Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Yogi

Yogesh Malhotra, PhD
Global Risk Management Network, LLC
757 Warren Road, Cornell Business & Technology Park, Ithaca, NY 14852-4892
http://www.linkedin.com/in/yogeshmalhotra
dr.yogesh.malhotra@gmail.com

Presentation at the Cybersecurity Summit
Altria Group Inc. Headquarters,
6601 W Broad St, Richmond, VA

Tuesday, September 15, 2015

Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Four Parts: Intuition, Data, Humans, Models

1. The Cyber-Finance-Trust ™ Framework, 1993-2015
2. Latest Vulnerabilities, Threats, & Risk Mitigation…
3. The Human Factor: The Non-Deterministic 'Variable'
4. Cyber Risk: Quantifying, Modeling, & Valuation

Cybersecurity & Cyber-Finance Risk Management Strategies, Tactics, Operations, &, Intelligence

Enterprise Risk Management to Model Risk Management

Understanding Vulnerabilities, Threats, & Risk Mitigation

Four Parts: Intuition, Data, Humans, Models

Part 1: Intuition

1. The Cyber-Finance-Trust ™ Framework, 1993-2015
2. Latest Vulnerabilities, Threats, & Risk Mitigation…
3. The Human Factor: The Non-Deterministic 'Variable'
4. Cyber Risk: Quantifying, Modeling, & Valuation

"**Intuition** takes intimate knowledge of the world that can be acquired only by careful observation and painstaking effort."

- Dr. Emanuel Derman

Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Cyber Risk

Cyber Risk Loss

Cyber Insurance

Cyber Risk Models

Beyond VaR to

ES, EVT, Power Laws

FINANCE

CYBER

Cyber-Finance Risk Management

From 'Prediction' to "Anticipation of Surprise"

From Risk Modeling to Uncertainty Management

Threat & Vulnerability Analysis

Risk Mitigation

Risk Transfer

Risk Acceptance

Enterprise Risk Management

Finance ⟷ **C**yber

PDC x **T**S ➡ (**E**EO) ➡ **F** ⟷ **C**

Production **D**istribution **C**onsumption Across **T**ime and **S**pace
Efficiency **E**ffectiveness **O**ptimization

ASSESS Risk

Quantitative

Qualitative

- **Pen** Testing

Deterministic

Stochastic

Non-Deterministic

- Scenarios

MANAGE Risk

Enterprise Risk Management

Given enterprise focus on uncertainty management and risk modeling, **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."

- COSO (Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management): Integrated Framework Executive Summary September 2004.

PDC x TS ➡ (EEO) ➡ F ⟷ C

Cyber Risk… A Different Kind of Risk

"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 ICTs and standard computing network protocols."

http://www.FutureOfFinance.org/

PDC x TS ➡ (EEO) ➡ F ⟷ C

Malhotra, Yogesh. Jan. 2015. ***Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance & Advanced Analytics.***

Post-Doctoral Thesis. Thesis Committee: Distinguished Computer Scientists and Cybersecurity Specialists, ***Air Force Research Lab, New York State Cyber Research Institute, New York State.***

Of 'Written' Record

Europe

Kremlin security agency to buy typewriters 'to avoid leaks'

12 July 2013 | Europe

Russia's agency responsible for the Kremlin security is buying typewriters - a move reportedly prompted by recent leaks by WikiLeaks and Edward Snowden.

"Never write if you can speak; never speak if you can nod; never nod if you can wink."

-- 'Same Gaffes, but Now on Twitter', New York Times, June 12, 2011

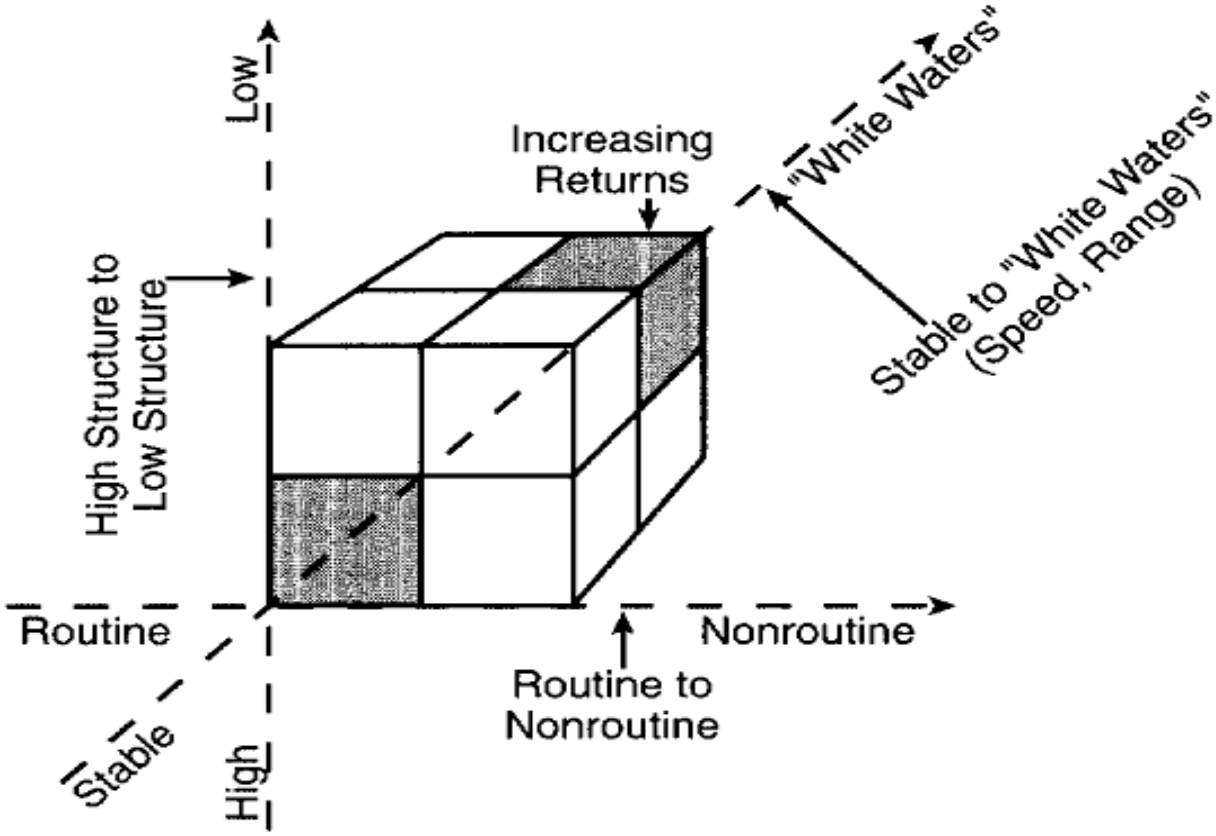
PDC x TS ➡ (EEO) ➡ F ⟷ C

Malhotra, Y. Enabling Knowledge Exchanges for E-Business Communities. Information Strategy: The Executive's Journal, 18(3), Spring 2002, pp. 26-31.

http://www.yogeshmalhotra.com/publications.html

*Malhotra, Y., Enabling Next Generation e-Business Architectures: Balancing Integration and Flexibility for Managing Business Transformation. **Intel Corporation**. Summer 2001.*

Exhibit 1. *KM Performance Continuum*



http://www.brint.org/KnowledgeExchanges.pdf

http://brint.org/KMEbusiness.pdf

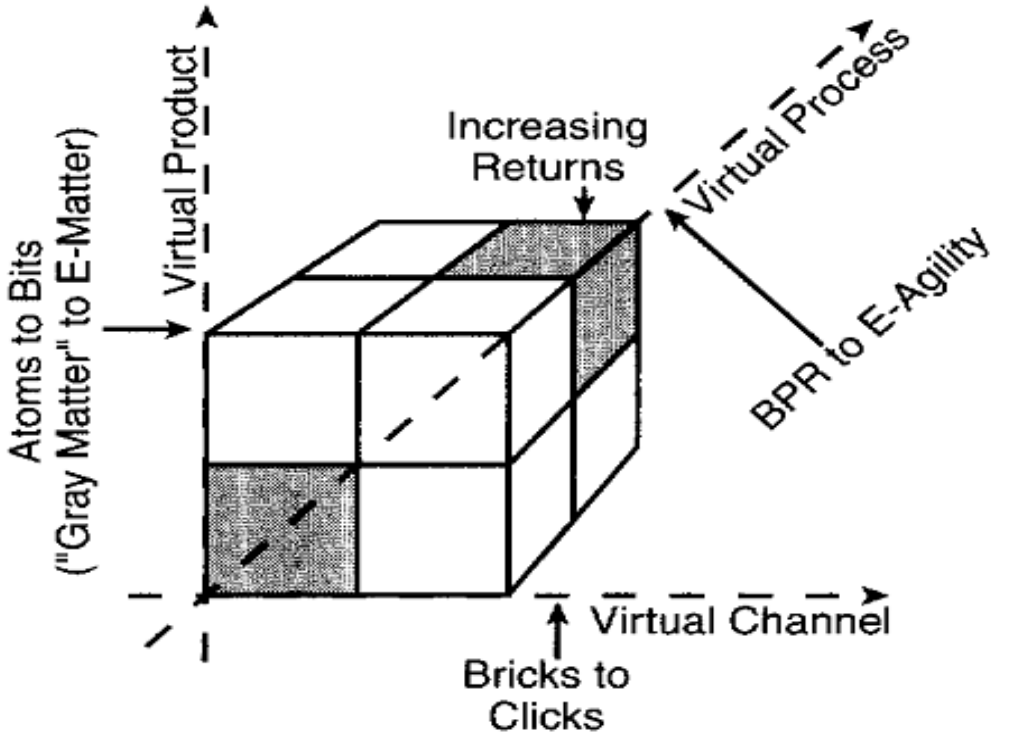
PDC x TS ➡ (EEO) ➡ F ⟷ C

Malhotra, Y. Enabling Knowledge Exchanges for E-Business Communities. Information Strategy: The Executive's Journal, 18(3), Spring 2002, pp. 26-31.

http://www.yogeshmalhotra.com/publications.html

Malhotra, Y., Enabling Next Generation e-Business Architectures: Balancing Integration and Flexibility for Managing Business Transformation. ***Intel Corporation****. Summer 2001.*

Exhibit 2. *E-Business Performance Continuum*



http://www.brint.org/KnowledgeExchanges.pdf

http://brint.org/KMEbusiness.pdf

“History doesn’t repeat itself.”

PDC x TS ➡ (EEO) ➡ F ⟷ C

From ‘Prediction’ to “Anticipation of Surprise”

“The future is moving so quickly that you can’t anticipate it… We have put a tremendous emphasis on quick response instead of planning...
We will continue to be surprised, but we won't be surprised that we are surprised. ***We will anticipate the surprise****.”*

http://www.yogeshmalhotra.com/blackswans.html

Goldman Sachs

Goldman Sachs CEO Lloyd Blankfein told the Australian Institute of Company Directors at a breakfast briefing on Friday, July 26 2013, how investors should prepare for the most extreme risk scenario. His comments about risk management capture the essence of the 'anticipation of surprise' model mentioned above and explained in Dr. Yogesh Malhotra's research papers and research monographs published over the last decade or so.

"The future is moving so quickly that you can’t anticipate it... We have put a tremendous emphasis on quick response instead of planning. We will continue to be surprised, but we won't be surprised that we are surprised. We will anticipate the surprise." - Anticipation of Surprise Framework

Risk Management Analytics beyond 'Prediction' to 'Anticipation of Risk'™ (1993-Current)
On the Origin of the Model Risk Management (MRM) Research Program

Goldman Sachs

"Welcome to the new world of [e-]business!!" Advancing Global ERM and MRM since 1993!

The concept of 'anticipation of surprise' articulated in a strategy journal by scholar-practitioner Steve Kerr, the Chief Learning Officer of GE, and the future Goldman Sachs MD responsible for Goldman Sachs Leadership Development caught Yogesh Malhotra's fascination in 1995. Malhotra's research developed that concept into a comprehensive and actionable framework of **model risk management** of non-deterministic risks such as those associated with black swans through '**anticipation of surprise**' by '**effective challenge of models**'....*

...Over subsequent years, Yogesh Malhotra's influential research and practices on realizing and executing the cyberspace era vision of risk modeling and risk management have guided world's

Goldman Sachs

...Subsequently, the Model Risk Guidance SR11-7/OCC 2011-12 was issued by US Federal Reserve and OCC in aftermath of the Global Financial Crisis of 2008... in 2011-2012. Just around the same time, as illustrated here, Wall Street CEOs, CFOs, and CROs started noting that "we must anticipate risk"...

*...Coincidentally, this applied research program supported by a digital social enterprise has been already developing frameworks and models for the anticipated **future of finance** and **future of risk** starting with the first WWW-browser in 1993... adopted by worldwide firms, governments, and institutions... and written about and recommended by greatest tech visionaries such as Microsoft founder Bill Gates...*

*...Whether you are a pioneer in the **ERM** and **MRM** game or just getting started, you are all "welcome to the new world of*

From 'Prediction' to "Anticipation of Surprise"

PDC x TS ➡ (EEO) ➡ F ⟷ C

Enterprise Risk Management

Risk Management **Analytics** beyond 'Prediction' to 'Anticipation of Risk'™

Model Risk Management *program that anticipated needs of OCC and Wall Street CROs to "anticipate risk" over a decade before they said "we must anticipate risk": with research advancing execution of Model Risk Management (see, e.g., US Fed & OCC SR11-7 & OCC2011-12) such as 'anticipation of risks' by 'effective challenge of models'.*

http://www.yogeshmalhotra.com/ModelRiskManagement.html

Download Research: The Model Risk Management Research Program (1993-Current)
Risk Management Analytics beyond 'Prediction' to 'Anticipation of Risk'™

Model Risk Management program that anticipated needs of OCC and Wall Street CROs to "anticipate ris they said "we must anticipate risk": with research advancing execution of Model Risk Management (see, SR11-7 & OCC2011-12) such as 'anticipation of risks' by 'effective challenge of models'.

- Princeton Quant Trading Conference: Post-HFT Model Risk Management:
  - On the Future of Finance, Future of Risk, & Future of Quant
  Princeton Quant Trading Conference, **2015, April 04**.
  Sponsored by Princeton University Bendheim Center & ORFE, Citadel, KCG.

- SSRN Top-10 Papers: 24 Top-10 Rankings in Model Risk Management, **2015 Jan-May**.
  Econometrics, Stochastic Models, Capital Markets, Risk Modeling, Risk Management, Systemic Risk, VaR, Computational Techniques, Mathematical Methods & Programming, Decision-Making under Risk & Uncertainty, Uncertainty & Risk Modeling.

- Model Risk Management for Quantitative Finance & Cyber Risk Insurance:
  - Risk, Uncertainty, and, Profit for the Cyber Era: 'Knight Reconsidered'
  Post-2008 & Post-Cyber Quantitative Finance Model Risk Management Post Doc Thesis, **2015 Jan**.

- 'Bayesian vs. VaR' to Model Risk Management for Multi-Asset Portfolios
  Advanced Practice beyond MIT Sloan Management Review's Post-Crisis 'MRM Dilemma', **2014 Dec**.

- Quantitative Modeling of Trust Protocols for Mobile Wireless Networks
  Quantitative Models of Trust Frameworks for Mobile Wi-Fi Social Networks, **2014 Dec**.

- Markov Chain Monte Carlo Models for High-Dimension Stochastics
  Advanced Statistical Computing Algorithms for Model Risk Management of Systemic Risks, **2014 May**.

- Penetration Testing Frameworks for Stress Testing Banking VoIP Networks
  Stress Testing Frameworks for Emerging Quantitative Finance Cyber Risk Concerns, **2014 May**.

- Hong Kong Institute of CPAs Interview on the Future of Bitcoin
  Preceded Multiple Predicted Global Regulatory Developments on Bitcoin, **2014 Jan**.

- Bitcoin Protocol, 'Cryptographic Proof', &, Transaction Block Chain
  First Technical Research Report on Bitcoin's Cryptographic 'Proof of Work', **2013 Dec**.

- Number Field Sieve Cryptanalysis Algorithms for Breaking Encryption
  Preceded Google's Public Announcement of Switch from 1024- to 2048-bit RSA, **2013 May**.

- JP Morgan Multi-Asset Portfolio Liquidity Assessment Framework
  Presentation to JP Morgan Senior Leaders, Managing Directors, Portfolio Managers, **2012 Jun**.

- Measuring Financial Risks with Improved Alternatives Beyond VaR
  Preceded *Risk* Magazine Report about Basel Moving Beyond VaR, **2012 Jan**.

- AACSB Reports Impact of Research on Model Risk Management Practices
  AACSB International, **2008 Feb**.

May 3, 2013: Dr. Malhotra calls attention to growing cyber risk in presentation 15 miles from the Air Force Research Laboratory, *"The current officially "recommended" most widely used global standard of encryption [1024-bit RSA] may have already been compromised..."*

May 23, 2013 *8:00 AM : 'Changes to our SSL Certificates', "Google just announced that its HTTPS web pages will be ditching 1024-bit RSA keys in favour of 2048 bits."*

May 20, 2013*: Edward Snowden arrives in Hong Kong just after taking leave from his NSA contractor Booz Allen Hamilton.*

Dr. Malhotra calls attention to growing market risk & operational risk for financial firms:
Excerpt from his presentation 15 miles from the Air Force Research Laboratory (AFRL)

"First, based on available evidence, it is not improbable that the **current officially "recommended" most widely used global standard of encryption [1024-bit RSA] may have already been compromised**. Second, **it would *not* really be a 'surprise'** given that the infamous '40 quadrillion years' challenge for an earlier version of the standard was unraveled in mere 17 years. Third, given recent multi-billion dollar global Finance deals blown by compromise of such technologies, **it is increasingly *critical* to recognize the *exponentially increasing* cybersecurity risk among other Financial Risks**." -- Dr. Yogesh Malhotra in Number Field Sieve Cryptanalysis Algorithms for Most Efficient Prime Factorization on Composites presentation, **May 1, 2013**. *Related Paper published online on May 3, 2013*:
Malhotra, Y. 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, Griffiss Cyberspace, Global Risk Management Network, LLC, **May 3, 2013**.

"**Google** just announced that its HTTPS web pages **will be ditching 1024-bit RSA keys** in favour of 2048 bits." - Anatomy of a change - **Google** announces it will double its SSL key sizes, ***nakedsecurity***, **May 27, 2013**.

Google

http://www.yogeshmalhotra.com/GriffissCyberspace.html

PDC x TS ➡ (EEO) ➡ F ⟷ C

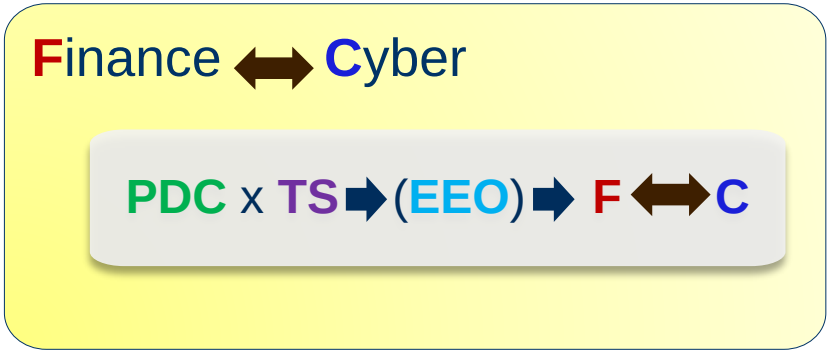
"Almost all risks characterizing *today's information-based financial products and services, financial markets, financial exchanges, financial currencies, and financial economies* are however first and foremost Information risks and Cyber risks. Such Information risks and Cyber risks may not only escalate traditional risks but may also subsume traditional financial risks as brick-and-mortar institutions such as NYSE 'trading floors' become 'museums of financial history'."
-- Dr. Yogesh Malhotra on launch of Griffiss Cyberspace ™, Summer 2013, Rome, NY

Models are Backward Looking…

"I'd just caution you that models are backward-looking.

The future isn't the past."

-- Jamie Dimon, Chairman & CEO, JP Morgan Chase & Co., US Senate Banking Committee hearing, June 13, 2012

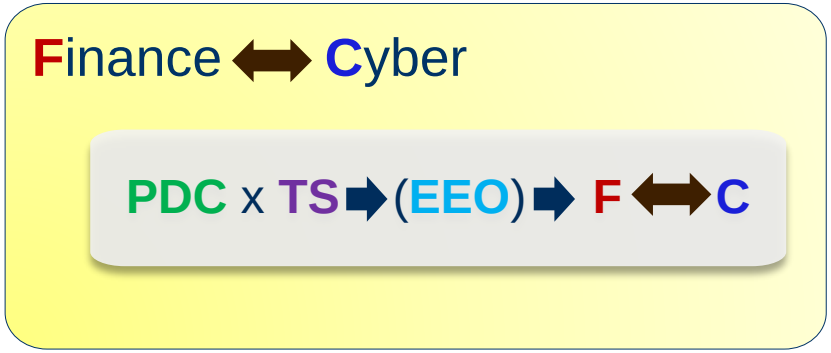


Models are Backward Looking...

"The only Constant used to be Change...
Even it is not Constant anymore...."

-- Dr. Yogesh Malhotra, circa 2011 based on published research circa 1993-2008.

Bayesian vs. VaR: http://www.yogeshmalhotra.com/risk.html



OFFICE OF THE UNDER SECRETARY OF DEFENSE
(COMPTROLLER)

U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller)
"There are many definitions of knowledge management. It has been described as "a systematic process for capturing and communicating knowledge people can use." Others have said it is "understanding what your knowledge assets are and how to profit from them." Or the flip side of that: "to obsolete what you know before others obsolete it." (Yogesh Malhotra)

Inc.

