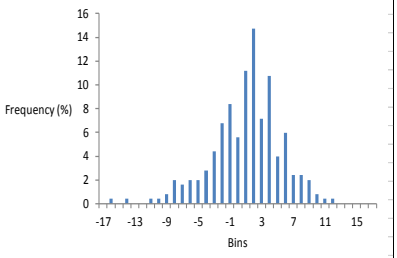
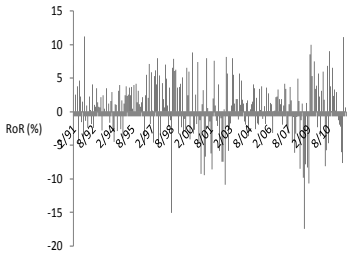
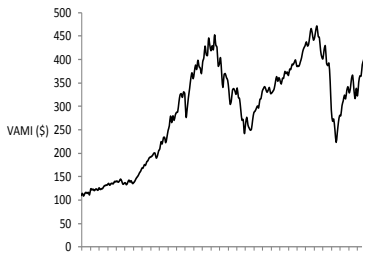
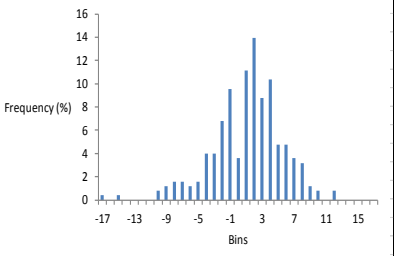
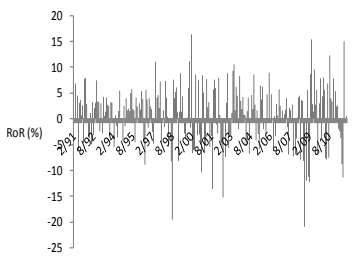
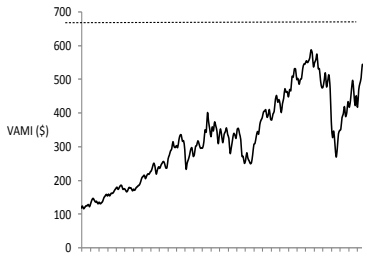
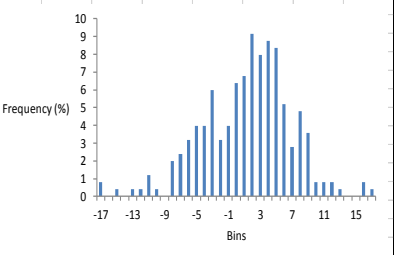
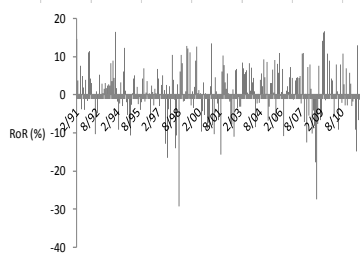
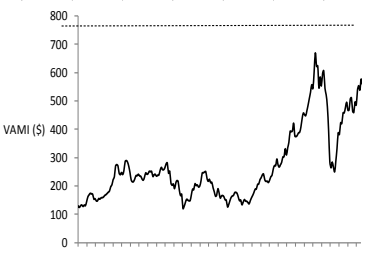
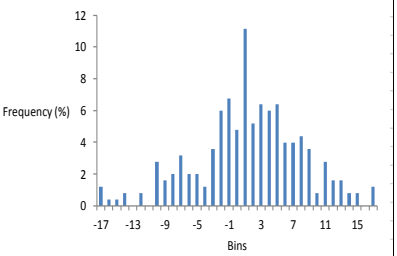
INDEX	RETURNS	VAMI	HISTOGRAM
SPY			
RIY			
RTY			
MXEF			

Table 5-2. Performance Plots: Returns, VAMI, Histogram for Asset Classes (contd.)

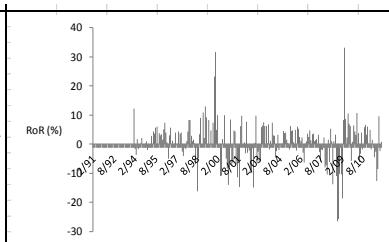
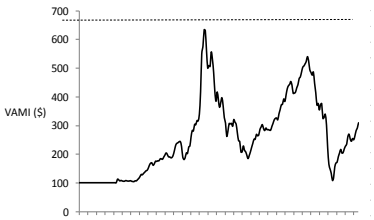
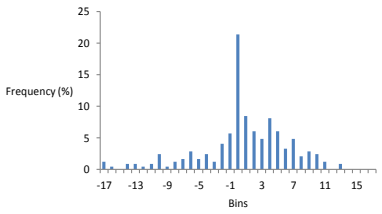
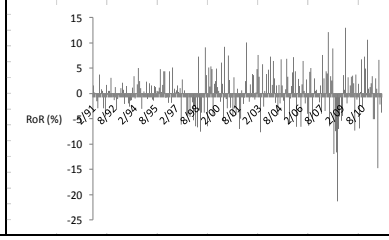
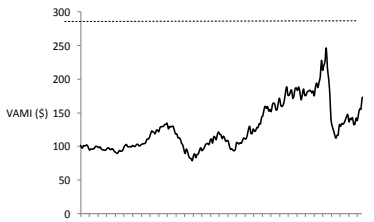
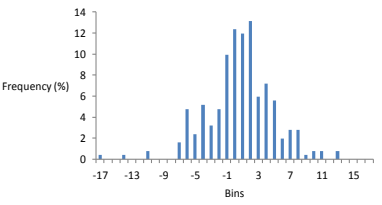
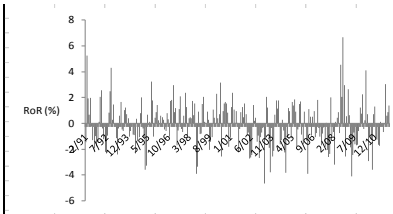
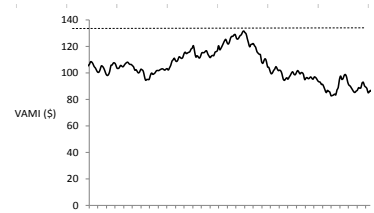
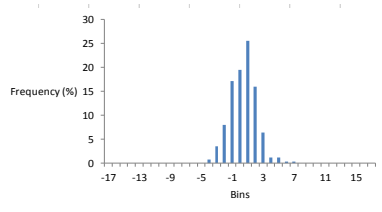
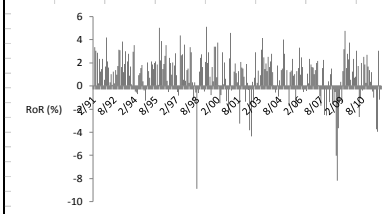
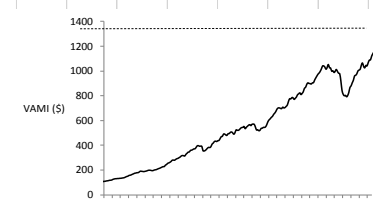
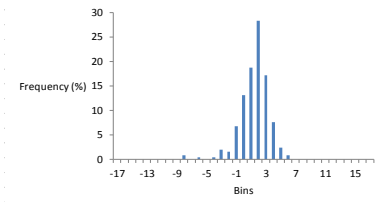
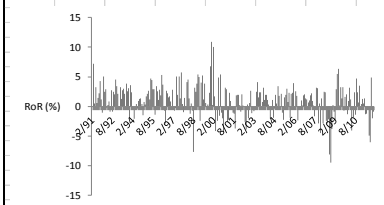
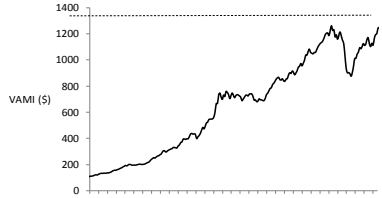
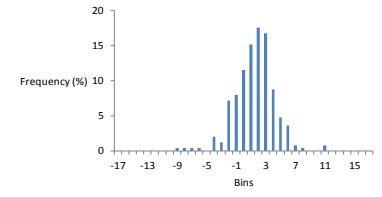
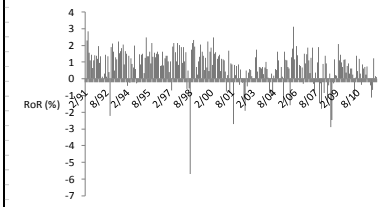
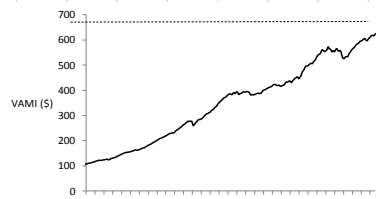
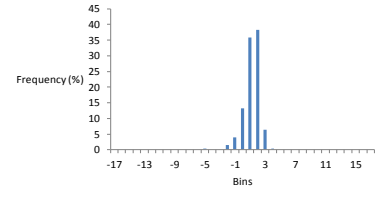
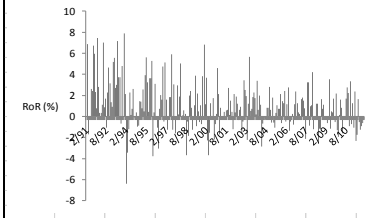
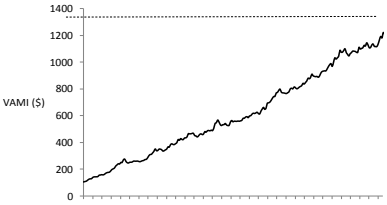
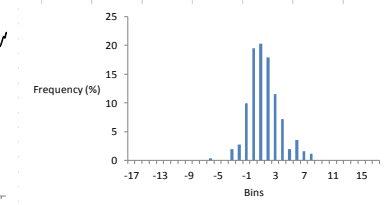
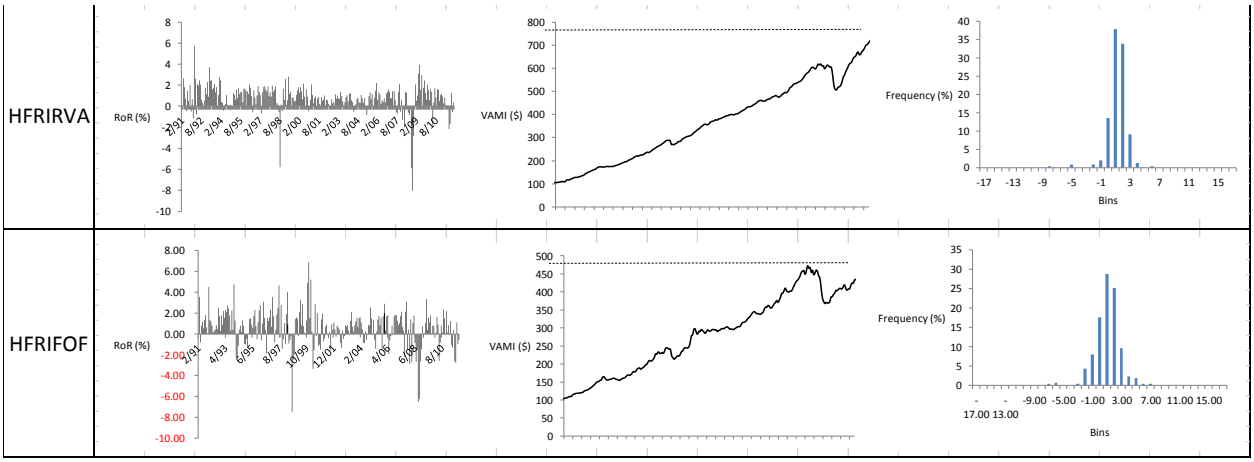
LPX50TR			
DJUBS			
USTW$			
HFRIEDI			
HFRIEHI			
HFRIMAI			
HFRIMI			

Table 5-2. (contd.) Performance Plots: Returns, VAMI, Histogram for Asset Classes



Relative performance of VAMI for the hedge fund asset classes is clearly evident in Tables 5-1 and 5-2, and, Fig 5-1 which shows their comparison over the years.

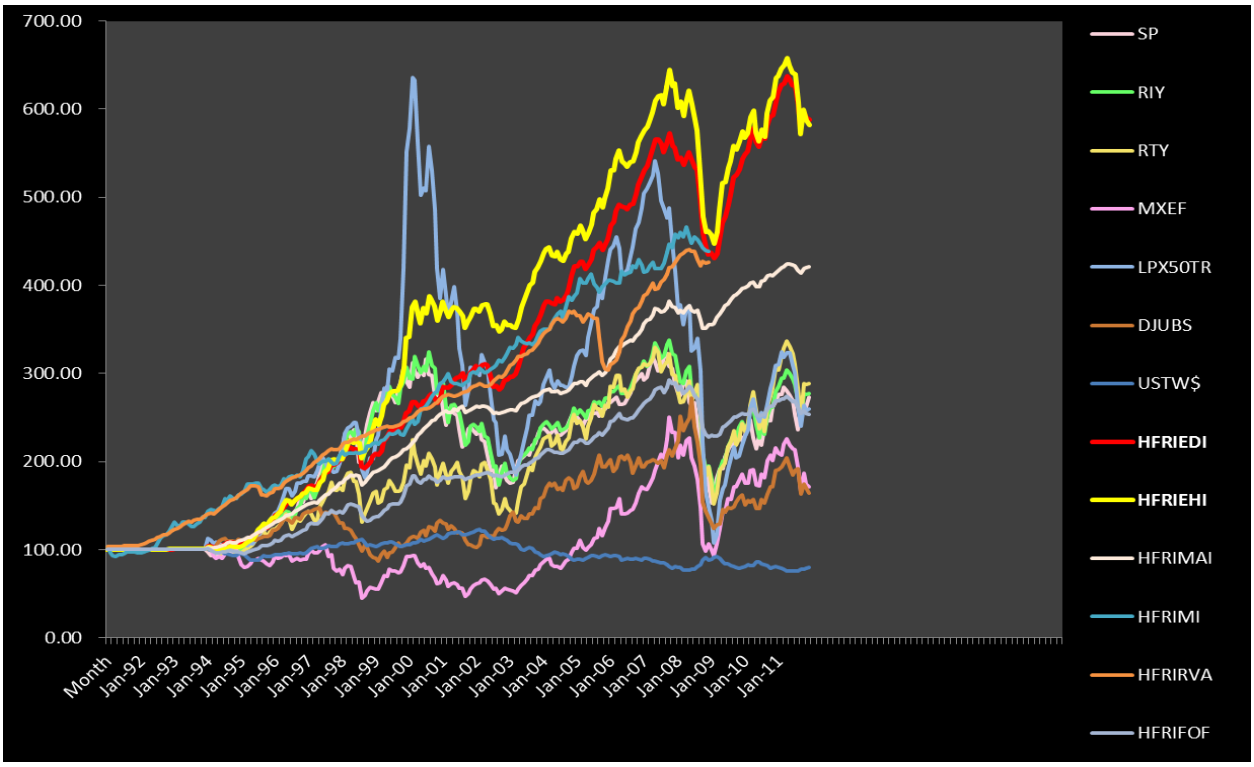


Fig. 5-1: VAMI Values for All Asset Classes in the Multi-Asset Portfolio: HFRIEDI and HFRIEHI are Shown as Solid Yellow Line and Red Line on Top

The ROR% charts show that while returns volatility of RIY, RTY, DJUBS, is comparable to the SPY benchmark; MXEF has more downside risk; LPX50TR has more upside return as well as downside risk; the currencies index USTW$ as well as all the

six hedge fund indexes HFRIEDI, HFRIEHI, HFRIMAI, HFRIMI, HFRIRVA, HFRIFOF have *lower upside return as well as downside risk* relative to the benchmark. Relative indicates that the effect of hedges for the various hedge funds is realized consistent with hedging expectations. VAMI plots for various asset classes show different risk-return behaviors relative to the market index. VAMI for RIY tracks the market VAMI most consistently, whereas RTY VAMI lags the market VAMI for first half but tracks it more consistently for the second half. While USTW$ VAMI remains around the starting value for most of the duration, VAMI for MXEF and DJUBS that lag the market for the first two-thirds period, track the market closely over the last third. *VAMI for all other asset classes show consistent outperformance of market VAMI with VAMI for two of the hedge fund asset classes, HFRIEHI* Equity Hedge Fund *and HFRIEDI* Event Driven Hedge Fund *demonstrating consistently higher highs and higher lows relative to all other asset classes*.

Table 5-3 shows the comparison of the empirical distributions of the benchmark return. Besides visual analysis of normality and respective Q-Q normality plots, normality of the distributions is also assessed using the Jarque-Barra Test that jointly checks for skewness and excess kurtosis. In addition to the above findings, Table 5-3 also lists observed values of the first four moments of distribution for all asset class returns: mean, standard deviation (S.D.), skewness and excess kurtosis.

Table 5-3. Normality Tests: Asset Returns: Distributions, QQ-Plots, Jarque-Bera

TABLE 3

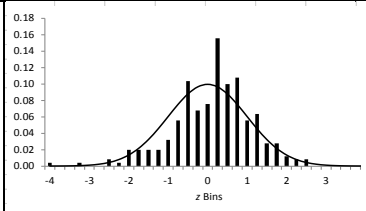
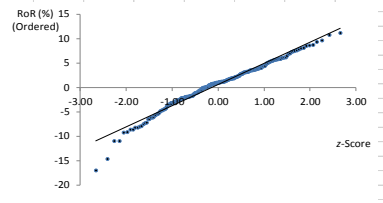
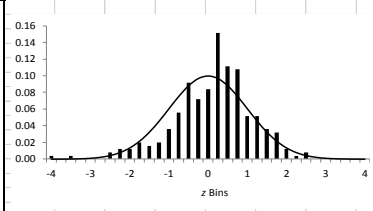
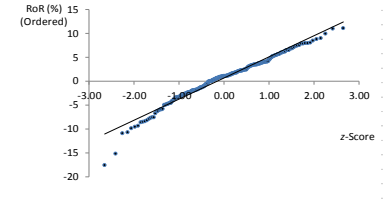
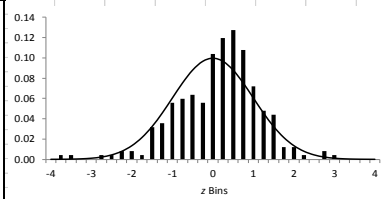
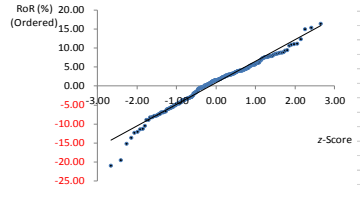
INDEX	EMPRICAL vs. NORMAL DISTBNS.	Q-Q NORMALITY PLOT	MOMENTS & JARQUE-BERA TEST
SPY			**Moments** Mean 7.25 St. Dev. 15.03 Skewness -0.6027 **Excess Kurtosis 1.2005** **Normality Test** Jarque-Bera Value 30.2687 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO Null Hypothesis of Normality is Rejected
RIY			**Moments** Mean 6.94 St. Dev. 15.86 Skewness -0.6815 **Excess Kurtosis 1.0725** **Normality Test** Jarque-Bera Value 27.0705 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO Null Hypothesis of Normality is Rejected
RTY			**Moments** Mean 9.79 St. Dev. 19.57 Skewness -0.5102 **Excess Kurtosis 1.1073** **Normality Test** Jarque-Bera Value 23.7136 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO Null Hypothesis of Normality is Rejected

Table 5-3. Normality Tests: Asset Returns: Distributions, QQ-Plots, Jarque-Bera (contd.)

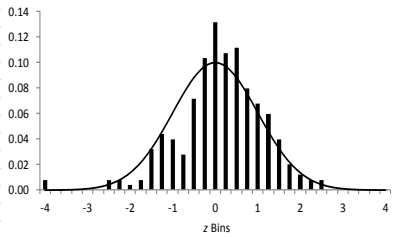
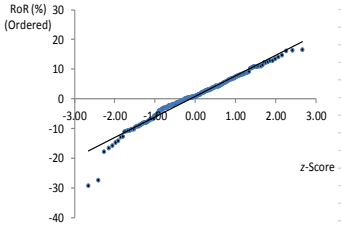
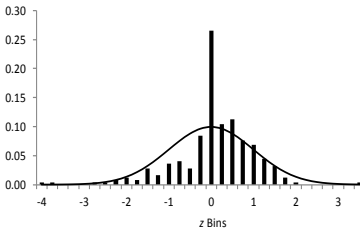
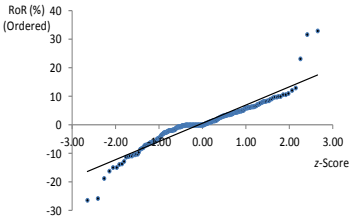
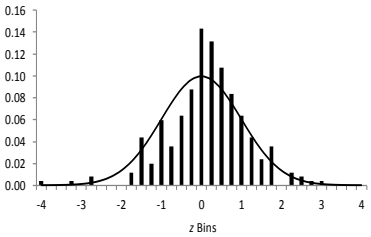
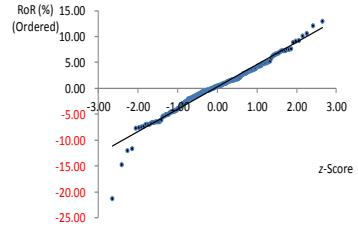
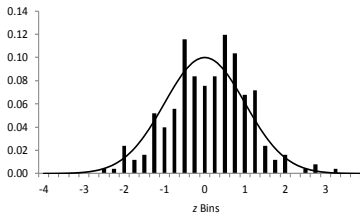
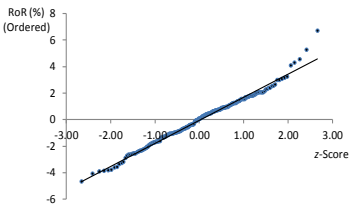
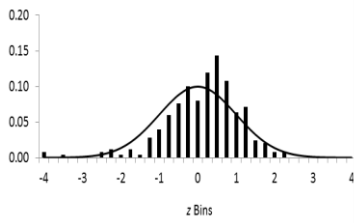
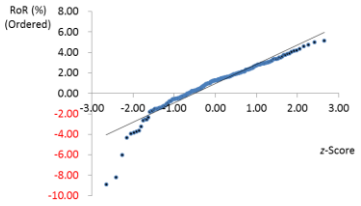
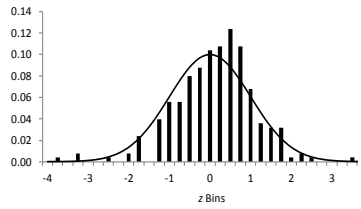
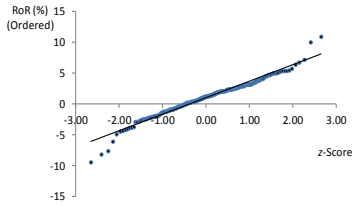
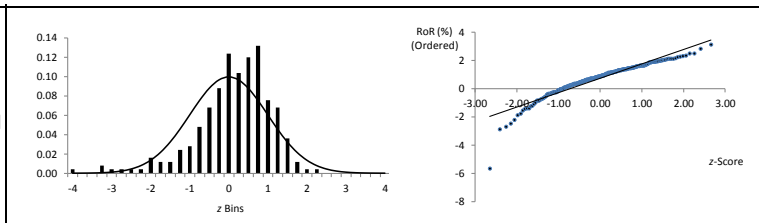
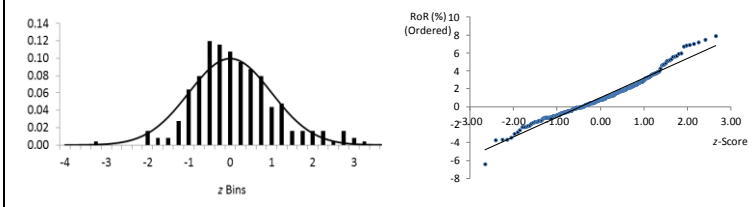
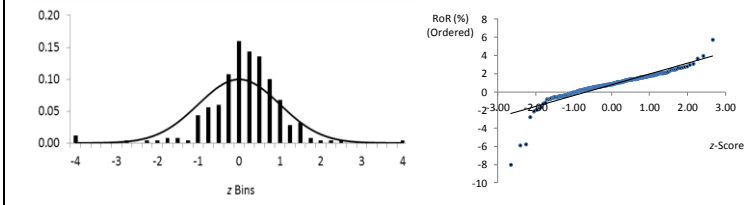
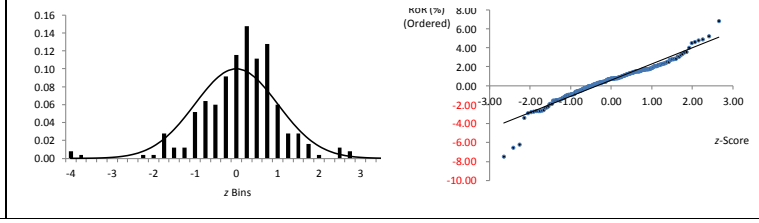
MXEF	 	**Moments** Mean 10.25 St. Dev. 23.94 Skewness -0.7002 **Excess Kurtosis 1.9299**	**Normality Test** Jarque-Bera Value 59.4637 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO Null Hypothesis of Normality is Rejected
LPX50TR	 	**Moments** Mean 8.36 St. Dev. 24.78 Skewness 0.0725 **Excess Kurtosis 4.5070**	**Normality Test** Jarque-Bera Value 183.0062 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO Null Hypothesis of Normality is Rejected
DJUBS	 	**Moments** Mean 3.05 St. Dev. 14.97 Skewness -0.5479 **Excess Kurtosis 2.7376**	**Normality Test** Jarque-Bera Value 90.9380 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO Null Hypothesis of Normality is Rejected
USTW$	 	**Moments** Mean -1.07 St. Dev. 5.90 Skewness 0.0491 **Excess Kurtosis 0.7959**	**Normality Test** Jarque-Bera Value 7.7128 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0211 **Critical Test** ***p* Test** Normality NO NO Null Hypothesis of Normality is Rejected
HFRIEDI	 	**Moments** Mean 10.09 St. Dev. 6.96 Skewness -1.2760 **Excess Kurtosis 4.0689**	**Normality Test** Jarque-Bera Value 282.5562 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO Null Hypothesis of Normality is Rejected
HFRIEHI	 	**Moments** Mean 10.23 St. Dev. 9.46 Skewness -0.2129 **Excess Kurtosis 1.9992**	**Normality Test** Jarque-Bera Value 44.2843 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO Null Hypothesis of Normality is Rejected

Table 5-3. Normality Tests: Asset Returns: Distributions, QQ-Plots, Jarque-Bera (contd.)

HFRIMAI		**Moments** Mean 8.05 St. Dev. 3.68 Skewness -1.6106 **Excess Kurtosis 6.1270** **Normality Test** Jarque-Bera Value 458.8732 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO **Null Hypothesis of Normality is Rejected**
HFRIMI		**Moments** Mean 8.40 St. Dev. 6.69 Skewness 0.1786 **Excess Kurtosis 0.9909** **Normality Test** Jarque-Bera Value 21.9863 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO **Null Hypothesis of Normality is Rejected**
HFRIRVA		**Moments** Mean 8.15 St. Dev. 4.37 Skewness -2.8779 **Excess Kurtosis 15.9776** **Normality Test** Jarque-Bera Value 2046.5842 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO **Null Hypothesis of Normality is Rejected**
HFRIFOF		**Moments** Mean 5.33 St. Dev. 6.10 Skewness -0.6651 **Excess Kurtosis 3.6812** **Normality Test** Jarque-Bera Value 161.1758 Level of Significance 5% Degrees of Freedom 2 Critical Value 5.9915 *p*-Value 0.0000 **Critical Test** ***p* Test** Normality NO NO **Null Hypothesis of Normality is Rejected**

Null hypothesis of normality is rejected for all the asset class return distributions. Highest mean value is 10.25 for the MXEF asset class (S.D. 23.94). *Next highest mean values are 10.23 (S.D. 9.46) and 10.09 (S.D. 6.96) for HFRIEHI and HFRIEDI respectively. Based on per unit risk analysis for the three highest mean returns, highest mean return per unit risk is delivered by HFRIEDI and HFRIEHI in that order.* The superiority of a portfolio that is composed of these two specific asset is thus confirmed by most of the simple models that address third and fourth moments of statistical profit and loss distribution as well as more advanced models discussed later.

The correlation matrix showing relative strength of variability of returns of the asset classes with respect to each other is shown in Table 5-4. *All asset classes show relatively low correlations with the market index which is a characteristic feature of the hedge funds as active fund managers are compensated for beating the market*. Each of the asset class returns was regressed against the benchmark and Adjusted R-Square for all regressions

was found to be insignificant or negligible. *Even though less correlated with the market index, all asset class indices are strongly correlated with each other except for Currencies.* Currencies (USTW$) show low to moderate negative correlation with all other asset classes.

Table 5-4. Correlation Matrix of Asset Returns

	SP	RIY	RTY	MXEF	LPX50TR	DJUBS	USTW$	HFRIEDI	HFRIEHI	HFRIMAI	HFRIMI	HFRIRVA	HFRIFOF
SP	1.000												
RIY	0.099	1.000											
RTY	0.103	0.835	1.000										
MXEF	0.023	0.751	0.732	1.000									
LPX50TR	0.130	0.730	0.745	0.679	1.000								
DJUBS	(0.033)	0.331	0.337	0.455	0.292	1.000							
USTW$	(0.043)	(0.251)	(0.220)	(0.320)	(0.131)	(0.309)	1.000						
HFRIEDI	0.109	0.750	0.802	0.747	0.723	0.415	(0.273)	1.000					
HFRIEHI	0.115	0.781	0.843	0.759	0.766	0.462	(0.244)	0.872	1.000				
HFRIMAI	0.150	0.596	0.615	0.574	0.501	0.322	(0.143)	0.769	0.679	1.000			
HFRIMI	(0.063)	0.345	0.380	0.458	0.315	0.365	(0.106)	0.517	0.563	0.343	1.000		
HFRIRVA	0.129	0.596	0.579	0.606	0.609	0.459	(0.295)	0.815	0.721	0.693	0.315	1.000	
HFRIFOF	0.050	0.616	0.655	0.732	0.662	0.463	(0.190)	0.850	0.869	0.633	0.715	0.751	1.000

Interestingly, most other asset classes show moderate to strong positive correlations with each other. In particular, three asset classes, HFRIEDI and HFRIEHI besides HFRIFOF, have correlations exceeding 50% with all other asset classes except for commodities with which they have correlations exceeding 40%. As the 'most diversified' portfolio is the market index portfolio, it is expected that the hedge funds will be least correlated with it given the very raison d'être of hedge funds is to beat the market by active investment management. Ergo, it is plausible that the above very high correlations of HFRIEDI (52% to 87%) and HFRIEHI (56% to 87%) besides HFRIFOF (62% to 87%) with most other asset classes relate to hedging characteristics (which as observed above are) uncorrelated with the market index.