"KM is obsoleting what you know before others obsolete it and profit by creating the challenges and opportunities others haven't even thought about."
-- Dr. Yogesh Malhotra in **Inc.** Interview

"A viable competitive strategy seems to be one that is based upon making your own knowledge obsolete before it is obsolesced by the competition or the environment."

- Yogesh Malhotra in **Business Standard** (India) interview, 2007.


Business Standard
Diwali cheer escapes stock exchanges

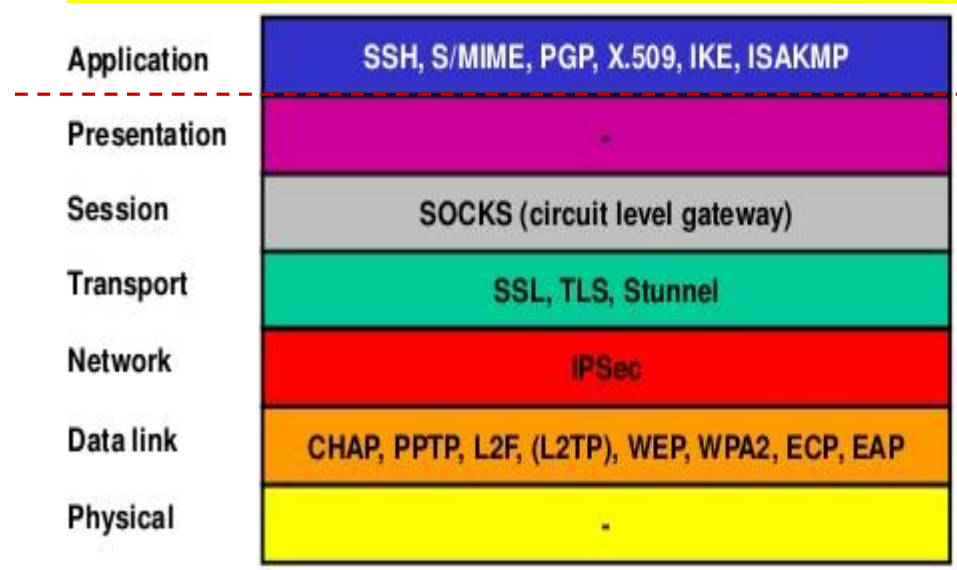
"KM is obsoleting what you know before others obsolete it and profit by creating the challenges and opportunities others haven't even thought about." -- Dr. Yogesh Malhotra, Inc. Technology"
- **U.S. Defense Information Systems Agency Interoperability Directorate**

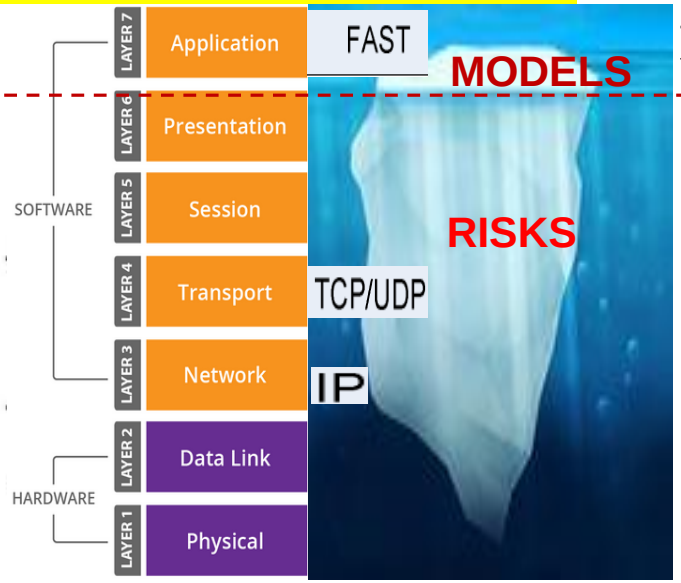
DISA
Defense Information Systems Agency
Department of Defense

EncoreII

Malhotra, Yogesh. Knight Reconsidered: Risk, Uncertainty, and Profit for the Cyber Era: Future of Finance: Cyber-Finance?: Uncertainty Modeling & Model Risk Management, Princeton Quant Trading Conference 2015, Princeton University (April 04, 2015).

CYBER-FINANCE RISK HIDDEN FROM THE HUMAN EYE…
in TIME, and, in SPACE

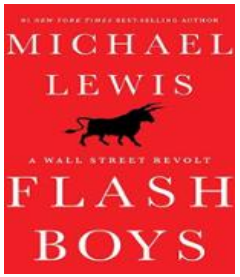




CHAP:	CHallenge Authentication Protocol	IPSec:	IP Security	IKE:	Internet Key Exchange
PPTP:	Point to Point Tunneling Protocol	SSL:	Secure Socket Layer		
L2F:	Layer 2 Framing Protocol	TLS:	Transport Layer Security		
(L2TP:	Layer 2 Tunneling Protocol)	Stunnel:	Secure Tunnel		
WEP:	Wired Equivalent Privacy	SSH:	Secure SHell		
ECP:	Encryption Control Protocol	S/MIME:	Secure MIME		
EAP:	Extensible Authentication Protocol	PGP:	Pretty Good Privacy		
WPA2:	Wireless Protected Access	ISAKMP:	Internet Sec. Assoc. And Key Mgt. Prot.		

Source: indigoo.com

Increasing Knightian Uncertainty



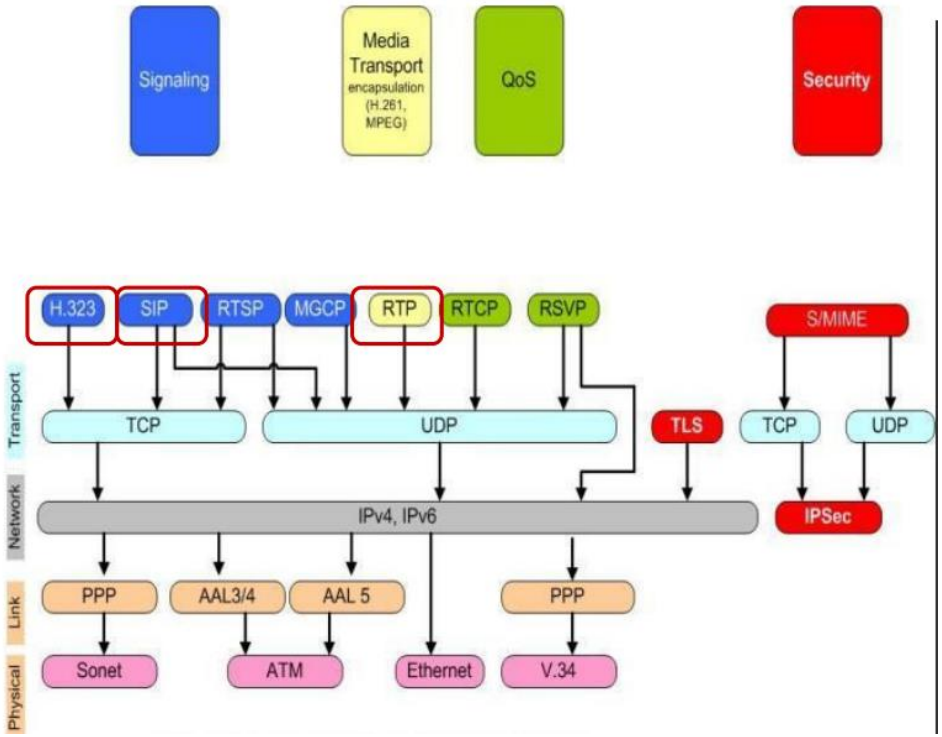
4.5 millisecond - $300 Million

Many Quant Risk Management Groups…

A Risk Management Framework for Penetration Testing of Global Banking & Finance Networks VoIP Protocols, May 8, 2014.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2555098

"A vulnerability inside all current Cisco IP phones allows hackers to take complete control of the devices… It's relatively easy to penetrate any corporate phone system, any government phone system… All current Cisco IP phones, including the ones seen on desks in the White House and aboard Air Force One, have a vulnerability that allows hackers to take complete control of the devices."

Malhotra, Y. A Risk Management Framework for Penetration Testing & Security of Global Banking & Finance networks Voice Over Internet Protocols (May 3, 2014). WWW: Columbia University and Palindrome Technologies.



Future of Bitcoin & Statistical Probabilistic Quantitative Methods: Interview, Hong Kong Institute of CPAs, A+, January 20, 2014.
http://yogeshmalhotra.com/Future_of_Bitcoin.html

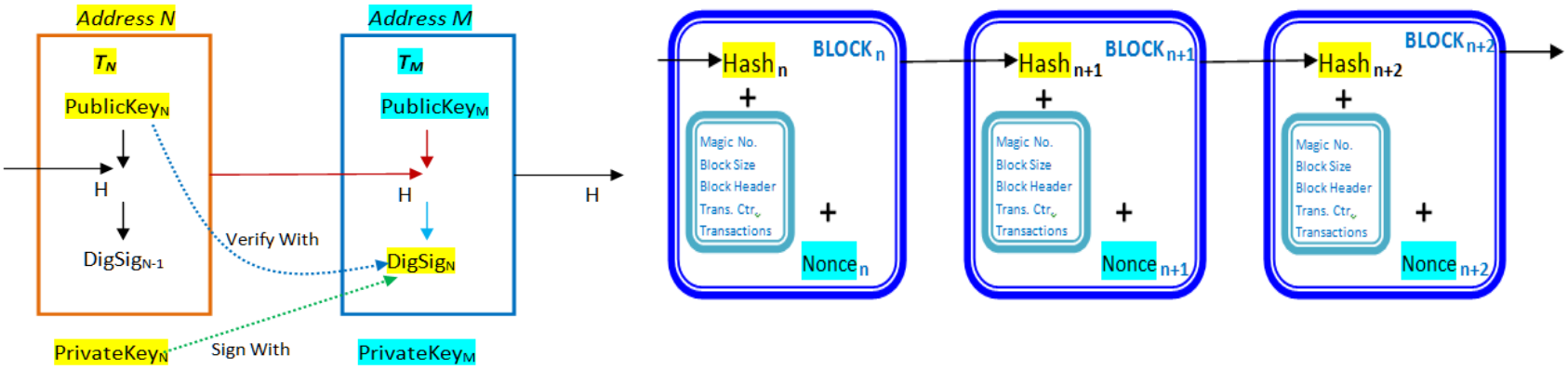
"Recently, such **probabilistic, statistical, and numerical methods** related concerns are in globally popular press related to **cybersecurity controls and compliance**. Earlier, similar probabilistic, statistical, and numerical methods related concerns were in the global popular press in the context of the **global financial crisis**… Likewise, recent developments about **mathematical entropy measures** shedding new light on apparently **greater vulnerability** of prior **encryption mechanisms** may offer additional insights for compliance and control experts. For instance, given related mathematical, statistical and numerical frameworks, analysis may also focus on **potential implications for pricing, valuation and risk models**. The important point is that many such **fundamental assumptions and logic underlying widely used probabilistic, statistical, and numerical methods** may **not as readily meet the eye**."

Bitcoin Protocol: Model of 'Cryptographic Proof' Based Global Crypto-Currency & Electronic Payments System, December 04, 2013.
http://yogeshmalhotra.com/BitcoinProtocol.html

"**Money** is an **interesting construct** that continues to occupy the fancy of many ranging from economists to quantum physicists... The **future of money** becomes "**entangled**" with **future of money laundering** when focus is not on privacy and anonymity alone, but also lack of traceability...

Situated somewhere along the **trajectory** between **real money** and **quantum money**, virtual crypto-currencies based upon '**cryptographic proof**' represent a natural stage in the evolution of global finance... The **future of money**, whatever form it may take – **virtual or quantum**, will quite likely be "entangled" with the future evolution of '**cryptographic proof of work**.'"

Bitcoin Protocol: Model of 'Cryptographic Proof' Based Global Crypto-Currency & Electronic Payments System, December 04, 2013.
http://yogeshmalhotra.com/BitcoinProtocol.html



NIST Guidelines for Public Key Sizes for AES			
ECC key size (bits)	RSA key size (bits)	Key size ratio	AES key size (bits)
163	1,024	1:6	
256	3,072	1:12	128
384	7,680	1:20	192
512	15,360	1:30	256

$$Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z)$$
$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

$$\sum_0^{\{256\}}(x) = ROTR^{2}(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$$
$$\sum_1^{\{256\}}(x) = ROTR^{6}(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)$$
$$\sigma_0^{\{256\}}(x) = ROTR^{7}(x) \oplus ROTR^{18}(x) \oplus SHR^{3}(x)$$
$$\sigma_1^{\{256\}}(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$$

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, May 3, 2013.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553544

Number Field Sieves: Most powerful family of factoring algorithms

1970: 20-digit becoming feasible
1977: RSA "**40 quadrillion years**" challenge by R
1980: 50-digit commonplace, 1984: $2^{251} - 1$ (300 yr. ago…)
1990: 116-digit *quadratic sieve* QS… Pomerance
1994: 129-digit RSA challenge won… within **17 years**!
1996: 130-digit NFS … Pollard, 15% time of QS
2003: 174-digit RSA-576 NFS *number field sieve*
2005: 193-digit RSA-640 NFS
2009: 232-digit RSA-768 NFS
309-digit RSA-1024 Major security implications! $100K.
2012: **S**NFS Factorization of Mersenne number, $2^{1061} - 1$

Size of composite of prime factors being factored.

Number Field Sieve (NFS)
Special Number Field Sieve (SNFS)
General Number Field Sieve (GNFS)
Quadratic Sieve (QS)
Rational Sieve (RS)

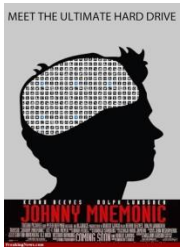
Quantum Computing…

Malhotra, Yogesh. (Invited Presentation). Quantum Computing, Quantum Cryptography, Shannon's Entropy and Next Generation Encryption & Decryption, November 2013.

$$H = -\sum p(x) \log p(x)$$

Information entropy of 27-char. language ~ 4.8 bits per char.
Information entropy of 5,000-char. language ~ 12.3 bits per char.

Entropy increases with a larger repertoire of symbols.
Entropy increases when **meanings detached from symbols**.

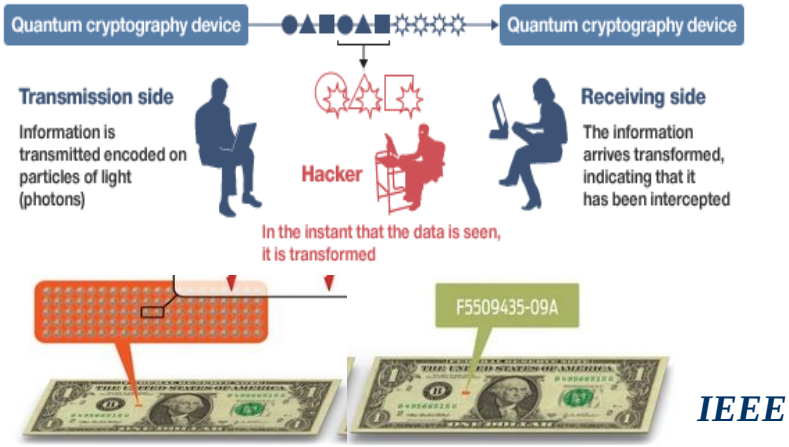


Quantum computer: **qubits**… can be 0, 1, or any **superposition** of both. **n-qubit system**: **superposition** of up to 2^n states ***simultaneously.*** 2^k dimensional vector (a, b, c, d, e, f, g, h)…
complex values: $|a|^2 + |b|^2 + \ldots + |h|^2 = 1$,
$|x|^2$ is probability amplitude of respective state. *Phase* between any two states (complex-valued coefficients)… meaningful.

Quantum Cryptography & Quantum Money

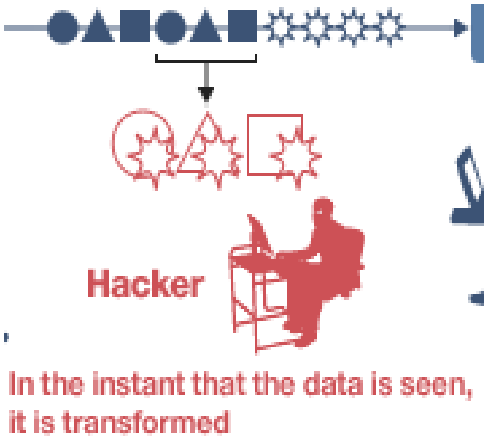
Quantum Cryptography, Shor's algorithm, and Quantum Money
Integer Factorization of large primes and Discrete Logarithm problem.
Quantum computer efficiently find such factors using **Shor's algorithm**.
Decrypt many critical cryptographic systems in polynomial time:
RSA, secure Web pages, encrypted email, many other types of data.

"For a 1024-bit number, Shor's Algorithm requires on the order of 1024^3, about one billion, operations. If each quantum operation took one second, our factorization would last 34 years. If a quantum computer could run at the speed of today's electronic computers (100 million instructions per second and up) then factorization of the 1024-bit number would be a matter of seconds."



IEEE

MITSUBISHI



Cyber-Finance Risk Management

Cyber Risk

Cyber Risk Loss

Cyber Insurance

Cyber Risk Models

Beyond VaR to

ES, EVT, Power Laws

Malhotra, Yogesh. Jan. 2015. Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance & Advanced Analytics. Post-Doctoral Thesis. Thesis Committee: Distinguished Computer Scientists and Cybersecurity Specialists, ***Air Force Research Lab, New York State Cyber Research Institute, New York State.***

http://www.futureoffinance.org/

Malhotra, Yogesh, Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management: How to Manage Risk (After Risk Management Has Failed) for Hedge Funds (December 4, 2014). http://ssrn.com/abstract=2538401. ***JP Morgan Private Bank*** *Quantitative Risk Modeling.*

Malhotra, Yogesh, Markov Chain Monte Carlo Models, Gibbs Sampling, & Metropolis Algorithm for High-Dimensionality Complex Stochastic Problems (May 8, 2014). http://ssrn.com/abstract=2553537.

ASSESS Risk

Quantitative

Qualitative

- **Pen** Testing

Deterministic

Stochastic

Non-Deterministic

- Scenarios

MANAGE Risk

Cyber-Finance Risk Management

SSRN Top Ten Paper Rankings in Quantitative Finance & Econometrics

1. Econometrics: Mathematical Methods & Programming eJournal: May 2015.
2. Information Systems & Economics eJournal: May 2015.
3. Econometrics: Mathematical Methods & Programming eJournal: April 2015.
4. ERN: Computational Techniques (Topic): April 2015.
5. Econometric Modeling: Risk Management eJournal: March 2015.
6. Econometric Modeling: Capital Markets - Risk eJournal: March 2015.
7. Econometric Modeling: Capital Markets - Risk eJournal: March 2015.
8. MRN Operations Research Network eJournal: March 2015.
9. OPER Subject Matter eJournal: March 2015.
10. Systemic Risk (Topic): March 2015.
11. Econometrics: Mathematical Methods & Programming eJournal: March 2015.
12. Econometric & Statistical Methods - Special Topics eJournal: February 2015.
13. Microeconomics: Decision-Making under Risk & Uncertainty eJournal: February 2015.
14. VaR Value-at-Risk (Topic): February 2015.
15. ERN: Uncertainty & Risk Modeling (Topic): February 2015.
16. ERN: Econometric & Statistical Methods (Topic): February 2015.
17. Computational Techniques (Topic): February 2015.
18. OPER: Analytical (Topic): February 2015.
19. ERN: Other Econometrics: Mathematical Methods & Programming (Topic): February 2015.
20. Stochastic Models eJournal: February 2015
21. Econometric Modeling: Capital Markets - Risk eJournal: January 2015.
22. Microeconomics: Decision-Making under Risk & Uncertainty eJournal: January 2015.
23. Uncertainty & Risk Modeling (Topic): January 2015.
24. VaR Value-at-Risk (Topic): January 2015.

Cyber Risk

Cyber Risk Loss

Cyber Insurance

Cyber Risk Models

Beyond VaR to

ES, EVT, Power Laws

ASSESS Risk

Quantitative

Qualitative

- **Pen** Testing

Deterministic

Stochastic

Non-Deterministic

- Scenarios

MANAGE Risk

http://www.futureoffinance.org/

Cyber-Finance Risk Hidden From the Human Eye...

RISK HIDDEN FROM THE HUMAN EYE… in TIME, and, in SPACE

"[T]he approaches to mitigate operating risk associated with the use of models need to evolve to reflect recent trends in the Finance Industry. 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 in high frequency algorithmic trading, or for portfolio risk measurement models 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."
– *Source*: Largest Wall Street Investment Bank

http://www.yogeshmalhotra.com/rankings.html

Of Unknowns: Known* & Unknown*

"As we know,
There are known knowns.
There are things we know we know.
We also know
There are **known unknowns***.
That is to say
We know there are some things
We do not know.
But there are also **unknown unknowns***,
The ones we don't know

We don't know."