Mean-variance optimization was used to compute portfolio asset allocations for minimizing variance and for maximizing returns and compared with portfolio

containing equal weights for all asset classes. The covariance matrix created for portfolio mean-variance optimization is shown in Table 5-5.

Table 5-5. Covariance Matrix of Asset Returns

	SP	RIY	RTY	MXEF	LPX50TR	DJUBS	USTW$	HFRIEDI	HFRIEHI	HFRIMAI	HFRIMI	HFRIRVA	HFRIFOF
SP	0.002043	0.000204	0.000272	7.2E-05	0.000419	-6.8E-05	-3.3E-05	9.88E-05	0.000142	7.18E-05	-5.5E-05	7.34E-05	3.94E-05
RIY	0.000204	0.002086	0.00223	0.002423	0.002378	0.000693	-0.00019	0.000687	0.000972	0.000288	0.000303	0.000343	0.000494
RTY	0.000272	0.00223	0.003419	0.003021	0.003109	0.000905	-0.00022	0.00094	0.001344	0.000381	0.000428	0.000426	0.000673
MXEF	7.2E-05	0.002423	0.003021	0.004983	0.003421	0.001473	-0.00038	0.001056	0.001461	0.000429	0.000623	0.000539	0.000907
LPX50TR	0.000419	0.002378	0.003109	0.003421	0.005093	0.000957	-0.00016	0.001034	0.001489	0.000379	0.000433	0.000547	0.000829
DJUBS	-6.8E-05	0.000693	0.000905	0.001473	0.000957	0.002105	-0.00024	0.000381	0.000578	0.000157	0.000323	0.000265	0.000373
USTW$	-3.3E-05	-0.00019	-0.00022	-0.00038	-0.00016	-0.00024	0.000288	-9.3E-05	-0.00011	-2.6E-05	-3.5E-05	-6.3E-05	-5.7E-05
HFRIEDI	9.88E-05	0.000687	0.00094	0.001056	0.001034	0.000381	-9.3E-05	0.000402	0.000476	0.000163	0.000199	0.000206	0.000299
HFRIEHI	0.000142	0.000972	0.001344	0.001461	0.001489	0.000578	-0.00011	0.000476	0.000743	0.000112	7E-05	9.24E-05	0.000118
HFRIMAI	7.18E-05	0.000288	0.000381	0.000429	0.000379	0.000157	-2.6E-05	0.000163	0.000196	0.000112	7E-05	9.24E-05	0.000118
HFRIMI	-5.5E-05	0.000303	0.000428	0.000623	0.000433	0.000323	-3.5E-05	0.000199	0.000295	7E-05	0.000371	7.64E-05	0.000242
HFRIRVA	7.34E-05	0.000343	0.000426	0.000539	0.000547	0.000265	-6.3E-05	0.000206	0.000247	9.24E-05	7.64E-05	0.000159	0.000166
HFRIFOF	3.94E-05	0.000494	0.000673	0.000907	0.000829	0.000373	-5.7E-05	0.000299	0.000416	0.000118	0.000242	0.000166	0.000308

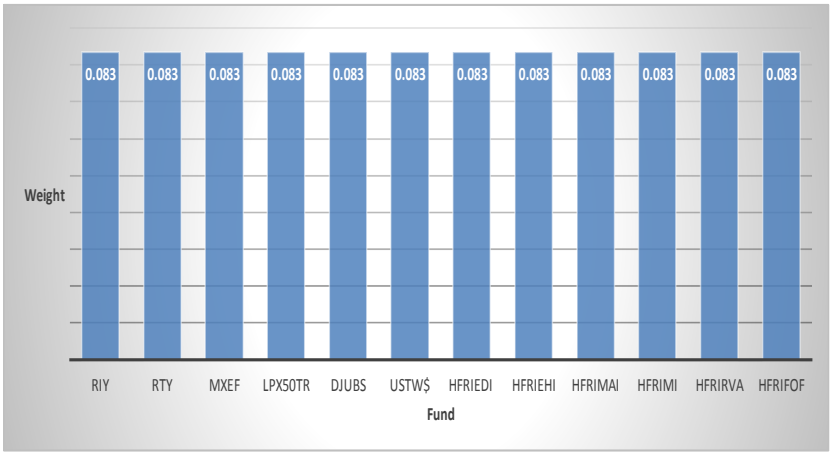
Tables 5-6 (a), (b), (c), and, (d) show the Mean-Variance Optimization Portfolios based upon the following criteria listed below.

Table 5-6 (a) Equal Weights Portfolio

Return 6.879%, Variance 0.071%, Sharpe Ratio 2.58

Optimization Portfolios based upon Equal Weights

Return Matrix (*R*)		Weight Matrix (*W*)		
Fund	Return (%)	Fund	Weight	Limit
SP	6.83%	SP	0.000	0.000
RIY	6.94%	RIY	0.083	0.500
RTY	7.95%	RTY	0.083	0.500
MXEF	6.06%	MXEF	0.083	0.500
LPX50TR	8.36%	LPX50TR	0.083	0.500
DJUBS	4.04%	DJUBS	0.083	0.500
USTW$	-1.07%	USTW$	0.083	0.500
HFRIEDI	10.09%	HFRIEDI	0.083	0.500
HFRIEHI	10.23%	HFRIEHI	0.083	0.500
HFRIMAI	8.05%	HFRIMAI	0.083	0.500
HFRIMI	8.40%	HFRIMI	0.083	0.500
HFRIRVA	8.15%	HFRIRVA	0.083	0.500
HFRIFOF	5.33%	HFRIFOF	0.083	0.500
			1.00	



Portfolio Return (%) 6.879%

Target Return (%) 6.879% Maximize

Target Variance (%) 0.071% Minimize

Sharpe Ratio 2.58 Assuming Rf = 0

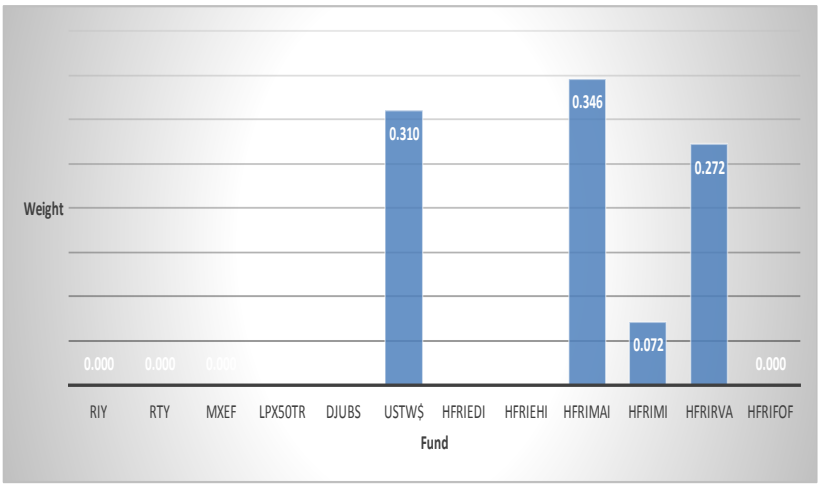
Table 5-6 (b) Minimizing Variance Portfolio

Return 5.273%, Variance 0.006%, Sharpe Ratio 6.75

31% USTW$, 34.6% HFRIMAI, 7.2% HFRIMI, and 27.2% HFRIRVA

Optimization Portfolios based upon Minimizing Variance

Return Matrix (*R*)		Weight Matrix (*W*)		
Fund	Return (%)	Fund	Weight	Limit
SP	6.83%	SP	0.000	0.000
RIY	6.94%	RIY	0.000	0.500
RTY	7.95%	RTY	0.000	0.500
MXEF	6.06%	MXEF	0.000	0.500
LPX50TR	8.36%	LPX50TR	0.000	0.500
DJUBS	4.04%	DJUBS	0.000	0.500
USTW$	-1.07%	USTW$	0.310	0.500
HFRIEDI	10.09%	HFRIEDI	0.000	0.500
HFRIEHI	10.23%	HFRIEHI	0.000	0.500
HFRIMAI	8.05%	HFRIMAI	0.346	0.500
HFRIMI	8.40%	HFRIMI	0.072	0.500
HFRIRVA	8.15%	HFRIRVA	0.272	0.500
HFRIFOF	5.33%	HFRIFOF	0.000	0.500
			1.00	



Portfolio Return (%) 5.273%

Target Return (%) 5.273% Maximize

Target Variance (%) 0.006% Minimize

Sharpe Ratio 6.75 Assuming Rf = 0

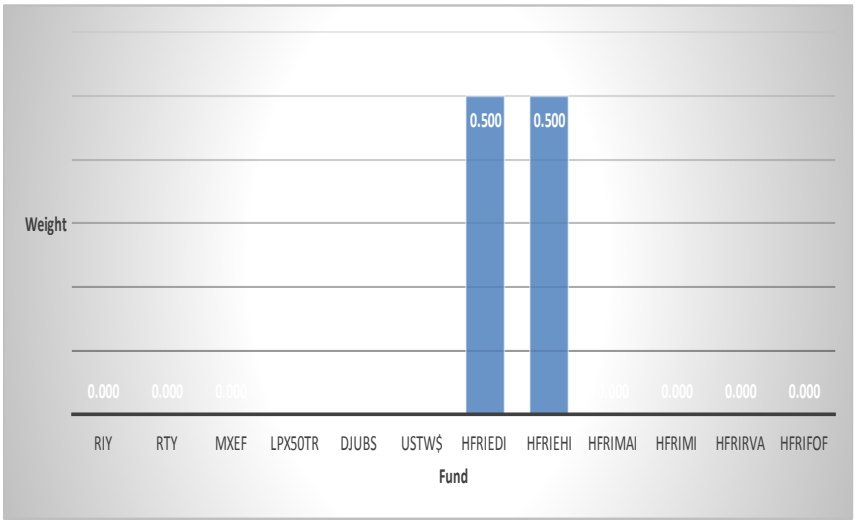
Table 5-6 (c) Maximizing Return Portfolio

Return 10.161%, Variance 0.052%, Sharpe Ratio 4.44

50% HFRIEDI and 50% HFRIEHI

Optimization Portfolios based upon Maximizing Return

Return Matrix (*R*)		Weight Matrix (*W*)		
Fund	Return (%)	Fund	Weight	Limit
SP	6.83%	SP	0.000	0.000
RIY	6.94%	RIY	0.000	0.500
RTY	7.95%	RTY	0.000	0.500
MXEF	6.06%	MXEF	0.000	0.500
LPX50TR	8.36%	LPX50TR	0.000	0.500
DJUBS	4.04%	DJUBS	0.000	0.500
USTW$	-1.07%	USTW$	0.000	0.500
HFRIEDI	10.09%	HFRIEDI	0.500	0.500
HFRIEHI	10.23%	HFRIEHI	0.500	0.500
HFRIMAI	8.05%	HFRIMAI	0.000	0.500
HFRIMI	8.40%	HFRIMI	0.000	0.500
HFRIRVA	8.15%	HFRIRVA	0.000	0.500
HFRIFOF	5.33%	HFRIFOF	0.000	0.500
			1.00	



Portfolio Return (%) 10.161%

Target Return (%) 10.161% Optimize

Target Variance (%) 0.052% Minimize

Sharpe Ratio 4.44 Assuming Rf = 0

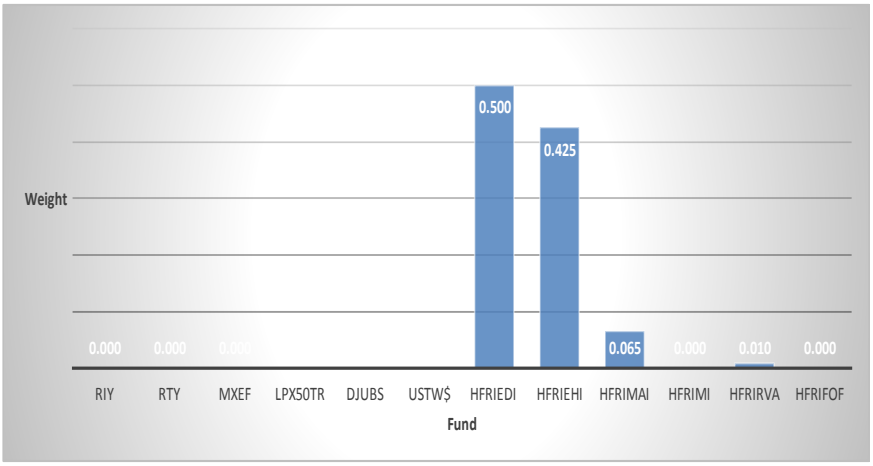
Table 5-6 (d) Targeted Return 10%

Return 10.000%, Variance 0.046%, Sharpe Ratio 4.66

Portfolio of 50% HFRIEDI, 42.50% HFRIEHI and 6.5% HFRIMAI

Optimization Portfolios based upon Targeted Return 10%

Return Matrix (*R*)		Weight Matrix (*W*)		
Fund	Return (%)	Fund	Weight	Limit
SP	6.83%	SP	0.000	0.000
RIY	6.94%	RIY	0.000	0.500
RTY	7.95%	RTY	0.000	0.500
MXEF	6.06%	MXEF	0.000	0.500
LPX50TR	8.36%	LPX50TR	0.000	0.500
DJUBS	4.04%	DJUBS	0.000	0.500
USTW$	-1.07%	USTW$	0.000	0.500
HFRIEDI	10.09%	HFRIEDI	0.500	0.500
HFRIEHI	10.23%	HFRIEHI	0.425	0.500
HFRIMAI	8.05%	HFRIMAI	0.065	0.500
HFRIMI	8.40%	HFRIMI	0.000	0.500
HFRIRVA	8.15%	HFRIRVA	0.010	0.500
HFRIFOF	5.33%	HFRIFOF	0.000	0.500
			1.00	



Portfolio Return (%) 10.000%

Target Return (%) 10.000% Optimize

Target Variance (%) 0.046% Minimize

Sharpe Ratio 4.66 Assuming Rf = 0

Another portfolio o9f Maximizing Return While Minimizing Variance Portfolio yielded with (Return 7.305%, Variance 0.008%, Sharpe Ratio 8.00) including the following asset classes: 9% USTW$, 50% HFRIMAI, 12% HFRIMI, and 29% HFRIRVA. As return is maximized at the cost of increasing variance, Sharpe ratio is penalized accordingly. Risk-adjusted return measures for all asset classes including M1/M2, Sharpe Ratio, MSR, Sortino Ratio, DD Ratio, Information Ratio, M-Squared Ratio, Treynor Ratio, and Jensen Ratio are shown in Tables 5-7 (a), (b), and (c).

Table 5-7 (a) Risk-Adjusted Return Measures for All Asset Classes

	M1/M2	Sharpe	MSR	Sortino	DD Ratio	Information	M squared	Treynor	Jensen
SP	0.436	0.236	0.523	0.607	0.139	-	-	-	-
RIY	**0.439**	0.241	0.538	0.624	0.145	0.063	0.640	38.157	3.400
RTY	**0.393**	0.238	0.516	0.700	0.129	0.554	0.597	36.284	4.233
MXEF	**0.248**	0.120	0.283	0.349	0.070	(0.321)	(1.253)	83.123	2.870
LPX50TR	**0.338**	0.212	0.438	0.695	0.090	0.670	0.185	25.511	4.255
DJUBS	**0.254**	0.057	0.132	0.097	0.027	(1.474)	(2.230)	(27.320)	1.224
USTW$	**(0.182)**	(0.714)	(1.553)	(1.147)	(0.390)	(5.590)	(14.316)	260.688	(3.986)
HFRIEDI	**1.454**	1.003	2.183	1.922	0.501	2.386	12.580	144.022	6.833
HFRIEHI	**1.083**	0.752	1.401	1.723	0.349	2.354	8.642	101.927	6.852
HFRIMAI	**2.194**	1.341	2.814	1.506	0.603	0.943	17.865	140.008	4.860
HFRIMI	**1.260**	0.791	1.341	1.396	0.502	1.086	9.249	(195.247)	5.551
HFRIRVA	**1.870**	1.152	4.487	1.502	0.464	1.012	14.908	139.942	4.960
HFRIFOF	**0.876**	0.362	0.769	0.514	0.164	(1.089)	2.535	114.262	2.227

Table 5-7 (b) Ranked Risk-Adjusted Return Measures for All Asset Classes

M1/M2		Sharpe		MSR		Sortino		DD Ratio	
HFRIMAI	2.194	HFRIMAI	1.341	HFRIRVA	4.487	HFRIEDI	1.922	HFRIMAI	0.603
HFRIRVA	1.870	HFRIRVA	1.152	HFRIMAI	2.814	HFRIEHI	1.723	HFRIMI	0.502
HFRIEDI	1.454	HFRIEDI	1.003	HFRIEDI	2.183	HFRIMAI	1.506	HFRIEDI	0.501
HFRIMI	1.260	HFRIMI	0.791	HFRIEHI	1.401	HFRIRVA	1.502	HFRIRVA	0.464
HFRIEHI	1.083	HFRIEHI	0.752	HFRIMI	1.341	HFRIMI	1.396	HFRIEHI	0.349
HFRIFOF	0.876	HFRIFOF	0.362	HFRIFOF	0.769	RTY	0.700	HFRIFOF	0.164
RIY	0.439	RIY	0.241	RIY	0.538	LPX50TR	0.695	RIY	0.145
SP	0.436	RTY	0.238	SP	0.523	RIY	0.624	SP	0.139
RTY	0.393	SP	0.236	RTY	0.516	SP	0.607	RTY	0.129
LPX50TR	0.338	LPX50TR	0.212	LPX50TR	0.438	HFRIFOF	0.514	LPX50TR	0.090
DJUBS	0.254	MXEF	0.120	MXEF	0.283	MXEF	0.349	MXEF	0.070
MXEF	0.248	DJUBS	0.057	DJUBS	0.132	DJUBS	0.097	DJUBS	0.027
USTW$	(0.182)	USTW$	(0.714)	USTW$	(1.553)	USTW$	(1.147)	USTW$	(0.390)

Table 5-7 (c) Ranked Risk-Adjusted Return Measures for All Asset Classes

Sharpe		Information		M squared		Treynor		Jensen	
HFRIMAI	1.341	HFRIEDI	2.386	HFRIMAI	17.865	HFRIEDI	144.022	HFRIEHI	6.852
HFRIRVA	1.152	HFRIEHI	2.354	HFRIRVA	14.908	HFRIMAI	140.008	HFRIEDI	6.833
HFRIEDI	1.003	HFRIMI	1.086	HFRIEDI	12.580	HFRIRVA	139.942	HFRIMI	5.551
HFRIMI	0.791	HFRIRVA	1.012	HFRIMI	9.249	HFRIFOF	114.262	HFRIRVA	4.960
HFRIEHI	0.752	HFRIMAI	0.943	HFRIEHI	8.642	HFRIEHI	101.927	HFRIMAI	4.860
HFRIFOF	0.362	LPX50TR	0.670	HFRIFOF	2.535	MXEF	83.123	LPX50TR	4.255
RIY	0.241	RTY	0.554	RIY	0.640	RIY	38.157	RTY	4.233
RTY	0.238	RIY	0.063	RTY	0.597	RTY	36.284	RIY	3.400
SP	0.236	SP	0.000	LPX50TR	0.185	LPX50TR	25.511	MXEF	2.870
LPX50TR	0.212	MXEF	(0.321)	SP	0.000	SP	0.000	HFRIFOF	2.227
MXEF	0.120	HFRIFOF	(1.089)	MXEF	(1.253)	DJUBS	0.000	DJUBS	1.224
DJUBS	0.057	DJUBS	(1.474)	DJUBS	(2.230)	USTW$	0.000	SP	0.000
USTW$	(0.714)	USTW$	(5.590)	USTW$	(14.316)	HFRIMI	(195.247)	USTW$	(3.986)

For computation of risk-adjusted return measures, Risk-Free rate was considered as the average T-bill % rate of 3.13 based upon St. Louis Fed data for test duration of Jan '94 - Dec '11. The ranked ordered risk-adjusted return measures show some interesting patterns consistent with observations from prior risk models about the relative risk return characteristics of various asset classes. *Highest risk-adjusted returns in case of each risk-adjusted-measure (RAM) model were demonstrated by the hedge fund asset classes.* Currencies showed the lowest (negative) return in 8 of 9 RAM models. Commodities showed the second lowest (some negative) return in 6 of 9 RAM models. *All three of Sortino ratio, Jensen ratio, and Information Ratio show both HFRIEDI and HFRIEHI as the top two best performing asset classes*.

In terms of aggregate RoR% rankings HFRIEDI is ranked 1st by Sortino, Information, and Treynor ratios; 2nd by Jensen ratio; and 3rd by M1/M2, Sharpe, MSR, DD, and M-squared ratios. HFRIEHI is ranked 1st by Jensen ratio and 2nd by Sortino and Information ratios. It is also plausible that the specific fund strategies that exploit known limitations of some ratios and non-stationarity and non-paramaetricity of returns distributions may be influencing finer ranking order of hedge funds relative to each other. *In any case, the broader pattern ranking the two hedge fund asset classes HFRIEDI and HFRIEHI is clearly discernible with this set of risk models and is consistent with prior findings with other risk models.*

Following upon earlier discussion about VaR and its various types as well as ES, Historical Simulation based VaR, Parametric VaR, Modified VaR, and Expected Shortfall were computed for the specific Mean Variance Portfolio Optimizations discussed above and summarized earlier in Table 6. The empirical results of Historical Simulation based VaR, Parametric VaR, Modified VaR, and Expected Shortfall for all asset classes equally weighted portfolio, variance minimizing portfolio, and return maximizing portfolio are presented in Tables 5-8 (a), (b), and (c) respectively. Parametric VaR is computed based upon mean-variance optimization. Modified VaR takes into consideration and accounts for non-normality of the returns. Expected Shortfall takes into consideration subadditivity responsible for portfolio diversification of risk with diverse assets, a factor missing from VaR models.

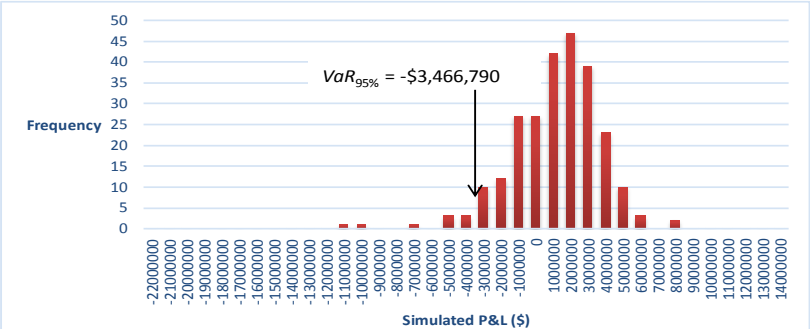
Table 5-8 (a) VaR and Expected Shortfall: At 95% confidence level, Optimization Portfolios based upon Equal Weights shows monthly Historical Simulation VaR of -$3,466,790 (indicating 5% chance of monthly losses exceeding this figure in any given month, and so on); Parametric VaR of -$4,382,848; Modified VaR of -$7,361,621; and, Expected Shortfall of -$5,258,022 (indicating *average* expected loss of -$5,258,022 if the threshold level α of 5% was exceeded without any indication of worst case loss).

Table 5-8 (a) 3 VaR Models and Expected Shortfall for Equal Weights

Historical Simulation VaR

PORT Index AuM ($)	100,000,000
Confidence Level	95%
Critical Value (z_α)	1.645

$VaR_{95\%}$ = -$3,466,790



Parametric VaR

PORT AuM ($)	100,000,000
Variance (Min.)	7.10
St. Dev.	2.66%
Confidence Level	95%
Critical Value (z_α)	1.645

$VaR_{95\%}$ = -$4,382,848

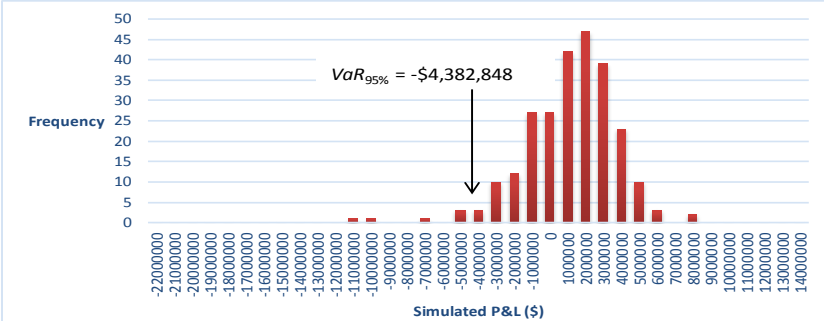
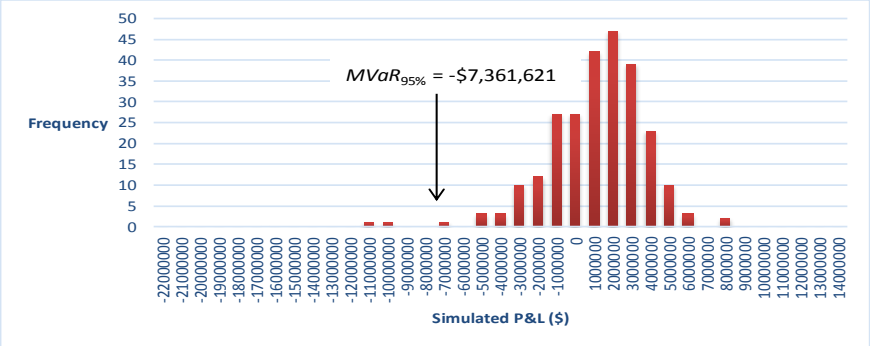


Table 5-8 (a) 3 VaR Models and Expected Shortfall for Equal Weights (contd.)

Modified VaR

PORT Index AuM ($)	100,000,000
Mean P&L ($)	694,724
St. Dev. P&L ($)	2,549,081
Confidence Level	95%

$MVaR_{95\%}$ = -$7,361,621



Expected Shortfall

PORT Index AuM ($)	100,000,000
Mean P&L ($)	694,724
St. Dev. P&L ($)	2,549,081
Confidence Level	95%

$ES_{95\%}$ = -$5,258,022

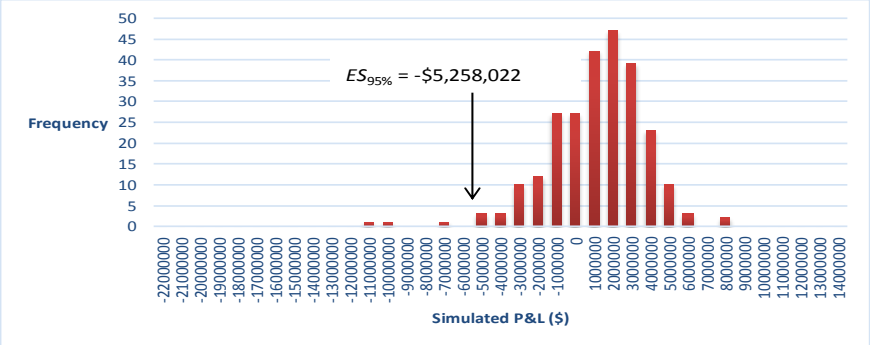


Table 5-8 (b) VaR and Expected Shortfall: At 95% confidence level, Optimization Portfolios based upon Minimum Variance shows Historical Simulation VaR of -$783,190; Parametric VaR of -$1,284,507; Modified VaR of -$1,884,524; and, Expected Shortfall of -$1,681,629.

Table 5-8 (b) 3 VaR Models and Expected Shortfall for Minimum Variance

Historical Simulation VaR

PORT Index AuM ($)	100,000,000
Confidence Level	95%
Critical Value (z_α)	1.645

$VaR_{95\%}$ = -$783,190

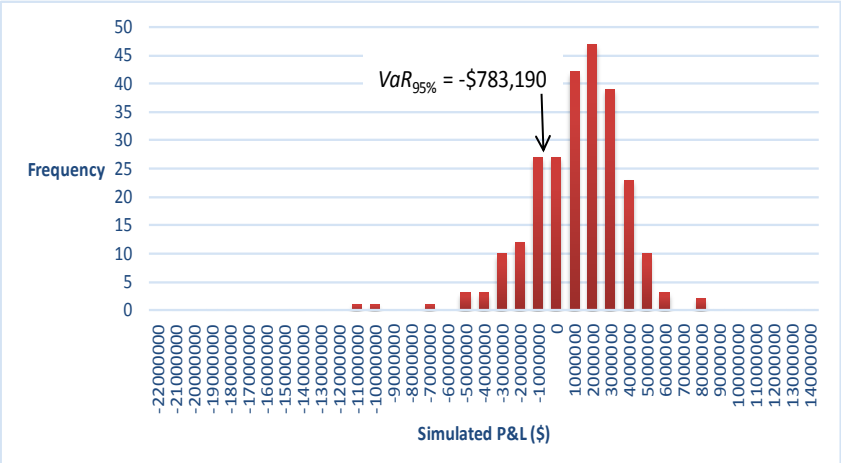
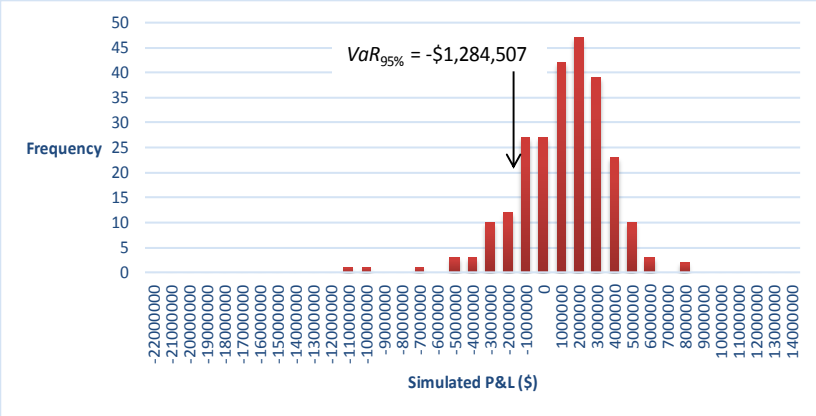


Table 5-8 (b) 3 VaR Models and Expected Shortfall for Minimum Variance (contd.)

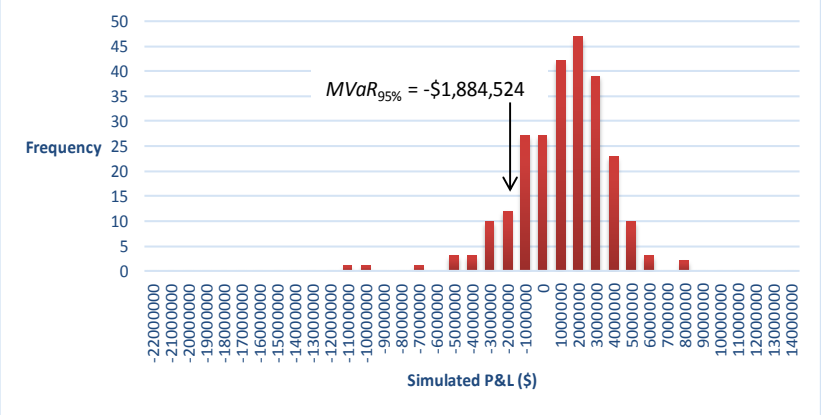
Parametric VaR

PORT AuM ($)	100,000,000
Variance (Min.)	0.61
St. Dev.	0.78%
Confidence Level	95%
Critical Value (z_α)	1.645
$VaR_{95\%}$ = -$1,284,507	



Modified VaR

PORT Index AuM ($)	100,000,000
Mean P&L ($)	533,059
St. Dev. P&L ($)	815,251
Confidence Level	95%
$MVaR_{95\%}$ = -$1,884,524	



Expected Shortfall

PORT Index AuM ($)	100,000,000
Mean P&L ($)	533,059
St. Dev. P&L ($)	815,251
Confidence Level	95%
$MVaR_{95\%}$ = -$1,681,629	

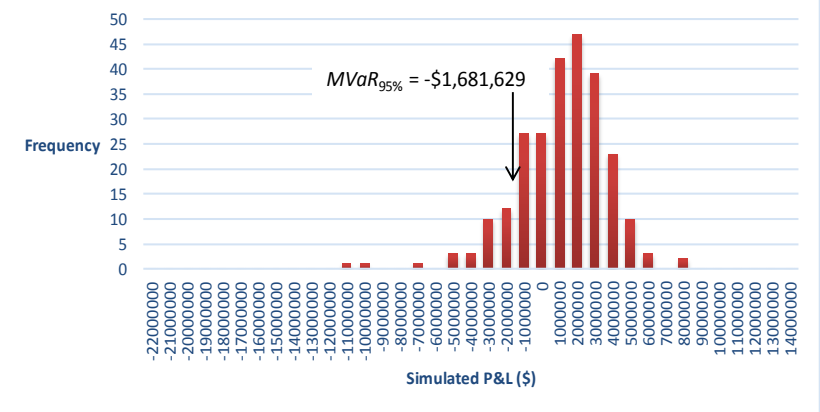


Table 5-8 (c) VaR and Expected Shortfall: At 95% confidence level, Optimization Portfolios based upon Maximizing Return shows Historical Simulation VaR of -

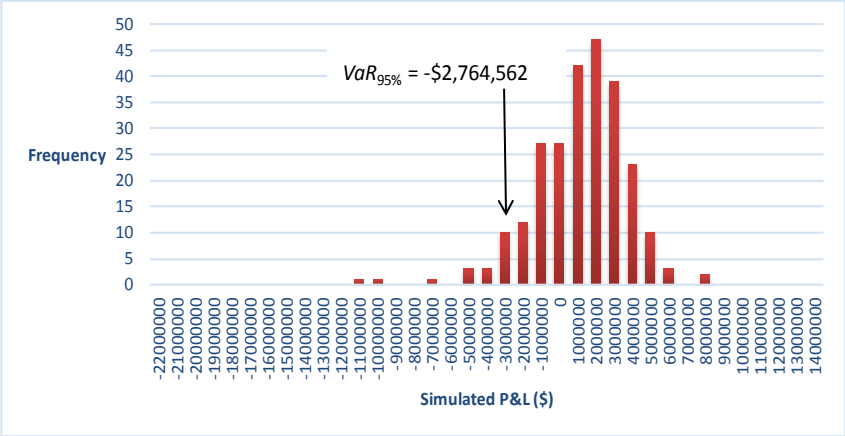
$2,764,562; Parametric VaR of -$3,766,260; Modified VaR of -$5,733,689; and, Expected Shortfall of -$4,575,377.

Table 5-8 (c) 3 VaR Models and Expected Shortfall for Maximizing Return

Historical Simulation VaR

PORT Index AuM ($)	100,000,000
Confidence Level	95%
Critical Value (z_α)	1.645

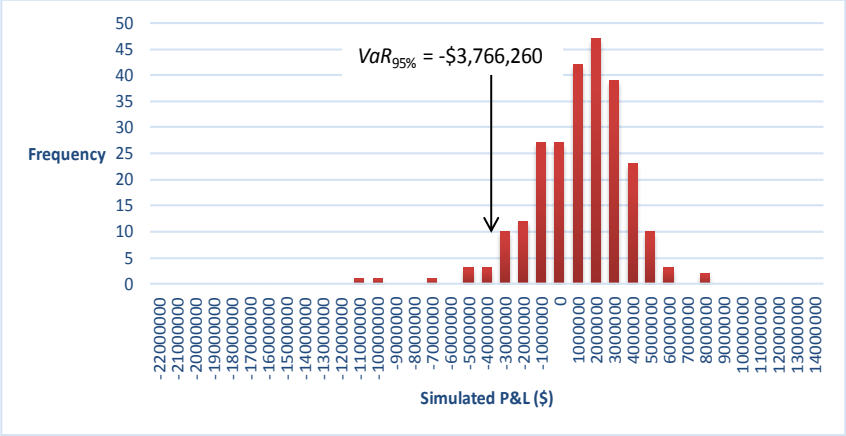
$VaR_{95\%}$ = -$2,764,562



Parametric VaR

PORT AuM ($)	100,000,000
Variance (Min.)	5.24
St. Dev.	2.29%
Confidence Level	95%
Critical Value (z_α)	1.645

$VaR_{95\%}$ = -$3,766,260



Modified VaR

PORT Index AuM ($)	100,000,000
Mean P&L ($)	994,581
St. Dev. P&L ($)	2,218,136
Confidence Level	95%

$MVaR_{95\%}$ = -$5,733,689

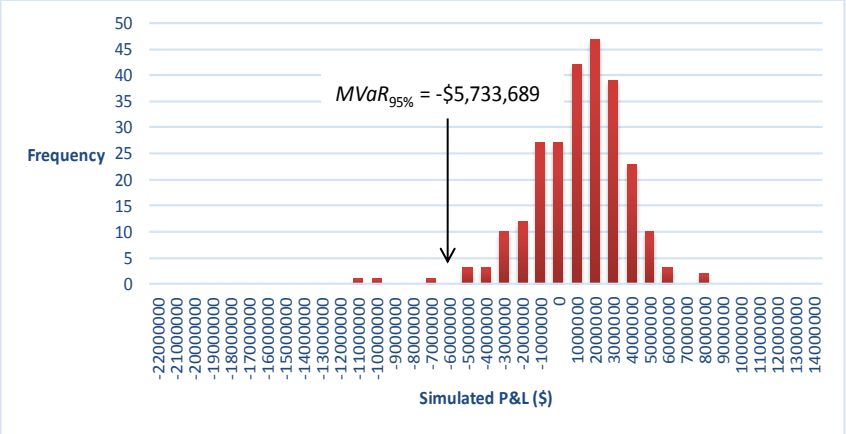
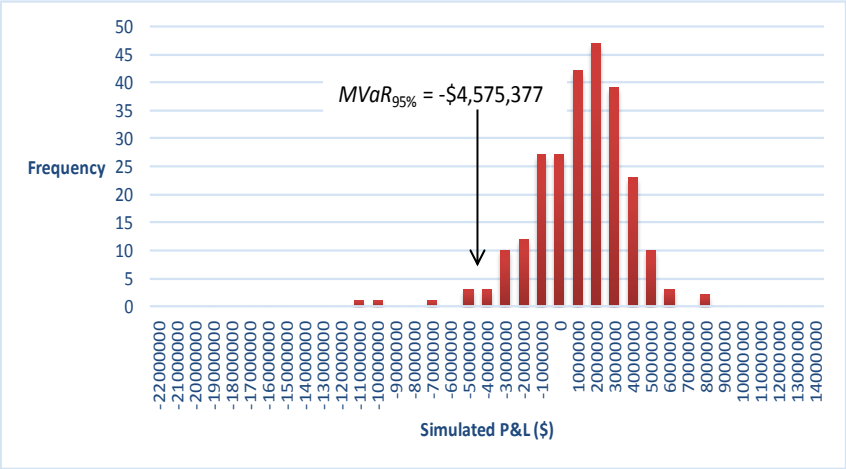


Table 5-8 (c) 3 VaR Models and Expected Shortfall for Maximizing Return (contd.)

Expected Shortfall	
PORT Index AuM ($)	100,000,000
Mean P&L ($)	994,581
St. Dev. P&L ($)	2,218,136
Confidence Level	95%

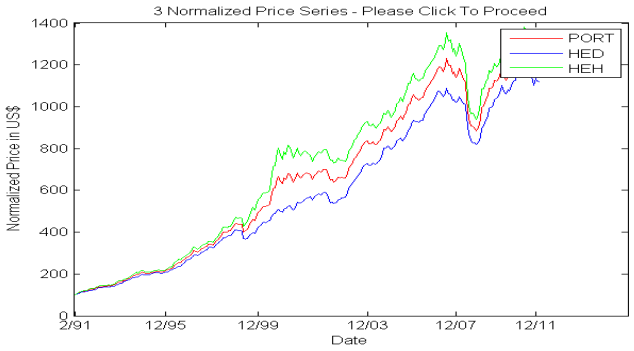
$MVaR_{95\%}$ = -$4,575,377

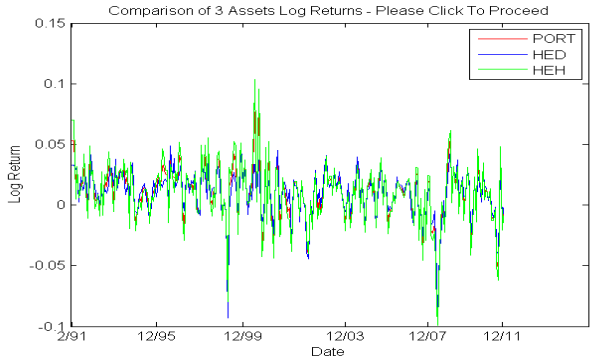


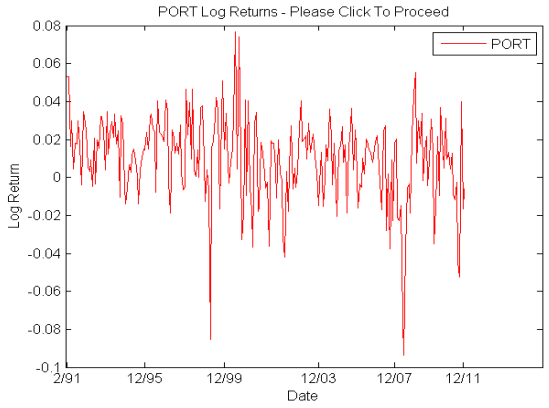
The specific values of various types of VaR and ES within the portfolio categories as well as across the categories are consistent with prior observations and discussions. Minimum Variance portfolio is oriented toward minimization of risk and hence demonstrates the lowest values for each type of VaR and ES relative to other portfolio categories. Maximizing Return portfolio is relatively a riskier portfolio and hence shows higher values for each of VaR types as well as for ES relative to Minimum Variance portfolio. The equally weighted portfolio is sub-optimized as apparent from its lowest Sharpe Ratio of 2.58 as compared with all other portfolio categories shown earlier in Table 5-6: Minimizing Variance portfolio with Sharpe Ratio of 6.75 and Maximizing Return portfolio with Sharpe Ratio of 4.44.

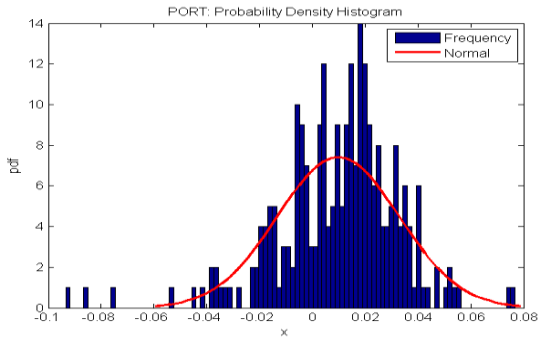
Within each portfolio category, Historical Simulation VaR has the smallest (negative) value (implying least loss), followed by Parametric VaR, Expected Shortfall, and Modified VaR in increasing order of loss. Parametric VaR is limited by its assumption of linear relationships between risk variables (because of exposure to non-linear asset classes such as derivatives) and the assumption of normality about distributions of hedge fund returns. Modified VaR (MVaR) explicitly accounts for the non-normality of hedge fund returns by taking into account skewness and excess kurtosis using the Cornish-Fisher expansion for the z_{α} critical value from the normal distribution for the respective confidence interval c. Table 5-9 shows the results of the Portfolio modeling with the Returns Maximizing portfolio chosen for further advanced analysis using VaR, CVAR, ARCH/GARCH, and EVT.

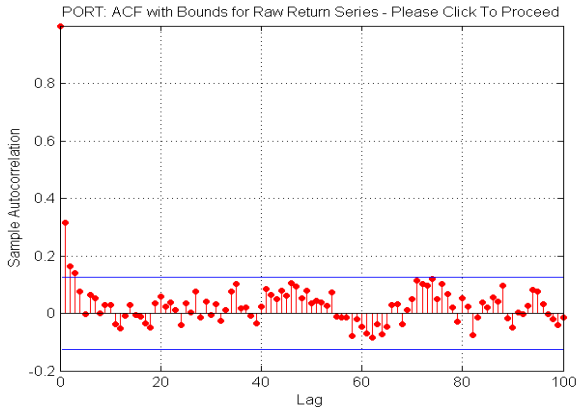
Table 5-9 Portfolio Modeling with the Returns Maximizing Portfolio

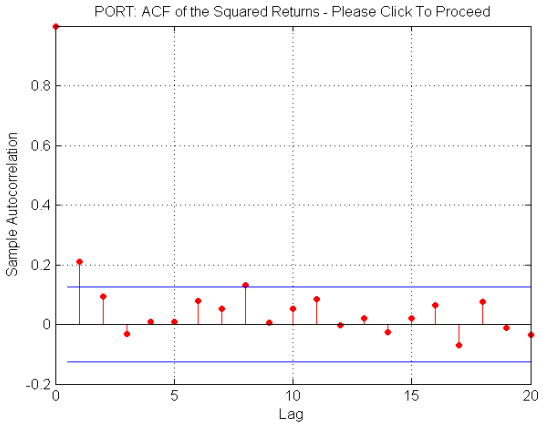


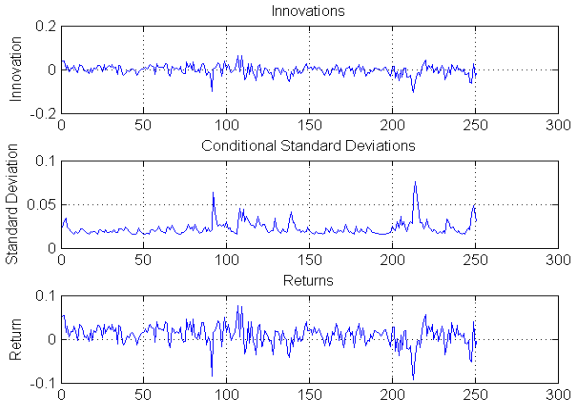












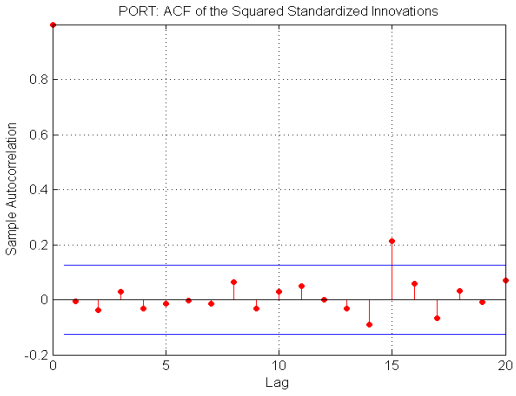
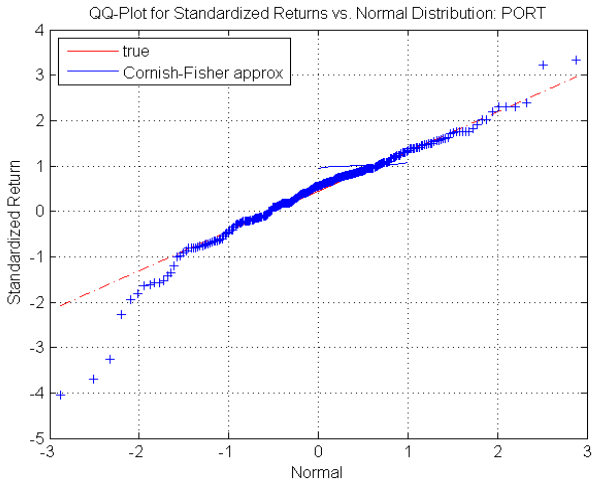
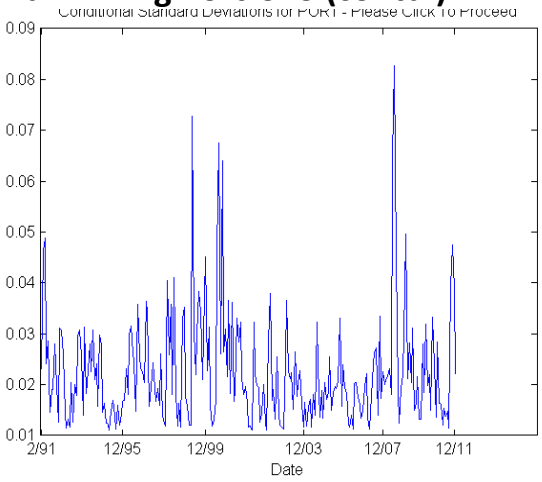
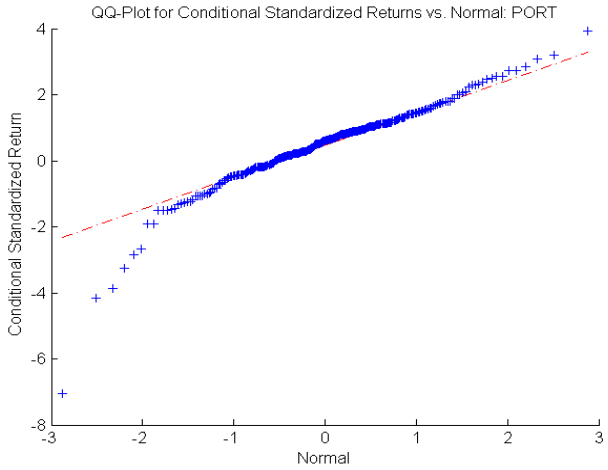
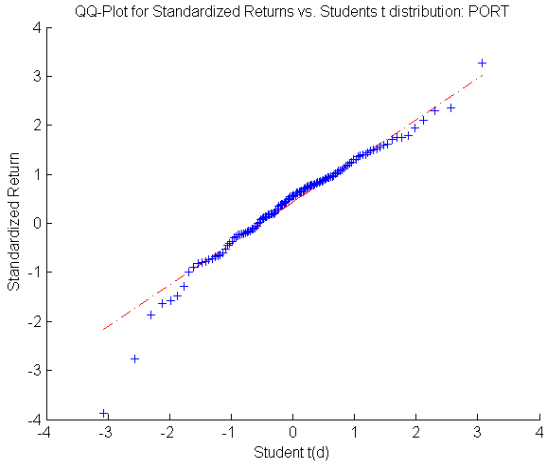


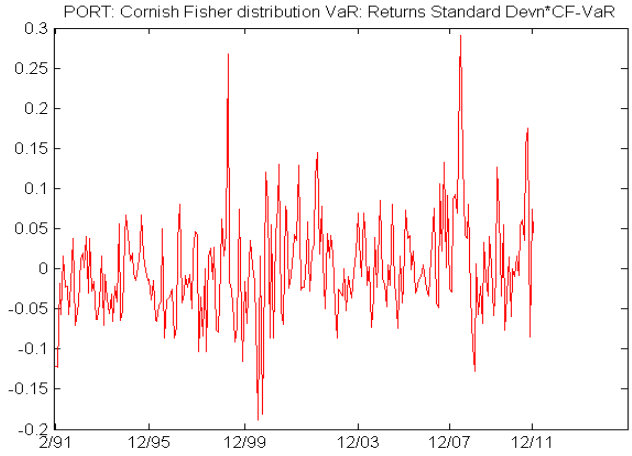
Table 5-9 Portfolio Modeling with the Returns Maximizing Portfolio (contd.)

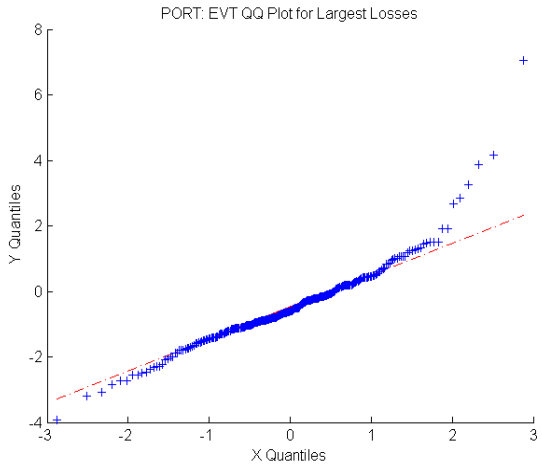












Portfolio PDF histogram shows it to have a negative skew with a long left tail and mass of the distribution concentrated on the right. Raw returns and squared returns show positive autocorrelations for short lags which decay to zero as the number of lags

increases. Presence of heteroscedasticity in previous analysis indicates GARCH modeling is appropriate and model parameters are first estimated with the default GARCH (1,1) model shown in the table. Based upon the model fitting with GARCH, generated residuals (innovations) and conditional standard deviations (sigmas) are examined showing volatility clustering. Standardized innovations show existence of autocorrelations. VaR Models examined include conditional VaR, Cornish-Fisher VaR, and EVT with observed findings shown in the table. Portfolio Cornish-Fisher VaR is found to be about 50% of the sum of individual funds VaRs.

5.11 Summary, Limitations, and, Future Research

Current empirical model risk management research was motivated by ambiguity in recent research between model risk, modeling method (such as VaR), and statistical inference methodology (such as Bayesian). The ambiguity results from confusing choosing one model over another (or, one inference methodology over another) *ipso facto* as elimination of model risks. Such ambiguity may have serious consequences in further escalating *specification* and *estimation* errors in risk modeling. Ambiguity becomes all the more confusing when it is proposed that replacing a modeling method (such as VaR) with an inference methodology (such as Bayesian) will minimize the problems of (model) risk management (Borison & Hamm, 2010). Consistently, the current chapter focused on resolving the *Bayesian vs. VaR* dilemma to minimize model *specification* and *estimation* errors in risk modeling (Boucher et al., 2014).

The focus of the current chapter is *Bayesian vs. VaR* has two related objectives to enlighten concerns about model risk management. First, empirical demonstration of using VaR as *one of multiple risk measures* clearly highlights the empirical application of model risk management in using multiple models, simple and advanced, to cross-check the validity of VaR. In fact, the opening note at the beginning of the chapter by a top investment bank CFO about using VaR as "just one of many measures" is congruent with the empirical model risk management demonstration of the current chapter. Hence, if cyber insurance modelers and users are categorically positive that no systemic risks or tail risks (discussed in prior chapters) are 'material' (discussed in earlier chapter), then they can go ahead and use VaR while ensuring to cross-check its reliability and validity with other measures independent of VaR. In case, they know

that systemic risk and tail risks are of critical importance, they now know how to empirically apply coherent risk measures such as ES (also called as T-VAR, ETL, etc.).

The second set of issues beyond model risk management of a model such as VaR is that of model risk of a methodology (such as NHST, or, Bayesian) as discussed earlier. This second concern about model risk management of classic statistical inference also known as frequentist or NHST methodology is alleviated by offering Bayesian as an alternative methodology for minimizing model risk. Related concern also resulted from observed ambiguity about some practitioners confusion about the model risk related to the model and the methodology. The specific example noted at the beginning of the current chapter is a case in point: a high visibility journal article recommending replacing VaR models with Bayesian models *and* suggesting that it will minimize model risk; VaR research survey that clearly established its practice in *both* non-Bayesian and Bayesian forms since its beginning; and, Bayesian statistical inference modeling survey that clearly *established as critical a need (if not more)* for model risk management *than* is necessary in VaR modeling. Most importantly, the current focus of financial regulators on model risk management in aftermath of the Global Financial Crisis signifies its critical real world import for risk modeling practice.

The above contexts motivated our delineation of research and practice frameworks for both Bayesian inference as well as VaR modeling. Our primary focus on model risk management guided those delineations as well as related discussions. The same focus also guided the choice of our empirical context of demonstrating how model risk management can be applied in real practice for a top Wall Street investment bank *without replacing* 'VaR with Bayesian.' The choice of the frequentist methodology also underscores that it is *neither easy nor inexpensive* to do Bayesian *right* despite its many advantages over the frequentist methodology.

Further, even if the extra effort and (computational) expense is invested in Bayesian, it still doesn't do away with model risk management. In fact, based on the review of Bayesian VaR methodologies (Aussenegg & Miazhynskaia, 2006; Casarin et al., 2013; Danielsson et al., 2014; Hoogerheide & van Dijk, 2008; Meucci, 2009; Miazhynskaia et al., 2003; Osiewalski & Pajor, 2010), it is apparent that the need for model risk management is probably even more. This is not counterintuitive as often

parsimony and transparency of modeling methods and modeling inference methodologies are recommended and preferred for this very reason.

This study has several limitations as choice of any *quantitative* statistical model or methodology entails model risk (Derman, 1996; Morini, 2011). Choosing frequentist inference methodology and VaR models – just like any other methodology and model – results in choosing to 'live with' (*but not at all ignore*) the limitations inherent in *each* such choice. Hence, use of multiple diverse modeling methods and methodologies at various levels of analysis can help cross-check for the various assumptions and boundaries that may not be within scope of one specific methodology or model (Danielsson et al., 2014). Having focused on the specific research for resolving the *Bayesian vs. VaR* dilemma *and* empirically demonstrating its application at a Wall Street bank, subsequent research plans to further address such methodological limitations. Such future research plans to focus on using VaR (and its various extensions including CVAR, ES, and EVT empirically demonstrated herein) as well as other models for analyzing market risk in portfolio construction and optimization. Further, given well-known advantages of Bayesian over frequentist inference (Kruschke, 2011) *as well as* its growing feasibility *with* MCMC (Gelfand & Smith, 1990; Malhotra, 2014), such future research plans to advance on the Bayesian and VaR analytical frameworks proposed herein for empirical analysis of such models.

Appendix 5-1. Bayesian Inference: Probability Background

How likely an event is, the *likelihood* of a specific outcome, is with respect to the *sample space* which is the set of all mutually exclusive (and) cumulatively exhaustive (MECE) possibilities. Specific *parameter* such as bias (i.e., *probability of a specific outcome*) of a process can be denoted as θ so that the *degree of belief about that parameter value* θ is p(θ). The *possibilities sample space* or *outcome events sample space* consists of all MECE possibilities or possible outcome events. The *parameter sample space* consists of all values that the specific parameter can have. If the parameter bias can vary from 0% to 100%, respective parameter sample space consists of all continuous data values between 0 and 1. When a specific process is sampled, it is sampled from the parameter sample space. For the specific parameter sampled, the outcome events are then sampled from the outcome events sample space. For specific outcome events that can be observed, *probability* of occurrence of any specific event is its *long-run relative frequency*. Such long-run relative frequency can be observed by actually sampling from the sample space and tracking counts of different outcomes. Sampling can be done using *computerized simulation* in which the computer generates the outcomes randomly. A long run, being a finite random sample, can only approximate the probability by long-run relative frequency. Or, it can be calculated with greater precision by *deriving it mathematically* based on known properties of the process.

Probabilities are non-negative numbers assigned to the set of MECE possibilities. The probabilities should sum to 1.0 for all MECE possibilities. For two mutually exclusive, i.e., independent events, the probability that one *or* the other occurs equals the sum of respective individual probabilities. *Probability distribution* is the list of all possible MECE outcomes *and* their corresponding probabilities. The probability of discrete outcome value is called *probability mass* to distinguish it from the probability of continuous outcome value which is called *probability density*. If a continuous distribution is discretized then the amount of the probability in a specific interval is given by its probability mass. *Probability density* of an interval is the probability mass of that interval divided by the interval width. For a continuous distribution, since the probability of any specific discrete *exact* infinitesimal point is zero, probability is denoted as *probability density* which is the ratio of the probability to the respective interval width. Hence for a *uniform* scale that is divided into N intervals, the probability of any infinitesimal interval converges to zero in the limit as N grows to infinity. However, its probability

density which is the ratio of probability mass (1/N) to its width (1/N) always remains 1 = ((1/N)/ (1/N)).

Probability mass cannot exceed 1, however probability density being a ratio of probability mass to respective interval width can be lesser or greater than 1. If the uniform interval scale is changed from 0–1 to 0-0.5, then the amount of probability per unit interval width doubles, hence probability density becomes 2 everywhere (((1/N)/ (0.5/N))). In case of a logarithmic scale, every additional unit interval width contains lesser and lesser probability in a smaller interval width thus having exponentially smaller probability density. For instance a log-10 circular scale will contain 1 to 10 (10^0 to 10^1) within the first half, i.e., 0.5 probability mass, and 10 to 100 (10^1 to 10^2) in the second half.

Let continuous variable be denoted as x and interval width by Δx. Let interval index be denoted as i, and the interval between x_i and $x_i+\Delta x$ be denoted as $[x_i, x_i+\Delta x]$. Then,

Probability mass of the i^{th} interval: $p([x_i, x_i + \Delta x])$ and

Sum of probability masses for all the intervals: $\sum_i \; p([x_i, x_i + \Delta x]) = 1.0$

Dividing and multiplying by the interval width Δx: $\sum_i \; \Delta x \; \frac{p([x_i, x_i+\Delta x])}{\Delta x} = 1.0$

As $\Delta x \to 0$, the above equation becomes: $\int \; dx \; p(x) \; = 1.0$ where $p(x)$ is the *probability density*.