-- Donald Rumsfeld, US Secretary of Defense, Feb. 12, 2002

Expert Systems for Knowledge Management: Crossing The Chasm Between Information Processing and Sense Making. Journal of Expert Systems with Applications (Malhotra, 2001).

http://www.brint.org/expertsystems.pdf

Finance ⟷ Cyber

PDC x TS ➡ (EEO) ➡ F ⟷ C

Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Cyber Risk

Cyber Risk Loss

Cyber Insurance

Cyber Risk Models

Beyond VaR to

ES, EVT, Power Laws

FINANCE

CYBER

Cyber-Finance Risk Management

From 'Prediction' to "Anticipation of Surprise"

From Risk Modeling to Uncertainty Management

Threat & Vulnerability Analysis

Risk Mitigation

Risk Transfer

Risk Acceptance

Enterprise Risk Management

Finance ⟷ **C**yber

PDC x **T**S ➡ (**E**EO) ➡ **F** ⟷ **C**

Production **D**istribution **C**onsumption Across **T**ime and **S**pace
Efficiency **E**ffectiveness **O**ptimization

ASSESS Risk

Quantitative

Qualitative

- **Pen** Testing

Deterministic

Stochastic

Non-Deterministic

- Scenarios

MANAGE Risk

Cybersecurity & Cyber-Finance Risk Management Strategies, Tactics, Operations, &, Intelligence

Enterprise Risk Management to Model Risk Management

Understanding Vulnerabilities, Threats, & Risk Mitigation

Four Parts: Intuition, Data, Humans, Models

Part 2: Data

1. The Cyber-Finance-Trust ™ Framework, 1993-2015
2. Latest Vulnerabilities, Threats, & Risk Mitigation…
3. The Human Factor: The Non-Deterministic 'Variable'
4. Cyber Risk: Quantifying, Modeling, & Valuation

"In God we trust, all others bring **Data**."
- Dr. William Edwards Deming

Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Cyber Risk

Cyber Risk Loss

Cyber Insurance

Cyber Risk Models

Beyond VaR to

ES, EVT, Power Laws

FINANCE

CYBER

Cyber-Finance Risk Management

From 'Prediction' to "Anticipation of Surprise"

From Risk Modeling to Uncertainty Management

Threat & Vulnerability Analysis

Risk Mitigation

Risk Transfer

Risk Acceptance

Enterprise Risk Management

Finance ⟷ **C**yber

PDC x **TS** ➡ (**EEO**) ➡ **F** ⟷ **C**

Production **D**istribution **C**onsumption Across **T**ime and **S**pace
Efficiency **E**ffectiveness **O**ptimization

ASSESS Risk

Quantitative

Qualitative

- **Pen** Testing

Deterministic

Stochastic

Non-Deterministic

- Scenarios

MANAGE Risk

Latest Threats & Vulnerabilities Updates

Insider Risk… State of the Art

"Some 88% of companies questioned said they had suffered a security 'incident' over the past year, of which **73%** were **caused by** employees, former employees or customers/suppliers…"

"Nearly half (48%) of respondents claimed finance departments and their employees posed the biggest threat, versus 42% for HR."

"Middle management (37%) was pegged as the highest risk group, compared with just 19% who thought senior managers were the biggest threat, and 12% for execs/admins."

"over two-thirds (67%) of respondents claimed that those working in the office represented a bigger data security risk than those off-site."

"Firms must use a mix of **people, policy and technology** to lock down **insider risk**."

Muncaster, Phil. Finance and HR Staff Labeled Biggest Security Risks, Infosecurity Magazine, 3 Sep. 2015.

'External' & Insider Risk… State of the Art

Four Out of Five US Healthcare Firms Have Been Hit by Cyber-Attacks: "two-thirds claiming **external hackers are the greatest threat**."

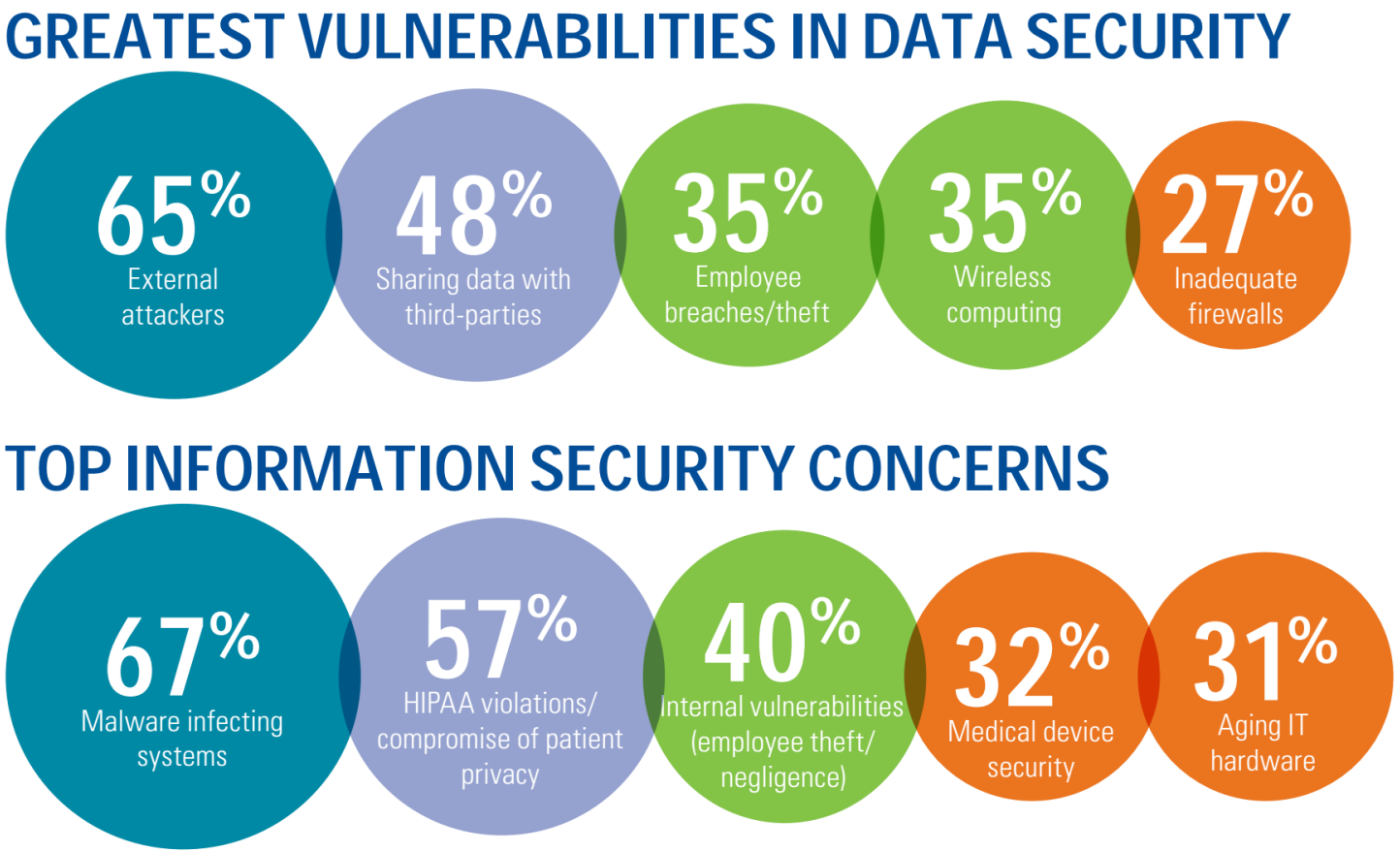
Malware infections (67%), patient privacy-related compromises (57%).

"Outdated clinical technology, insecure network-enabled medical devices, and an overall lack of information security management processes…"

"Healthcare organizations are facing an ever-growing threat thanks to several evolving trends. These include the adoption of digital patient records; the use of antiquated electronic medical record (EMR) systems; the ease of distributing patient data; the internet-facing nature of many systems; and the growing sophistication of attacks."

KPMG (2015). Health Care And Cyber Security: Increasing Threats Require Increased Capabilities.

‘External’ & Insider Risk… Healthcare



KPMG (2015). Health Care And Cyber Security: Increasing Threats Require Increased Capabilities.

‘External’ & Insider Risk… Healthcare

TOP CONCERNS FOR PROVIDERS	
Regulatory enforcement	50%
Litigation	45%
Financial loss	44%
Reputation	39%
Job security	6%

TOP CONCERNS FOR PAYERS	
Financial loss	57%
Reputation	46%
Litigation	38%
Regulatory enforcement	35%
Job security	3%

KPMG (2015). Health Care And Cyber Security: Increasing Threats Require Increased Capabilities.