Appendix 5-2. Hedge Fund Risk-Adjusted Return Metrics

Tracking Error, or Standard Deviation of Excess Return, is a statistical measure of dispersion measuring volatility of excess returns over a given period (J.P. Morgan, 2008). For each asset class modeled, tracking error was measured in terms of quadratic standard deviation (SD) and linear mean absolute deviations (MAD). The tracking error measures how closely the fund follows the index to which it is benchmarked: lower the error, more closely the fund follows risk-and-return characteristics of the benchmark. While SD being the quadratic form may be more difficult to interpret, its linear alternative MAD seems more intuitive for hedge fund managers who may prefer seeing it in linear terms.

Quadratic Tracking Error

$$SD = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(r_{N-1,N} - r_{N-1,N}^{bm})^2}$$

Linear Tracking Error

$$MAD = \frac{1}{N-1}\sum_{i=1}^{N}|r_{N-1,N} - r_{N-1,N}^{bm}|$$

N = No. of sample data points, $r_{N-1,N}$= Fund return, $r_{N-1,N}^{bm}$ = Benchmark return

Basic performance plots for each asset included historical performance of RoR%, VAMI, and, histogram of monthly returns. Tests for normality of each asset's returns statistical distribution included charts of empirical versus normal distribution and normal Q-Q plots as well as the Jarque-Bera Normality Test which is a joint test of skewnesss and excess kurtosis. Descriptive statistics included the first four moments of distribution. The correlation matrix was computed to show relative strength of variability of returns of the asset classes with respect to each other. Mean-variance optimization (Markowitz, 1952) was used to compute the portfolio asset allocations for minimizing variance and for maximizing returns and then compared with the portfolio with equally weighted asset classes.

Relative risk and returns behavior of different asset classes and robustness in consistency of their behavior was monitored in course of risk modeling using different models. Different risk measures based on varying risk estimation assumptions facilitated stress testing and sensitivity analysis. As risk and returns may not vary proportionally for all indexes or portfolios, their relative performance can be more accurately measured by using *risk-adjusted return measures*. *Risk Adjusted Return* is an ex-post risk measure in which the portfolio return is

adjusted by the standard deviation or beta of the portfolio (J.P. Morgan, 2008). Most commonly used risk-adjusted return measures in the hedge fund industry are based upon the ratio of risk free returns to risk:

$$Risk\ adjusted\ returns = \frac{R_P - R_F}{Risk}.$$

The risk-adjusted return measures help assess the true performance of the hedge fund managers delivering real alpha (reflecting real skill) compared to others delivering sophisticated alternative beta (available at a lower cost) or traditional market beta (available free). Alpha is a measure of performance on a risk-adjusted basis as it takes into consideration the risk-free rate. In current context, it refers to the excess return of the portfolio relative to the return of the benchmark. Beta is a measure of the volatility, or systematic risk, of a fund or portfolio in relation to the overall market. Beta of 1 indicates moment in same direction and by same percentage as the overall market. Beta greater (lesser) than 1 indicates that the fund is expected to move more (less) than the market and hence is more (less) risky. Portfolio Beta is the weighted average of the Betas of the various assets held in the portfolio.

The ratio of annualized first and second moments of distributions is another such measure:

$$M1/M2 = \frac{Return}{Volatility}.$$

In the above computation, R_P is the annualized return while R_F is the annualized risk-free rate (such as for a US treasury bill). *Sharpe ratio* (Sharpe, 1994) uses the volatility of returns σ_P as the measure of risk:

$$Sharpe\ Ratio = \frac{R_P - R_F}{\sigma_P} = \frac{Return\ -Risk\ Free\ Return}{Standard\ Deviation\ Of\ Returns}.$$

Also known as the "reward to variability ratio, it relates the reward to the portfolio's risk, as measured by the portfolio's standard deviation (J.P. Morgan, 2008). By using the standard deviation, Sharpe Ratio measures the total risk of the portfolio, not just risk in relation to the market. As compared with prior measure M1/M2, Sharpe Ratio introduces a static benchmark to the numerator by subtracting the risk-free rate from the return. Sharpe ratio thus penalizes the fund manager whose return is lower than risk-free rate and shows negative Sharpe ratio for managers delivering returns lower than the risk-free rate.

The *Modified Sharpe Ratio* introduced earlier in the discussion on MVaR accounts for the third and fourth moments of the returns (and P&L) distribution, skewnes and excess kurtosis, and is given by:

$$\text{MSR} = \frac{R_P - R_F}{\text{MVaR}_{1-\alpha}} = \frac{Return\ -Risk\ Free\ Return}{Modified\ VaR}.$$

The *Sortino Ratio* (Sortino & Forsey, 1996) modifies Sharpe Ratio so that the fund manager is penalized only for downside risk (volatitlity) but not for upside volatility which enhances returns. It uses the concept of the minimum acceptable return (MAR). It divides the returns into those that are greater than MAR and those that are less than MAR. Higher Sortino ratio implies that the manager is better at controlling downside risk and is not penalized for producing high upside returns.

$$Sortino\ Ratio = \frac{R_P - MAR}{\sqrt{\frac{1}{T}\sum_{t,R_P<MAR}^{T}\left(R_{P,t} - MAR\right)^2}} = \frac{Return\ - Risk\ Free\ Return}{Negative\ Semi - Deviation\ of\ Returns}.$$

The *Drawdown Ratio*, another variant of Sharpe Ratio, uses maximum historical drawdown as the risk measure.

$$DD\ Ratio = \frac{R_P - R_F}{|\max DD|}.$$

Maximum drawdown is defined as maximum loss in VAMI or NAV terms from the preceding highest high to the lowest low during the period that the fund has not recovered its value to the last highest high. Variants of Drawdown Ratio include the *Sterling Ratio* which uses an average of the most significant drawdowns and the *Burke Ratio* which uses the square root of the sum of the squares of each drawdown. The key idea in both the variations is about penalizing significant long-term drawdowns relative to several milder drawdowns.

The *Information Ratio* (Goodwin, 1998) measures a portfolio's performance against risk and return relative to a benchmark or alternative measure. The higher the Information Ratio, the greater the added value for a given level of risk, relative to the benchmark. Information Ratio uses a market reference benchmark instead of the risk-free rate. Thus, greater added value for a given level of risk, relative to the benchmark, i.e. excess returns on a benchmark portfolio B in period t, can be described as:

$\Delta_t = R_{P,t} - R_{B,t}$ and their arithmetic average from t = 1 to T is given by: $\bar{\Delta} = \frac{1}{T}\sum_{t=1}^{T}\Delta_t$. Then, standard deviation of the excess returns from the benchmark is given by $\sigma_\Delta = \sqrt{\frac{1}{T}\sum_{t=1}^{T}(\Delta_t - \bar{\Delta})^2}$. Then,

$$Information\ Ratio = \frac{\bar{\Delta}}{\sigma_\Delta} = \frac{Excess\ Return}{Std.\ Devn.\ of\ Tracking\ Error}\ .$$

The *M-Squared Metric* helps see how the hedge fund outperforms the benchmark return to which it has had its risk profile matched. It does so by interpreting the fund's return as the

return that would have been produced had the fund's volatility been equal to that of the market benchmark.

$$M^2 = \frac{\sigma_M}{\sigma_P}(R_P - R_F) - R_F \ .$$

The *Treynor Ratio*, also known as the "reward to volatility ratio," measures the excess return achieved by a fund manager per unit of risk incurred (J.P. Morgan, 2008). Based on systematic risk, it uses the beta of the fund relative to a benchmark as the risk measure in the denominator:

$$Treynor\ Ratio = \frac{R_P - R_F}{\beta_P}.$$

Treynor Ratio, just like Information Ratio, is more commonly used for active traditional equity portfolios.

Jensen's Alpha (Jensen, 1967) is used to determine the Excess Return over the required rate of return as predicted by the Capital Asset Pricing Model (CAPM) given the portfolio's beta and the average market return (J.P. Morgan, 2008). It is the sum of risk-free rate and beta adjusted market excess returns subtracted from fund's net return:

$\alpha_P = R_P - [R_F + \beta_P (R_M - R_F)]$ based upon CAPM: $(R_P - R_F) = \alpha_P + \beta_P (R_M - R_F)$.

The above expression highlights the three parts that make up a hedge fund return: alpha (measurable skill), beta continuum (from skill to no skill) (Anson 2008) and the risk-free rate (no skill).

Jensen's Alpha Ratio (J.P. Morgan, 2008) is a risk-adjusted performance measure that represents the average return on a portfolio over and above that predicted by the Capital Asset Pricing Model (CAPM), given the portfolio's beta and the average market return (Jensen's Alpha).

$$\textit{Jensen's Alpha Ratio} = \frac{Average\ Jensen's\ Alpha}{Std.\ Devn.\ of\ Jensen's\ Alpha} \ .$$

Appendix 5-3. Value Added Monthly Index (VAMI) Method

The VAMI method generally assumes an initial investment of $100 or $1,000 and shows how such an investment would have fared over a certain period of time. In order to calculate annual ROR using VAMI, first calculate value of the investment at end of each subperiod or month. The following example from National Futures Association (2013) assumes initial investment of $1,000.

Annual and Year-to-Date Rates of Return

In first month of the period: VAMI for month = (1 + ROR for month) x 1000 For all subsequent months: VAMI for month = (1 + ROR for month) x VAMI for prior month

Annual ROR calculated as follows:

Annual ROR = (year-end VAMI - $1,000) divided by $1,000. When calculating the annual RORs for subsequent years, the value of the initial investment should be the prior year-end VAMI.

Computing Monthly and Peak-to-Valley Draw-Downs

Draw-down means losses experienced by a pool or trading program over a specified period.

Worst monthly draw-down is the program's worst monthly percentage ROR.

Worst peak-to-valley draw-down is the largest cumulative percentage decline in month-end net asset value (NAV) due to losses sustained by the accounts during any period in which the initial month-end NAV is not equaled or exceeded by a subsequent month-end NAV. To calculate this amount, calculate a continuous VAMI for the time period presented. Using this method, determine the first month in which the VAMI is not followed by a VAMI that is greater than or equal to that month's VAMI. This would be seen as the first peak. The next peak is seen for the next month in which VAMI is greater than the previous peak's VAMI and followed by a lower VAMI. Once all the peaks are identified, determine all months having the lowest VAMIs during a period between two peaks which would be the valleys. Determine the percentage change between each peak and valley as follows:

(Valley VAMI – Peak VAMI) divided by Peak VAMI

The worst peak-to-valley draw-down is the largest percentage change from a peak to a valley. The peak month and the valley month should be reported.

Chapter 6.

Markov Chain Monte Carlo for Bayesian

> "[T]he development of this methodology has not only changed our solutions to problems, but has changed the way we think about problems."
> -- Robert & Cassella, A Short History of Markov Chain Monte Carlo, *Statistical Science*, 26(1), 2011.

6.1 Markov Chain Monte Carlo Models, Gibbs Sampling and Metropolis-Hastings Statistical Computing Algorithms

In this chapter, we develop an analysis of the Markov Chain Monte Carlo Models, Gibbs Sampling and Metropolis-Hastings statistical computing algorithms for enabling Bayesian statistical inference methodologies to minimize model risk in cyber risk and cyber Insurance modeling for the specific context of cybersecurity.

Markov chain Monte Carlo (MCMC) methods have an important role in solving high-dimensionality stochastic problems characterized by computational complexity. Given their critical importance, there is need for network and security risk management research to relate the MCMC quantitative methodological concerns with network and security risk applications. This article contributes to that research stream. The core quantitative methodological focus of the article is on Monte Carlo Models and MCMC Algorithms, Gibbs Sampling and Metropolis-Hastings Algorithm. Network and security risk management application focus is on how MCMC methods help solve previously unsolvable problems in computational statistical modeling of cryptography, cryptanalytics, and penetration testing; intrusion detection & prevention and anomaly detection; and, privacy in anonymity systems and social networks. Future quantitative methods applied research and development in MCMC and computational statistical computing to address systemic risk and model risk management is recommended.

6.2 Markov chain Monte Carlo (MCMC) Methods

Markov chain Monte Carlo (MCMC) is widely used for solving complex problems related to probability distribution integration and combinatorial optimization

(Beichl & Sullivan 2000). It is perhaps the only known general quantitative method that can find approximate solutions to complex problems in polynomial time in some contexts (Jerrum & Sinclair 1996). MCMC methods such as Gibbs sampling (Geman & Geman 1984) and Metropolis-Hastings algorithm (Metropolis et al. 1953, Hastings 1970) have influenced multiple fields of research and practice including computer science, physics, statistics, finance, economics, and engineering (Beichl & Sullivan 2000, Eraker 2001, Gilks et al. 1996). Beichl and Sullivan (2000) describe Metropolis-Hastings algorithm of which Gibbs Sampling is a special case as one of 'top 10 algorithms' in computing and 'the most successful and influential of Monte Carlo method': "Today, topics related to this algorithm constitute an entire field of computational science supported by a deep theory and having applications ranging from physical simulations to the foundations of computational complexity."

MCMC algorithms have an increasingly important and growing role in network and computer security and cybersecurity, analysis of adversary attacks, penetration testing, and information assurance research and practices. Our review of research establishes increasing relevance of MCMC, Gibbs Sampling, and Metropolis Algorithm in network and computer security contexts spanning cryptography and cryptanalytic password attacks and authentication analysis (e.g. Chen & Rosenthal 2012, Diaconis 2009, Hanawal & Sundaresan 2010, Muramatsu et al. 2006, Furon et al. 2012, Matsui et al. 2004), signature and anomaly based network intrusion detection and prevention systems (e.g. Scott 1999, 2001, 2004; Zhao & Nygard 2010, Ihler et al. 2006, Jyothsna et al. 2011, Shi & Mei-Feng 2012), and analyzing potential vulnerabilities in anonymity based systems such as Tor network based on onion-routing protocol and other 'social networks' (e.g. Danezis and Troncoso 2009, Troncoso and Danezis 2009).

There also seems growing interest among the broader network and computing security researcher and practitioner communities to develop better grasp of sophisticated quantitative methods such as Bayesian inference and MCMC methods. An example of such interest is evident in the community dialog on cryptography and encryption: 'Schneier on Security' blog on the topic 'TSA Uses Monte Carlo Simulations to Weigh Airplane Risks'.[151] In response to a debate among the readers on his blog about Monte Carlo methods, the renowned cryptography and encryption expert Bruce Schneier acknowledged his own interest in knowing more about Monte Carlo methods.

[151] https://www.schneier.com/blog/archives/2007/06/tsa_uses_monte.html

Despite tomes of research published on the topic over last 60 or so years, palpable interest among mainstream researchers and practitioners is understandable. Most research published on Monte Carlo and MCMC methods has grown out of mathematical physicists', mathematicians', and statisticians' academic research characterized by understandable disciplinary formalism and diverse notational styles. Hence, there seems to be a critical need for research to bridge theory and practice by spanning disciplinary formalism of mathematicians and statisticians with applied concerns of network and computer security researchers. The current chapter with quantitative methods focus in the context of network and computer security contributes to that research stream aiming to further advance research and practice in MCMC methods.

After the above introduction outlining increasingly important role of MCMC in network and computer security, the remaining sections of the discussion proceed as follows. Next section provides an overview of how these sophisticated quantitative methods came to be known as a 'revolution' and 'quantum leap' in statistical computing. Subsection section on Markov chain Monte Carlo Models and MCMC Algorithms forms the core focus of this article with its quantitative methods focus for readers new to these methods. It develops a technical introduction to Markov chain Monte Carlo Models and MCMC Algorithms, Gibbs Sampling and Metropolis-Hastings Algorithm based upon analysis and synthesis of research. Section thereafter on applications of MCMC methods in network and computer security provides an overview of examples from network and computer security research. Readers interested in MCMC methods can relate to specific instances from their own research or practice and may consider applying those methods in their own work. The final section concludes with a discussion of key benefits of MCMC methods and algorithms in network and computer security and underscores the need for future research on systemic risk management issues including model risk management.

6.3 MCMC: A Revolutionary Leap in Statistical Computing

A paper on the history of MCMC interestingly observes about MCMC that (Robert & Cassella 2011a, 2011b emphasis added): "the development of this methodology has *not only changed our solutions to problems*, *but has changed the way we think about problems*." The MCMC methods originally conceptualized in 1940s at the Los

Alamos National Lab during World War II led to the Metropolis algorithm, the first key MCMC algorithm in the early 1950s (Metropolis et al. 1953). The MCMC was the result of research by the same group of research scientists as those working on the atomic bomb including Stanislaw Ulam and John von Neumann at Los Alamos who around the same time had also created Monte Carlo (MC) methods (Eckhardt 1987). John von Neumann was using MC to study thermonuclear and fission problems in the late 1940s after the first computer, ENIAC, was developed. For high-dimensionality numerical problems, MC methods, though more efficient than conventional numerical methods, may require sampling from high-dimensionality probability distributions often making them infeasible and inefficient in practice given computational complexity (Hastings 1970). Affected problems in combinatorics, data mining, machine learning, numerical analysis, and sampling show exponential increase in multi-dimensional space with increased high-dimensionality. Resulting sparseness of data is problematic as data needs grow exponentially with increased dimensionality for doing tests of statistical significance. To solve such problems, Hastings (1970), followed by Peskun (1973, 1981), generalized the Metropolis algorithm as a statistical simulation method for overcoming the 'curse of dimensionality'. In particular, as Bayesian inference based on posterior distributions with many parameters compounds the curse of dimensionality, MCMC has a particularly important role in advancing simulation-based Bayesian inference.

MCMC represents a 'quantum leap' in computational statistics (Robert & Cassella 2011) that shifts the emphasis from "closed form" solutions to improved numerical algorithms for solving "real" applied problems where "exact" now means "simulated." Since late 1980's, MCMC has become an all-pervasive method in statistical computation especially for Bayesian inference and for analyzing complex stochastic systems (Green 2014). The power of MCMC particularly in the context of Bayesian inference, besides other areas of computational statistics, results from two key flexibilities it affords for modeling and inference. First, MCMC allows the analyst to be closer to the reality of the process generating the data in terms of analysis as being well-suited for models based upon sparse data. It thus liberates the modeling process from constraints related to the curse of dimensionality. Second, on a related note, it also liberates the modeling process from dimensionality related constraints that earlier limited features of the target distribution to be modeled. The 'revolutionary' Gelfand and Smith paper (1990), one of top-three most cited papers in mathematics in last 20 years (Holmes 2008), is considered as "the genuine starting point for an intensive use of

MCMC methods by the mainstream statistical community." Given necessary computing power and statistical computing algorithms such as the Gibbs sampler and the Metropolis–Hastings algorithm, it represented a 'paradigm shift' of interest in Bayesian methods, statistical computing, algorithms and stochastic processes (Robert & Cassella 2011). MCMC is an instance of revolutionary statistical computing methods enabled by computing advances that dramatically increase our ability to solve highly complex problems using statistical inference across multiple domains. MCMC models enable us to make statistical inferences that were infeasible just a few years ago (Tsay 2010).

The above introductory overview of MCMC developed a perspective of how and why MCMC methods and algorithms came to be known as a 'revolution' and 'quantum leap' in statistical computing. The following section develops a technical introduction to the Markov chain Monte Carlo Models and the MCMC Algorithms, Gibbs Sampling and Metropolis-Hastings Algorithm based upon analysis and synthesis of prior research.

6.4 Markov chain Monte Carlo Models and Algorithms

Markov Process, Monte Carlo, and Markov chain Monte Carlo Models

The Metropolis algorithm is an example of a MCMC process (Kruschke 2010). To understand MCMC, we need to recognize what is a Markov chain as well as what is a Monte Carlo process. *Random walk* is a mathematical formalization of a succession of *random* steps as in steps taken by the proverbial drunk which have equal probability of going to each of the available next steps. For a given step or position, the probabilities of transition or *transition probabilities* to any next step depend only on the current step and next steps and are independent of prior events and steps.

A *Markov chain* is a succession of random steps (from one state to another) characterized by the Markov property of being 'memory-less.' It is memory-less in the sense that each next random step has no memory of, i.e., is totally independent of, all prior states (as well as prior sequence of steps and events) except for the current state from which it moves to the next state. Such a process characterized by the Markov property is called a *Markov process*.

Monte Carlo simulation is a simulation based upon repeated sampling of a lot of random input values from a distribution of inputs to assess the properties of the target outputs distribution by generating representative random values. Hence, it is a quantitative method of translating uncertainties in input variables as represented by

their probability distributions to uncertainties of outcome variables represented by their probability distributions. Resulting quantified probabilities of specific outcomes form a probability distribution of predicted outcomes resulting from propagation or translation of input uncertainties into outcome uncertainties (GoldSim 2014). The Metropolis algorithm is a specific type of a Monte Carlo process (Kruschke 2010).

Bayesian forecasting with MCMC methods is a natural way to consider parameter and model uncertainty in forecasting (Tsay 2010). Considering above concepts, in statistical terms, it is useful to think of a stochastic process $\{X_t\}$ where each observed data X_t assumes a value in the parameter space Θ (Tsay 2005, 2010). The *Markov process* $\{X_t\}$ with memory-less property is one for which given value of X_t, values of X_h, $h > t$, do not depend on values of X_s, $s < t$. Such a Markov process $\{X_t\}$ has the following conditional distribution function (Tsay 2005, 2010):

$$P(X_h \mid X_s, s \leq t) = P(X_h \mid X_t),\ h > t$$

For a discrete time stochastic process $\{X_t\}$, the above property will become:

$$P(X_h \mid X_t, X_{t-1}, \ldots) = P(X_h \mid X_t),\ h > t$$

Expressed differently, the stochastic process $X = \{X_0, X_1, X_2, \ldots X_T\}$ is a *Markov process* because for all $t = 0, 1, \ldots, T-1$, $f(X_{t+1} \mid x_t, x_{t-1}, \ldots, x_0) = f(X_{t+1} \mid x_t)$, i.e., a sequence $X_0, X_1, \ldots$ of random elements of some set is a *Markov chain* if the conditional distribution of X_{t+1} given $x_t, x_{t-1}, \ldots, x_0$ depends on x_t only. The set in which X_t assumes values is called the *state space* of the Markov chain (Geyer 2011). Further, a *stochastic process* X is a random variable X (t, ω), a function of both time t and state ω, for any $\omega \in \Omega$. For stochastic process $X = \{X_0, X_1, X_2, \ldots X_T\}$, if the change process of X is given by: $C_1 = X_1 - X_0$, $C_2 = X_2 - X_1, \ldots, C_T = X_T - X_{T-1}$, then the stochastic process X is called a *martingale* if $E(C_{t+1} \mid x_t, x_{t-1}, \ldots, x_0) = 0$, or equivalently,

$E(X_{t+1} \mid x_t, x_{t-1}, \ldots, x_0) = x_t$ for all $t = 0, 1, \ldots, T-1$. The stochastic process X with the same change process is called a *random walk* if $C_1, C_2, \ldots, C_T$ are independent and identically distributed (i.i.d.) with $E(|C_t|) < \infty$ for all $t = 0, 1, \ldots, T$.

Following from (1) and (2) above, if A is a subset of parameter space Θ, the *transition probability function* of the above Markov process will be expressed as follows to connote the transition of X_i from time t to time h (Tsay 2005, 2010).

$$P_t(\theta, h, A) = P(X_h \in A \mid X_t = \theta),\ h > t$$

The above Markov process is said to have a *stationary distribution* if the transition probability depends upon incremental change in time, $h - t$, but not on specific time t.

Hence, a Markov chain has *stationary transition probabilities* if the conditional distribution of X_{t+1} given x_t does not depend on t: this is the primary type of Markov chain of interest for MCMC models (Geyer 2011). A Markov model whose elements follow a Markov chain with stationary transition matrix is called a *Hidden Markov Model* (HMM). HMM, a mixture model with mixing distribution as a finite state Markov chain, assumes that the distribution of an observed data point depends upon an unobservable or *hidden* state.

To make statistical inference for a parameter vector θ and data X, where $\theta \in \Theta$, the distribution $P(\theta|X)$ needs to be determined. To use Markov chain simulation for doing so, we need to simulate a Markov process on parameter space Θ, which converges to a stationary distribution $P(\theta|X)$. The key to finding such convergence is to use a Markov chain with stationary distribution pre-specified as $P(\theta|X)$ and run it until it results in approximate convergence of distribution of current values with the stationary transition distribution (Tsay 2005, 2010). For some transition probability distribution, the initial distribution is said to be *stationary* or *equilibrium* if the Markov chain specified by it and the transition probability distribution is stationary. This can be re-stated as (Geyer 2011): 'the transition probability distribution preserves the initial distribution'. The result will be the determination of many Markov chains that have the desired property noted above. Such Markov chain simulation methods used for determining the stationary distribution $P(\theta|X)$ are known as MCMC methods as they make combined use of Markov chain processes and Monte Carlo simulations.

Monte Carlo approach developed at Los Alamos prior to MCMC was devised as a method for using random number generation for computing complex integrals (Walsh 2004). A complex integral such as $\int_a^b h(x)dx$ is expressed as product of function $f(x)$ and probability density function $p(x)$ is: $\int_a^b f(x)\, p(x)dx$. That product expressed as the expectation of $f(x)$ over density $p(x)$, $E_{p(x)}\,[f(x)]$, can be approximated as the average of the summation of function $f(x)$ over a large number of random variables $x_1,\ldots, x_n$ from density $p(x)$. Mathematically,

$$\int_a^b h(x)dx = \int_a^b f(x)\, p(x)dx = E_{p(x)}\,[f(x)] \approx \frac{1}{n}\sum_{i=1}^{n} f(x_i)$$

The above method known as *Monte Carlo integration* is used in Bayesian inference to approximate posterior or marginal posterior distributions. Extending above computation to a conditional function such as $f(y|x)$ results in an analogous simplification of the integral expression in the context of Bayesian inference:

$$I(y) = \int f(y|x)p(x)dx \approx \frac{1}{n}\sum_{i=1}^{n} f(y|x_i)$$

6.5 Gibbs Sampling Algorithm

Influenced by the 'landmark paper' (Robert & Cassella 2011a, 2011b) of Geman and Geman (1984) that developed Gibbs Sampling, Gelfand and Smith (1990) advanced Gibbs Sampling into perhaps the most popular MCMC method (Tsay 2010). Gibbs sampler is the MCMC technique used for generating random variables from a marginal distribution indirectly without the need for calculating the distribution density (Casella & George, 1992). The key advantage of Gibbs sampling is in decomposing high-dimensional estimation problems such as in complex stochastic models into lower-dimensional simpler and more manageable form problems using full conditional distributions of the parameters (Scollink 1996). An extreme example of its use is in the solution of a complex multivariate stochastic model with N parameters (i.e., N-dimensions) using N univariate (i.e., one-dimensional) conditional distributions. When parameters are highly correlated, it may be advisable to use joint draws as it may not be efficient to reduce Gibbs draws into univariate problems (Kruschke 2010, Tsay 2010).

Consistent with Walsh (2004), Tsay (2010) explains Gibbs sampling in the context of estimation of parameters so that the fitted model can be used for making inference. Consider three parameters θ_1, θ_2, and θ_3 for a collection of observed data X and M as the contemplated model to be fitted. Here the word *parameter* is used very generally. For instance, in MCMC framework, a parameter may denote a missing data point or an unobservable latent or "true" variable underlying the observed variable. Following Casella & George (1992) and Scollink (1996), assume that the three conditional distributions of any parameter θ_i given the others are available for θ_1, θ_2, and θ_3 but the likelihood function of the model cannot be analytically or numerically computed. (In statistics, *likelihood function* (or likelihood) of a set of parameter values θ_i, given observed data X_i, is the probability of those observed variables given the respective parameter values, i.e., $L(\theta|X) = P(X|\theta)$.) Statistically, $f_1(\theta_1|\theta_2, \theta_3, X, M)$, $f_2(\theta_2|\theta_3, \theta_1, X, M)$, $f_3(\theta_3|\theta_1, \theta_2, X, M)$ denote the three conditional distributions for θ_1, θ_2, and θ_3. Generally, $f_i(\theta_i|\theta_{j\neq i}, X, M)$ represents the conditional distribution of parameter θ_i given the other two parameters θ_j and θ_k, the data X, and the model M. In practice, the exact form of the conditional probability distribution function doesn't need to be known; we

should be however able to draw a random number from each of the relevant conditional distributions.

Assume notation $\theta_{a,b}$ wherein a= probability distribution, and, b = specific numeric order or sequence of the draw from that distribution. Then, the computational logic of one iteration of the Gibbs sampling algorithm given arbitrary initial values for θ_2 and θ_3 being $\theta_{2,0}$ and $\theta_{3,0}$ is listed below (Tsay 2010).

a. Draw a random sample from $f_1(\theta_1 | \theta_{2,0}, \theta_{3,0}, X, M)$ denoting random draw as $\theta_{1,1}$.
b. Draw a random sample from $f_2(\theta_2 | \theta_{3,0}, \theta_{1,1}, X, M)$ denoting random draw as $\theta_{2,1}$.
c. Draw a random sample from $f_3(\theta_3 | \theta_{1,1}, \theta_{2,1}, X, M)$ denoting random draw as $\theta_{3,1}$.

At end of the first iteration of draws from each distribution, the parameters $\theta_{1,0}$, $\theta_{2,0}$, and $\theta_{3,0}$ become $\theta_{1,1}$, $\theta_{2,1}$, and $\theta_{3,1}$. Using the updated parameters as input, the second iteration results in updated parameters as $\theta_{1,2}$, $\theta_{2,2}$, and $\theta_{3,2}$. Repetition of the iteration m times will yield the following sequence of random draws: $(\theta_{1,1}, \theta_{2,1}, \theta_{3,1}), \ldots, (\theta_{1,m}, \theta_{2,m}, \theta_{3,m})$. By taking large enough *m*, i.e., simulating a large enough sample, the m^{th} draw, $(\theta_{1,m}, \theta_{2,m}, \theta_{3,m})$ (under some weak regularity conditions requiring prior Gibbs iteration's traversal of full parameter space (Tsay 2010)) is approximately equivalent to a random draw from the joint probability distribution of the three parameters, $f(\theta_1, \theta_2, \theta_3 | X, M)$. For real application, Tsay (2010) recommends using sufficiently large *n* and dropping first *m* random draws (called *burn-in* sample) from the Gibbs iterations yielding the final Gibbs sample: $(\theta_{1,m+1}, \theta_{2,m+1}, \theta_{3,m+1}), \ldots, (\theta_{1,n}, \theta_{2,n}, \theta_{3,n})$. Prior *m* random draws are dropped to ensure that the final residual sample converges as close as possible to a random sample from the joint distribution $f(\theta_1, \theta_2, \theta_3 | X, M)$. The final Gibbs sample being close enough to the random sample from the joint distribution can then be used for computation, for example, of point estimate and variance (Tsay 2010, Walsh 2004).

Metropolis Algorithm

Originally, attempts to integrate very complex functions using random sampling by mathematical physicists' such as Metropolis & Ulam (1949), Metropolis et al. (1953), and, Hastings (1970) led to development of MCMC methods and Metropolis-Hastings algorithm. Those attempts were aimed at resolving the problems inherent in obtaining samples from complex probability distributions while applying Monte Carlo integration.

Consistent with Walsh (2004), Tsay (2010) considers the case of the conditional probability distribution $p(\theta|X) = f(\theta|X)/K$ (where K is the normalizing constant) for which it is infeasible or very time intensive to compute the normalization constant or

for which random draws are unavailable. Given an approximation of that distribution for which random draws are feasible, the Metropolis algorithm (Metropolis & Ulam 1949, Metropolis et al. 1953) generates a sequence of random draws from it whose distributions converge to $f(\theta|X)$ as follows (Walsh 2004, Tsay 2010, Kruschke 2010).

a. Start with a random draw of some initial value θ_o: $f(\theta_o|X) > 0$.
b. Given previous draw θ_{t-1} for the t^{th} iteration, draw a candidate sample θ_* from a known distribution and call it *jumping distribution* $J_t(\theta_t|\theta_{t-1})$, also known as *proposal distribution* or *candidate-generating distribution* (Gelman et al. 2003). The jumping distribution denoting the probability of returning value of θ_t given previous value of θ_{t-1} must be symmetric, i.e., $J_t(\theta_i|\theta_j) = J_t(\theta_j|\theta_i)$ for all θ_i, θ_j, and t.
c. Given candidate sample θ_*, calculate the ratio r of the density at the candidate point θ_* and at the current point θ_{t-1}: $r = p(\theta_*|X) / p(\theta_{t-1}|X) = f(\theta_*|X) / f(\theta_{t-1}|X)$. As the ratio $f(\theta_i|X)$ is being computed for the same probability distribution with two different i-values, the normalization constant K cancels out in both the numerator and the denominator. That is how MCMC Metropolis algorithm resolves the original problem of computing the normalization constant that motivated the discussion.
d. If the jump from θ_{t-1} to θ_* *increases* the conditional posterior density, i.e., $r > 1$, accept the candidate point θ_* as θ_t, i.e., set $\theta_t = \theta_*$ and return to step b. If the jump *decreases* the conditional posterior density, i.e., $r < 1$, accept the candidate and set $\theta_t = \theta_*$ with probability r; else reject it, i.e. set $\theta_t = \theta_{t-1}$, and return to step b.

As per Walsh (2004), the Metropolis algorithm can be summarized in terms of first computing the acceptance probability of candidate as $r = \min [f(\theta_*|X) / f(\theta_{t-1}|X), 1]$ and then accepting a candidate point with probability r called the *probability of the move* to the proposed position, $p_{move} = \min [P(\theta_{proposed}) / P(\theta_{current}), 1]$ (Kruschke 2010). This generates a Markov chain $(\theta_0, \theta_1, \ldots, \theta_k, \ldots)$, as the transition probabilities from θ_t to θ_{t+1} depend only on θ_t and not on $(\theta_0, \ldots, \theta_{t-1})$. Following a sufficient burn-in period of say prior m of n steps, the chain approaches its stationary distribution, and then the samples from the vector $(\theta_{m+1}, \ldots, \theta_n)$ are the samples from $p(\theta|X)$.

6.6 Metropolis-Hastings Algorithm

Hastings algorithm (Hastings 1970, Tsay 2010) based upon generalization of the Metropolis algorithm uses an arbitrary transition probability function $J_t(\theta_i|\theta_j) = \Pr(\theta_i \rightarrow \theta_j)$. Correspondingly, it calculates the ratio r of the density at the candidate point θ_* and at the current point θ_{t-1}: $r = (f(\theta_*|X) / J_t(\theta_*|\theta_{t-1})) / (f(\theta_{t-1}|X) / J_t(\theta_{t-1}|\theta_*))$

$$= (f(\theta_*|X)\ J_t(\theta_{t-1}|\theta_*)) / (f(\theta_{t-1}|X)\ J_t(\theta_*|\theta_{t-1}))$$

It also sets acceptance probability of the candidate point (Hastings 1970, Walsh 2004):

$r = \min [(f(\theta_* | X) / J_t(\theta_* | \theta_{t-1})) / (f(\theta_{t-1} | X) / J_t(\theta_{t-1} | \theta_*)), 1]$

$= \min [(f(\theta_* | X) J_t(\theta_{t-1} | \theta_*)) / (f(\theta_{t-1} | X) J_t(\theta_* | \theta_{t-1})), 1]$

As apparent, the Hastings algorithm represents a more general case of the Metropolis algorithm: when jump density is symmetric, i.e., $J_t(\theta_i | \theta_j) = J_t(\theta_j | \theta_i)$, it reduces to the original Metropolis algorithm. The modified algorithm is known as the *Metropolis-Hastings algorithm* which is very general and broadly applicable. A caveat about the Metropolis-Hastings algorithm is that the algorithm's convergence to a solution is contingent upon the availability of a fine-tuned proposal distribution. Otherwise, if the proposal distribution is too narrow or too broad, greater proportion of the proposed jumps will be rejected or the move will be restricted to a narrow localized parameter space. Gibbs sampling, in contrast, is more forgiving as it does not require 'artful tuning' of a proposal distribution (Kruschke 2010).

The above discussion on Monte Carlo Models and MCMC Algorithms, Gibbs Sampling and Metropolis-Hastings Algorithm developed the core quantitative methodological focus of this article. Next section develops an understanding of how network and computer security research and practice represent increasingly important domains for application of above research methods based upon MCMC algorithms and Bayesian inference. The following discussion also provides specific examples from three key domains of network and computer security research wherein solutions to complex high-dimensional stochastic problems relied upon creative applications of MCMC.

6.7 MCMC Models in Computer & Network Security

The following review of research establishes increasing importance of MCMC, Gibbs Sampling, and Metropolis Algorithm in three key contexts of network and computer security research and practice. Related discussion on application of MCMC methods in network and computer security highlights selective examples from network and computer security research. The discussion is illustrative given the methodological focus of the article. Focus is on demonstrating through specific examples how MCMC methods and MCMC algorithms are applied in practice in the given contexts. The three specific contexts of network and computer security research that are the focus of the following research methods discussion on MCMC are listed below.

(1) Cryptography, Cryptanalytics & Penetration Testing

(e.g. Chen & Rosenthal 2012, Diaconis 2009, Hanawal & Sundaresan 2010, Muramatsu et al. 2006, Furon et al. 2012, Matsui et al. 2004),

(2) Intrusion Detection & Prevention and Anomaly Detection
(e.g. Scott 1999, 2001, 2004; Zhao & Nygard 2010, Ihler et al. 2006, Jyothsna et al. 2011, Shi & Mei-Feng 2012), and,

(3) Privacy in Anonymity Systems and Social Networks
(e.g. Danezis and Troncoso 2009, Troncoso and Danezis 2009).

6.7.1 Cryptography, Cryptanalytics & Penetration Testing

Author's interest in MCMC for network and computing security was motivated in course of applied R&D on quantitative risk management models for global banking and finance model risk, market risk and operational risk management (Malhotra 2014a, 2014b, 2014c, 2014d, 2014e). His prior research focused on analyzing vulnerabilities in the mainstream global encryption standards and cryptographic protocols based on mathematical and algebraic analysis of cryptanalytic algorithms such as algebraic number sieves (Malhotra 2013a, 2013b, 2013c, 2013d). While analyzing the mathematical and statistical foundations of computing and network encryption schemes, his interest focused on computational and statistical foundations of cryptography and cryptanalysis using cryptanalytic tools. In that process he found some very interesting research in MCMC methods by statisticians and mathematicians advancing quantitative methods research on cryptography and cryptanalysis. Three such examples of cryptography and cryptanalysis-related MCMC research are outlined below.

An interesting research stream in this applied area is focused on decrypting and attacking ciphers underlying network and computing encryption mechanisms (Chen & Rosenthal 2010, Diaconis 2009). Research pioneering integrated use of cryptography and MCMC algorithms by Chen & Rosenthal (2010) advances MCMC for decryption of substitution ciphers, transposition ciphers, and substitution-plus-transposition ciphers. Based on the frequency analysis of combinations of characters such as bi-grams and tri-grams, their research has delved into in-depth statistical analysis for optimization of such decryption attacks. They analyzed the transitions of consecutive text symbols in bi-grams to develop a matrix of such transitions then used it for computing the probability of the respective transitions. MCMC algorithms were used for searching the probability maximizing functions given the high-dimensionality of the search space of such functions. Their analysis has examined diverse combinations of variables such as

MCMC iterations, scaling parameter, cipher text amount, number of repetitions, and, swap vs. slide vs. block-slide moves. They report success rates of up to 70% and above with transposition key lengths up to 40.

Diaconis (2009) motivates MCMC application in the context of cryptography and cryptanalysis and provides an analytical treatment of the Metropolis algorithm and related theorems. Advancing upon Diaconis (2009), Hanawal and Sundaresan (2010) develop an empirical study in which they generate randomized passwords using MCMC and the Metropolis algorithm. They show how a high-dimensional problem characterized by a distribution with difficult to compute normalizing constant can be reframed using the Metropolis algorithm after which the solution is no longer hindered by the need for the normalizing constant. Related MCMC enabled credential authentication and decoding research includes examples such as dynamic signature verification (Muramatsu et al. 2006), decoding fingerprints (Furon et al. 2012), and face recognition (Matsui et al. 2004). Above examples illustrate use of MCMC methods such as Metropolis algorithm in solving difficult to compute or otherwise infeasible high-dimensionality problems in cryptography, cryptanalysis, and penetration testing.

6.7.2 Intrusion Detection & Prevention and Anomaly Detection

Intrusion detection and intrusion prevention is another network and computer security research and practice area that has benefited from applications of MCMC methods and algorithms (e.g. Scott 1999, 2001, 2004; Zhao & Nygard 2010, Ihler et al. 2006). Many such models depend upon anomaly detection wherein behavior of traffic generated by the customers is distinguished from that of the attackers based upon distinct probability distributions. Scott (1999, 2001) distinguished customers' traffic as a Poisson process from the traffic from the two-state continuous time Markov process generated by attackers breaking into and exiting the accounts. The presence of the attacker also generates additional traffic as an independent second Poisson process. Given all processes as homogeneous, account traffic data is represented as discrete time Hidden Markov Models in which case the hidden state indicates intrusion or attack status and presence of absence of the attacker (Scott 2001, 2004).

The above studies used the MCMC algorithm Gibbs sampler for sampling each state in the hidden Markov chain given most recent draws of nearest neighbors. MCMC is critical for solution of such high-dimensionality problems as the likelihood function for the HMM quickly becomes infeasible to compute even for small values of hidden

chain's size of the state space. Using a Bayesian approach to learning and inference for time series data, Ihler et al. (2006) use a similar Hidden Markov-Poisson model for an adaptive anomaly detection algorithm. Their study determined the time complexity of each MCMC iteration as O(T), linear in the length of the time series, and the series shows rapid convergence. Given the high false-positive rate of anomaly detection intrusion systems, Shi & Mei-Feng (2012) show how several research studies using HMM benefited from MCMC and related methods for analyzing intrusion detection systems. Their study uses HMM given high-dimensionality resulting from number of states, the classic problem for which MCMC was devised as a solution as discussed earlier.

Similarly, Zhao & Nygard (2010) use the Metropolis-Hastings algorithm to infer the distribution of intruders in a wireless network from limited local information used by a fuzzy logic algorithm to assess the impact of the intruders on a monitored point. A comprehensive review of MCMC and other related Bayesian inference and machine learning models for anomaly based intrusion detection and prevention systems is available in Jyothsna et al. (2011). They review key distinctions between statistical models (such as: threshold model, Markov process model, statistical moments model, multivariate model, time series model), cognition models (such as finite state machine, description scripts, and adept systems), cognition based techniques (such as boosted decision tree, support vector machine, artificial neural network), machine learning based detection techniques, kernel based online anomaly detection, and detection models based on computer immunology and models based on user intention. Use of MCMC also optimizes use of computational processing power needed by the wireless base station which then only needs to query and process network packets to the specific nodes identified by the conditional distribution. Above examples illustrate the use of MCMC methods such as Gibbs sampling and Metropolis-Hastings algorithm in solving difficult to compute or otherwise infeasible high-dimensionality problems in intrusion detection and prevention and anomaly detection such as for telecom networks.

6.7.3 Privacy in Anonymity Systems and Social Networks

Anonymity systems such as Tor network based on onion-routing allow two parties to exchange information without disclosing their network identifiers to each other or to any other third party. The engineering principle underlying such communications is that the messages entering and leaving the network should be

cryptographically unlinkable (Danezis and Troncoso 2009, Troncoso and Danezis 2009). Privacy of such networks which ensure that anonymity is safeguarded is prized across commercial, social, and government and military communications. The application of MCMC algorithms in case of such anonymity systems is to make it statistically and computationally feasible to infer who is talking with who based upon network traffic patterns of messages.

Anonymity is measured as the uncertainty that the adversary has about who is conversing with who by using information theoretic measures of entropy (Danezis and Troncoso 2009). The key limitations of those measures include measuring anonymity of a single message and *not* the systems as a whole, and, most seriously, statistical infeasibility of computing relevant probability distributions. Contribution of the Danezis and Troncoso (2009) at Microsoft Research is to address the 'hard problem' of calculating the probability distributions over senders or receivers of messages. To solve the above statistical computational problems, they demonstrate the use of probabilistic modeling and Bayesian inference, which despite their power, are handicapped by considerable computational complexity that often makes it not possible to compute the probability distributions. It is in this specific context that MCMC sampling algorithms, including Metropolis-Hastings (MH) algorithm and Gibbs sampler, come to the rescue for extracting samples that provide approximations of relevant probability distributions from observations of 'rather complex systems' (Danezis and Troncoso 2009).

Above review of MCMC methods and algorithms advancing research and practice in network and computer security and cybersecurity, analysis of adversary attacks, penetration testing, and information assurance establishes their increasingly important and growing role. Given the methodological scope and focus of the discussion, only specific examples and contexts within network and computer security research could be addressed. The concluding discussion further highlights some of the broader implications of this stream of research with both methodological and applied recommendations.

6.8 Summary and Future Research

Markov chain Monte Carlo (MCMC) may be described as a widely used set of general quantitative methods to find approximate solutions to complex problems in polynomial time. Recognized as one of top-10 computing algorithms with underlying research among top-3 mathematics papers, its impact across diverse fields including

computer science, physics, statistics, finance, economics, and engineering is evident. The article focuses on highlighting the increasingly important and critical role of MCMC algorithms in network and computer security research and practice. The greatest impact of MCMC methods and algorithms is probably in case of problems where outputs lack interpretability because of high-dimensionality and complex interactions in inputs. Several of the network and computer security contexts highlighted in the discussion reviewed such problems and their resolution using MCMC. Our review established increasing importance of MCMC, Gibbs Sampling, and Metropolis Algorithm in modeling cryptography and cryptanalytic password attacks and authentication analysis; signature and anomaly based network intrusion detection and prevention systems; and analyzing potential vulnerabilities in anonymity based systems such as Tor network based on onion-routing protocol and other 'social networks'.

Beyond the focus of the current discussion, there are two key important issues to focus on for future research and development. First is the development of quantitative methods and algorithms for addressing high-dimensional computationally complex problems relevant to emerging paradigms such as big data analysis and quantum computing. We need to recognize that modern statistical paradigms such as Bayesian inference are themselves reliant on computational statistical methods such as MCMC for their prowess. Second is increasing and critical need for recognition and resolution of problems at general systems level where they are sometimes called *systemic* problems. Some of our methodological and applications discussion explicitly or implicitly recognized this systemic concern. Particularly, in the case of computer and network security, the problems across most domains being addressed relate to the broader focus on risk management as well.

Relating above methodological and applied concerns together, one focus of future research needs to be on *model risk management*. Solving complex high-dimensional problems with inaccurate models is often punished in any domain, whether it is computing or (say) investment banking. Model risk management has gained currency in investment banking but is equally important for any domain reliant upon high-dimensional and computationally complex problems such as network and computer security. 'Model risk arises from the potential adverse consequences of making decisions based on incorrect or misused model outputs and reports.' Knowing history of applications of MCMC ranging from chemical-physics to network computing,

most readers can perhaps relate to the above concern about model risk. Few may, however, recognize that the above statement is from a top investment bank strategy document.

Whether it is quantum computing or quantitative finance, regardless, it is imperative to ensure that models perform as specified and intended; models are conceptually sound and used appropriately and that model users are aware of the models' strengths and limitations and how these can impact their decisions. That is essentially model risk management. Advancing beyond network computing to investment banking, one may possibly discern that the computational statistical methods and models related concerns impact both fields (and others) as well. Following prior discussion, one may even speculate that Wall Street and Pentagon (among others) may be probably grappling with similar model risk management concerns; albeit probably oblivious of the commonality of systemic problems they may share.

In any case, the approaches to mitigate operating risk associated with the use of models needs to evolve to reflect recent trends in practice. In particular, there are a number of new areas where it is not possible for the "human eye" to necessarily detect material flaws: in the case of models operating over very small time scales, or where outputs lack interpretability due to high-dimensionality and complex interactions in inputs, the periodic inspection of predicted versus realized outcomes is unlikely to be an effective risk mitigate. These situations require a holistic validation framework of the system focused on identifying and mitigating potential failures, taking into account the models' objectives, their implementation including the joint interaction of software and hardware, their response to potential input shocks in real time and the fail-safe mechanisms. The above quote is attributed to a top investment bank as well.

Chapter 7.

VaR and Beyond VaR for Cyber Insurance

> "Normality has been an accepted wisdom in economics and finance for a century or more. Yet in real-world systems, nothing could be less normal than normality. Tails should not be unexpected, for they are the rule. As the world becomes increasingly integrated – financially, economically, socially – interactions among the moving parts may make for potentially fatter tails. Catastrophe risk may be on the rise."
>
> -- Andrew G Haldane, Executive Director, Financial Stability and member of the Financial Policy Committee and Benjamin Nelson, Economist, Financial Stability, Bank of England, in 'Tails of the unexpected' speech at "The Credit Crisis Five Years On: Unpacking the Crisis", 8 June 2012.

7.1 Portfolio Theory based Framework for Cyber Insurance

In the current chapter, we develop the first known portfolio theory based framework for cyber insurance modeling with guidance to minimize model risks, tail risks, and systemic risks inherent in models in commercial cyber insurance modeling.

The fundamental basis of risk measurement underlying the VaR model lies in the *portfolio theory*, also known as *modern portfolio theory* (MPT) (Markowitz, 1952). Mean variance optimization (MVO) in the context of portfolio theory aims to achieve a desired level of portfolio return (given by mean) for a degree of portfolio risk (given by standard deviation). MVO is expected to maximize expected return of the portfolio for any given portfolio standard deviation, or, alternatively minimize standard deviation of the portfolio for any given expected return. A key insight of the portfolio theory is that it is not the riskiness (i.e., standard deviation w.r.t. to its mean return) of any specific asset that matters, but, the *correlation or covariance of its return with the returns to the other assets* in the portfolio that matters. *The **lower the correlation**, other things being equal, the less the asset contributes to overall risk. If the correlation is sufficiently negative, it will offset existing risks and lower the portfolio risk (standard deviation).* Following discussion describes the finance portfolio theory underlying VaR relating it to the cyber domain for cyber insurance modeling.

7.2 Portfolio Theory Mapped to Cyber Insurance Modeling

Mapping from the finance domain to the cyber domain, it follows that the riskiness of an individual cyber risk is not which really matters. Rather, what matters is how it correlates with other cyber risks, which determines the overall risk of the 'portfolio' of cyber risks. The *lower the correlation of the cyber risk with other cyber risks, the lower the overall risk of the portfolio of cyber risks*. *More importantly, conversely, the higher the correlation of the cyber risk with other cyber risks, the higher the overall risk of the portfolio of cyber risks*. Given the extremely high correlations between cyber risks as discussed in the prior analyses, the above observation further reaffirms the support for our prior hypotheses. Specifically, *as cyber risks are highly correlated to each other given their intrinsic nature* (as compared with financial risks), *cyber risks are much more risky as compared with financial risks*. Secondly, assets in a financial portfolio typically may offset their individual riskiness given low correlations or negative correlations with other assets. However, given high positive correlations among cyber risks, *most cyber risks will be positively and highly correlated and thus contribute to very high riskiness of the portfolio of cyber risks*. Such portfolio of risks could be considered at the intra-firm level or at (systemic) inter-firm level, in either case, *the unique character of cyber risks is expected to result in 'portfolios' of extremely highly interdependent and highly correlated cyber risks*.

VaR, typically expressed as a percent of capital, is the statistical measure of the amount of loss *not* to be exceeded in a *given time frame* with a *certain probability*. It is the *maximum amount of money* likely to be lost over a *specific time period*, at a *specific confidence level*. In the context of portfolio theory, VaR was developed as a system to measure risks across different trading positions, across the whole institution, and also aggregate these risks into a single risk measure. VaR was estimated from a system based on standard portfolio theory, using estimates of the standard deviations and correlations between the returns for different assets in the portfolio. The theoretical basis of VaR is the portfolio theory while other approaches such as historical simulation and Monte Carlo simulation do not completely rely upon the actual risk return data. Many finance experts question the validity of relying upon the statistical assumptions underlying VaR which are based upon physical sciences such as Physics for application in the

sociotechnical world of *social systems* such as financial markets (Heires,2012[152]; Lohr, 2008[153]; Derman & Wilmott[154]). Our related point underscored in the prior analysis about *social engineering* being a key determinant of cyber risks in contrast to the finance domain is most relevant in the above context[155].

7.3 Mean Variance Framework for Cyber Risk of Loss

In portfolio modeling, financial risk is modeled using the Mean-Variance framework in terms of mean and variance of asset returns assumed normally distributed. This framework considers a random variable (r.v.) X representing normally distributed daily returns with mean μ and variance σ^2 (i.e., standard deviation σ) where the probability f(x) that r.v. X = x is given by the probability density function (pdf):

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2}((x-\mu)/\sigma)^2\right]$$

s.t. X: $-\infty < x < \infty$. A normal pdf with $\mu = 0$ and $\sigma = 1$ known as a *standard normal* (corresponding to $f(x) = \frac{1}{\sqrt{2\pi}}\, e^{-\frac{1}{2}x^2}$) is shown in the left panel of Fig. 7-1.

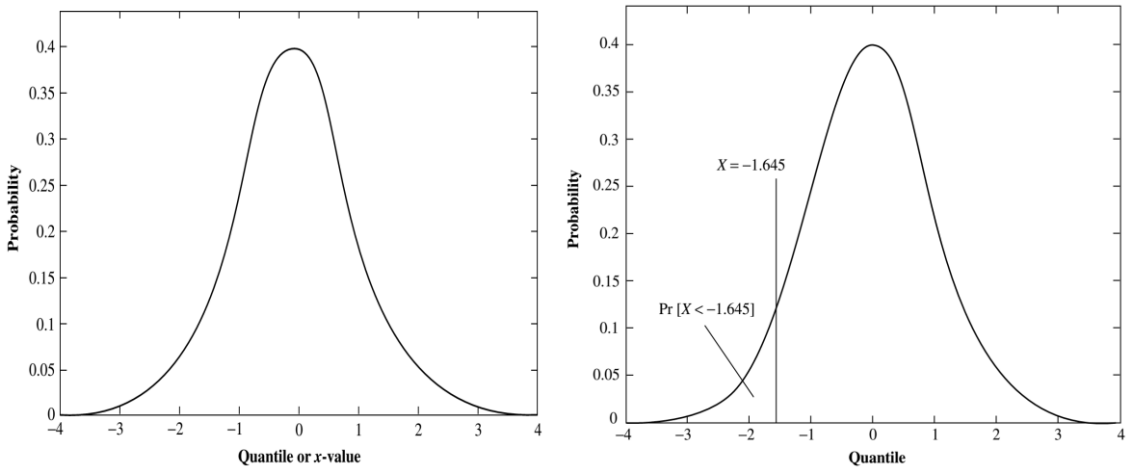


Fig. 7-1. Normal PDF and Normal Quantiles and Probabilities

[152] http://www.rmmagazine.com/2012/08/29/finance-isnt-science-why-wall-streets-models-will-always-have-limitations/
[153] http://www.nytimes.com/2008/11/05/business/05risk.html
[154] http://www.businessweek.com/stories/2008-12-30/financial-models-must-be-clean-and-simple
[155] http://blog.trendmicro.com/employees-may-companys-biggest-cybersecurity-risk-threat-social-engineering/

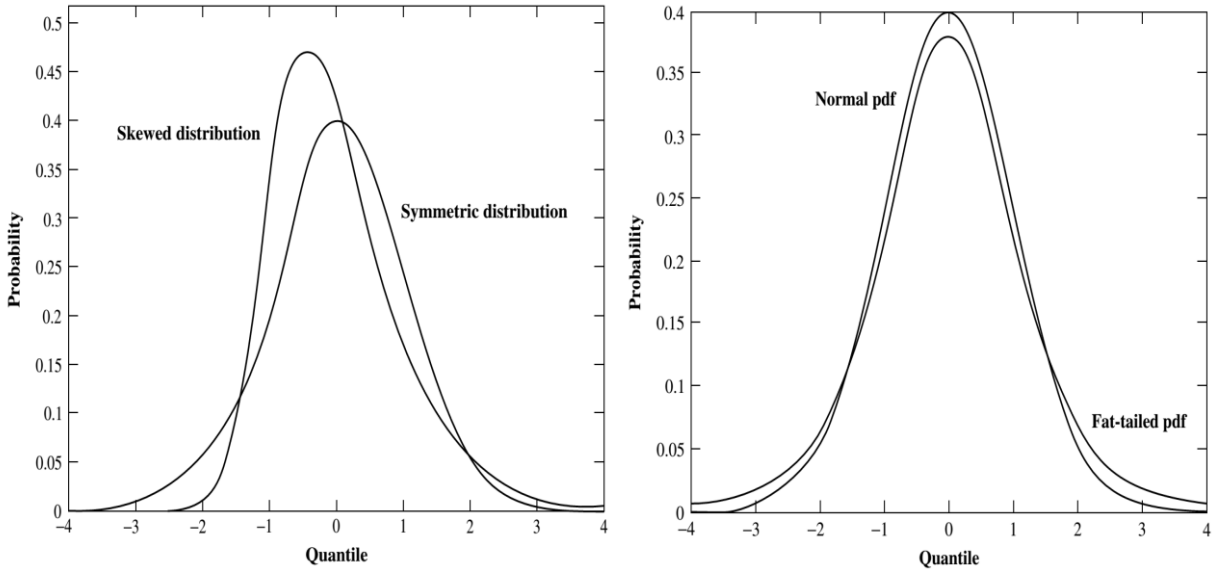
The right panel of Fig. 7-1 shows the probability of the portfolio returns less than -1.645 (i.e., loss greater than 1.645) as shown by the area under the left hand tail which is equal to 0.05, or 5%.

Hence, there is 5% probability that the portfolio returns will be less than -1.645 (i.e., loss will be greater than 1.645). Conversely, *at the 95% confidence level, the maximum likely portfolio loss can't exceed 1.645*, i.e., *portfolio VaR = 1.645*. Hence, the cumulative probability is given by the cumulative density function which gives the normal probability of x ≤ X as follows:

$$\Pr[x \le X] = \int_{-\infty}^{X} \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2}((x-\mu)/\sigma)^2\right] dx$$

Corresponding quantile or x-value is given by: $X_{cl} = \mu + \alpha_{cl}\sigma$ where cl=confidence level such as 95% in the above case, and α_{cl} is the *standard normal variate* $\alpha_{cl} = \frac{X_{cl} - \mu}{\sigma}$ corresponding to the cl such as 1.645 in the above case ($\alpha_{0.95} = -1.645$).

Tail risks can be recognized from analysis of higher (third and fourth) moments of distribution. The third and fourth moments of distribution called *skewness* and *kurtosis* seen in Fig. 7-2 characterize *long tails* and *fat tails* respectively in a distribution (Dowd, 2007).



$Skew = E(x-\mu)^3/\sigma^3$ $Kurtosis = E(x-\mu)^4/\sigma^4$

Fig. 7-2. Skewness and Kurtosis Denote 'Tail Risks' in Non-Normal Distributions

Skew parameter is 0 for a (symmetric) normal distribution. Positive skew results in a left short tail and right long tail, whereas a negative skew results in a left long tail and right short tail. Therefore, negative skew with a *left long tail* indicating *greater concentration of risk of loss* (i.e., 'negative profit') is particularly relevant for modeling of cyber risk related losses and cyber insurance modeling. Kurtosis characterizes flatness of the tails resulting in corresponding concentration of risks in the tails. Kurtosis parameter is equal to 3 for a normal distribution. Relative to the normal distribution, fat-tailed distributions with kurtosis greater than 3, and, thin-tailed distributions with kurtosis less than 3 are characterized. As compared with normal, for cyber risk loss estimates, *left fat tail* indicating *extreme events* being more likely and inflicting large losses are particularly relevant. Therefore, *if the actual cyber risk loss distribution is non-normal, assumption of normality can result in significant underestimation of cyber risk*. Our prior analysis established that *cyber risks are highly correlated and highly interdependent*. Hence, the assumption of normality can cause significant underestimation of cyber risk when using portfolio theory based models such as VaR.

Using the portfolio theory underlying VaR to model cyber risk entails critical assumptions of normality. We need to assume that cyber risk losses are multivariate normally distributed. Or, less restrictively, we need to assume that our cyber risk portfolio has normally distributed losses. In either case, we need to rely upon the key assumption of the portfolio of cyber risk losses being normally distributed (Dowd, 2007). Consequently, we rely upon a framework that isn't as reliable for cyber insurance modeling when normality assumptions are violated. That happens in presence of long tails and fat tails. In particular, we need to be concerned about the *long tail* and *fat tail* of the distribution on the left side which imply extreme losses.