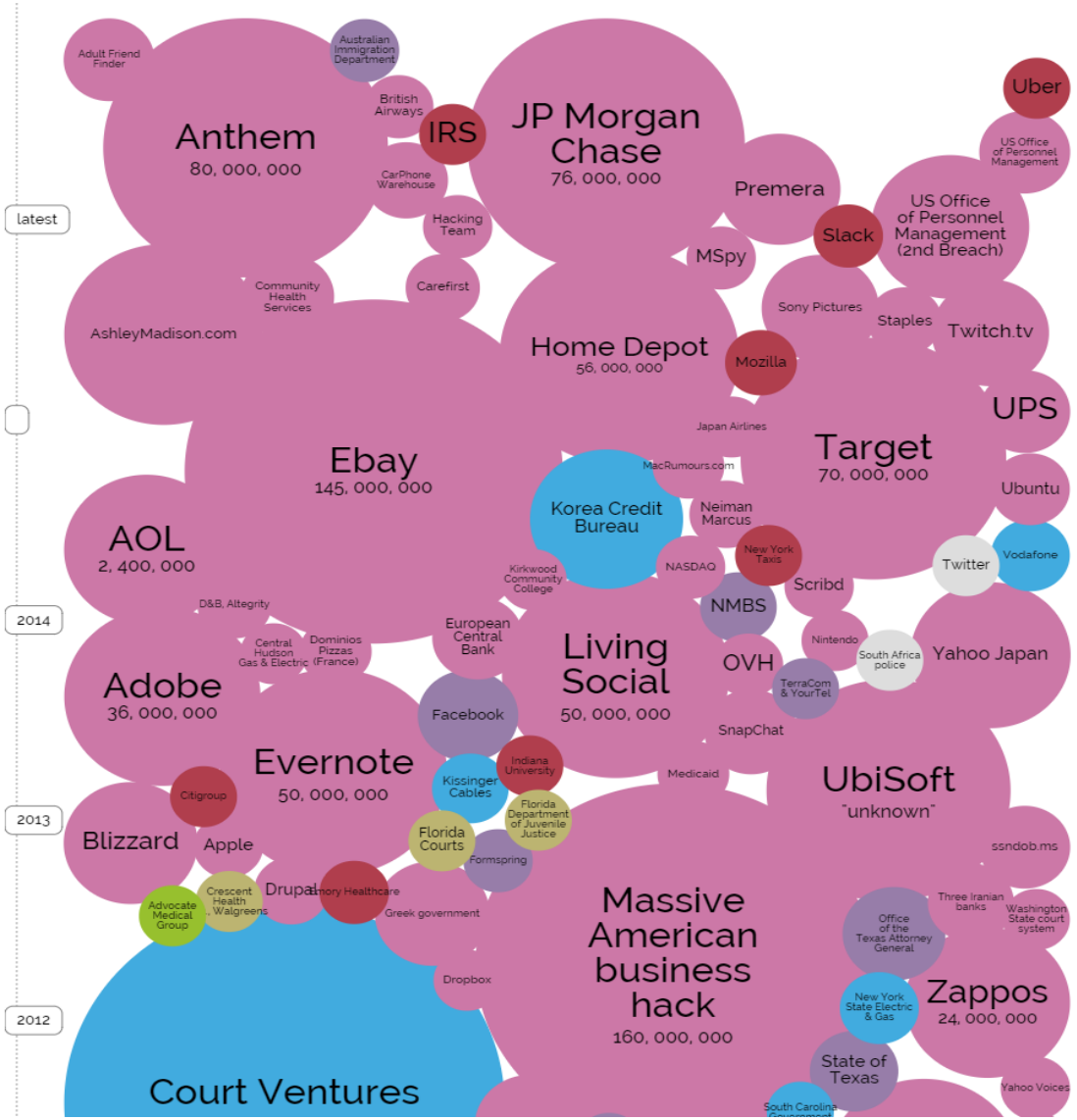
http://www.informationisbeautiful.net

World's Biggest Data Breaches

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

No. of Records Stolen



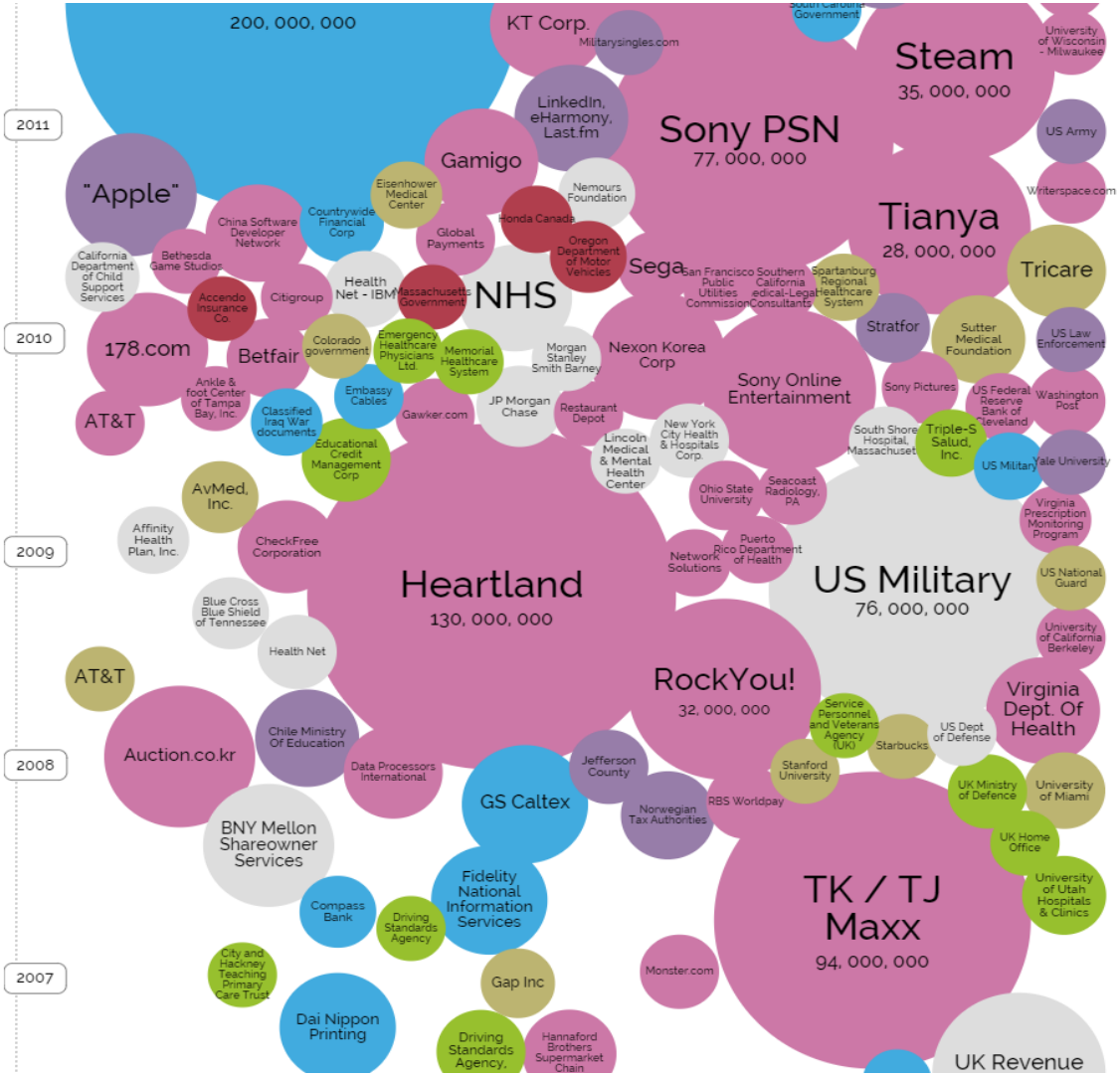
http://www.informationisbeautiful.net

World's Biggest Data Breaches

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

No. of Records Stolen



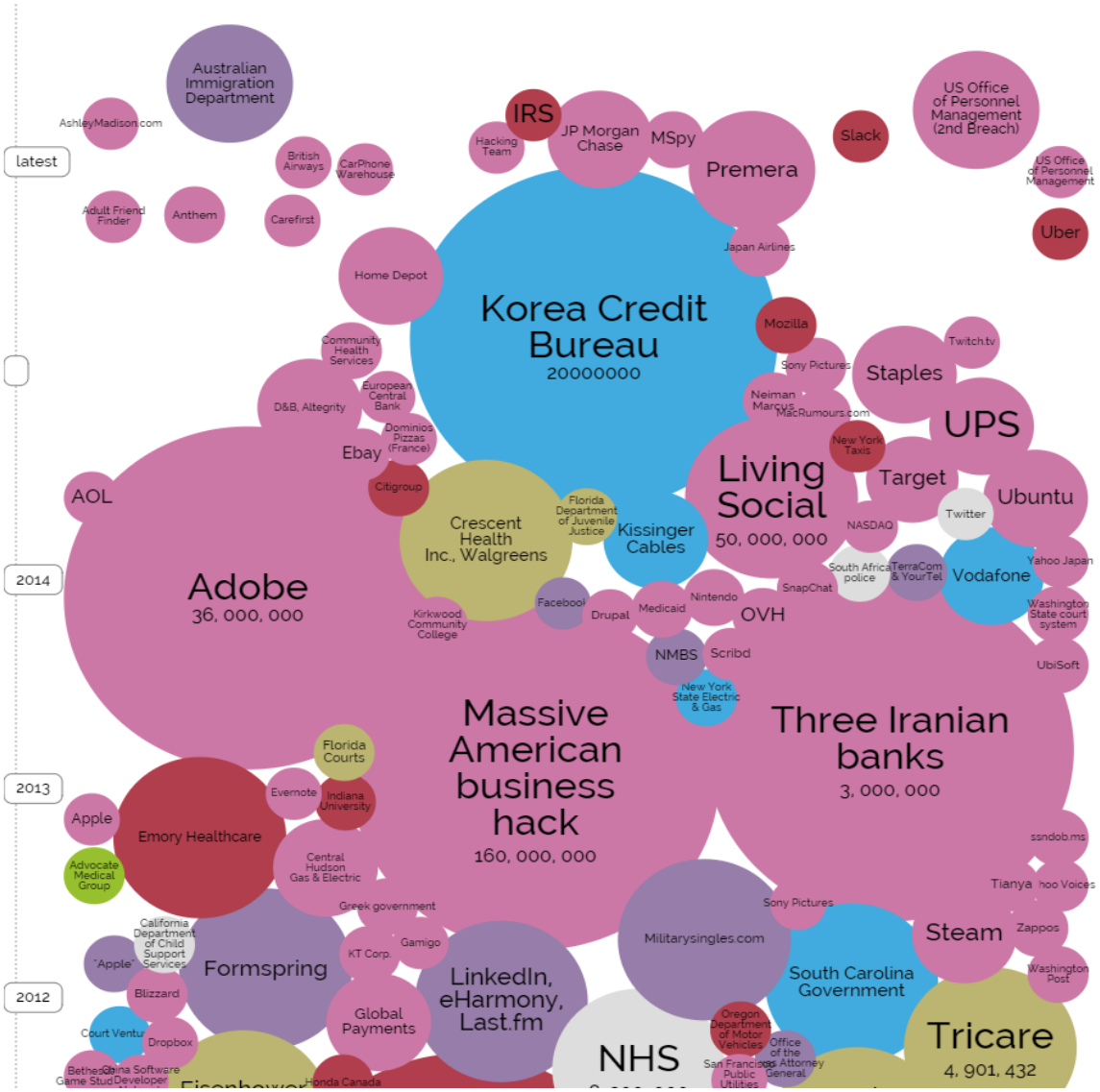
http://www.informationisbeautiful.net

World's Biggest Data Breaches

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

Data Sensitivity



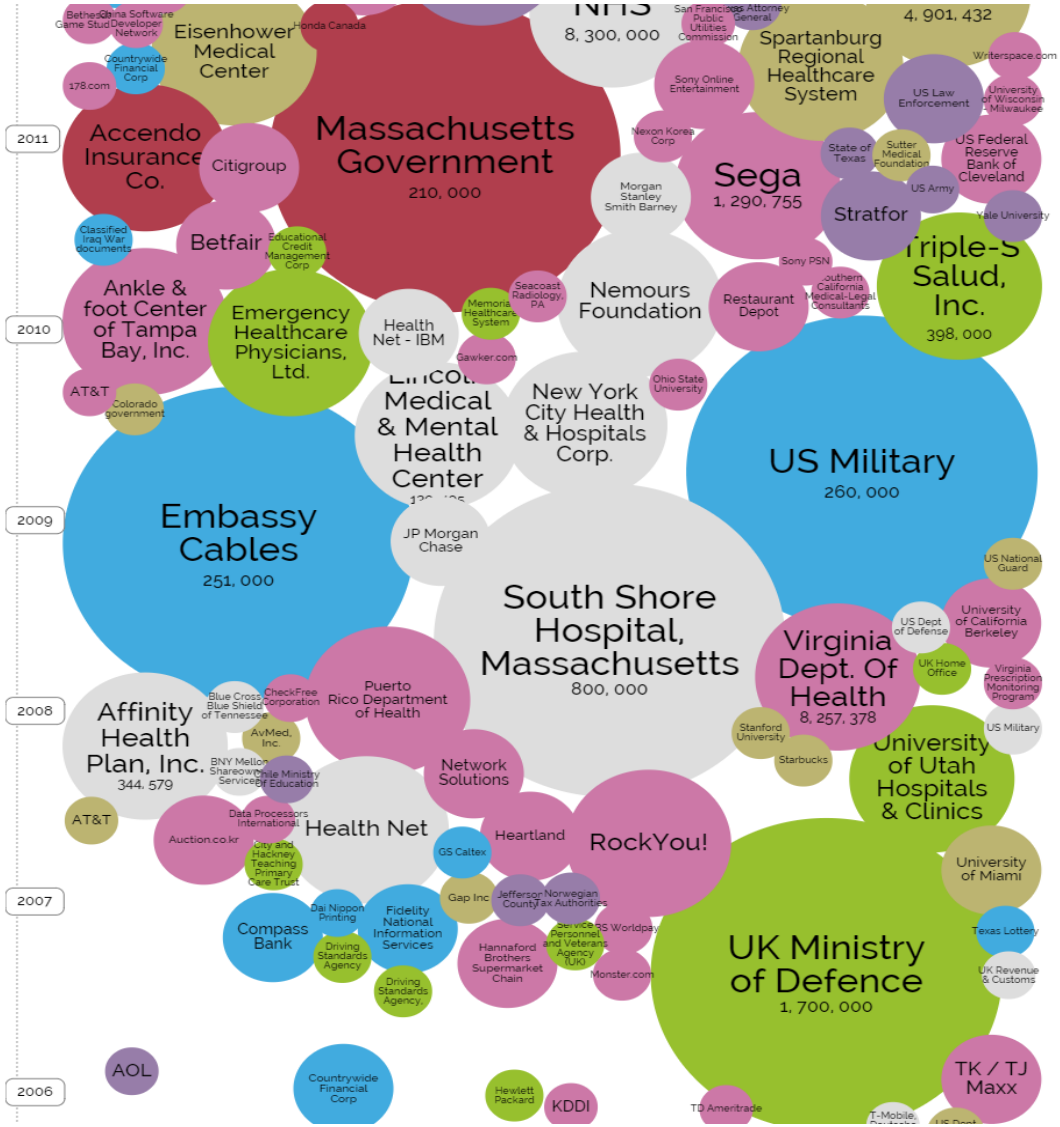
http://www.informationisbeautiful.net

World's Biggest Data Breaches

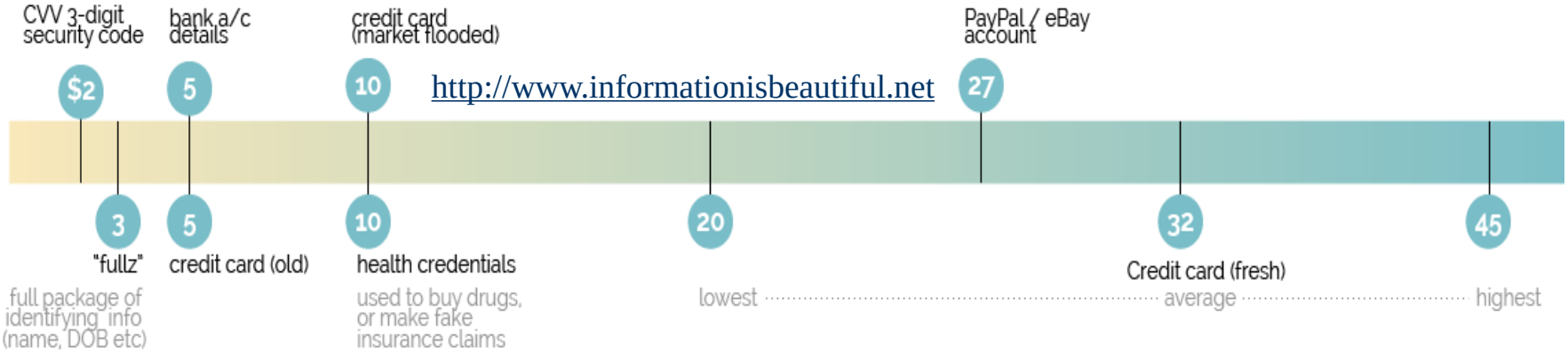
METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

Data Sensitivity



How Much is Hacked Data Worth?



"The value of personal financial and health records is two or three times [the value of financial information alone], because there's so many more opportunities for fraud…" - *Pittsburgh Post-Gazette, March 2015*

"Cyber criminals are selling the information on the black market at a rate of **$50 for each partial EHR**, compared to **$1 for a stolen social security number or credit card number**. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. **EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.**" – *FBI Bulletin, April 2014*

‘External’ Insider Risk… Healthcare

“**Cyber actors will likely increase cyber intrusions** against health care systems—to include medical **devices—due to mandatory transition from paper to electronic health records (EHR), lax cybersecurity standards, and a higher financial payout for medical records in the black market**.

“The **deadline to transition to EHR is January 2015**, which will create an influx of new EHR coupled with more medical devices being connected to the Internet, generating a rich new environment for cyber criminals to exploit.”

“…The **health care industry is not technically prepared to combat against cyber criminals’ basic cyber intrusion tactics, techniques and procedures (TTPs)**, much less against more advanced persistent threats (APTs).”

– FBI Bulletin, April 2014

Increasing External & Insider Risk… Healthcare

More than **90%** of healthcare organizations had a data breach.
40% had more than five data breaches over past two years.

Average cost of a data breach estimated more than **$2.1 million**.

50% have **~0 confidence** in ability to detect all patient data loss or theft.

For first time **criminal attacks** top cause of data breaches in healthcare.

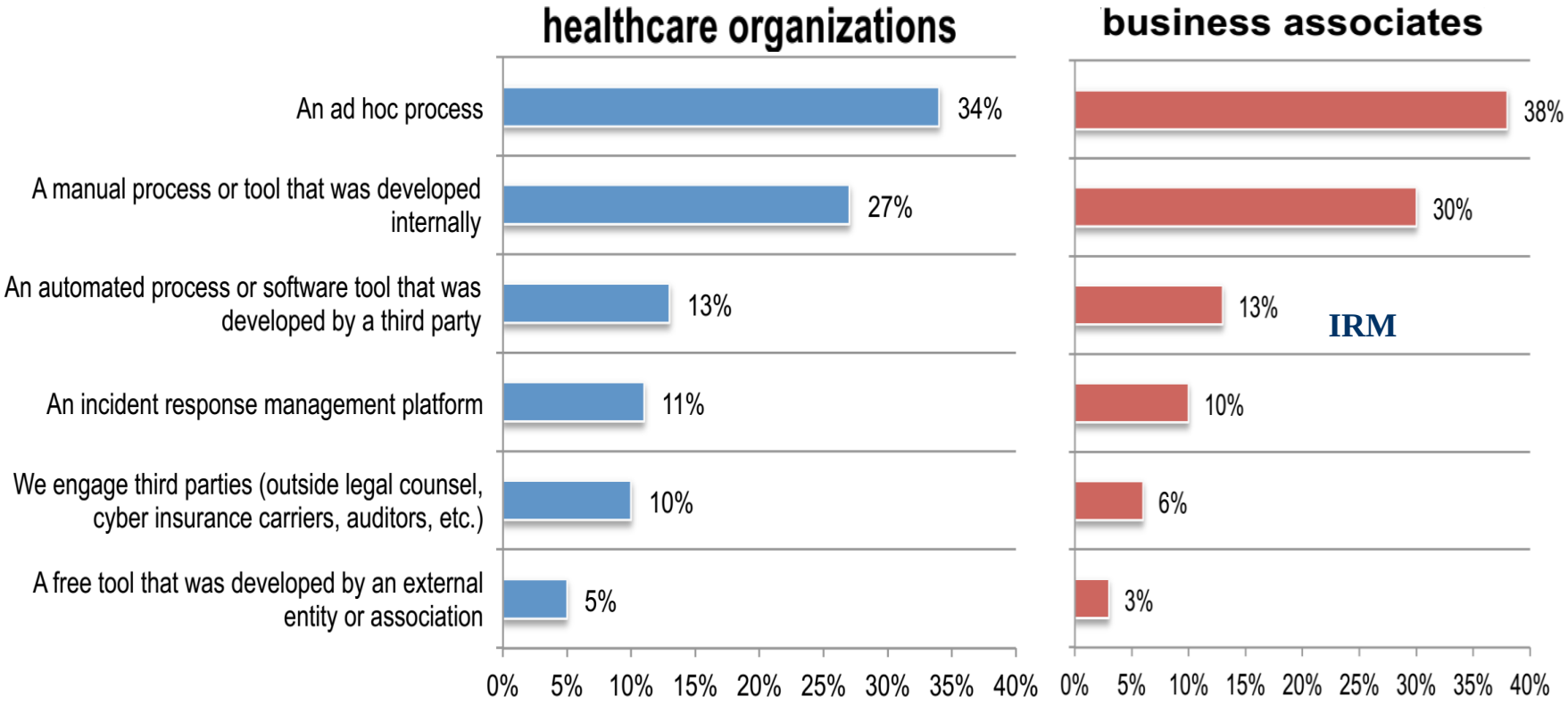
Web-based malware attacks caused **~80%** security incidents

According to the FBI, criminals are targeting the information-rich healthcare sector because **individuals' personal information, credit information, and protected health information (PHI) are accessible in one place, which translates into a high return when monetized and sold**.

Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

Increasing External & Insider Risk… Healthcare

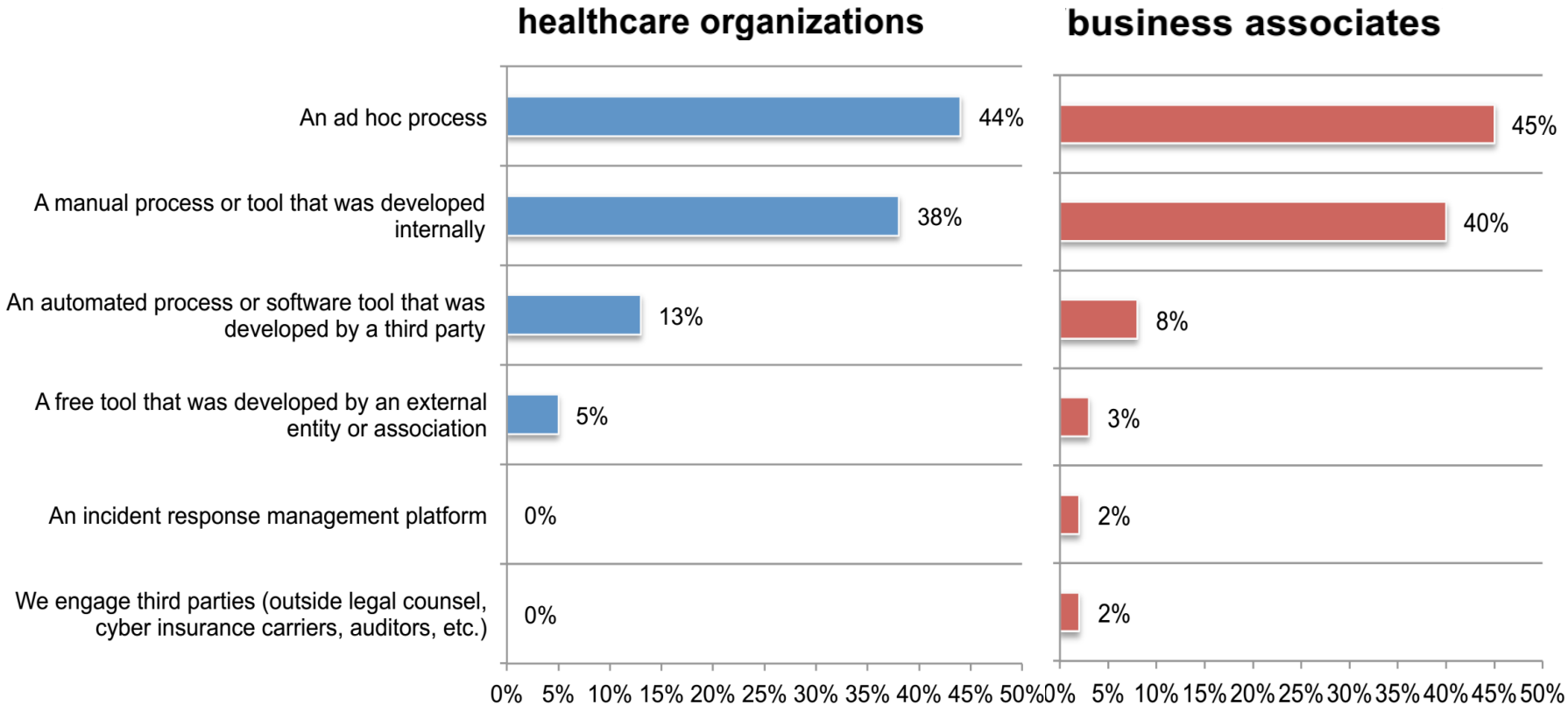
Assessment of risk following security incidents involving electronic documents



Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

Increasing External & Insider Risk… Healthcare

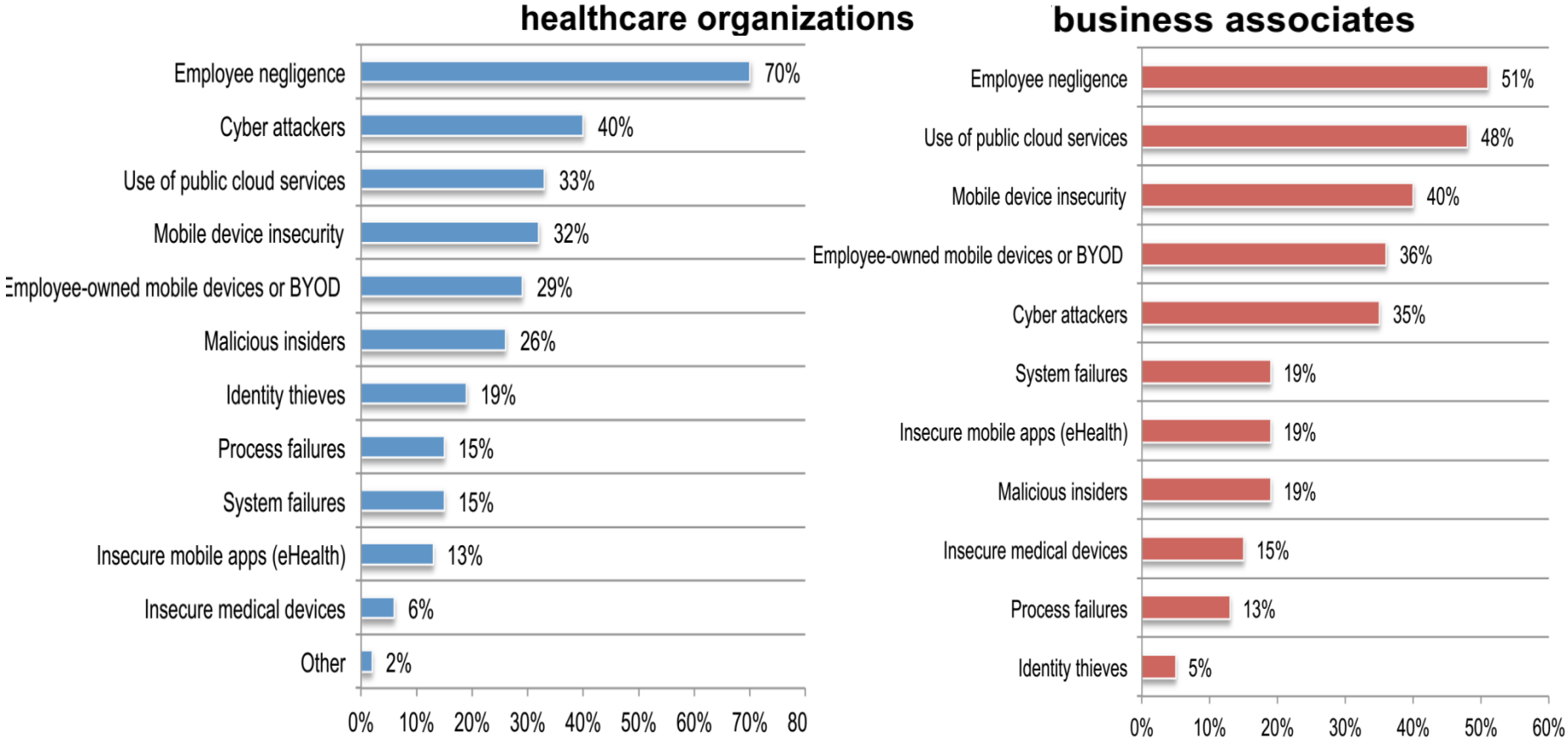
Assessment of risk following security incidents involving paper documents



Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

Increasing External & Insider Risk… Healthcare

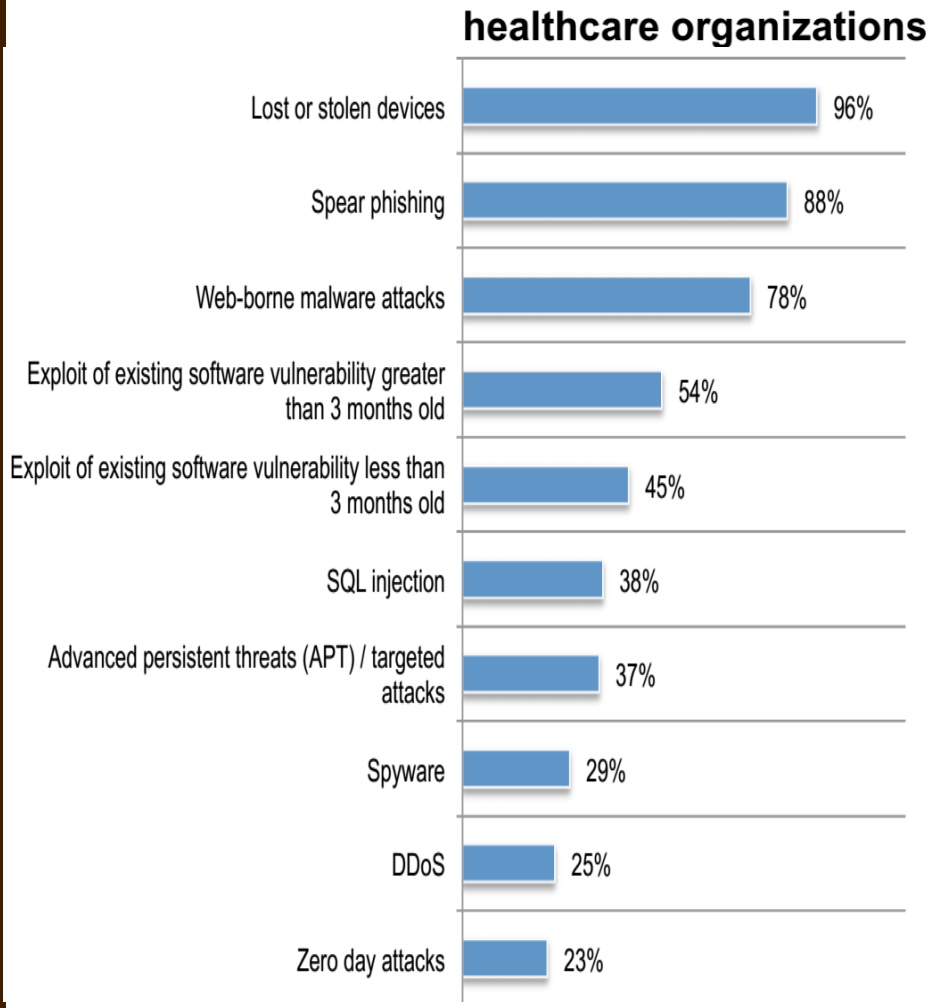
What security threats healthcare organizations worry about most

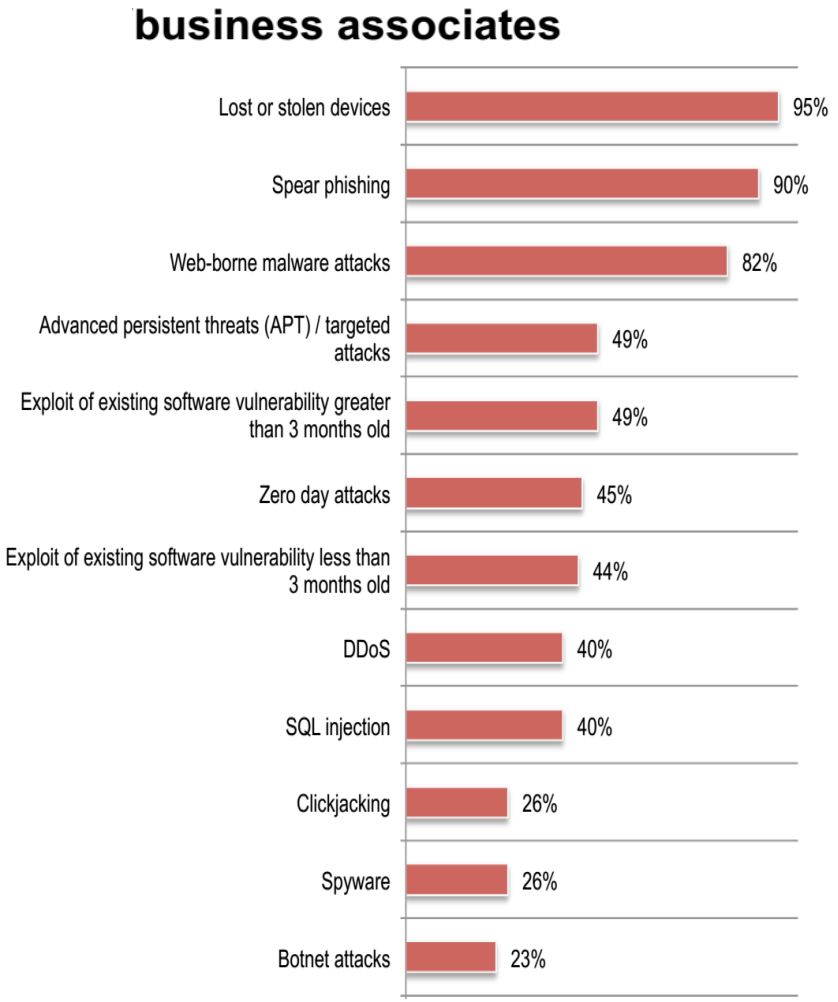


Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

Increasing External & Insider Risk… Healthcare

Security incidents healthcare organizations experienced

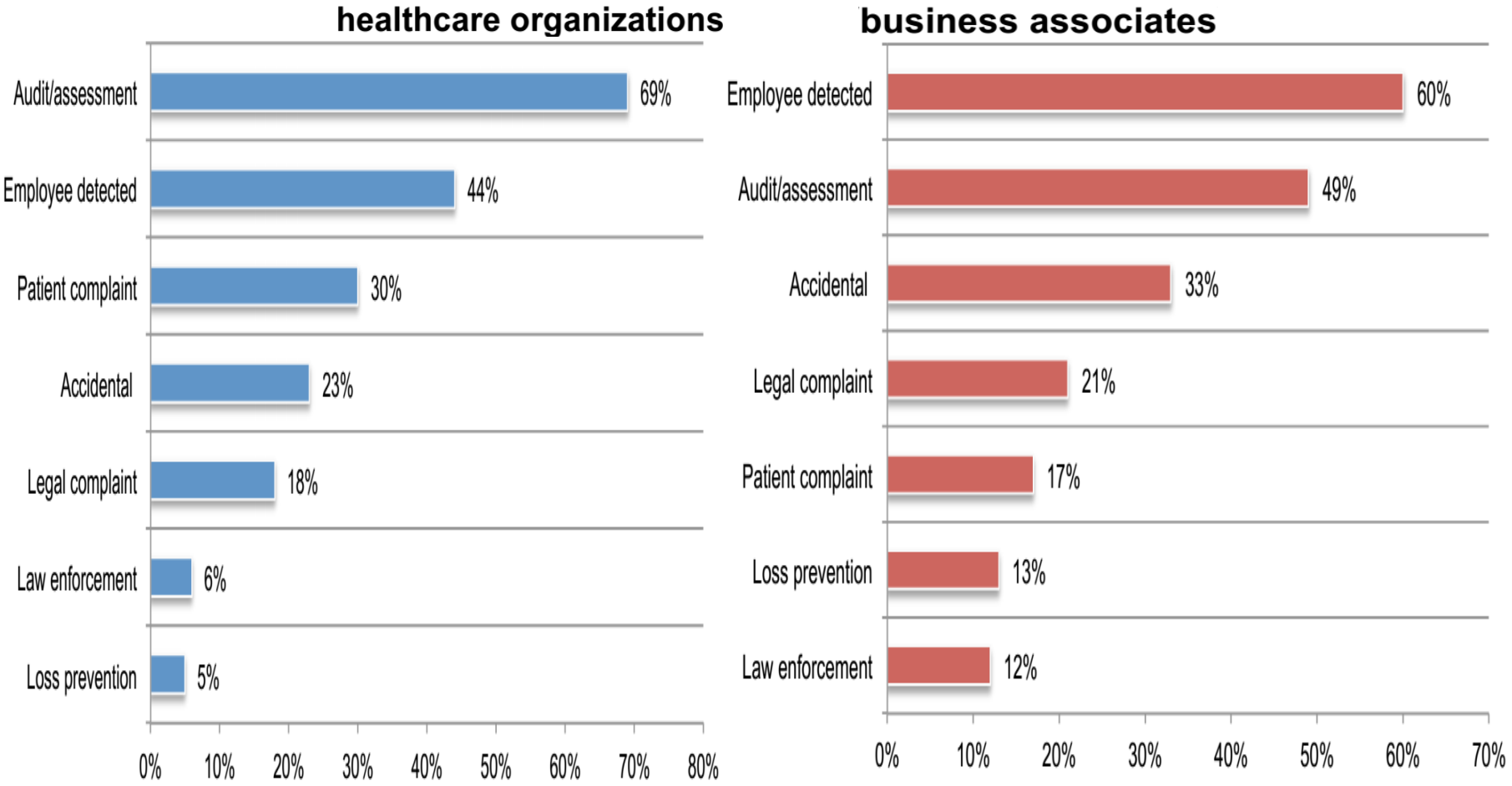




Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

Increasing External & Insider Risk… Healthcare

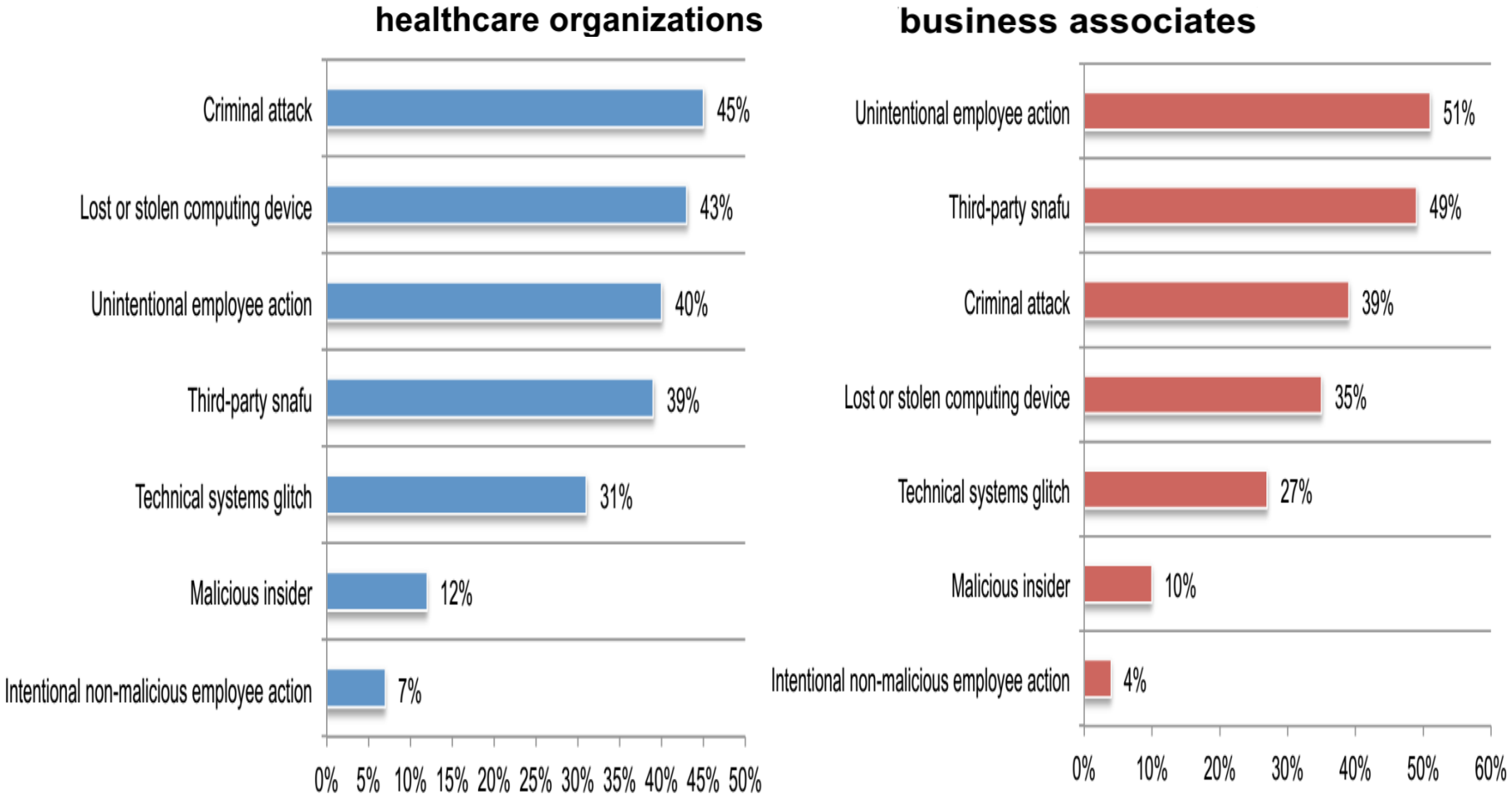
How the data breach was discovered



Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

Increasing External & Insider Risk… Healthcare

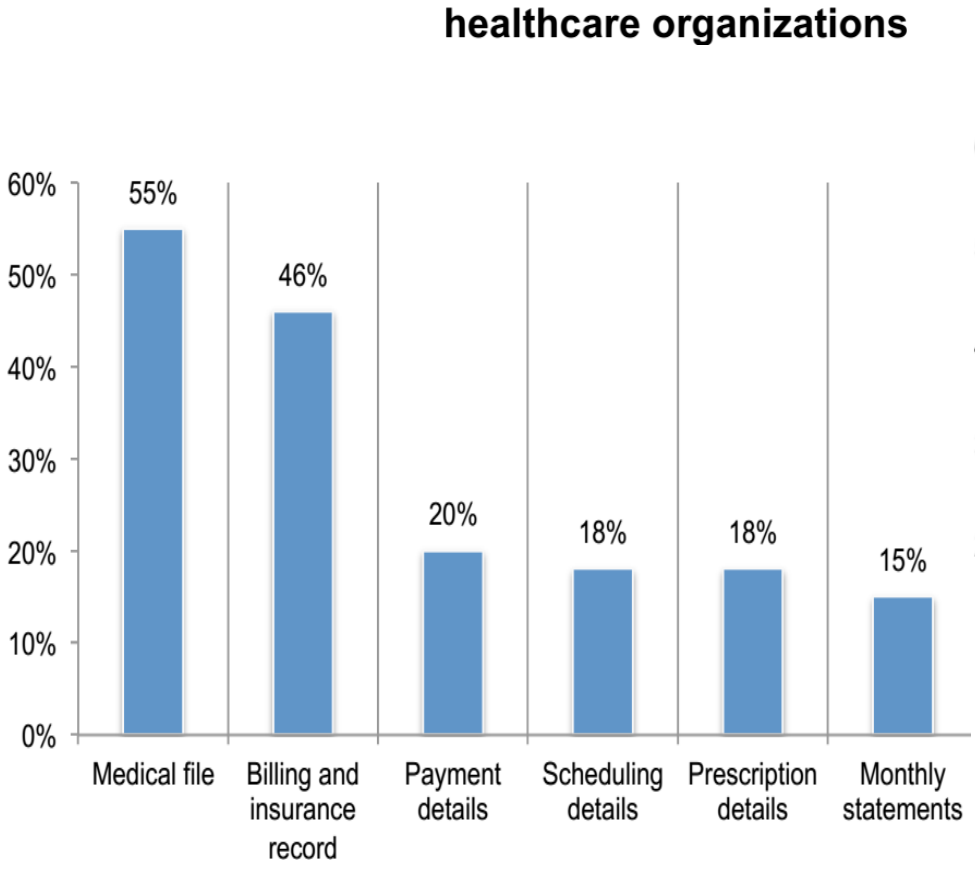
Root cause of the healthcare organizations' data breach

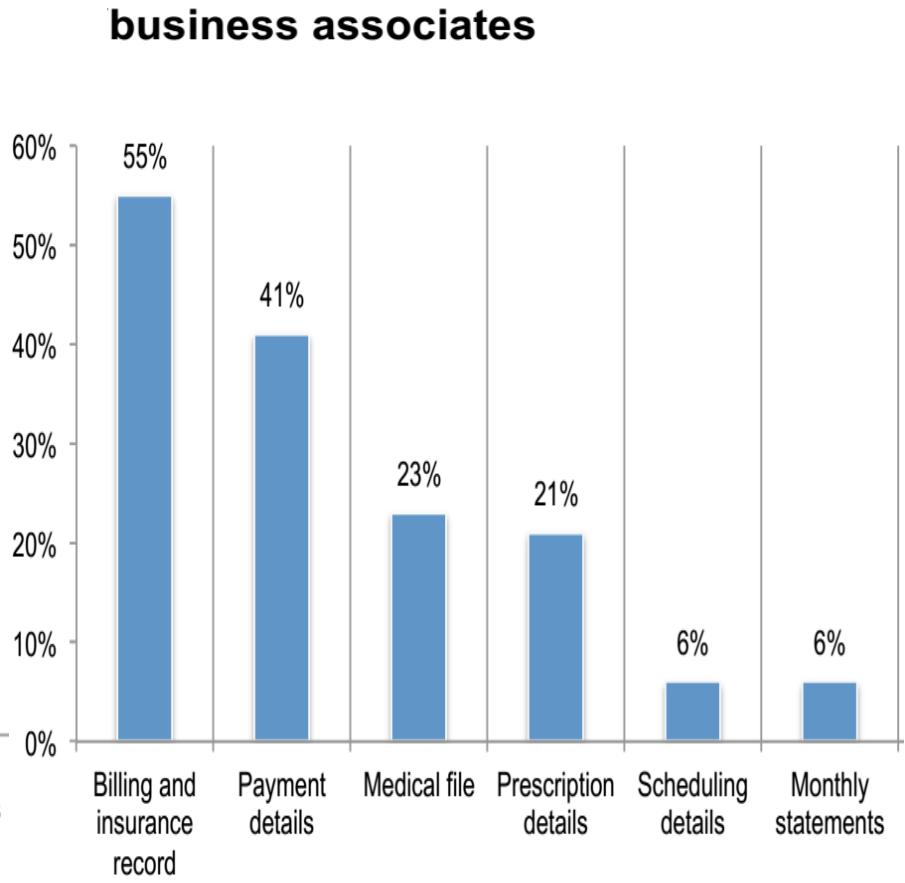


Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

Increasing External & Insider Risk… Healthcare

Patient data successfully targeted



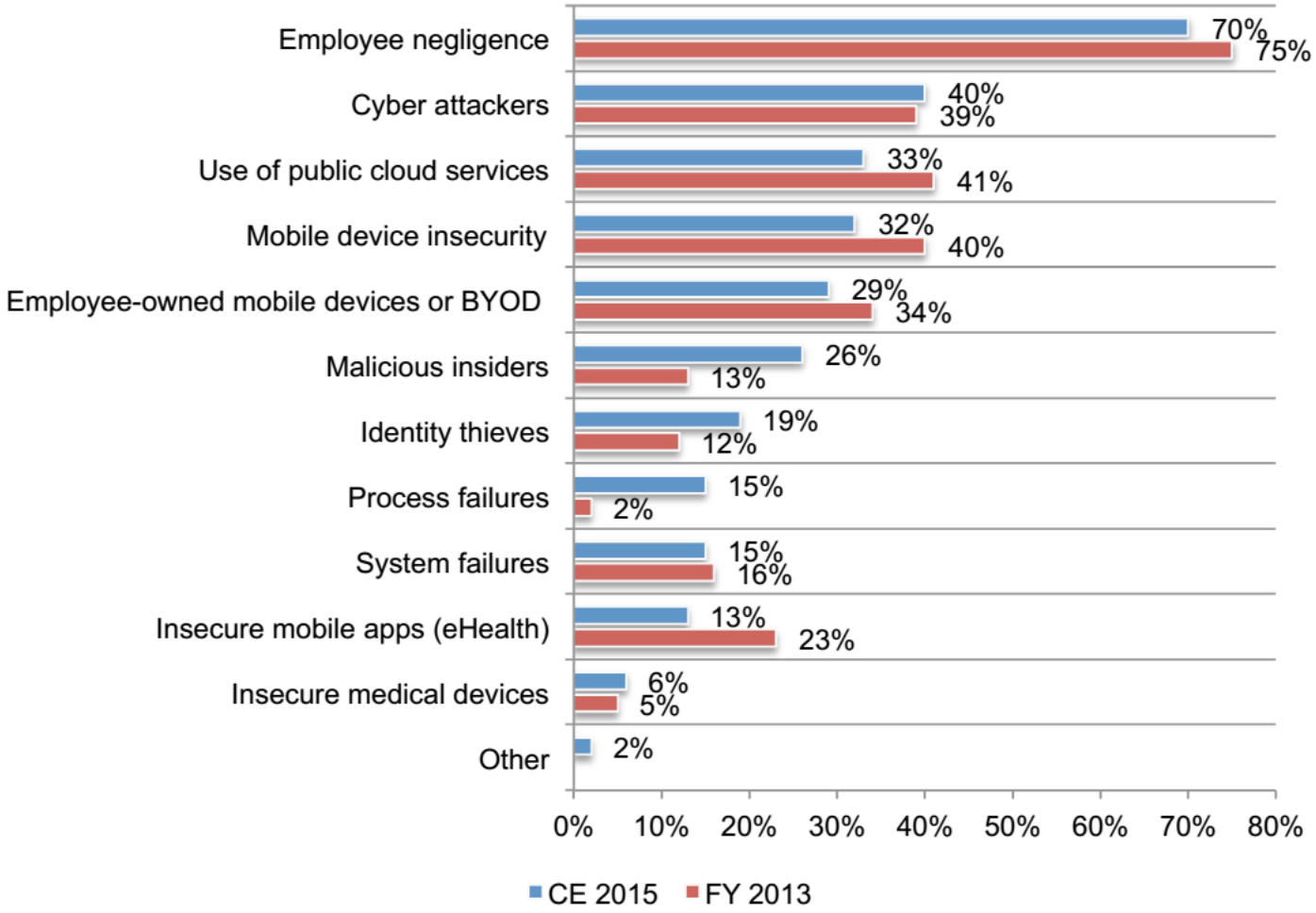


There are exponentially more security incidents than data breaches.
Only self-determined 'data breaches' require reporting.

Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

Increasing External & Insider Risk… Healthcare

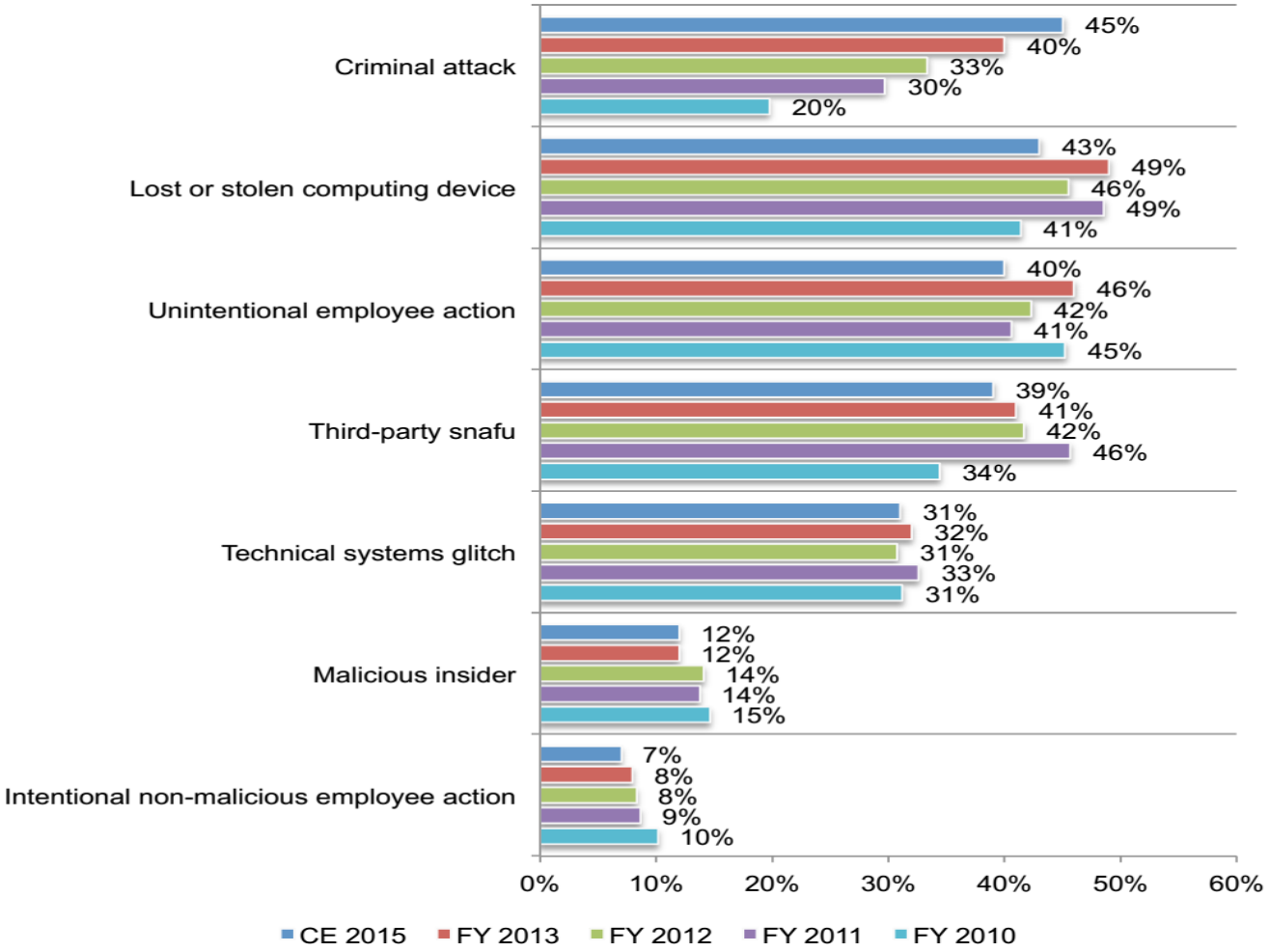
Trends in security threats facing healthcare organizations



Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

Increasing External & Insider Risk… Healthcare

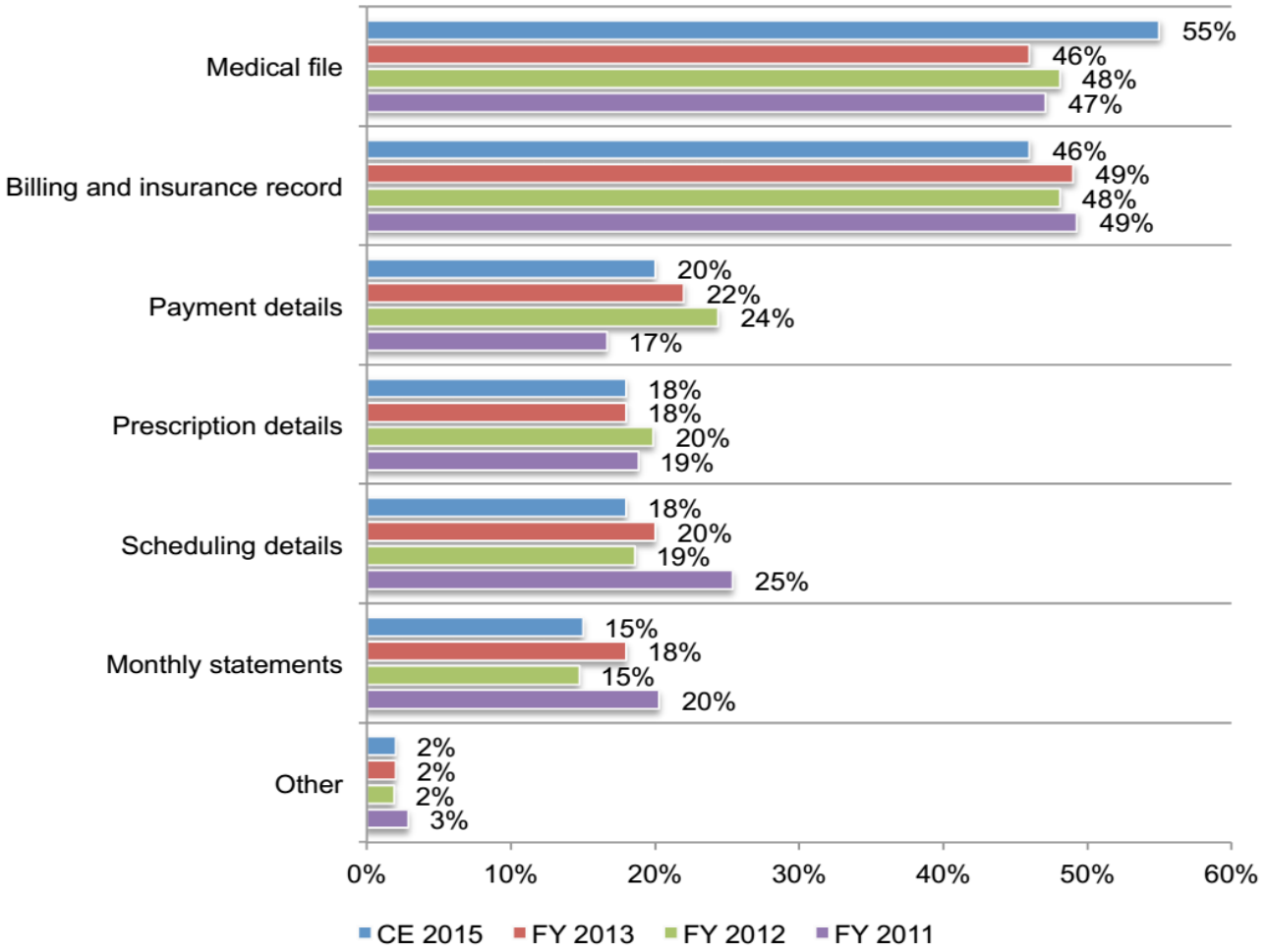
Trends in the nature of the incident



Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

Increasing External & Insider Risk… Healthcare

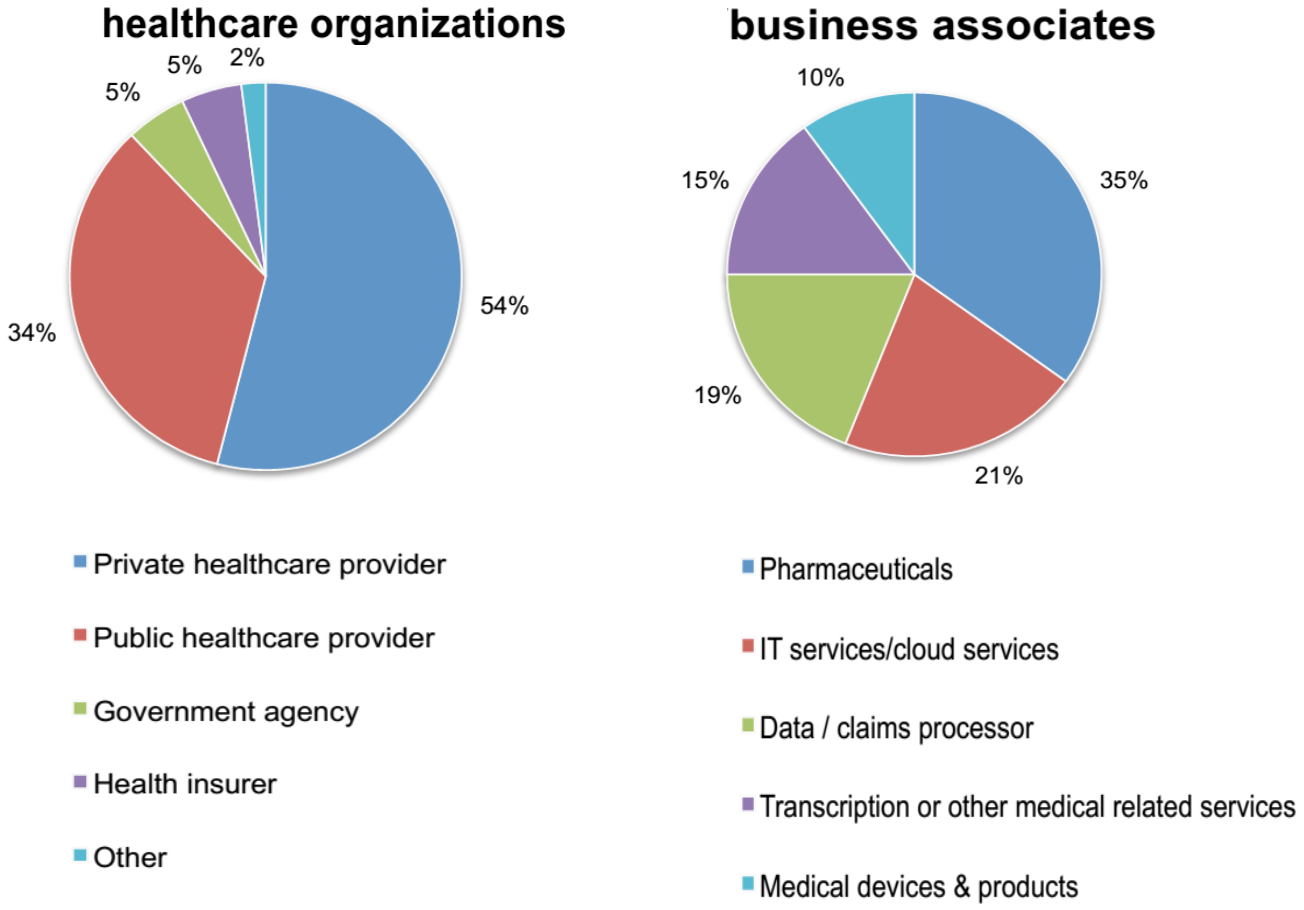
Trends in the type of patient data lost or stolen



Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

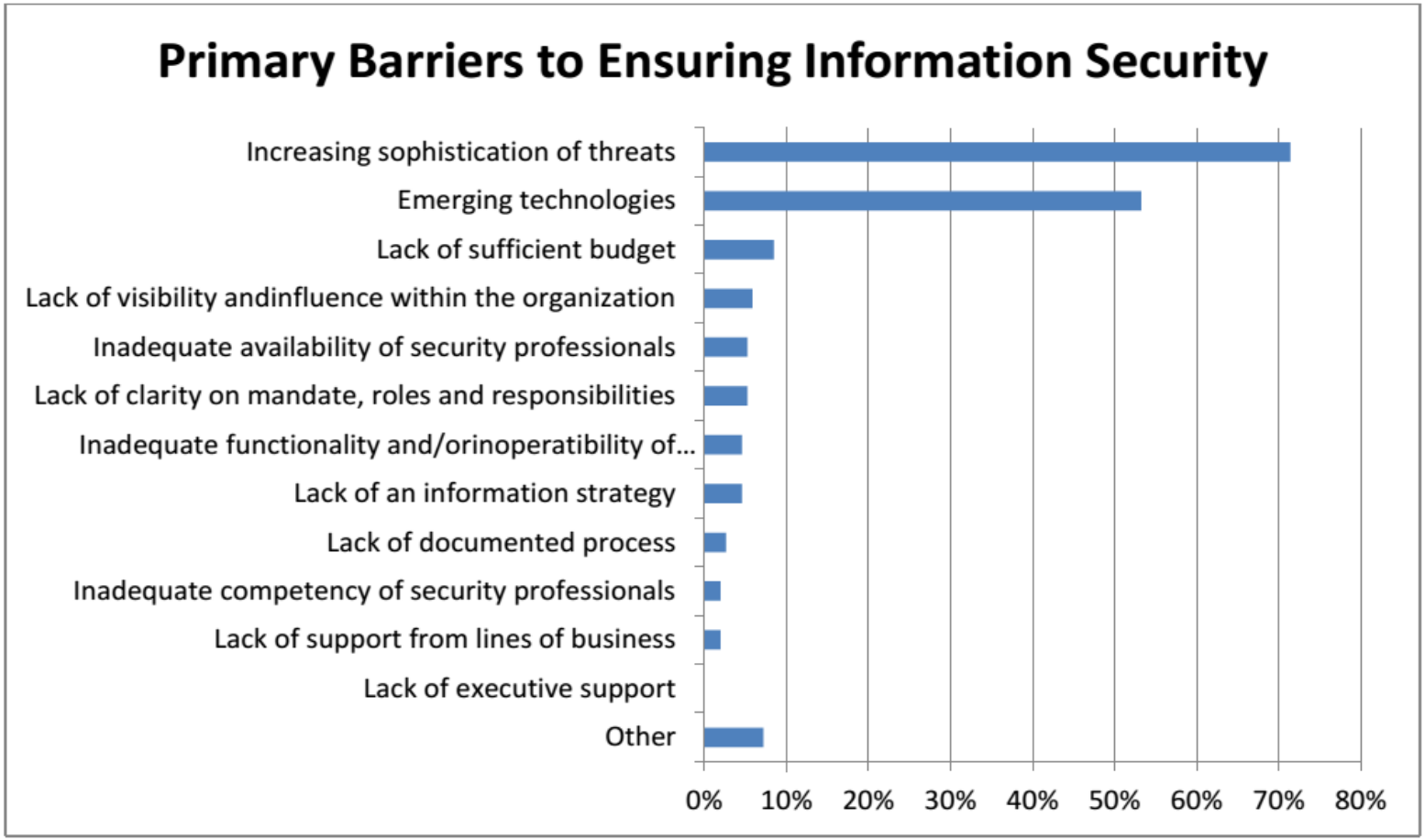
Increasing External & Insider Risk… Healthcare

Type of Covered Entity and Business Associate



Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015.

Increasing External & Insider Risk… Finance



Report on Cyber Security in the Banking Sector, New York State Department of Financial Services, May 2014

Increasing External & Insider Risk… Finance

Largest Financial Institutions are Most Likely Targets of… Malware and Phishing.

Most institutions irrespective of size experienced intrusions or attempted intrusions into their IT systems over the past three years. The attempted methods ran the gamut, with most institutions reporting incidents involving malicious software (malware) (22%), phishing (21%), pharming (7%), and botnets or zombies (7%). The larger the institution, the more likely it appeared to experience malware and phishing attempts. About 13% of small institutions reported being attempted targets of malware, as compared to 21% of medium institutions and 35% of large institutions. Similarly, about 16% of small institutions reported attempted phishing, as compared to 22% of medium institutions and 33% of large institutions. It is unclear whether the variation between large and small institutions represents an actual difference in the type of attempted intrusions experienced by these organizations or whether it is an indication that larger institutions are better equipped to identify systems intrusions.

Report on Cyber Security in the Banking Sector, New York State Department of Financial Services, May 2014

Increasing External & Insider Risk... Finance

Most Often The Greatest Risk Starts from Account Takeovers...

The most frequent types of wrongful activity resulting from a cyber intrusion reported by institutions were account takeovers (46%), identity theft (18%), telecommunication network disruptions (15%), and data integrity breaches (9.3%). Third-party payment processor breaches were also reported by 18% and 15% of small and large institutions, respectively. Large institutions also cited mobile banking exploitation (15%), ATM skimming/point-of-sale schemes (23%), and insider access breaches (8%).

Report on Cyber Security in the Banking Sector, New York State Department of Financial Services, May 2014

Increasing External & Insider Risk… Finance

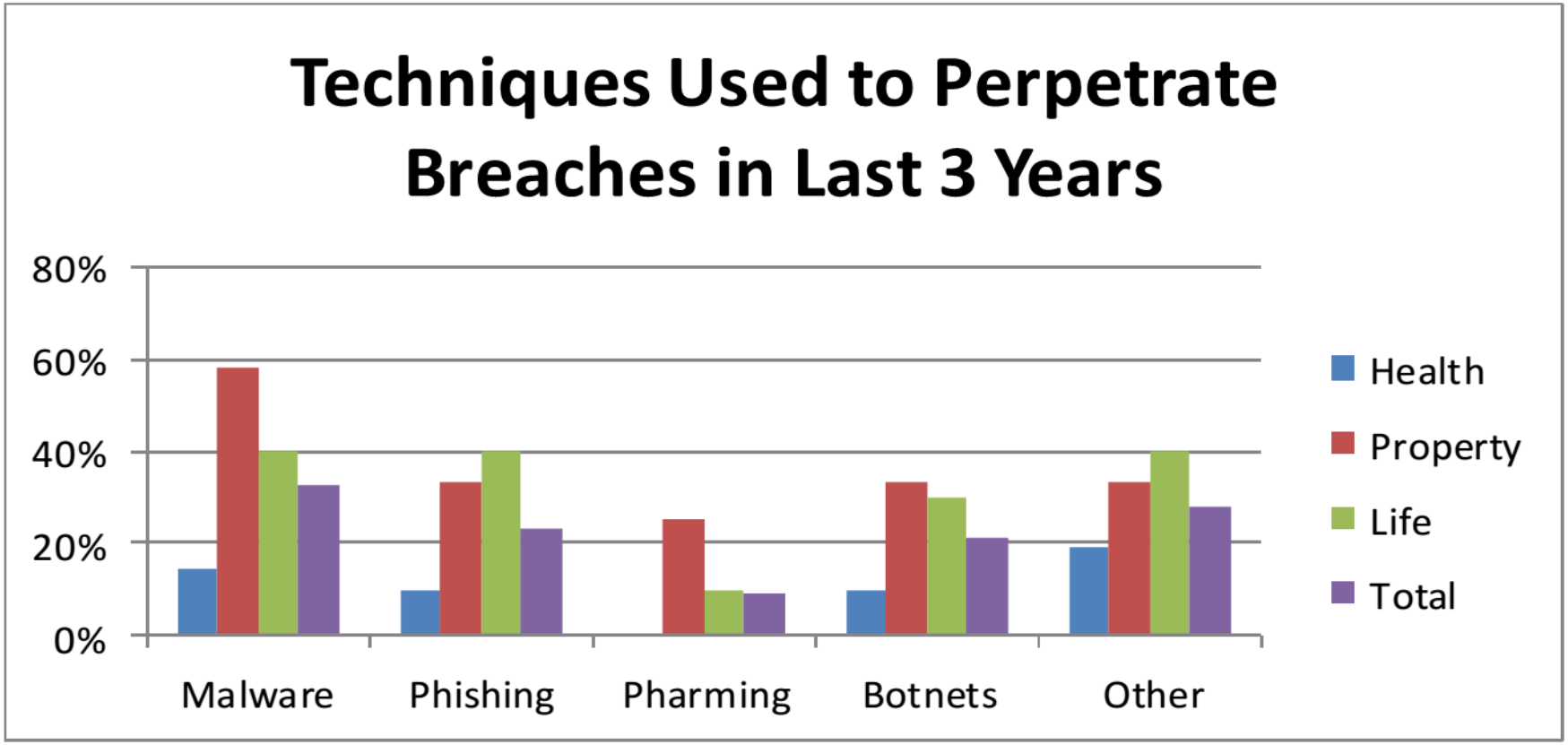
Calculation of Monetary Loss has Greatest Factor of… Customer Reimbursement...

For those institutions that experienced a monetary loss in the past three fiscal years due to cyber security breaches, the top two factors included in calculating the monetary loss as reported by the institutions were: (1) customer reimbursements (76%), (2) audit and consulting services (52%), and (3) deployment of detection software, services and policies (45%). Although many institutions factored loss of customer business (38%) and damage to brand/reputation (31%) into their total loss calculations, these losses in many cases were likely too difficult to quantify for institutions to factor into their overall monetary loss resulting from a cyber breach.

Report on Cyber Security in the Banking Sector, New York State Department of Financial Services, May 2014

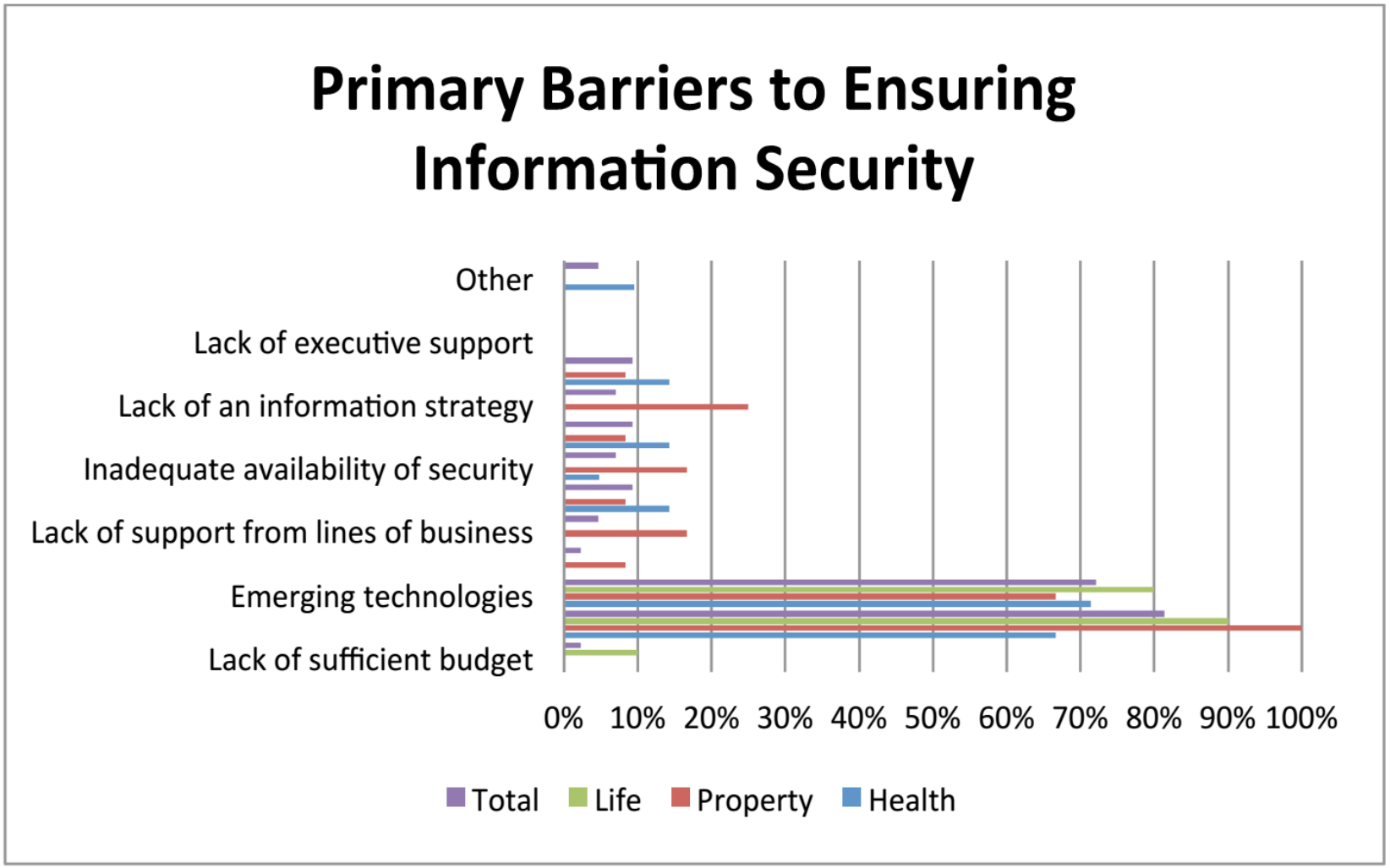
Increasing External & Insider Risk... Insurance

Malware and Phishing are Top-2 Threats to Insurance Sector...