7.4 Value-at-Risk (VaR) for Cyber Risk Insurance Modeling

Advancing from portfolio theory to VaR allows lesser restrictions on the returns distribution but focuses on the tails of the distribution. *VaR is the maximum likely loss over some target period at a specified probability level.* It is the maximum amount of loss *not* to be exceeded with a *certain probability* or *level of confidence* in a given time frame. VaR provides a common risk measure for different types of positions and risk factors. It also takes into account correlations between risk factors to help measure risk in a statistically meaningful manner. Broadly speaking, VaR can be applied in various ways: (a) as a

point estimate measure of *maximum probabilistic loss*, (b) as an *estimation procedure*, (c) as a *methodology* that can estimate other risks as well, and, (d) as an *approach to risk management* for strategic decision-making (Dowd, 2007). Our primary focus on VaR in the current discussion on cyber risk assessment and cyber insurance modeling is related to (a), (b), and (c). In that context, tail risks are even more critical as compared with finance.

VaR is based upon two parameters: holding period of time over which portfolio profit or loss are measured and confidence level denoting probability of loss. Holding period could specify any duration such as daily, weekly, monthly, or annual. Confidence level (cl) could be any percentage of probability between 0 and 1 such as 95% and 99%. Assuming holding period as daily, daily VaR for those two confidence levels is shown in the left and right panels of Fig. 7-3. Both schematics show probability of loss on the y-axis and monetary profit (+) or loss (-) of the portfolio on the x-axis. Since cyber risks are different from financial risks in that there is no upside or profit involved, there is only downside or risk of loss. Hence, creativity is needed for mapping the notions of financial portfolio returns to cyber risk modeling. For instance, negative and positive returns describing 'losses' and 'profits' in finance may be mapped to cyber risk related 'losses' and 'losses averted'.

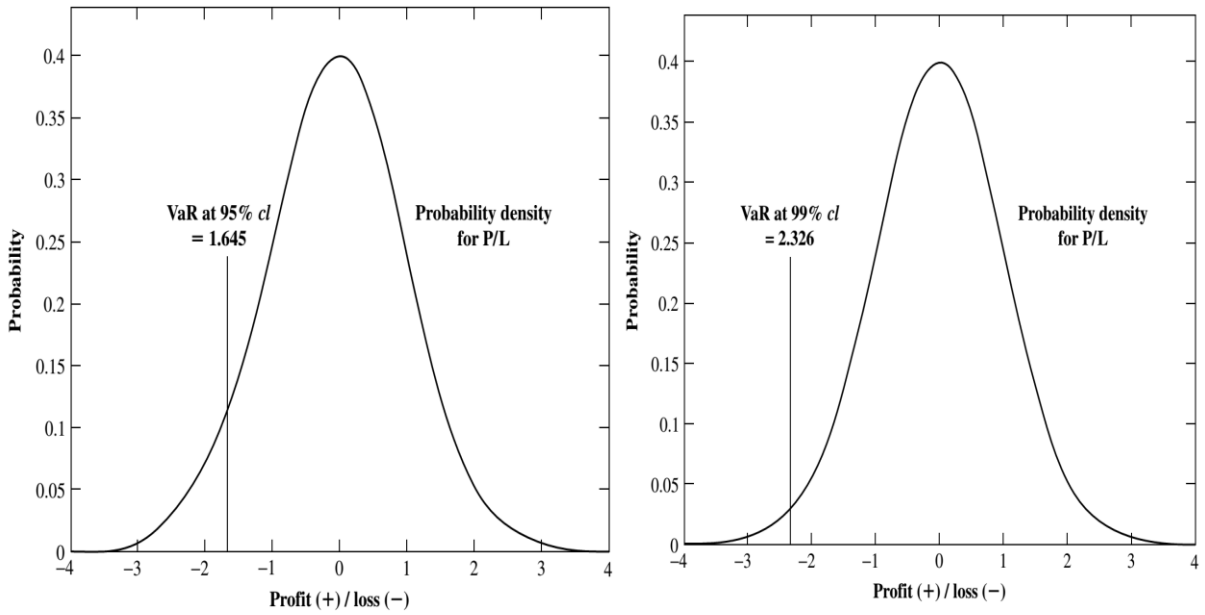


Fig. 7-3. How Tail Risks Vary for Different Point Estimates of Normal VaR

Comparing the two panels in Fig. 7-3 (Dowd, 2007), we can see that at 95% confidence level, the critical value is -1.645. It denotes that 95% of the time the *maximum loss* is *not* expected to *exceed* 1.645σ. However at the same confidence level, 5% of the time, the maximum loss *can* exceed 1.645 σ. Similarly, at 99% confidence level, the critical value is -2.326. It denotes that 99% of the time the *maximum loss* is *not* expected to *exceed* 2.326σ. However, 1% of the time, the maximum loss *can* exceed 2.326 σ.

Hence, VaR measure can help us assert that: "We are X percent certain that we will not lose *more than* V dollars in time T" (Hull, 2012). For the 1-day holding period, we can therefore conclude that we are 95% certain that we will not lose more than 1.645 σ dollars in the next trading day. We can similarly conclude that we are 99% certain that we will not lose more than 2.326σ dollars in the next trading day. Of course, the above conclusions are based on the assumption of normality of portfolio returns. As the confidence level increases (such as from 95% to 99%), the tail percentage probability of loss decreases (correspondingly from 5% to 1%), and, VaR value increases (1.645σ to 2.326σ). Hence, *at higher confidence intervals* (i.e., with increasing confidence), other thing remaining same, the *maximum expected loss* that will *not* be exceeded typically *grows at increasing rate* as seen in the left panel of Fig. 7-4 (Dowd, 2007).

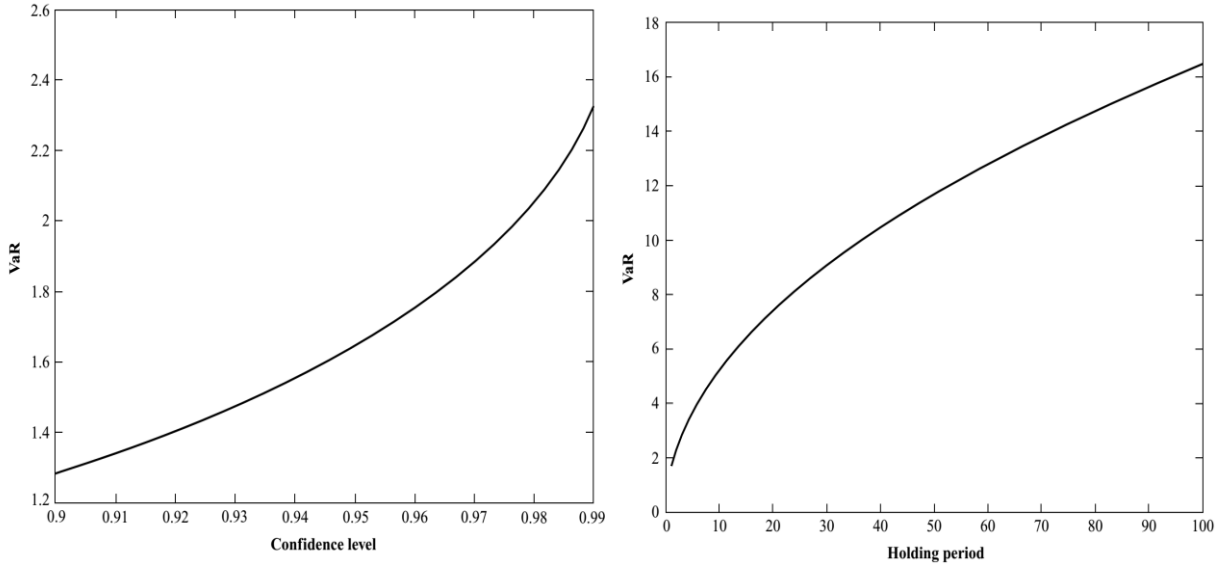


Fig. 7-4. How Normal VaR Measure Varies with Change in its Two Parameters

Similarly, as the holding period increases, VaR tends to increase. That implies that other thing remaining same, *for increasing holding periods*, the *maximum expected loss* that will *not* be exceeded typically *increases* but at a decreasing rate as seen. It should be noted that the behaviors of VaR shown above are commonly noted, even though other behaviors are possible. Dowd (2007) suggests varying both parameters, confidence level and holding period, together to 'form a more complete picture' of VaR Surface as shown in Figure 7-5 below (Dowd, 2007).

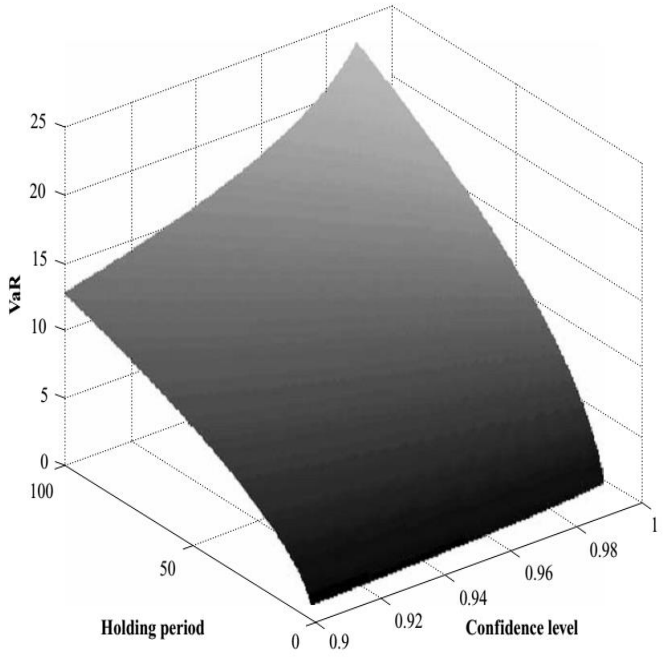


Fig. 7-5. Varying both Parameters Shows a More Complete Picture of Normal VaR

The VaR surface provides a much better view of the *extreme* risks corresponding to very severe possible losses as both parameters approach their extreme values. It is evident in the spike corresponding to a maximum possible loss approaching 25σ dollars! Of course the above picture presented is of normally distributed portfolio returns. For example, we do not see any *regime shifts* over the time duration. Regime shifts denote abrupt and persistent structural breaks impacting dramatic changes in the behavior of financial time series data. Such regime shifts typically coincide with economic and financial crises. As illustrated in Fig. 7-6, compared with normal distribution, the real world of *power-law distributions* is characterized by much greater

tail risks (Mandelbrot & Taleb, 2006[156]; Mandelbrot & Taleb, 2005[157]; Sexauer & Siegel, 2012[158]). Such tail risks involve both higher frequency of occurrence and much greater magnitude of extreme losses than predicted based on assumptions of normality.

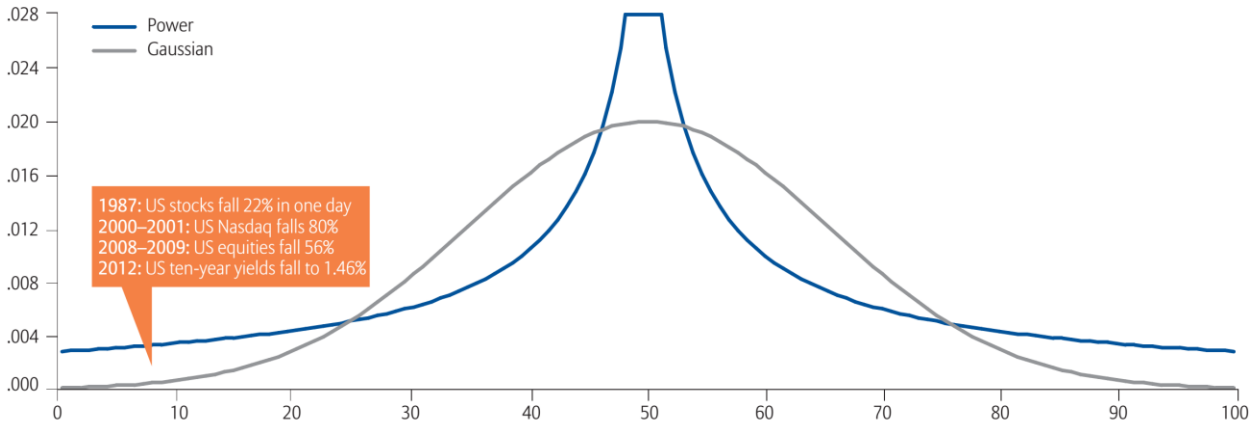


Fig. 7-6. Most of Sociotechnical World is Non-Normal and Governed by Power Laws

7.5 Fundamental VaR Risks in Cyber Insurance Modeling

An example from the world of finance can help given that the cyber insurance modelers are enamored about using VaR 'because finance uses VaR'[159]. The simplicity of VaR in terms of ease-of-application and understanding has made it popular as a worldwide risk model in finance. However, as most portfolio managers assert: 'risk is in the tails', and it is on that most critical point where VaR is not only silent but may in fact mislead *if* relied upon for the wrong reasons by naïve modelers and users. Haldane and Nelson (2012) note that: "VaR suffers a fatal flaw as a risk management and regulatory measure: it is essentially silent about risks in the tail beyond the confidence interval. For example, even if a trader's 99% VaR-based limit is $10 million, there is nothing to stop them constructing a portfolio which delivers a 1% chance of a $1 billion loss. VaR would be blind to that risk and regulatory capital requirements seriously understated. Worse still, the fatter the tails of the risk distribution, the more misleading VaR-based risk measures will be. Consider holding a portfolio of world equities and, based on data

[156] http://www.ft.com/cms/s/2/5372968a-ba82-11da-980d-0000779e2340.html
[157] http://money.cnn.com/sales/major_moments/moneymanage/risk.html
[158] http://us.allianzgi.com/MarketingPrograms/External%20Documents/Managing_Tail_Risk.pdf
[159] http://www.cert.org/flocon/2013/presentations/ulrich-james-cybervar.pdf

from 1693 to 2011, calculate the VaR. The 99% VaR assuming the data are normal gives a loss of $6 trillion at today's prices. Using the actual data raises the estimated VaR by one third to $7.8 trillion. Finally, calculating the risk conditional on being in the 1% tail of the distribution gives a loss of $18.4 trillion. Simple VaR underestimates risk by a factor of 1.5 and 3." [160]

Our prior analysis of extant quantitative models in predominant use for cyber risk and cyber insurance modeling indicated primary reliance of most commercial providers on VaR. Current analysis facilitates understanding of VaR so that such providers can make informed choices about (not) using VaR while being aware of its strengths as well as its limitations. Recent history of VaR modeling in finance is characterized by headlines related to major firm level and systemic crises. Hence, it is all the more critical to know the boundaries and assumptions of VaR to preempt and prevent similar mishaps in cyber risk and cyber insurance modeling. Prior analysis demonstrated keen interest of the cyber risk modeling commercial providers in mapping risk modeling using VaR from finance to cyber insurance modeling. In response, our finance empirical study in a prior chapter helped the cyber insurance modelers understand both the content and the context of VaR's native application (Malhotra, 2014)[161].

More importantly, given key focus on model risk management related to VaR, that empirical study also demonstrated how to manage the model risk associated with use of VaR. Specifically, it used multiple models to cross-check the reliability of the VaR models. Such approach for managing the risk of any specific model by cross-validating the findings by using multiple independent models and methods is a key model risk management strategy (Morini, 2011). Such methods included basic quantitative models that compared VaR findings by taking into consideration third and fourth moments of the distribution. Such methods also included advanced quantitative finance analytics methods such as expected shortfall (also known as expected tail loss), extreme value theory, and Cornish-Fisher approximations.

Prior analysis clearly established that cyber risks entail much higher interdependence and correlations than do financial risks typically modeled using VaR.

[160] http://www.bankofengland.co.uk/publications/Documents/speeches/2012/speech582.pdf
[161] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2538401

Key limitations of VaR models given their inability in dealing with such interdependencies and correlations has also made it the subject of very strong criticism in finance (Malhotra, 2012)[162]. Given such *known* limitations of VaR, in our prior analysis we concluded that continued use of VaR in for cyber risk modeling is expected to result in extreme *model risks*, *tail risks*, and, *systemic risks*. Following discussion helps further understand how to manage model risks arising from reliance upon VaR for cyber insurance modeling.

As discussed before, being a point-estimate, VaR is not a reliable estimator of *maximum expected loss* as it is not designed to measure the tail risks. Following upon that discussion, VaR underestimates risks particularly when those risks are concentrated in the tails, specifically *left* tails in the case of cyber risks. That observation is depicted in the illustration in Fig. 7-7 which shows that the left panel and the right panel both have the exact same VaR (Hull, 2012). However, the right panel shows *non-normality* in which the probability of risk is concentrated in the left tail, a *fat tail* resulting from kurtosis.

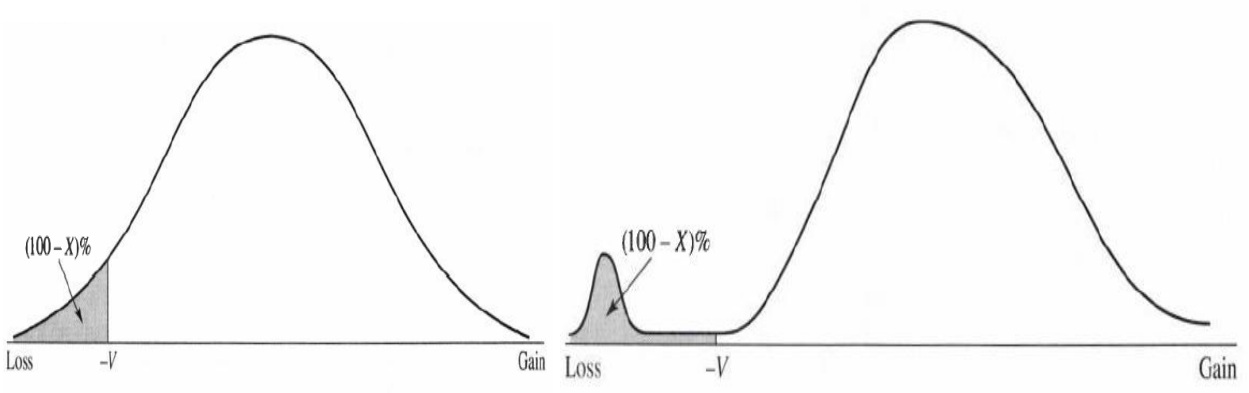


Fig. 7-7. VaR is an unreliable estimate of Tail Risk.

As evident from the above analysis, VaR can be a misleading risk measure when the returns are not normally distributed. Also, as it is a point estimate measure of risk at a particular point in the distribution, it measures *neither* the distribution *nor* the extent of risk in the tail (Hull, 2012).

Consistently, if VaR is applied to cyber risk modeling based upon the assumption of normality, it can be an inherently incorrect assumption as our prior analysis established cyber risks as being highly interdependent and correlated. This

[162] http://www.yogeshmalhotra.com/BeyondVaR_YogeshMalhotra.pdf

specific problem will lead to significant underestimation of risk if normality is assumed. Hence, model risk management is most crucial if VaR is applied in cyber risk modeling. *Also, to accurately model cyber risks for cyber insurance, we need to advance beyond VaR to other models that can account for non-normality including the third and fourth moments*.

VaR also treats risk as *exogenous*. Our prior analysis, however, established that cyber risks are not only highly *interdependent* and *correlated*, but can be also be *endogenous* in nature. Specifically, 'spikes' in cyberattacks are determined in a large part by the behaviors as well as interaction between the various interacting entities. Hence, cyber risks can be endogenous in nature. For example, the Sandia National Labs report 'Mathematical Challenges in Cybersecurity' notes that (Dunlavy, et al., 2009)[163]: "Many cyberattacks work by spreading malware to a large number of vulnerable machines. While the details may vary (e.g., whether a human needs to be tricked into making a mistake, or the propagation happens automatically), this style of attack expands along linkages in a social or technological network, infecting some fraction of nodes as it goes. For these kinds of broad-target attacks, rapid propagation is important since cyber defenders are likely to add protections once the malware is detected and characterized." Rapid propagation of resulting from homogenous vulnerabilities *and* homogenous countermeasures can further escalate endogeneity of cyber risks. Resulting iterative process can built up into *systemic risks* such as those discussed earlier.

Another critical problem with using VaR for modeling cyber risk assessment and cyber insurance modeling is that it is *not* sub-additive. Sub-additivity of risk measure $\rho(.)$ implies that estimated loss from *combination* of risk A (e.g. spear phishing) and risk B (e.g. malware dropping) is less than or equal to the sum of potential losses from each of A and B considered separately on their own:

$$\rho(A + B) \leq \rho(A) + \rho(B)$$

The above two specific cyber risks are the two most frequent cyber risks for financial institutions as reported in the May 2014 'Report on Cyber Security in the Banking Sector' by the New York State Department of Financial Services. Also, "The larger the institution, the more likely it appeared to experience malware *and* phishing attempts.[164]"

[163] http://www.cs.sandia.gov/~dmdunla/publications/SAND2009-0805.pdf
[164] http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf

Based on the contagion like results from such cyber risks, recent history of enterprise level attacks suggests that risks from such *combinations* is much greater than respective risks in isolation. If cyber risks were sub-additive, adding those risks together ($\rho(A) + \rho(B)$) would give us an overestimate of combined risk ($\rho(A + B)$). Hence sum of the two risks could be used as a higher and thus conservative estimate of combined risk. As discussed above, that is however not the case. Additionally, given most primary barrier to sustaining cyber security as reported by 73% financial firms as being *increasing sophistication of threats*, we can expect more advanced and complex *combinations* in future. Thus VaR can severely underestimate potential losses in terms of severity and impact of cyber risks which in combination can cause much greater potential loss.

7.6 Improved Alternatives to VaR, Coherent Risk Measures

Some of the critical problems with VaR such as concerns related to non-normality, model risks, tail risks, and systemic risks can be minimized by use of other risks models. Given interest of cyber insurance modeling commercial providers in mapping risk modeling from finance, they would find it helpful to know what makes a better risk measure. The guiding thesis for selection of the risk measures in finance is the concept of a coherent risk measures. One aspect of such 'coherence' discussed above was the notion of sub-additivity. Including sub-additivity, there are four key aspects that characterize a coherent risk measure according to the theory of coherent risk measures developed by Artzner et al. (1997, 1999). If X and Y are the future expected 'values' of two risky portfolio positions, a risk measure $\rho(.)$ is coherent if it satisfies the following four postulates:

$$\begin{aligned} \rho(X) + \rho(Y) \leq \rho(X + Y) \quad & \text{(sub-additivity)} \\ \rho(tX) = t\rho(X) \quad & \text{(homogeneity)} \\ \rho(X) \geq \rho(Y), \text{if } X \leq Y \quad & \text{(monotonicity)} \\ \rho(X + n) = \rho(X) - n \quad & \text{(risk-free condition)} \end{aligned}$$

Homogeneity means that if the size of the portfolio as a unit is changed by a factor t, then the risk also is changed by the same factor t. *Monotonicity* means that if future value is lower, then risk is higher. The *risk-free condition* implies that if cash amount of n is added to a portfolio, its commensurate risk reduction should be n. Sub-additivity was defined earlier.

The notion of future 'values' in the above postulates of coherent risk measure requires further thoughtful consideration when used in cyber risk modeling. This is necessary given that unlike financial risk management there are no 'positive' returns in cyber risk management. Therefore, future 'values' may be considered as potential losses *averted* based on specific countermeasures. Or, they may be considered in terms such as the difference between cybersecurity investments and potential losses averted. Such investments may be further distinguished in risk management terms such as risk acceptance, risk avoidance, risk control, risk transfer, and risk monitoring[165]. Future research is recommended on finding more comparable analogs to cyber risks in the financial domain. It may be possible to conceptualize synthetic derivatives whose expected outcome can be only zero or negative where the objective is to minimize any change from zero. If financial derivatives are used, one may need to however contend with their non-linear behavior. Such adaptations may need further care if power law distributions are used to emulate real world scenarios instead of Gaussian distributions.

7.7 Expected Tail Loss (aka T-VaR) Coherent Risk Measure

Based upon the discussion on coherent risk measures, the focus of this section is on one such measure called **Expected Tail Loss** (**ETL**). It is also called **Tail-VaR** (**T-VaR**) or **Expected Shortfall** (**ES**)[166]. In the context of cyber insurance, it may be of interest to note that the ETL risk measure is quite similar to conditional average claim size used by casualty insurers. Insurers use another name for ETL calling it instead **Conditional Tail Expectation** (CTE) in the 'insurance industry'[167]. In aftermath of the Financial Crisis which raised questions about reliability of VaR given it is not a coherent risk measure, ETL has become the risk measure of choice[168,169]. The empirical study on Bayesian vs. VaR modeling in a prior chapter discussed the properties of Expected Shortfall as a coherent risk measure[170]. It also demonstrated empirical modeling of Expected Shortfall besides Historical Simulation, Parametric Method, and, Monte Carlo Simulation models of VaR. In finance, portfolio risk managers underscore that *risk is in*

[165] http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring
[166] http://arxiv.org/pdf/cond-mat/0105191.pdf
[167] https://www.soa.org/library/newsletters/risk-management-newsletter/2004/july/rm-2004-iss02-ingram-b.aspx
[168] http://www.bis.org/publ/bcbs219.htm
[169] http://www.bis.org/publ/bcbs219.pdf
[170] http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2538401_code2338267.pdf?abstractid=2538401&mirid=1

the tails. Managing *tail risk* therefore is important for those who want to control the *downside risk*. In cyber risk modeling, as all the risk is downside risk, ETL seems to make all the more sense as a measure of risk as compared with VaR.

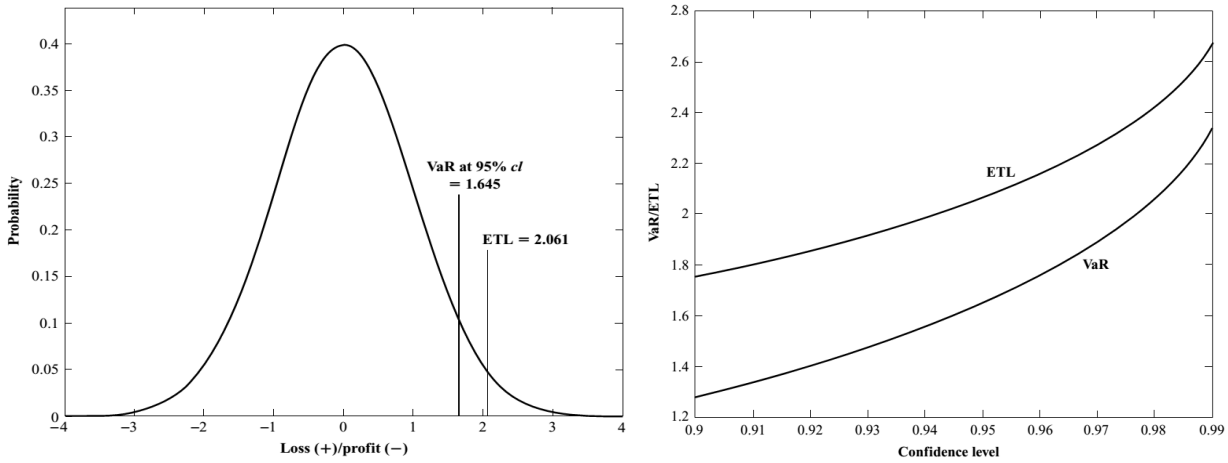


Fig. 7-8. VaR tells Loss If 'Tail' Doesn't Occur, ETL tells Loss if 'Tail' Does Occur.

As shown in Fig. 7-8 (Dowd, 2007), VaR measures the maximum expected loss if an extreme event i.e., 'tail,' *does not occur*, and the ETL measures expected loss *on average* if an extreme event i.e., 'tail,' *does occur*. If VaR is exceeded, ETL is the loss that can be expected *on average*. VaR estimates are needed for estimation of ETL, and if we can estimate VaR given the quantile threshold, we can also estimate ETL using the quantile average[171]. ETL is the conditional expectation of loss conditional on its value exceeding VaR_{cl}. It can be described as: $ETL_{1-\alpha} = E[L|L > VaR_{1-\alpha}]$ where $ETL_{1-\alpha}$ is estimated ETL at confidence level cl for a loss distribution continuous in α. ETL is the *average* loss in the distribution area beyond VaR in the extreme left-tail i.e. average of all VaRs from level α up to 1 (BCBS, 2011):

$$ETL_{\alpha} \equiv \frac{1}{1-\alpha}\int_{\alpha}^{1} VaR_{cl}(L)dc$$

where L = a random loss with distribution function F_L, $\propto \epsilon (0,1)$ = confidence level close to 1. Similar to VaR, ETL represents a common consistent risk measure across different portfolio assets made of different securities and takes account of correlations correctly. Besides satisfying the postulate of sub-additivity, ETL is also a better risk measure than

VaR given its greater generalizability as a risk measure as well as better optimization properties resulting in use with more efficient optimization methods (Dowd, 2007).

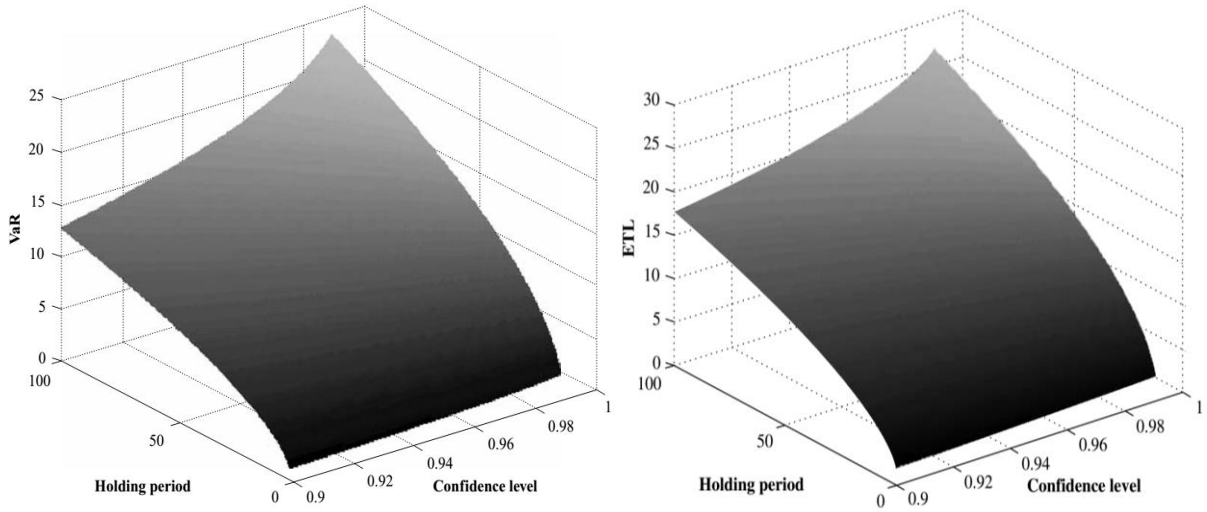


Fig. 7-9. Comparison of How VaR and ETL vary with the Two Parameters.