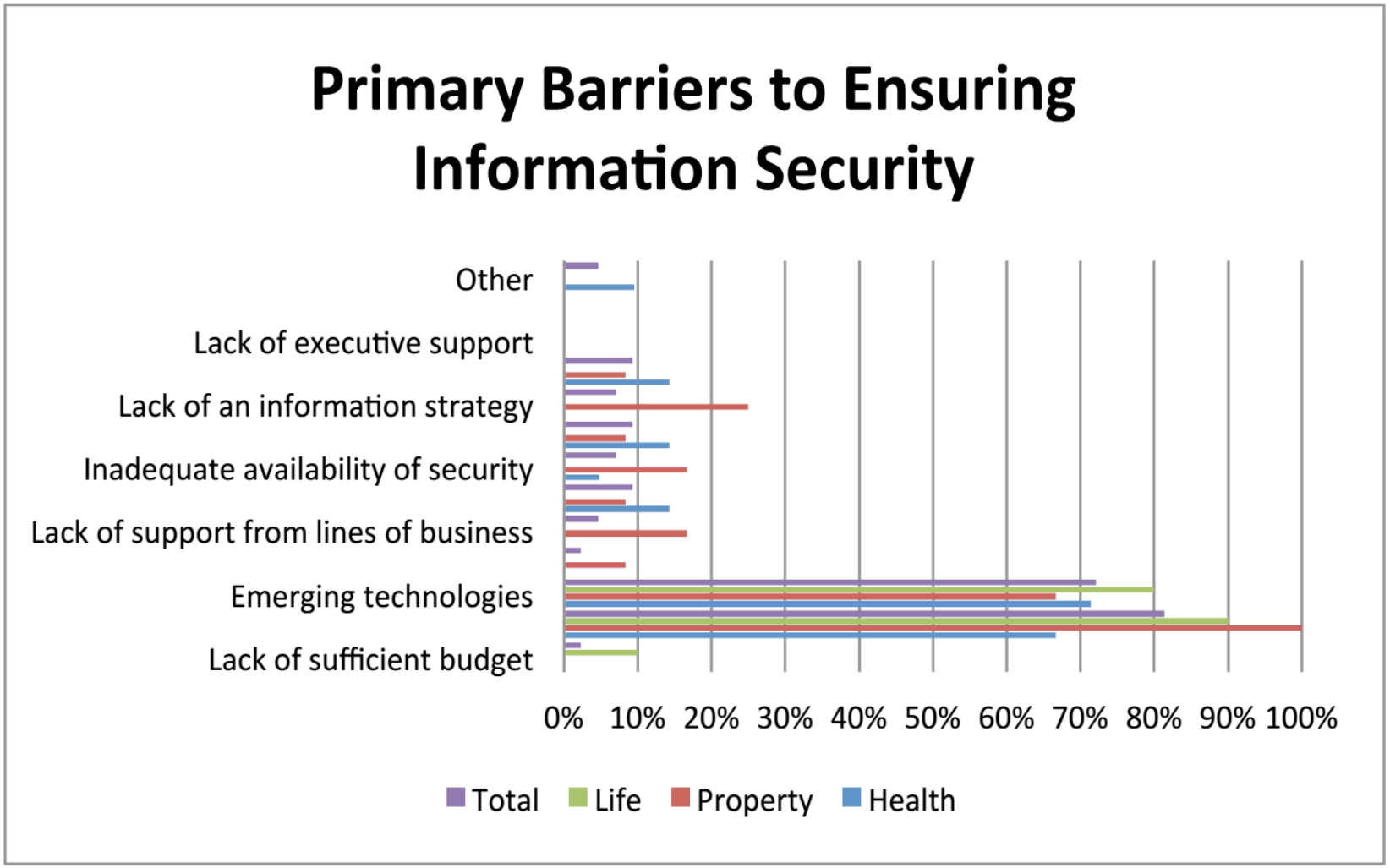
Report on Cyber Security in the Insurance Sector, New York State Department of Financial Services, April 2014

Increasing External & Insider Risk… Insurance



Report on Cyber Security in the Insurance Sector, New York State Department of Financial Services, April 2014

Increasing External & Insider Risk… Insurance



Report on Cyber Security in the Insurance Sector, New York State Department of Financial Services, April 2014

Increasing External & Insider Risk… Finance

Table 1: Summary of Firm Responses on Top Three Threats

	2014 Sweep Results (% of respondents ranking threat as 1st, 2nd or 3rd)			2011 Survey Results (% of respondents ranking threat as 1st, 2nd or 3rd)		
	1st	2nd	3rd	1st	2nd	3rd
Cyber risk of hackers penetrating systems for the purpose of account manipulation, defacement or data destruction, for example	33	28	11	38	33	19
Operational risk associated with environmental problems (*e.g.*, power failures) or natural disasters (*e.g.*, earthquakes, hurricanes)	22	17	17	31	16	29
Insider risk of employees or other authorized users abusing their access by harvesting sensitive information or otherwise manipulating the system or data undetected	22	11	33	24	35	22
Insider risk of employees or other authorized users placing time bombs or other destructive activities	0	11	0	0	4	5
Cyber risk of non-nation states or terrorist groups penetrating systems, for example, for the purpose of wreaking havoc	0	6	6	0	4	5
Cyber risk of nation states penetrating systems, for example, for the purpose of espionage	0	6	6	0	2	5
Cyber risk of competitors penetrating systems, for example, for the purpose of corporate espionage	0	0	0	0	2	4

FINRA Report on Cybersecurity Practices, February 2015

Increasing External & Insider Risk… Finance

Malware and Phishing CAUSE Employees Being Insider Threats…

Employees are one of the major sources of cybersecurity risk for firms. FINRA found that many of the cybersecurity attacks that firms identified were successful precisely because employees made mistakes, such as inadvertently downloading malware or responding to a phishing attack. For this reason, cybersecurity training is an essential component of any cybersecurity program. Even the best technical controls on a firm's systems can be rapidly undermined by employees who are inattentive to cybersecurity risks.

The importance of training is widely recognized. The NIST Framework identifies training as a critical piece of an organization's cybersecurity infrastructure.[29] NIST recommends that all users (from vendors to senior executives) are informed and trained, and users understand their specific roles and responsibilities. This includes educating those users on the risks associated with the data they may encounter. Training is also a key component in the SANS Top 20. SANS recommends that organizations perform an analysis to determine where the skill gaps and points of risk exposure exist, and develop and deliver training in those areas.

FINRA Report on Cybersecurity Practices, February 2015

Increasing External & Insider Risk... Finance

Financial Services Are the Most Highly Targeted and Attacked...

THE TOP SIX FINDINGS INCLUDE:

1. Financial Services Encounters Security Incidents 300 Percent More Frequently Than Other Industries
2. Thirty-three Percent of All Lure Stage Attacks Target Financial Services
3. Credential Stealing Attacks Set Sights on Banking
4. Fraudsters Switch-up Campaigns Frequently to Outfox Banking Security Measures
5. Financial Services Ranks Third for Targeted Typosquatting
6. Evidence Increasingly Suggests the Need for Global Economy Continuity and Cyber Insurance May be Hindering Real Security Adoption in Financial Services.

2015 Raytheon WebSense Industry Drill-Down Report Financial Services

Increasing External & Insider Risk… Finance

Financial Services Face Some of Most Sophisticated Attacks…

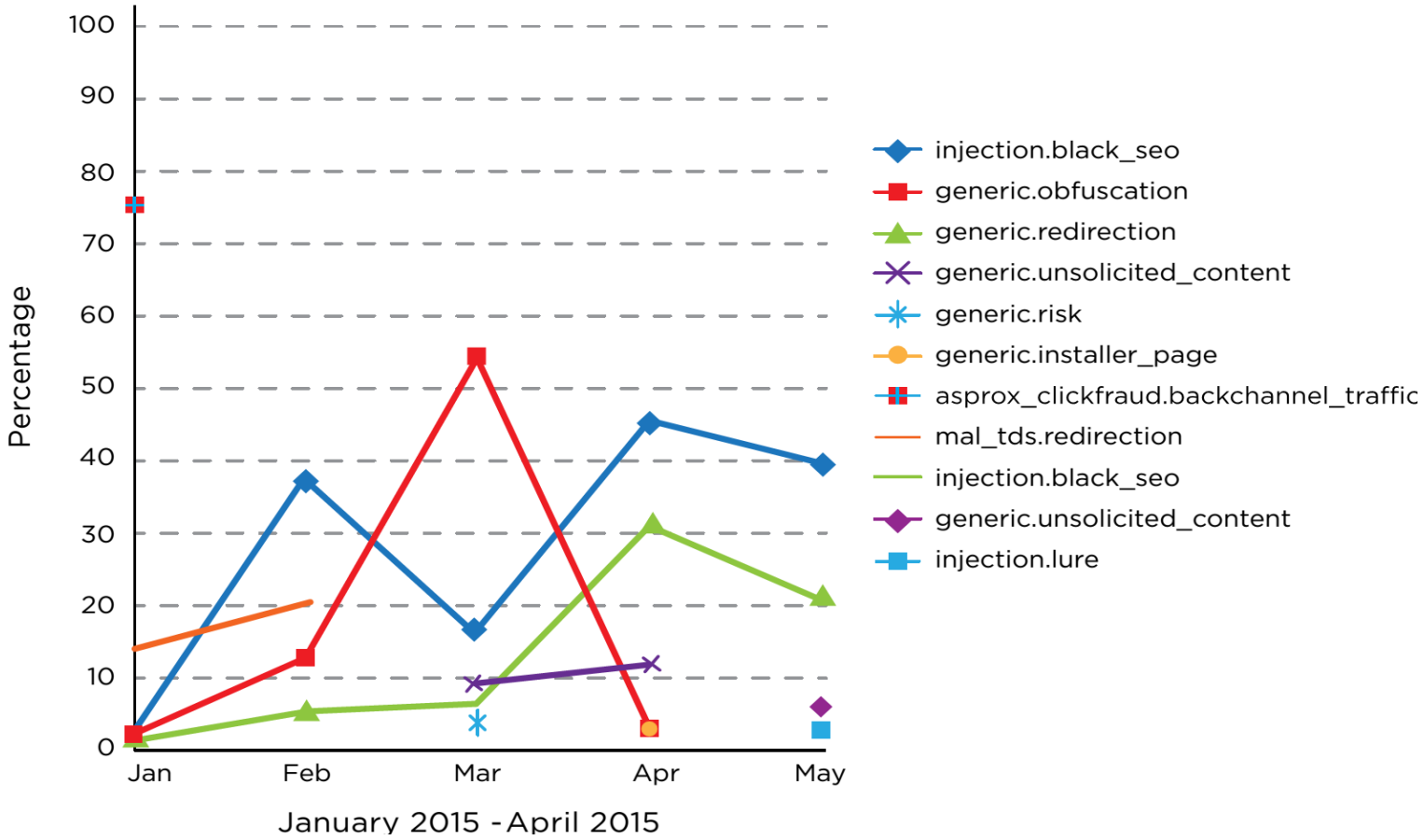
- Obfuscation and black search engine optimization continue to be more prevalent in attacks against financial services than other industries as a whole.
- Patterns in attack campaigns shift on a month-to-month basis, including huge spikes in malicious redirection and obfuscation detected in a wave of attacks in March 2015.
- This highlights an attack methodology designed for campaigns to be harder to detect and analyze by those charged with securing the finance sector.
- In addition, cybercriminals maintain a constant barrage of low-level attacks to keep security pros occupied dealing with a tremendous volume of background noise while targeted attacks are simultaneously occurring.
- Unsolicited content accounts for 10 percent of the security hits seen in financial services.

2015 Raytheon WebSense Industry Drill-Down Report Financial Services

Increasing External & Insider Risk… Finance

Financial Services Face Some of Most Sophisticated Attacks…

THREAT TYPES, FINANCIAL SERVICES – FROM JAN 2015 TO MAY 2015



2015 Raytheon WebSense Industry Drill-Down Report Financial Services

Increasing External & Insider Risk… Finance

Financial Services Face Some of Most Sophisticated Attacks…

Gatak is a trojan with both data-stealing and back door capabilities. First discovered in 2012, it has included a number of revisions since that time, designed to more successfully evade detection by today's security measures. Affecting Windows computers, once the endpoint is compromised, the malware creates a number of registry changes to boot each time the computer is turned on. The malware collects system information and sends to a remote server by injecting code into the following processes: explorer.exe; winlogon.exe; and svchost.exe

2015 Raytheon WebSense Industry Drill-Down Report Financial Services

Increasing External & Insider Risk… Finance

FINANCIAL SERVICES RANKS THIRD FOR TARGETED TYPOSQUATTING

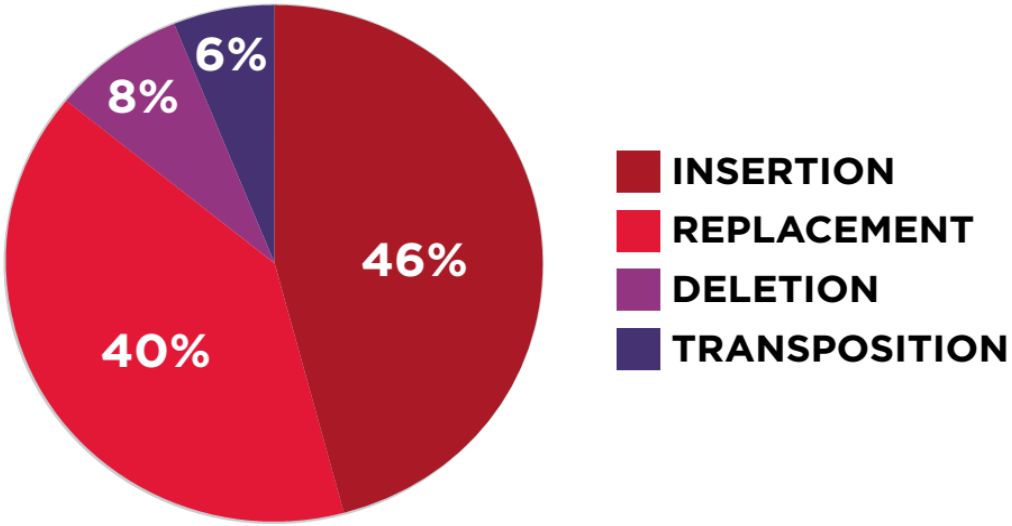
- While it may seem an antiquated methodology, the application of typosquatting has evolved into successful fraudulent incidents generating millions of dollars in financial losses and operational overhead.
- Websense researchers have seen an increase in the use of typosquatted domains in targeted attacks against financial services, usually combined with strong social engineering tactics.
- **When comparing more than 20 industries, financial services ranked as one of the highest for this highly successful type of attack.**
- These attacks are often combined with social engineering tactics via email to compromise hosts or to manipulate users (particularly in finance groups) to instigate an action (such as initiating an invoice payment or wire transfer).
- The average cost of such a spear-phishing incident averages to $130,000 per incident.
- There are many ways criminals use typosquatted domains in an attack;
  - *One of the most effective targeted attacks involves the use of .co domains, substituted for .com domains, particularly when combined with high-pressure social engineering.*

2015 Raytheon WebSense Industry Drill-Down Report Financial Services

Increasing External & Insider Risk… Finance

Financial Services Face Some of Most Sophisticated Attacks…

MOST POPULAR TYPES OF TARGETED TYPOSQUATTING SUBSTITUTIONS INCLUDE THE FOLLOWING:

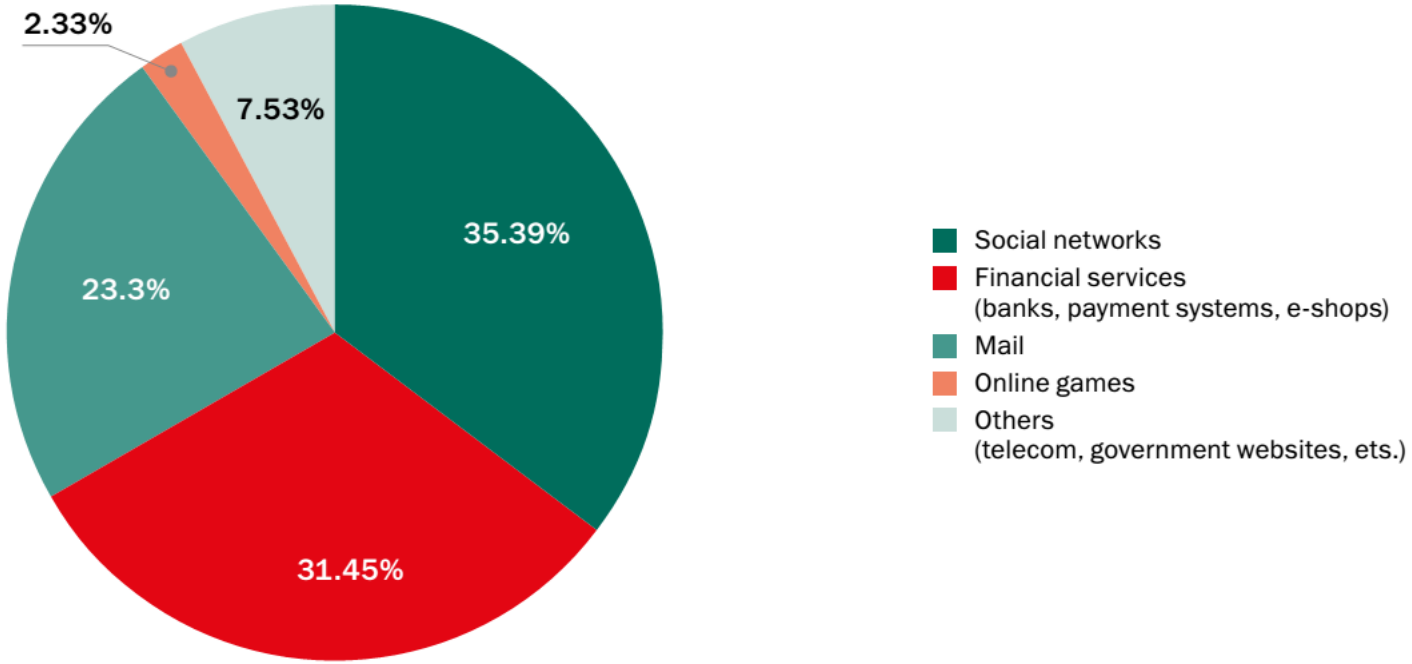


- **Single-Character Insertion**
  - Popular characters: i, l, r, t, s
  - Placement: middle of the word, beginning of the word
  - Benefit: The word is not visually widened / lengthened
- **Character Replacement**
  - Popular characters: i → l, e → a, g → q, o → 0
  - Placement: middle of the word, beginning of the word
  - Benefit: The word is not visually widened / lengthened
- **Character Replacement: TLD**
  - Popular characters: .co, .net
  - Placement: end of the word
  - Benefit: The change is not visually noticeable / identifiable
- **Character Transposition**
  - Popular characters: character order swap
  - Placement: middle of the word
  - Benefit: The word is not visually widened / lengthened
- **Character Deletion**
  - Benefit: Simple to execute and not always noticeable.

2015 Raytheon WebSense Industry Drill-Down Report Financial Services

Increasing External & Insider Risk… Finance

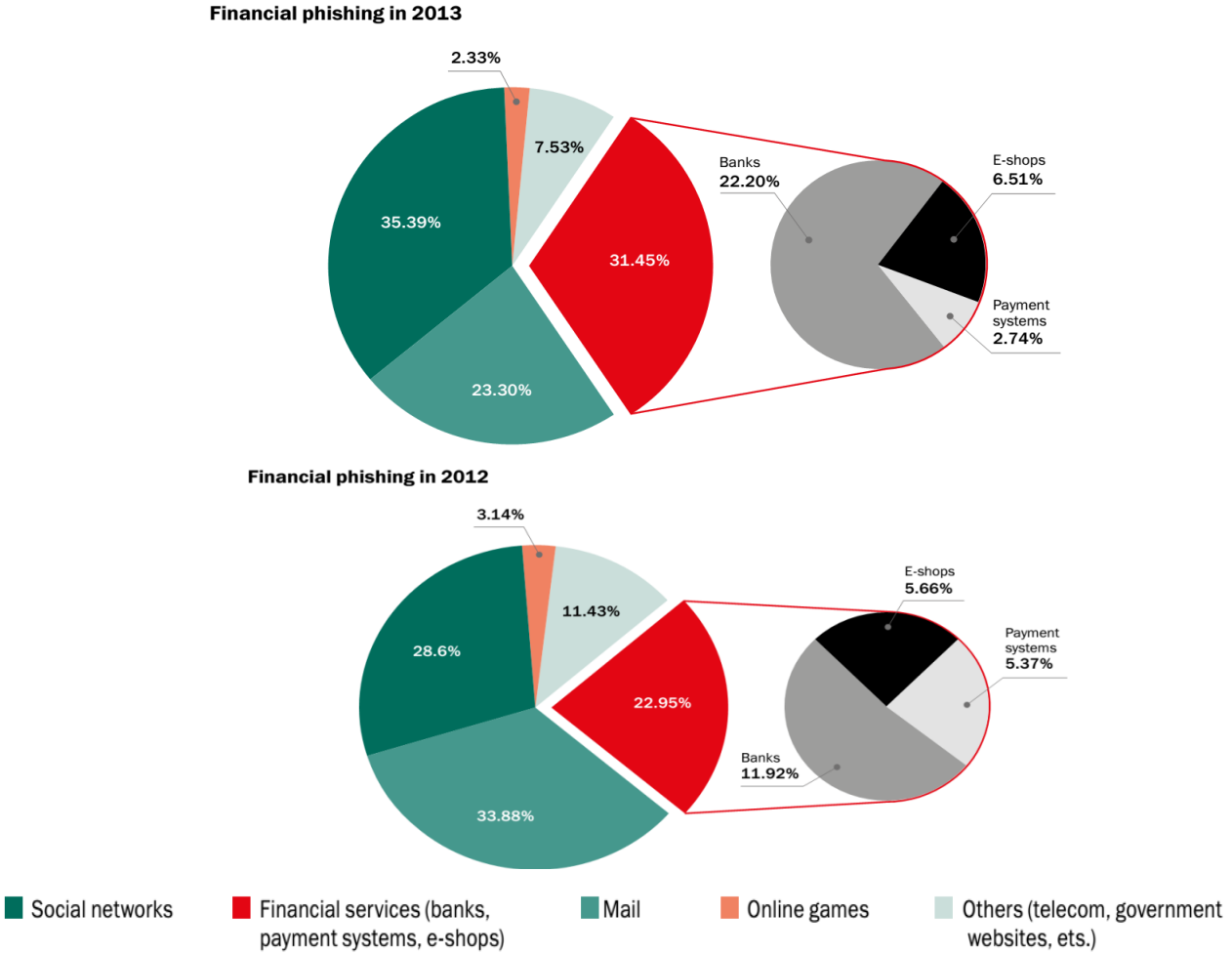
Top 3 Phishing Targets… Social Networks, Financial Services, E-Mail...