As seen in Fig. 7-9 (Dowd, 2007), just like the VaR surface, the ETL surface portrays its variation w.r.t. to the two parameters. A comparison of how VaR varies as compared with ETL surface showing maximum possible loss approaching 25σ for VaR relative to 30σ for ETL.

ETL, not being a point-specific estimate, also somewhat mitigates the influence of choosing different confidence intervals on risk management decisions. This point is all the more critical for cyber risk modeling given that point estimates cannot be modeled based on reliable historical data as such data is sparse. As frameworks of cyber risk management focus on categorical rank order of risks rather than specific point estimates, they also seem consistent with ETL. It is important to reiterate however that ETL gives only 'Expected' value that is the average value of risk in the left tail if the related VaR confidence level is exceeded. Hence, even though ETL is a more conservative estimate than VaR, it is only the average or 'expected' loss in the left tail beyond VaR α. *The actual loss (and related risk), however, could be more extreme than the average of the left tail risk. Hence, ETL does not provide any information about the severity of loss by which VaR is exceeded*. For more precise tail risk analysis of extreme events, *Extreme Value Theory* techniques (Embrechts et al., 1999; Gumbel, 2004; Pickands III, 1975) such as Block Maxima and Peaks over Threshold represent more sophisticated techniques. Computationally mathematically demanding and often constrained by lack

of adequate representative data for extreme events, those techniques may also result in broad confidence intervals and weak significance estimates.

7.8 Marginal and Systemic ETL for Cyber Risk Modeling

Related to Expected Shortfall or Expected Tail Loss are additional measures that focus on the incremental risk of each of the *units* (assets, portfolios, firms, entities, devices, agents, etc.) of risk in a given *risk portfolio* as well as the systemic (system wide) risk. **Marginal Expected Shortfall** (MES) or **Marginal Expected Tail Loss** (METL) measures how much incremental tail risk a specific *unit* adds to the overall tail risk of the *portfolio* of all such units. In the context of a financial institution, it helps determine how each group's risk taking adds to the financial institution's overall risk at intra-enterprise level, or, how each institution's risk taking adds to the overall financial system risk at the inter-enterprise level (Acharya et al. 2010). Mapped from finance to cyber domain, MES (or METL) measures the *incremental* tail risk that a specific cyber risk *unit* adds to the *overall* risk of the *portfolio* of such cyber risk units. As discussed in an earlier chapter, at the intra-enterprise level, such units could be units of cyber risks related to specific groups or departments or divisions. MES can then be estimated as the specific unit's expected cyber risk related loss as a part of the overall expected loss of the enterprise. At the inter-enterprise level, such units could be units of cyber risks related to specific enterprises. MES can then be estimated as the specific enterprise's cyber risk related loss as a part of the overall system wide loss where the system is composed of multiple enterprises.

The notion of **Systemic Expected Shortfall** (SES) or **Systemic Expected Tail Loss** (SETL) takes into account the *externalities* characterizing cyber risks discussed earlier. In finance domain, externalities result from specific units taking large risks and taking on too much leverage (debt) thus causing risk to other units system wide. In cyber domain, externalities result from specific units not taking specific cybersecurity countermeasures or 'taking on' (assuming) too much cyber risk such as by violating even the baseline norms (e.g. use of Windows XP systems with missing upgrade paths that are *known* to be vulnerable) thus causing risk to other units system wide. Mapping from finance domain to cyber domain, SES is therefore the probability of an aggregate cyber crisis times the conditional loss of a specific unit in such a crisis (Acharya et al. 2010). The important point is that the expectation is conditional on a system wide cyber crisis such

as at the inter-enterprise level. Hence, SES measures a specific unit's propensity to be exposed to cyber risk when the system as a whole is exposed to cyber risk. In turn, it further increases the interdependence and correlations of system wide cyber risks discussed earlier as well as related tail risks and systemic risks.

In the finance domain, both MES and SES calculations are based on the ES measure. Considering enterprise level return R as a sum of each unit's (negative loss, i.e.) return r_i, and considering y_i as the weight of the specific unit in the risk portfolio, total return is (Acharya et al. 2010):

$$R = \sum_i y_i r_i$$

From the definition of ES discussed before, the formulation of ES is then given by:

$$ES_\alpha = -\sum_i y_i E\left[r_i | R \leq q_\alpha\right].$$

MES is then interpreted as the sensitivity of the overall risk to exposure y_i to each unit i:

$$\frac{\partial ES_\alpha}{\partial y_i} = -E\left[r_i | R \leq q_\alpha\right] \equiv MES_\alpha^i.$$

The other measure, SES, would be of potential interest to regulators who are increasingly interested in determining and controlling externalities related to cyber risk exposures from specific firms. A recent example in Banking and Finance includes the December 10, 2014 'New Cyber Security Examination Process'[172] announced by the New York State Department of Financial Services[173] which is being interpreted by some as a 'signal of increased proactive regulator interest[174]'. Another recent example relevant to all US industries and companies is the US President's proposed legislation of Jan. 12, 2015 requiring all US companies to notify consumers of a data breach within 30 days[175].

In finance domain, SES is the key measure of each firm's expected contribution to systemic risk and thus captures externalities related to its assumed risk. That risk measure on a relative basis can be used for differential taxation of firms with differential respective (externalities related) contributions to systemic risk[176]. In the

[172] http://www.dfs.ny.gov/banking/bil-2014-10-10_cyber_security.pdf
[173] http://www.dfs.ny.gov/about/press2014/pr1412101.htm
[174] http://www.alston.com/Files/Publication/b9785fea-f457-46b8-9739-e1c558ff2d63/Presentation/PublicationAttachment/61c0d644-bb3f-49f9-a1f4-ecea6a9defce/Cyber-Alert-New-York-State-Inquiries-into-Insurance-Company-Cybersecurity-Practices.pdf
[175] http://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission
[176] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1595075

context of financial risk regulation, the default expected shortfall DES^i for bank i is defined as the expected loss in bankruptcy for bank i. A bank's SES is defined as the amount by which its equity w_1^i drops below its target level computed as fraction z of assets a^i in case of a systemic crisis. It is the shortfall relative to its capital asset holding requirement and is hence interpreted as shortfall contributing to systemic risk (Acharya et al. 2010).

$$SES^i \equiv E\left[\bar{I} \cdot (za^i - w_1^i)\right] \qquad DES^i \equiv -E\left[I_i \cdot w_1^i\right]$$

$\bar{I}$ is the indicator for the occurrence of systemic distress and I_i is the indicator of default by firm i in the above expressions for SES and DES.

The 'bankruptcy' event in the finance domain may be interpreted as 'complete business disruption' event in the cyber domain. A plausible example is the case of recent Sony (SPE) hack that was devastating enough to disrupt the firm's entire information infrastructure and destroy most of its data. Hence, in case of the SPE hack, DES will be the expected loss from 'complete business disruption' resulting from the cyberattack. Unless there are regulatory mandated expected levels of cybersecurity, it may be difficult to find a direct analog of SES in the cyber domain. Regardless, the point is evident that if any specific firm's cyber risk 'spills over' (because of externalities of cyber risk discussed earlier) and impacts other firms beyond it, the extent of that risk corresponds to SES. Another related measure that is used in finance called CoVaR has similar implications in capturing the marginal contribution of a specific firm to the overall systemic risk (Adrian & Brunnermeier, 2011). The above measures assess the risk posed by specific firms under financial distress ('business disruption') to other firms which can be controlled by using regulatory disincentives such as taxation and insurance mandates.

Prior discussion focused on the model risks, tail risks, systemic risks, and, ETL model and extensions which are useful improvements over the VaR models. It is important to mention extreme risks which seem particularly relevant to the cyber domain given the unique nature of cyber risks. The notion of extreme risks can be appreciated by thinking of very rare events which may happen very infrequently but may result in highly disastrous losses. In popular language, we hear about those events

in terms such as '100-year storm[177]', or '100-year flood[178]'. Such an event has 1% chance of occurring every year. Fig. 7-10 from a presentation at the Valuation Actuary Symposium of September 23-24, 2013, illustrates the point about 99% VaR denoting a 100-year storm.

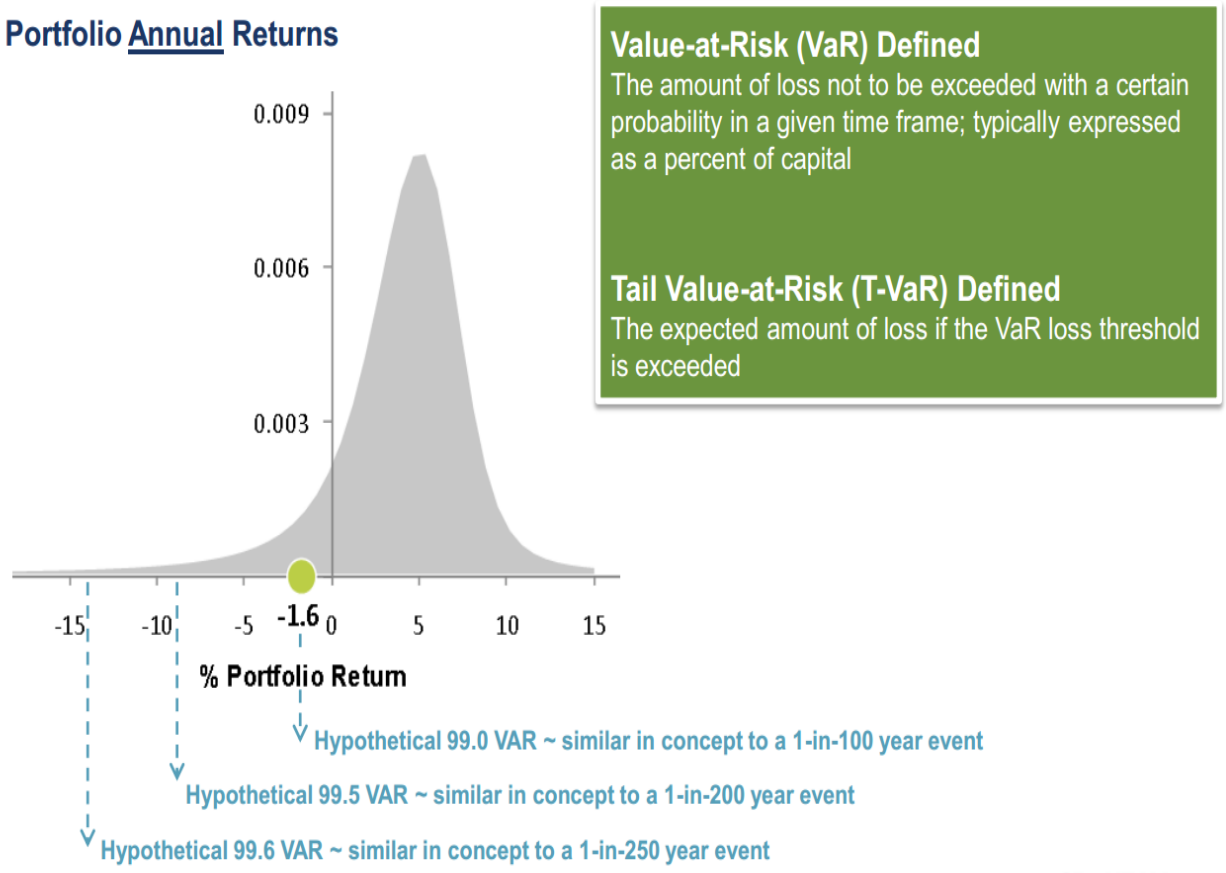


Fig. 7-10. How VaR and ETL Predict a '100-Year Storm'.

There is an important caveat about treating such statistical frequencies of occurrence *literally* particularly based on *normality* and *linearity* assumptions as most actuaries know. In the real world of *sociotechnical* phenomena such as financial markets and cyberspace, such assumptions of normality and linearity of models may simply not apply(Lohr, 2008[179]; Heires, 2012[180]; Derman & Wilmott[181]). Fig. 14 from the same SOA presentation shows another slide confirming that 'The world is usually not normal.'

[177] http://www.cnbc.com/id/101032241
[178] http://www.nytimes.com/2008/09/07/business/worldbusiness/07iht-07ltcm.15941880.html
[179] http://www.nytimes.com/2008/11/05/business/05risk.html

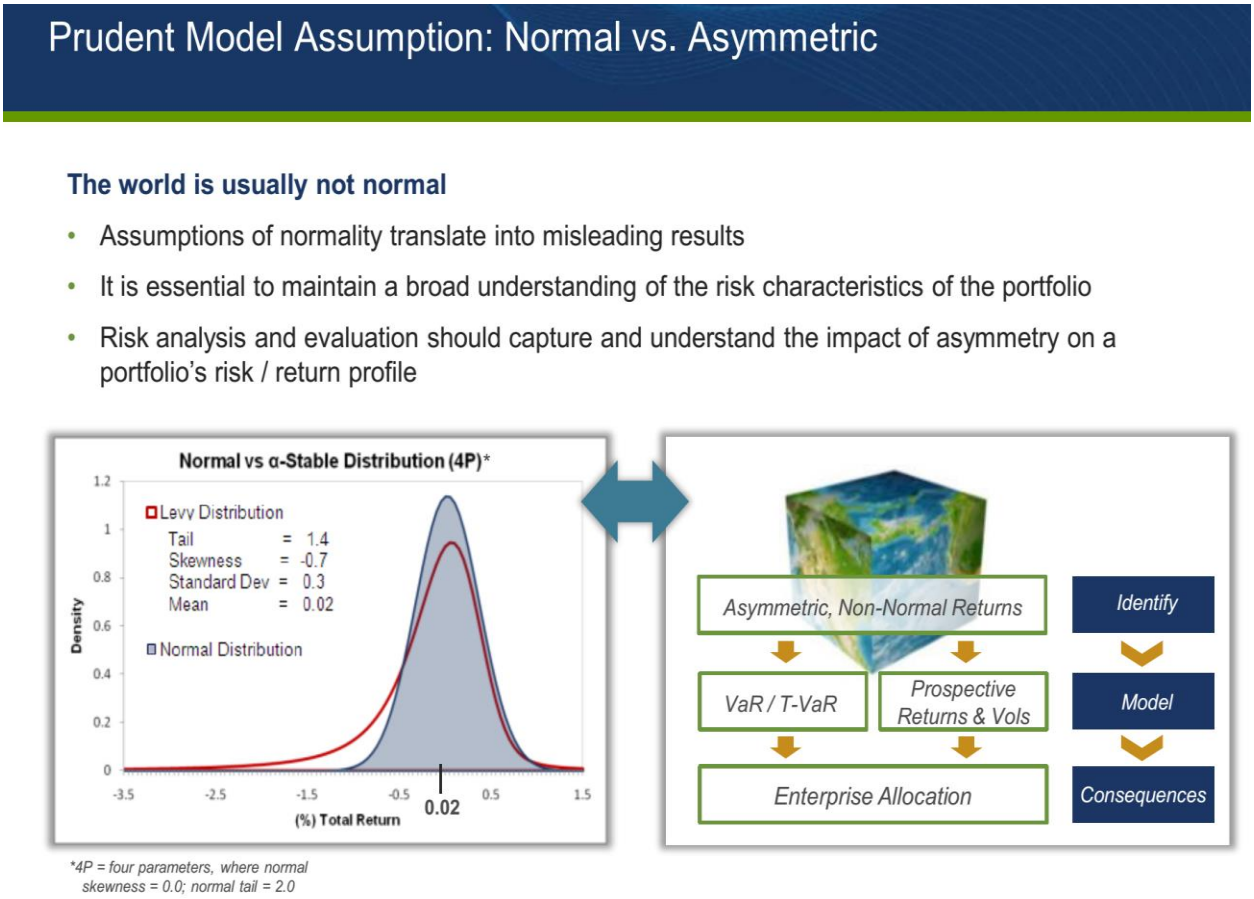


Fig. 7-11. 'The world is usually not normal.': World beyond Normality is Non-Normal

Consistently, many bankers too agree that most of the (sociotechnical)[182] world is *anything but normal* (Haldane & Nelson, 2012)[183]: "Normality has been an accepted wisdom in economics and finance for a century or more. *Yet in real-world systems, nothing could be less normal than normality. Tails should not be unexpected, for they are the rule.* As the world becomes increasingly integrated – financially, economically, socially – interactions among the moving parts may make for potentially fatter tails. Catastrophe risk may be on the rise." **The key problem seems in modeling *risk* while hoping to manage *uncertainty*** (Knight, 1921)[184,185,186]. More on this central concern of both theory

[180] http://www.rmmagazine.com/2012/08/29/finance-isnt-science-why-wall-streets-models-will-always-have-limitations/
[181] http://www.businessweek.com/stories/2008-12-30/financial-models-must-be-clean-and-simple
[182] http://www.yogeshmalhotra.com/publications.html
[183] http://www.bankofengland.co.uk/publications/Documents/speeches/2012/speech582.pdf
[184] http://www.econlib.org/library/Knight/knRUP.html
[185] http://www.yogeshmalhotra.com/blackswans.html

and practice of cyber risk modeling and risk management is discussed in the next concluding chapter.

7.9 Recommended Future Research

Our prior analysis established much stronger and greater *interdependence* and *correlations* in case of cyber risks as compared with financial risks modeled by VaR. Hence, it can be expected in case of cyber risks that assumptions of normality and linearity may *not* hold[187,188]. Therefore, we need to further advance research on cyber risk modeling to *catastrophic* risks or *cat* risks mentioned in our earlier analysis. Related 'extreme events' are modeled using theories such as *extreme value theory*[189] (EVT) and statistical distributions such as *power law distributions*. Additionally, there is also critical need for advancing *risk modeling* research to focus on *uncertainty management* (Malhotra, 2004)[190], (Haldane & Nelson, 2012)[191].

Normality assumptions are justified by the Central Limit Theorem which applies only to the central mass of the probability density function, but not to the extreme tail risks. Hence, when dealing with extremes, i.e., very high or very low confidence levels, extreme value theory is used for modeling and not the normality assumptions. EVT is the theory of modeling events that occur with very small probability (Embrechts, et al, 1999). Hull[192] (2012) describes Extreme Value Theory (EVT) as the science of estimating the tails of a distribution that forms the theoretical underpinnings for the *power law*. The effect of EVT is to smoothen and extrapolate the tails of an empirical data distribution. EVT is the method of extracting an accurate measure of estimated loss given limited data around an extreme event (Darbyshire & Hampton, 2012)[193]. Implementation of EVT faces the challenges of lack of adequate and reliable extreme data (as is currently applicable in case of cyber risk attack losses), demarcating the beginning and end of the tail, distinguishing if it is a 'fat tail', and the choice of method for parameters estimation.

---

[186] http://www.yogeshmalhotra.com/risk.html
[187] Taleb, N. N. (2010). *The Black Swan: The Impact of the Highly Improbable Fragility*. Random House LLC.
[188] Taleb, N. (2004). *Fooled by randomness: The hidden role of chance in life & in the markets.* Random House LLC.
[189] http://www.casact.org/library/studynotes/embrechts_extremevalue.pdf
[190] http://www.yogeshmalhotra.com/blackswans.html
[191] http://www.bankofengland.co.uk/publications/Documents/speeches/2012/speech582.pdf
[192] Hull. (2012). *Risk Management and Financial Institutions*, John Wiley & Sons.
[193] Darbyshire, P., & Hampton, D. (2012). *Hedge Fund Modeling and Analysis Using Excel and VBA* (Vol. 644). John Wiley & Sons.

The greatest challenge particularly in case of cyber risk and cyber insurance modeling in using EVT and power law distribution analysis is that they require tail risk and tail loss data. The process of the EVT begins with the consideration of the exceedances over thresholds, i.e., data values that represent extreme values given the specification of the extreme. Our prior analysis already established the lack of available data on critical losses related to cyber risks given SEC filings which represent publicly available data indicate 'non-materiality.' Some of the recent regulatory and compliance trends at the Federal and state levels briefly reviewed in prior discussion may possibly facilitate availability of such data in the future. Hence, future research is recommended on advancing cyber risk and cyber insurance modeling with specific focus on extreme value theory and power law distributions as reliable data becomes available.

Chapter 8.

Beyond Risk Modeling to Uncertainty Management

> "It is this 'true' uncertainty, and not risk, as has been argued, which forms the basis of a valid theory of profit and accounts for the divergence between actual and theoretical competition."
> -- Frank H. Knight, in *Risk, Uncertainty, and Profit*, Houghton Mifflin, 1921.

8.1 Key Contributions to Cyber Risk Insurance Modeling

Unlike other risks, cyber risk poses a uniquely different set of exposures as it is intertwined with the ***medium*** *and the* ***message*** *in the increasingly global* ***interconnected***, ***distributed***, *and,* ***networked*** *world of* ***digital communications*** *powered by* ***universal use*** *and* ***reuse*** *of enabling* ***global monocultures*** *of information and communication technologies and* ***standard computing network protocols***.

To avert the impending national Cyber risk and Cyber-insurance disaster based upon large-scale commercial reliance upon quantitative models with inherent model risks, tail risks, and systemic risks in current form, this dissertation made the following key contributions.

- First, we developed the first known Cyber-Finance-Trust framework for Cyber insurance modeling to analyze how finance risk entangled with Cyber risk further exacerbates the systemic, interdependent, and correlated character of Cyber risks.
- Second, we developed the first known model risk management framework for Cyber insurance modeling as model risk management has received sparse attention in Cyber risk assessment and Cyber insurance modeling.
- Third, our review of quantitative models in Cyber risk and Cyber insurance modeling developed the first known analysis establishing significant and extreme *model risks*, *tail risks*, and, *systemic risks* related to predominant models in use.
- Fourth, we developed an empirical study of VaR and Bayesian statistical inference methodologies with specific guidance for containing model risks by applying multiple simple and advanced models for cross-checking the reliability of VaR.

- Fifth, we developed an analysis of the Markov Chain Monte Carlo Models, Gibbs Sampling and Metropolis-Hastings statistical computing algorithms for enabling Bayesian statistical inference methodologies to minimize model risk in Cyber risk and Cyber insurance risk modeling for the specific context of cybersecurity.

- Sixth, we developed the first known portfolio theory based framework for Cyber insurance modeling with guidance to minimize model risks, tail risks, and systemic risks inherent in models in commercial Cyber insurance modeling.

- Finally, given increasing role of uncertainty in cyber (and financial) risk modeling and management, we developed a framework for enabling Knightian uncertainty management relating it to model risk management.

The specific focus of respective contributions of corresponding chapters was as follows. **Chapter 1** developed the background context of the cyber risk assessment and cyber insurance modeling industry. **Chapter 2** developed the first known cyber-finance-trust framework to analyze how global financial risk intertwined with global cyber risk further exacerbates the *systemic*, *interdependent*, and *correlated* character of cyber risks. **Chapter 3** developed the first known systematic basis for analysis of model risk management for cyber risk and cyber insurance as model risk management has received sparse attention in cyber risk and cyber insurance related contexts. **Chapter 4** developed the first known analysis establishing significant and extreme model risk and *tail risk* based on a review of the quantitative models in predominant commercial application and use for cyber risk and cyber insurance modeling. **Chapter 5** developed a baseline empirical study of similar quantitative models with specific guidance for containing model risks related to above quantitative models and model risks associated with related statistical inference methodologies. **Chapter 6** developed an analysis of the statistical computing algorithms that can be used for enabling statistical inference methodologies for containing model risk in cyber risk and cyber insurance modeling for the specific context of cybersecurity. **Chapter 7** developed alternative quantitative models for cyber risk and cyber insurance modeling to minimize model risks, tail risks, and systemic risks inherent in currently predominant models in commercial cyber risk and cyber insurance modeling. **Chapter 8** develops a framework for enabling Knightian uncertainty management relating it to model risk management given increasing uncertainty related to risk modeling of cyber risk.

8.2 Recommendations for Cyber Risk Insurance Modeling

The objective of the above contributions is to advance modeling, use, practice, and research related to cyber insurance risk modeling. Specifically, by recognizing the unique defining characteristics of cyber risk as compared with financial risk, developers and users of such models can make prudent choices of quantitative models. The difference between making prudent choice and otherwise is amply evident in how misuse, abuse, or simply neglect of quantitative financial risk models contributed to drastic underestimation and mis-estimation of risk leading to the Global Financial Crisis.

To facilitate insight and intuition into the unique defining characteristics of cyber risk and how it is entangled with cyber finance and cyber warfare, we developed the above frameworks. Those frameworks facilitated our discovery and analysis of cyber risk. We anticipate others can also better understand both measurable and unmeasurable attributes of the dynamically evolving cyber risks with the aid of those frameworks. Such understanding should contribute to advancing both theory and practice of cyber risk assessment and cyber risk modeling.

Prior analyses determined exponentially high systemic risks and tail risks in the context of cyber risks as compared with financial risks modeled by VaR and other models. Above observations were based on observations about high levels of interconnections, correlations, and interdependencies in case of cyber risks not evident in case of other risks. Such characteristics of cyber risk will lead us to expect that statistical normality of distributions should be even less normal in case of cyber risk than in case of financial risk. Hence, models of statistical probabilistic distributions of expected losses based on normality assumptions cannot be relied upon for modeling cyber risk related losses.

Therefore, it follows that VaR will be even a less unreliable model for assessing potential financial loss in case of cyber risk than it has been in the case of financial risk. We developed focus on empirical application of model risk management of VaR models that are currently predominant in cyber insurance modeling. In ensuring that multiple simple as well as sophisticated models are used to cross-check reliability and validity of VaR models, we recommend other users to similarly focus on multi-methods to reduce model risks.

Also, given predominance of *known* systemic risks in case of cyber as compared to finance, VaR is not the right model to use given that it is unsuitable for modeling systemic risks. This specific point was discussed earlier in the discussion on statistical coherent risk measures. Specifically, VaR does not meet the criteria of sub-additivity as noted in that discussion, hence it is unsuitable for modeling systemic risks. Therefore, the *prudent choice* for cyber risk insurance models is to advance beyond VaR to T-VaR (also known as ETL, ES, etc. as discussed in a prior chapter). To enable the transition, we also empirically demonstrated the application of the proposed T-VaR (ES, ETL) models. Based on our analysis highlighting significant model risk of VaR in cyber risk modeling, specifically given its unsuitability for estimating systemic risk, it must be avoided for modeling systemic risks. T-VaR (ES, ETL) models, given their suitability as sub-additive measures, are better suited for modeling systemic risks compared to VaR.

Model risks *arise in use of* specific quantitative *models* (such as VaR vs. T-VaR) as well as specific quantitative *methodologies* (such as classical i.e. NHST vs. Bayesian). Above discussion focused on how to minimize model risks related to quantitative models such as VaR in cyber insurance modeling. In addition, to facilitate understanding about distinction between the two model risks (in use of models and methodologies), we developed analytical understanding of Bayesian inference statistical methodology. That quantitative methodology can facilitate minimization of known model risks inherent in the use of classical NHST inference methodology. As explained in the related chapter, it is not an easy choice given execution and computational resource requirements required for doing meaningful Bayesian analysis. Given computational statistical resource requirements on which Bayesian methodologies are reliant, we also provided analytical understanding about the Monte Carlo Markov Chain algorithms. With the various computational statistical models and methodologies, the cyber risk insurance modeler has a baseline of both classical and more sophisticated models and methodologies to build on and minimize model risk.

8.3 Recommendations for Insurers, Underwriters, Reinsurers

Besides model developers and uses, cyber insurance companies including underwriters and reinsurers need to understand the 'bottom line' of our analysis for helping their bottom line. A specific example provided by a couple of specialists from Bank of England should help drive our point home about understanding the model risk of the model that you are using[194]. Answering why tail risks that arise from fat tails (i.e.,

[194] http://www.bankofengland.co.uk/publications/Documents/speeches/2012/speech582.pdf

kurtosis) are critical, they consider example of an insurance contract designed to guard against catastrophes in the tail of the distribution of outcomes. Based on other contracts, they assume that the above contract pays out if outcomes are more than four-sigma (sigma stands for standard deviations) above their mean value in any one year (or below for the economic series). Under assumption of normality of a model (such as VaR), payouts would be expected very rarely. Such assumptions *implicit in use* of VaR will result in serious under-estimation and mis-estimation of the pricing of catastrophic insurance risk. They highlight that such mis-pricing of insurance contracts in the context of economic and financial series could be enormous and of two orders of magnitude, such as typical multiples of 100 or more.

Consistent with our analysis of sociotechnical risks being higher (as in the case of cyber risks), they further underscore that such mis-pricing is more acute in case of economic catastrophes (such as output crashes) as natural catastrophes (such as earthquakes). They further project the above example of the serious impact of incorrect assumption about statistical normality in terms of extreme events and black swans. Assuming normality, implied probability of a three-sigma decrease in GDP would occur once every 800 years in contrast to its actual occurrence eight times more frequently, i.e., almost once every century. Similarly, assuming normality, implied probability of a three-sigma decrease in equity prices occurs once every 64 years. In reality however it occurs eight times more frequently, i.e., almost once every 8 years. Such are the serious consequences of assuming normality or using a model that assumes normality when the phenomena being modeled is non-normal.

8.4 Recommendations for Cyber Risk Modeling Research

Based upon our analysis of Knight's distinction between risk and uncertainty, statistical distributions, including Gaussian and *all* others, can be used for modeling theoretical risk. Of course, more sophisticated statistical distributions, such as those based upon Power Law distributions, can be used for 'zooming in' specifically on tail risks. However, the model is *not* the reality. As models need to reflect key aspects of reality, they themselves are dependent upon reliable data both in their development and subsequently in their application. This is particularly applicable in the case of cyber risk assessment and cyber risk insurance models that are often hamstrung by lack of adequate and reliable data. Unquestioning reliance on any one specific model, whichever model it is, whether VaR or Gaussian Copula, is a recipe for disaster as the model gets misaligned from reality of the phenomena it is trying to model. The key

objective in using multiple measures and models is to cross-check the reliability and validity of any specific model.

We are observing the ongoing evolution in quantitative modeling from reliance upon point-specific estimates (such as VaR) to range estimates (such as T-VaR or ETL). In addition, we are also observing similar evolution in quantitative modeling methodologies from reliance upon point-specific estimates (such as p-values of NHST) to range estimates (such as Bayesian). In the not too historical past, just preceding mainstream popularity of WWW, statistical averages with their 'p-values' were deemed adequate in scientific research (Nuzzo, 2014)[195]. It was perhaps a function of both the state of the world at the time and the state of our models and measures that made us live with them. Over subsequent years, we have seen the point-estimate based metrics being questioned about actually reflecting the real state of the world. Even, the range-based estimates such as confidence intervals based on the classic NHST are being questioned about their reliability in specific sociotechnical domains[196] (Gelman, 2013). These developments seem to reflect increased uncertainty characterizing the state of the post-WWW cyber era increasingly globally interconnected and interactive sociotechnical world that we inhabit. Hence, risk modeling needs to advance beyond confines of deterministic probabilistic distributions to cater to the needs of an increasingly non-deterministic world challenged by high uncertainty.

8.5 Risk Modeling to Uncertainty Management for Profit

Most critically, it is important to recall what Knight (1921) originally observed and others recently focused on model risk management such as Derman (1996) have emphasized. Often, it is what that may not be measured, i.e., the *real* uncertainty, that may determine the difference between the theory and practice of risk management (or more precisely, 'uncertainty management'). Considering Knight's distinction between risk and uncertainty, he denotes uncertainty as the "true" uncertainty and not risk that really matters for actual purposes (Knight, 1921, p. 9): "It is this 'true' uncertainty, and not risk, as has been argued, which forms the basis of a valid theory of profit and accounts for the divergence between actual and theoretical competition." Hence the

[195] http://www.nature.com/news/scientific-method-statistical-errors-1.14700
[196] http://www.stat.columbia.edu/~gelman/research/published/pvalues3.pdf

theoretical world of academics needs to advance risk modeling to relate to the critical real world needs of uncertainty management.

The practical business challenge still remains in managing uncertainty which may be *objectively* unmeasurable in terms of statistical probabilities at least given currently known methods. In any case, whatever data distributions or combinations thereof are used, such as stochastic simulations and importance sampling, we need to be aware of the primary objective. That key objective of all modeling exercises is to ensure that models reflect the key aspects of reality. Hence the modeler, the decision-maker, the regulator, and, all others involved in developing, testing, managing, or using models need to ensure alignment of the models with the reality. That is simpler said than done given that the reality in the context of global cyberspace with increasing interactions is itself dynamically changing.

The practical experiential world of pragmatists and scholar-practitioners can also benefit by understanding risk modeling as well as its limitations vis-a-vis uncertainty management. For instance, they can benefit from Malhotra's (1999[197], 2002[198], 2001a[199], 2001b[200], 2004[201], 2005[202]) research on 'anticipation of surprise' uncertainty management frameworks[203]. Malhotra acknowledges developing those frameworks starting from the idea mentioned by another scholar-practitioner Steve Kerr.[204]'

Kerr (1995) had mentioned the notion of anticipation of surprise in a Planning Review article. Kerr later went on to be the Chief Learning Officer for General Electric and investment bank Goldman Sachs. Malhotra developed Kerr's idea into a scholarly research program which was applied in global uncertainty management practices by worldwide governments, firms, and institutions[205]. Just like the above frameworks of uncertainty management, practitioners can also benefit from recognizing the potential of advanced statistical and computational modeling technologies. They can apply

[197] http://brint.org/WhiteWaters.pdf
[198] http://www.brint.org/KMEcology.pdf
[199] http://brint.org/intelebusiness.pdf
[200] http://www.brint.org/expertsystems.pdf
[201] http://www.brint.org/WhyKMSFail.pdf
[202] http://www.kmnetwork.com/RealTime.pdf
[203] http://www.yogeshmalhotra.com/blackswans.html
[204] Academy of Management Journal,1975, pp 769-783.
[205] http://www.yogeshmalhotra.com/blackswans.html

creative intuition[206] for managing what Knight calls the critical *unmeasurable* uncertainty while delegating the measurable to human or artificial agent developed and executed models (Yuva, 2002)[207].

The distinction between risk and uncertainty drawn by Knight (1921) in his classic published in 1921 is even more critical today than it was ever before. Risk arises when the statistical distribution of the future can be calculated or is known. Uncertainty arises when this distribution is incalculable, perhaps unknown. As noted by real world practitioners knowledgeable about the greatest stalwarts of serious scholarship (Haldane & Nelson2012)[208]:

> "Many of the biggest intellectual figures in 20th century economics took this distinction seriously. Indeed, they placed uncertainty centre-stage in their policy prescriptions. Keynes in the 1930s, Hayek in the 1950s and Friedman in the 1960s all emphasised the role of uncertainty, as distinct from risk, when it came to understanding economic systems. Hayek criticised economics in general, and economic policymakers in particular, for labouring under a 'pretence of knowledge'. Yet it is risk, rather than uncertainty, that has dominated the economics profession for much of the past 50 years... Uncertainty was, quite literally, ruled out of the equation… But if economic and financial systems operate on the border between order and disorder, ignoring uncertainty is deeply unrealistic."

It is about time to put uncertainty back into the equation of serious uncertainty management and risk modeling scholarship that really matters to the most critical of today's real world concerns. Perhaps that can still save normal science (Kuhn, 2012) from becoming branded as a pseudo-science completely detached and apathetic to the most critical of the cyber era's real world concerns. To seek most empirical of truths, serious economic science, cyber science, and modeling science must all ground themselves in the empirical reality of the most critical concerns that matter to today's real world.

[206] http://blogs.reuters.com/emanuelderman/2011/10/28/intuition-initial-and-final/
[207] http://www.brint.org/SupplyChainManagement.pdf
[208] http://www.bankofengland.co.uk/publications/Documents/speeches/2012/speech582.pdf

References

1. Acharya, V. V., Pedersen, L. H., Philippon, T., & Richardson, M. P. (April 23, 2010). Measuring Systemic Risk. FRB of Cleveland Working Paper No. 10-02.
2. Adrian, T. & Brunnermeier, M.K. (2011, September 15). CoVaR.
3. Akerlof, G. A. (1970). The market for" lemons": Quality uncertainty and the market mechanism. The Quarterly Journal of Economics, 488-500.
4. Alloway, T. (2012, October 18). Morgan Stanley shows the 'flaky' side of model. Financial Times.
5. Artzner, P., Delbaen F., Eber, J.M., and Heath, D. (1997). Thinking Coherently. Risk, 10, November, 68-71.
6. Artzner, P., Delbaen, F., Eber, J. M., & Heath, D. (1999). Coherent Measures of Risk. Mathematical Finance, 9(3), 203-228.u
7. Aussenegg, W., & Miazhynskaia, T. (2006). Uncertainty in Value-at-Risk Estimates under Parametric and Non-Parametric Modeling. Financial Markets and Portfolio Management, 20(3), 243-264.
8. Baer, W.S. (2007, June). Cyberinsurance in IT Security Management. Security & Privacy, IEEE, 5(3), 50-56.
9. BCBS. (2011, January). Messages from the academic literature on risk measurement for the trading book, Bank for International Settlements, Working Paper No. 19, 31.
10. BCBS. (2013, October). Fundamental Review of the Trading Book: A Revised Market Risk Framework. Basel Committee on Banking Supervision.
11. Beichl, I. & Sullivan, F. The Metropolis Algorithm. Computing in Science and Engineering, 2(1), pp. 65-69, January/February 2000.
12. Berkowitz, J., & O'Brien, J. (2002). How Accurate Are Value-at-Risk Models at Commercial Banks? Journal of Finance, 57(3), 1093–1111.
13. Berkowitz, J., Christoffersen, P. F., & Pelletier, D. (2011). Evaluating Value-at-Risk Models with Desk-Level Data. Management Science, 57(12), 2213-2227.
14. Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis†. The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1), 131-158.
15. Bodin, L. D., Gordon, L. A., Loeb, M. P. (Feb. 2005). Evaluating Information Security Investment Using the Analytic Hierarchy Process. Communications of the ACM.
16. Borison, A., & Hamm, G. (2010, Fall). How to Manage Risk (After Risk Management Has Failed). MIT Sloan Management Review, 51–57.
17. Boucher, C. M., Daníelsson, J., Kouontchou, P. S., & Maillet, B. B. (2014). Risk models-at-risk. Journal of Banking & Finance.
18. Casarin, R., Chang, C.-L., Jimenez-Martin, J.-A., McAleer, M., & Pérez-Amarald, T. (2013). Risk management of risk under the Basel Accord: A Bayesian approach to forecasting Value-at-Risk of VIX futures. Mathematics and Computers in Simulation, 94, 183–204.
19. Casella, G. & George, E. I. (August, 1992). Explaining the Gibbs sampler. The American Statistician, 46 (3), pp. 167-174.
20. Cebula, J. J. & Young, L. R. (2010), "A Taxonomy of Operational Cyber Security Risks," Technical Note CMU/SEI-2010-TN-028, CERT Carnegie Mellon University.

21. Cebula, J. J.,Popeck, M.E., & Young, L. R. (2014), “A Taxonomy of Operational Cyber Security Risks Version 2,” Technical Note CMU/SEI-SEI-2014-TN-006, CERT Carnegie Mellon University.
22. Chen, J. & Rosenthal, J. S. (March, 2012). Decrypting Classical Cipher Text Using Markov Chain Monte Carlo. Statistics and Computing, 22(2), pp. 397-413.
23. Christoffersen, P. F. (2012). Elements of financial risk management (2nd ed.). Waltham, MA: Academic Press.
24. Cornish, E. A., & Fisher, R. A. (1937). Moments and Cumulants in the Specification of Distributions. Extrait de la Revue de l'Institute International de Statistique, 4, 1-14.
25. Danezis, G. & Troncoso, C. (18 August, 2009). The Application of Bayesian Inference to Traffic analysis. Technical Report: MSR-TR-2009-112. Microsoft Research.
26. Danielsson, J., James, K., Valenzuela, M., & Zer, I. (2014). Model Risk of Risk Models. Finance and Economics Discussion Series, Divisions of Research & Statistics and Monetary Affairs. Working Paper. Federal Reserve Board, Washington, D.C.
27. Darbyshire, P., & Hampton, D. (2012). Hedge fund modelling and analysis using Excel and VBA. Chichester, West Sussex; Hoboken, N.J.: Wiley.
28. Darbyshire, P., & Hampton, D. (2014). Hedge fund modelling and analysis using MATLAB®. Hoboken: Wiley.
29. Derman, E. & Wilmott, W. (2008, December 30). Financial Models Must Be Clean and Simple. Bloomberg BusinessWeek.
30. Derman, E. (1996). Model Risk Quantitative Strategies Research Notes (April ed.): Goldman, Sachs & Co.
31. Derman, E. (2009, November 24). On Fischer Black: Intuition is a Merging of the Understander with the Understood. Talk Delivered at Bloomberg, NYC.
32. Derman, E. (2014, March 21). Speech at Commencement 2014 to Berkeley MSE Grads. Berkeley MFE Commencement.
33. Diaconis, Persi. (April, 2009). The Markov Chain Monte Carlo Revolution. Bulletin of the American Mathematical Society, 46(2), pp. 179-205.
34. Dowd, K. (2007). Measuring market risk. John Wiley & Sons.
35. Dowdy, J., Hubback, J., Layton, D. & Solyom, J. (Autumn 2011) Can you hack it? Managing the cybersecurity challenge. McKinsey on Government.
36. Dunlavy, D.M., Hendrickson, B. & Kolda, T.G. (2009, February). Mathematical Challenges in Cybersecurity. Sandia Report SAND 2009-0805 Unlimited Release Printed February 2009. Sandia National Laboratories. CA.
37. Eckhardt, R. & S. Ulam. (1987). John von Neumann and the Monte Carlo Method. Los Alamos Science, Special Issue, pp. 131-141.
38. Embrechts, P., Resnick, S. I., & Samorodnitsky, G. (1999). Extreme Value Theory as a Risk Management Tool. North American Actuarial Journal, 3(2).
39. Eraker, B. (2001). “MCMC analysis of Diffusion Models with Application to Finance,” Journal of Business & Economic Statistics, 19 (2), pp. 177-191.
40. Evans, N.D. (2014, May 19). The importance of zero-trust and an adaptive perimeter in cyber fortifications. Computerworld.

41. Forrester. (2013, September). Supporting The Zero Trust Model Of Information Security: The Important Role of Today's Intrusion Prevention Systems. A Custom Technology Adoption Profile Commissioned By IBM. Forrester Research.
42. Furon, T., A. Guyader, and, F. Cerou. (Dec., 2012). Decoding fingerprints using the Markov Chain Monte Carlo method. IEEE International Workshop on Information Forensics and Security (WIFS). pp. 187-192.2-5.
43. Gamerman, Dani & Lopes, Hedibert F. (2006). Markov Chain Monte Carlo: Stochastic Simulation for Bayesian Inference (2nd edn). Chapman & Hall/CRC, Boca Raton, FL.
44. Gelfand, A. E., & Smith, A. F. M. (1990). Sampling-Based Approaches to Calculating Marginal Densities. Journal of the American Statistical Association, 85(410), 398-409.
45. Gelman, A., J. B. Carlin, H. S. Stern, & D. B. Rubin. (2003). Bayesian Data Analysis, 2nd ed., Chapman and Hall/CRC, London.
46. Geman, S. & Geman, D. (November, 1984). Stochastic relaxation, Gibbs distributions and the Bayesian restoration of images. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 6, pp. 721-741.
47. Geyer, C. J. (2011). "Introduction to Markov Chain Monte Carlo." In Handbook of Markov Chain Monte Carlo, Ed. Steve Brooks, Andrew Gelman, Galin L. Jones & Xiao-Li Meng. pp. 3-48. Chapman & Hall / CRC.
48. Gilks, W., S. Richardson, & D. Spiegelhalter, Markov Chain Monte Carlo in Practice. London, U.K.: Chapman and Hall, 1996.
49. GoldSim. (2014). What is the Monte Carlo method? Goldsim Technology Group.
50. Goodwin, T. H. (1998). The Information Ratio. Financial Analysts Journal, 54(4).
51. Green, P.J. (2014). A primer on Markov chain Monte Carlo. University of Bristol. Lecture Notes.
52. Gumbel, E. J. (2004). Statistics of Extremes: Courier Dover Publications.
53. Haldane, A. G., & Nelson, B. (2012, June). Tails of the Unexpected. In Presentation at the Conference: The Credit Crisis Five Years on: Unpacking the Crisis–University of Edinburgh Business School (Vol. 8).
54. Hanawal, M. K. & Sundaresan, R. (12 February, 2010). Randomised attacks on passwords. Technical Report TR-PME-2010-11, DRDO-IISc Programme on Advanced Research in Mathematical Engineering, IISc, Bangalore.
55. Hastings, W. (1970).Monte Carlo sampling methods using Markov chains and their application. Biometrika, 57, pp. 97-109.
56. Heires, K. (2012, August 29). Finance Isn't Science: Why Wall Street's Models Will Always Have Limitations. Risk Management. (Interview with Emanuel Derman).
57. Holmes, C. (2008). Markov Chain Monte Carlo and Applied Bayesian Statistics: A Short Course. Oxford Centre for Gene Function. Oxford University.
58. Hoogerheide, L. F., & van Dijk, H. K. (2008, September 30). Bayesian Forecasting of Value at Risk and Expected Shortfall using Adaptive Importance Sampling. Tinbergen Institute Discussion Paper. TI 2008-092/4.
59. Hu, J. & Yu, X. (January/February, 2009). "A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection" IEEE Network Journal, 23(1).
60. Hull, J., & White, A. (1998). Value at Risk When Daily Changes in Market Variables Are Not Normally Distributed. Journal of Derivatives, 5(3), 9-19.

61. Hull. (2012). Risk Management and Financial Institutions, John Wiley & Sons.
62. Hölmstrom, B. (1979). Moral hazard and observability. The Bell Journal of Economics, 74-91.
63. Ihler, A., J. Hutchins & P. Smyth. (Aug., 2006) “Adaptive event detection with time-varying Poisson processes” ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), Philadelphia, PA.
64. J.P. Morgan. (2008). Investment Performance, Analytics, and Risk: Glossary of Terms: J.P. Morgan Investment Analytics and Consulting.
65. Jackson, P., Maude, D. J., & Perraudin, W. (1998). Bank capital and Value at Risk: Bank of England.
66. Jensen, M. C. (1967). The Performance of Mutual Funds in the Period 1945-1964. Journal of Finance, 23(2), 389-416.
67. Jerrum, M. & Sinclair, A. (1996). “The Markov chain Monte Carlo method: An approach to approximate counting and integration,” in Approximations for NP-Hard Problems, D. Hochbaum, Ed. Boston, MA: PWS Publishing.
68. Jyothsna, V, Ramaprasad, V. V. & Prasad, K. M. (August, 2011). A Review of Anomaly based Intrusion Detection Systems. International Journal of Computer Applications, 28(7).
69. Kass, R., & Raftery, A. (1995). Bayes factor. Journal of American Statistical Association, 90, 773–792.
70. Kerr, S. (1995). Creating the boundaryless organization: the radical reconstruction of organization capabilities. Planning Review, p. 41-45 (September-October).
71. Knight, F. H. (1921). Risk, Uncertainty, and Profit. Hart, Schaffner, and Marx Prize Essays, no. 31. Boston and New York: Houghton Mifflin.
72. Kruschke, J. (October, 2010). Doing Bayesian Data Analysis: A Tutorial Introduction with R. Elsevier, New York.
73. Kruschke, J. K. (2011). Doing bayesian data analysis: a tutorial with R and BUGS. Burlington, MA: Academic Press.
74. Kuhn, T. S. (2012). The structure of scientific revolutions. University of Chicago press.
75. Li, D. X. (2000, April). On Default Correlation: A Copula Function Approach. The RiskMetrics Group. Working Paper Number 99-07.
76. Lohr, S. (2008, November 4). In Modeling Risk, the Human Factor Was Left Out. New York Times.
77. Lynch, S. M. (2007). Introduction to Applied Bayesian Statistics and Estimation for Social Scientists. New York, NY: Springer New York.
78. Malhotra, Y. (1999, March). Knowledge Management for Organizational White Waters: An Ecological Framework. Knowledge Management, 2(6), 18-21.
79. Malhotra, Y. (2001a, Summer). Enabling Next Generation e-Business Architectures: Balancing Integration and Flexibility for Managing Business Transformation. Expert Paper. Intel Corporation, Portland, Oregon.
80. Malhotra, Y. (2001b) Expert Systems for Knowledge Management: Crossing the Chasm between Information Processing and Sense Making, Expert Systems with Applications: An International Journal, 20(1), 7-16.

81. Malhotra, Y. (2002). Information Ecology and Knowledge Management: Toward Knowledge Ecology for Hyperturbulent Organizational Environments, Encyclopedia of Life Support Systems (EOLSS), UNESCO/Eolss Publishers, Oxford, UK.
82. Malhotra, Y. (2004). Why Knowledge Management Systems Fail? Enablers and Constraints of Knowledge Management in Human Enterprises. In Michael E.D. Koenig & T. Kanti Srikantaiah (Eds.), Knowledge Management Lessons Learned: What Works and What Doesn't, Information Today Inc. (American Society for Information Science and Technology Monograph Series), 87-112.
83. Malhotra, Y. (2005, April). Integrating Knowledge Management Technologies in Organizational Business Processes: Getting Real Time Enterprises to Deliver Real Business Performance, Journal of Knowledge Management, Vol. 9, 1, 7-28.
84. Malhotra, Y. (2013a). Bitcoin Protocol: Model of 'Cryptographic Proof' Based Global Crypto-Currency & Electronic Payments System. Global Risk Management Network, LLC, New York.
85. Malhotra, Y. (2013b). Cryptology Beyond Shannon's Information Theory: Preparing for When the 'Enemy Knows the System'. Global Risk Management Network, LLC, New York.
86. Malhotra, Y. (2013c). Number Field Sieve Cryptanalysis Algorithms for Most Efficient Prime Factorization on Composites. Global Risk Management Network, LLC, New York.
87. Malhotra, Y. (2013d). Quantum Computing, Quantum Cryptography, Shannon's Entropy and Next Generation Encryption & Decryption. Global Risk Management Network, LLC, New York.
88. Malhotra, Y. (2014). Markov Chain Monte Carlo Models, Gibbs Sampling, & Metropolis Algorithm for High-Dimensionality Complex Stochastic Problems: Applications in Network and Computer Security. Working Paper. Computational Quantitative Finance-Risk Management. Global Risk Management Network, LLC. Cornell Business & Technology Park, Ithaca.
89. Malhotra, Y. (2014, December 08). Beyond ‘Bayesian vs. VaR’ Dilemma to Empirical Model Risk Management: How to Manage Risk (After Risk Management Has Failed)
90. Malhotra, Y. (2014a). A Risk Management Framework for Penetration Testing of Global Banking & Finance Networks Voice over Internet Protocols. Technical Report. Global Risk Management Network, LLC, New York.
91. Malhotra, Y. (2014b). Analysis of FIX and FAST as Financial Securities Trading and Transactions Messaging Network Protocols. Technical Note. Global Risk Management Network, LLC, New York.
92. Malhotra, Y. (2014c). Analysis of Attack Trees for Mitigating Cybersecurity Attacks on Global Banking & Finance and SCADA Systems. Technical Note. Global Risk Management Network, LLC, New York.
93. Malhotra, Y. (2014d). Future of Bitcoin & Statistical Probabilistic Quantitative Methods: Global Financial Regulation (Interview: Hong Kong Institute of CPAs). Regulatory Compliance Report. Global Risk Management Network, LLC, New York.
94. Malhotra, Y. (2014e). Network Intrusion Detection and Prevention & Active Response: Frameworks, Systems, Methods, Tools & Policies. Technical Notes. Global Risk Management Network, LLC, New York.

95. Malhotra, Y. (2012, January 26). Measuring & Managing Financial & Systemic Risks with Improved Alternatives beyond Value-At-Risk (VaR)–Fordham University.
96. Mandelbrot, B. & Taleb, N. (2005, Jul 17). How the Finance Gurus Get Risk All Wrong. CNN Money.
97. Mandelbrot, B. & Taleb, N. (2006, March 23). A focus on the exceptions that prove the rule. Financial Times.
98. Markowitz, H. (1952). Portfolio selection. The Journal of finance, 7(1), 77-91.
99. Matsui, A., S. Clippingdale, F. Uzawa, & T. Matsumoto. (Aug., 2004).Bayesian face recognition using a Markov chain Monte Carlo method. Vol.3, pp. 918-921. 23-26.
100. Metropolis, N. & Ulam. S. (1949). The Monte Carlo Method. Journal of the American Statistical Association, 44, pp. 335-341.
101. Metropolis, N., Rosenbluth, A., Rosenbluth, M., Teller, A., and Teller, E. (1953). Equations of state calculations by fast computing machines. Journal of Chemical Physics, 21(6), pp. 1087-1092.
102. Meucci, A. (2009). Risk and Asset Allocation (Corr. 3rd printing 2009 edition ed.): Springer.
103. Miazhynskaia, T., Fruhwirth-Schnatter, S., & Dorffner, G. (2003). A Comparison of Bayesian Model Selection based on MCMC with an application to GARCH-Type Models. Adaptive Information Systems and Modelling in Economics and Management Science: Vienna University of Economics & University of Vienna.
104. Morini, M. (2011). Understanding and managing model risk a practical guide for quants, traders and validators (1. ed.). Hoboken: Wiley.
105. Morral, A. R., Price, C. C., Ortiz, D. S., Wilson, B., LaTourrette, T., Mobley, B. W., ... & Willis, H. H. (2012). Modeling Terrorism Risk to the Air Transportation System: An Independent Assessment of TSA's Risk Management Analysis Tool and Associated Methods. RAND Homeland Security and Defense Center.
106. Muramatsu, D., M. Kondo, M. Sasaki, S. & Tachibana. A. (March, 2006). Markov chain Monte Carlo algorithm for Bayesian dynamic signature verification. IEEE Transactions on Information Forensics and Security, 1(1), pp. 22-34.
107. National Futures Association. (2013). Disclosure Documents: A Guide for CPOs and CTAs.
108. Nuzzo, R. (2014, February 12). Scientific method: Statistical errors. Nature.
109. NYS DoFS. (2014, May). Report on Cyber Security in the Banking Sector. New York State Department of Financial Service.
110. Osiewalski, J., & Pajor, A. (2010). Bayesian Value-at-Risk for a Portfolio: Multi- and Univariate Approaches Using MSF-SBEKK Models. Central European Journal of Economic Modelling and Econometrics, 2, 253-277.
111. P Values and Statistical Practice. Gelman, A. (2013, January). Epidemiology. 24(1).
112. Pescatore, J. (2014, September 23). Simple Math: It Always Costs Less to Avoid a Breach Than to Suffer One. SANS Security Trend Line.
113. Peskun, P. (1973). Optimum Monte Carlo sampling using Markov chains. Biometrika, 60, pp. 607-612.
114. Peskun, P. (1981). Guidelines for choosing the transition matrix in Monte Carlo methods using Markov Chains. Journal of Computational Physics, 40, pp. 327-344.

115. Pickands III, J. (1975). Statistical inference using extreme order statistics. The Annals of Statistics, 3(1), 119-131.
116. Robert, C. & Casella, G. (2011b). “A Short History of MCMC: Subjective Recollections from Incomplete Data.” In Handbook of Markov Chain Monte Carlo, Ed. Steve Brooks, Andrew Gelman, Galin L. Jones & Xiao-Li Meng. Chapman & Hall / CRC. pp. 49-66. Chapman & Hall / CRC.
117. Robert, C. & Casella, G. A. (2011a). Short History of Markov Chain Monte Carlo: Subjective Recollections from Incomplete Data. Statistical Science, 26(1), pp. 102-115.
118. Schneier, B. (June 22, 2007). TSA Uses Monte Carlo Simulations to Weigh Airplane Risks.
119. Schneier, B. Did North Korea Really Attack Sony? (2014, December 22). Did North Korea Really Attack Sony? The Atlantic.
120. Scollnik, D. (1996). An Introduction to Markov Chain Monte Carlo Methods and Their Actuarial Applications. Proceedings of the Casualty Actuarial Society LXXXIII. 114-165.
121. Scott, S. L. (1999). Bayesian Analysis of a Two-State Markov Modulated Poisson Process, Journal of Computational and Graphical Statistics, 8, pp. 662-670.
122. Scott, S. L. (2001). Detecting Network Intrusion Using a Markov Modulated Non-homogeneous Poisson Process. Journal of the American Statistical Association.
123. Scott, S. L. (2004). Bayesian Methods for Hidden Markov Models: Recursive Computing in the 21st Century. 45 (1), pp 69-83.
124. Sexauer, S.C. & Siegel, L.B. (2012, June). Managing Tail Risk. Allianz Global Investors White Paper Series.
125. Sharpe, W. F. (1994). The Sharpe Ratio. The Journal of Portfolio Management, 21(1), 49–58.
126. Shi, S. & Mei-feng, S. (07 Sep - 09 Sep, 2012). Study on HMM Based Anomaly Intrusion Detection Using System Calls. 2nd International Conference on Electronic & Mechanical Engineering and Information Technology (EMEIT-2012), Liaoning, China.
127. Simons, K. (1996). Value at Risk - New Approaches to Risk Management. New England Economic Review: Federal Reserve Bank of Boston.
128. Sortino, F., & Forsey, H. (1996). On the Use and Misuse of Downside Risk. The Journal of Portfolio Management.
129. Strohm, C., Engleman, E., & Michaels, D. (Apr 3, 2013). Cyberattacks Abound Yet Companies Tell SEC Losses Are Few. Bloomberg.
130. Taleb, N. (2004). Fooled by randomness: The hidden role of chance in life & in the markets. Random House LLC.
131. Taleb, N. N. (2010). The Black Swan: The Impact of the Highly Improbable Fragility. Random House LLC.
132. Tasche, D. (2002). Expected shortfall and beyond. Journal of Banking and Finance, 26(7), 1519–1533.
133. Trevisan, L. (2012). Pseudo-randomness and de-randomization. ACM Crossroads 18(3), pp. 27-31.
134. Troncoso, C. & Danezis, G. (November 9–13, 2009). The Bayesian Traffic Analysis of Mix Network. CCS '09 Proceedings of the 16th ACM Conference on Computer and Communications Security. pp. 369-379. Chicago, Illinois, USA.

135. Tsay, R. S. (2005). Some MCMC Applications in Time Series Analysis. Lecture Notes: Time Series Analysis. University of Chicago Booth School of Business.
136. Tsay, R. S. (2010). Analysis of Financial Time Series. 3rd Edition. Wiley & Sons. New Jersey.
137. US Fed, & OCC. (2011). Supervisory Guidance on Model Risk Management. (SR Letter 11-7 / OCC 2011-12).
138. US Senate. (2013). JPMorgan Chase Whale Trades: A Case History Of Derivatives Risks And Abuses: U.S. Senate Committee on Homeland Security & Governmental Affairs Permanent Subcommittee on Investigations Hearing.
139. Venkataraman, S. (1997). Value at risk for a mixture of normal distributions: the use of quasi-Bayesian estimation techniques. Economic Perspectives (Vol. March/April, pp. 2-13): Federal Reserve Bank of Chicago.
140. Walsh, B. (26 April, 2004). Markov Chain Monte Carlo and Gibbs Sampling, Lecture Notes for EEB 581.
141. Wigderson, A. (2011, Winter). Randomness, Pseudorandomness, and Derandomization. The Fields Institute for Research in Mathematical Sciences, Fields Notes.
142. Yuva, J. (2002, July). Knowledge Management: The Supply Chain Nerve Center. Inside Supply Management, Institute for Supply Management, pp. 34-43.
143. Zangari, P. (1996). An improved methodology for measuring VAR RiskMetrics Monitor: Reuters/JP Morgan.
144. Zetter, K. (2014, December 17). The Evidence That North Korea Hacked Sony Is Flimsy. Wired.
145. Zhao, J. & K. E. Nygard. (2010). A Dendritic Cell Inspired Security System in Wireless Sensor Networks. FUTURE COMPUTING 2010: The Second International Conference on Future Computational Technologies and Applications.