Kaspersky Lab Report, Financial CyberThreats in 2013

Increasing External & Insider Risk… Finance

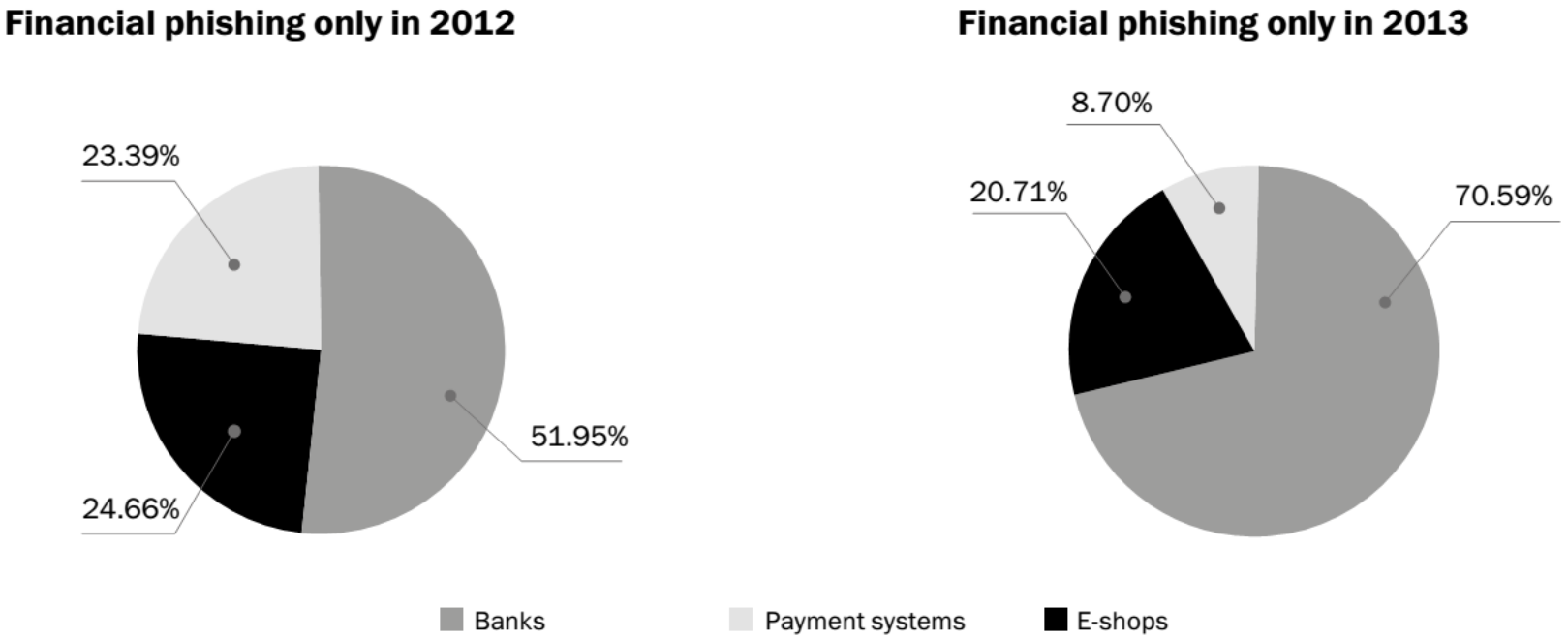
Increasing Phishing Increasingly Targeting Banks



Kaspersky Lab Report, Financial CyberThreats in 2013

Increasing External & Insider Risk… Finance

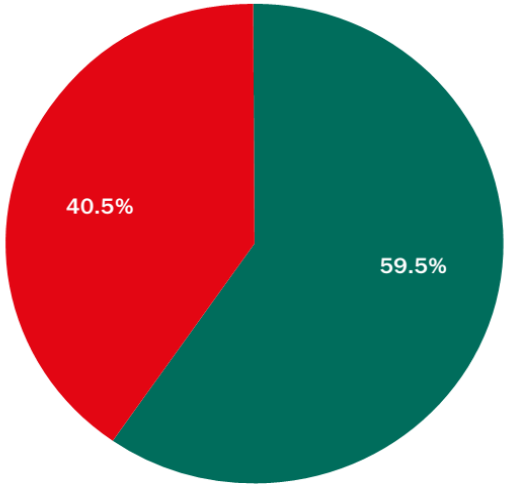
Increasing Phishing Increasingly Targeting Banks



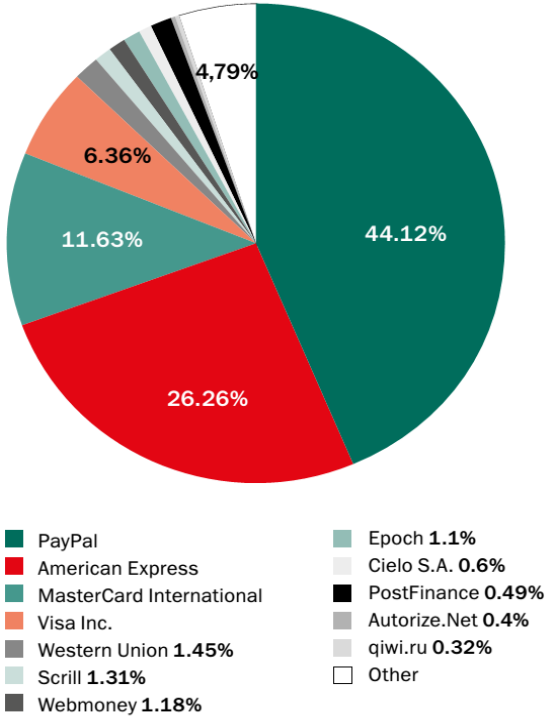
Kaspersky Lab Report, Financial CyberThreats in 2013

Increasing External & Insider Risk… Finance

Attacks against banks in 2013

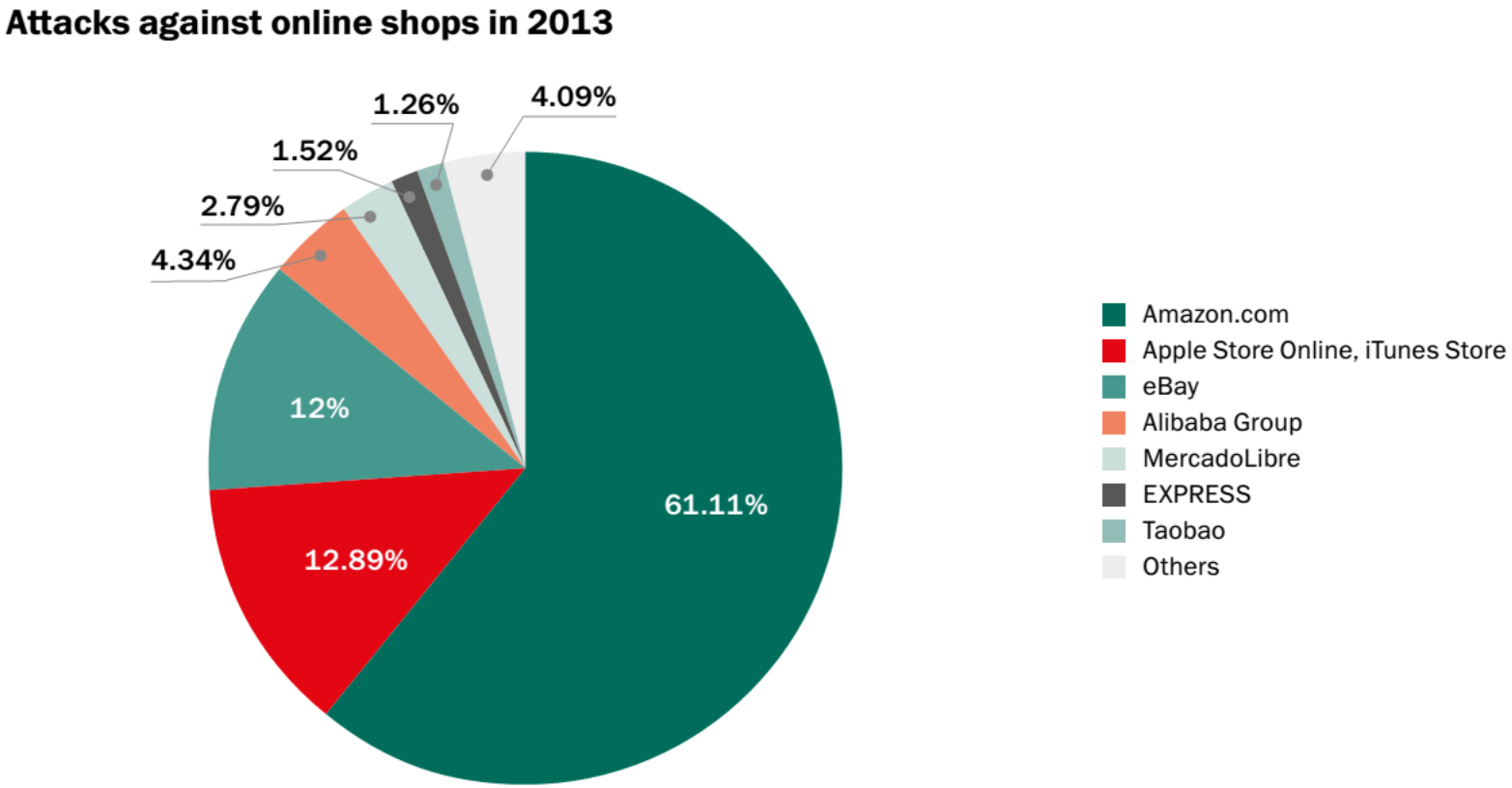


Attacks against payment systems in 2013



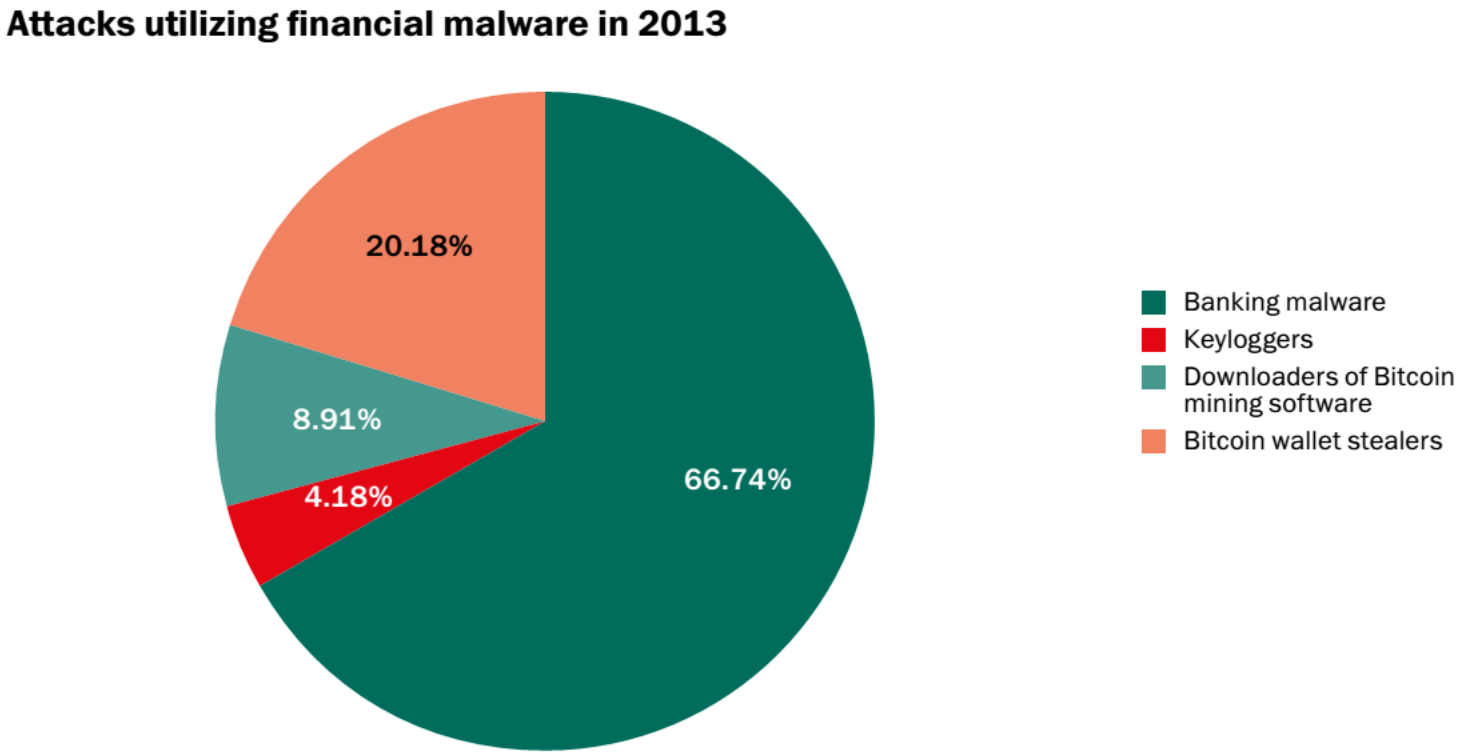
Kaspersky Lab Report, Financial CyberThreats in 2013

Increasing External & Insider Risk… Finance



Kaspersky Lab Report, Financial CyberThreats in 2013

Increasing External & Insider Risk… Finance

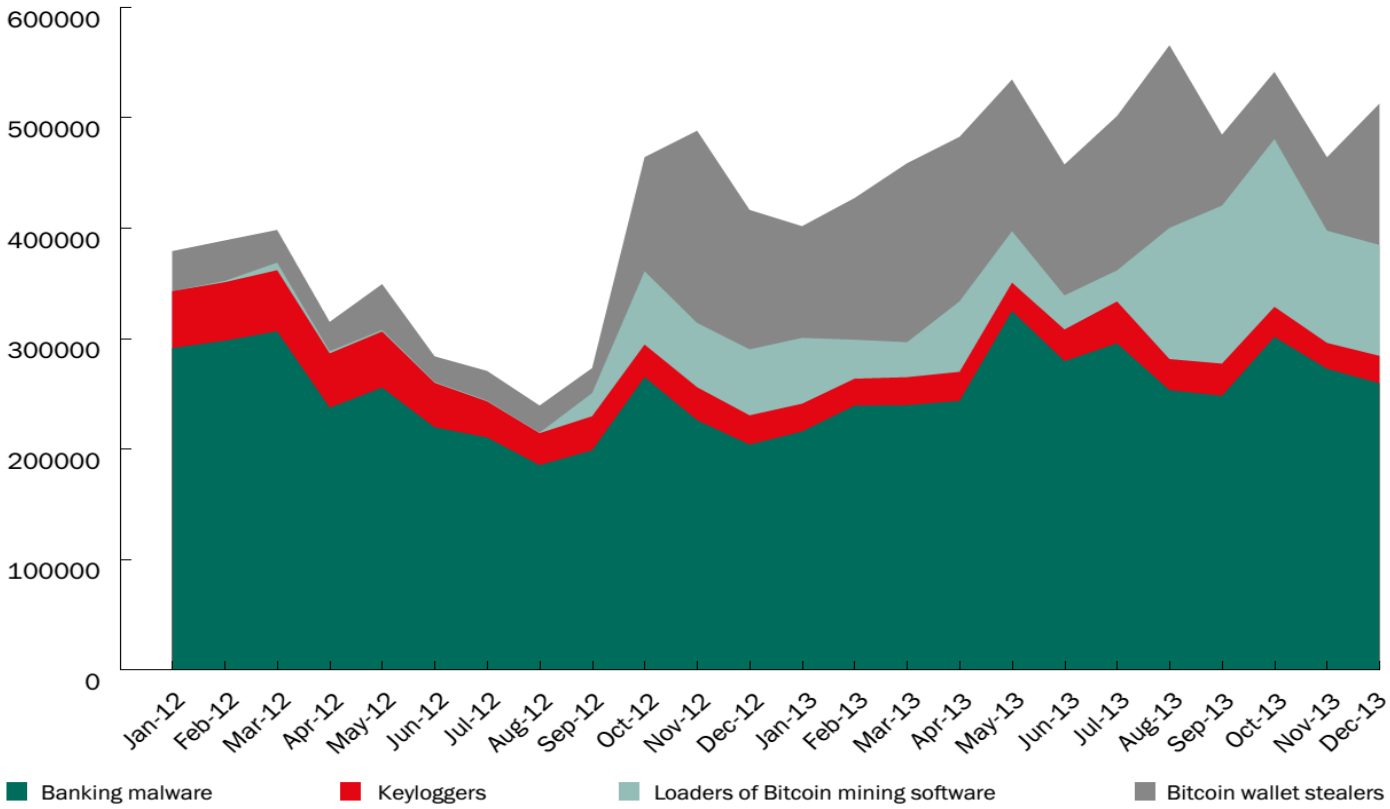


Kaspersky Lab Report, Financial CyberThreats in 2013

Increasing External & Insider Risk… Finance

Banking malware strikes

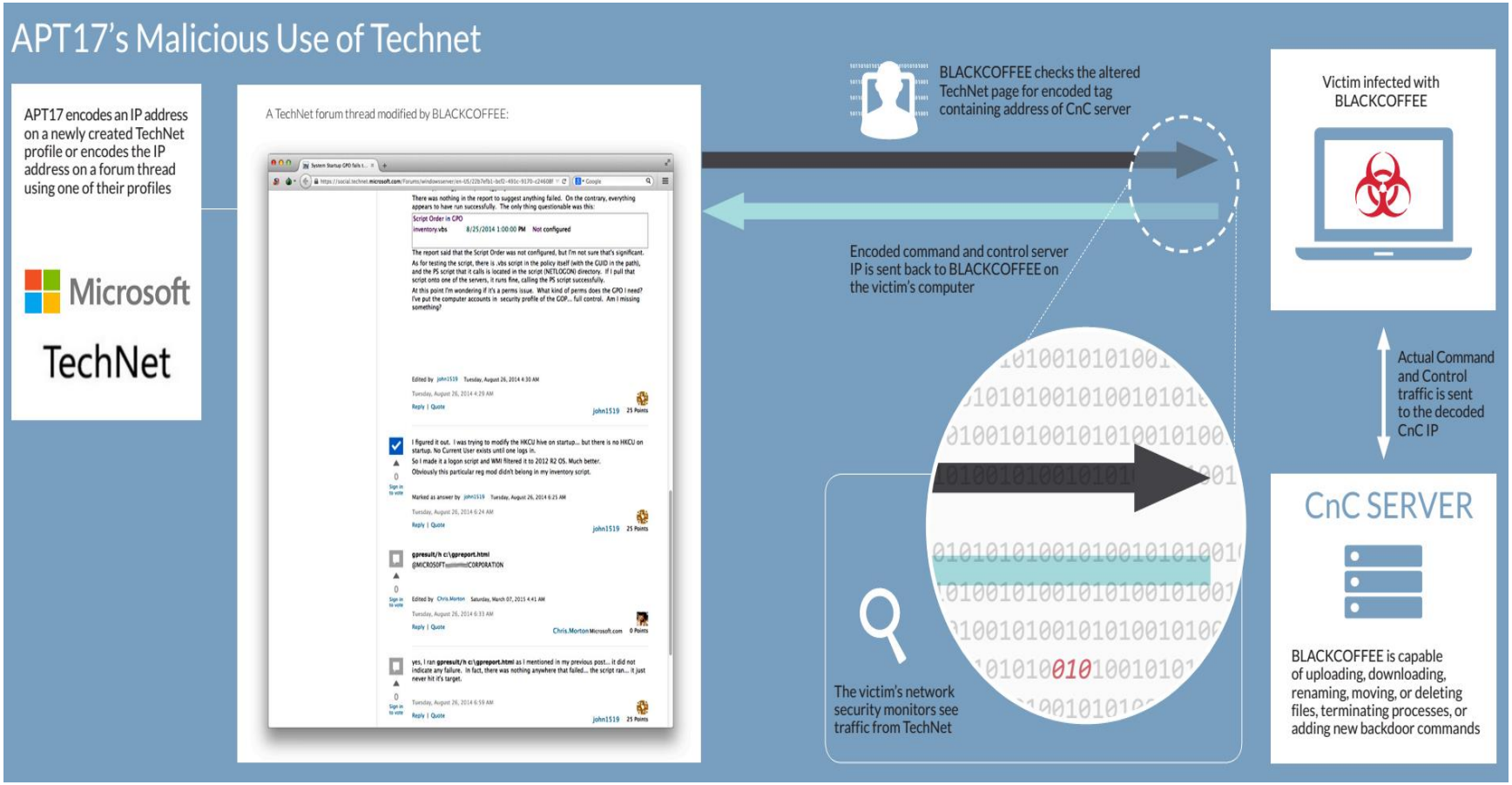
In 2013, banking malware – malicious programs that steal money from user accounts – played a leading role among financial cyber threats. Over the past year, at least 19 million cyber attacks were launched, representing two-thirds of all financial attacks involving malware.



Kaspersky Lab Report, Financial CyberThreats in 2013

External Threats Even Overwhelm Sophisticated Users

Using Microsoft TechNet, a web portal for IT professionals, APT17 posted in forum threads and created profile pages to host encoded CnC IP addresses that would direct a variant of the BLACKCOFFEE backdoor to their CnC server.



Hiding In Plain Sight: FireEye And Microsoft Expose Obfuscation Tactic, 2015

Latest Vulnerabilities, Threats, & Risk Mitigation…

Malicious Ads soared **260%** in the first half of 2015.
Unique Malvertisements rose 60% over same time.
Digital ads preferred method for distributing malware.
Fake **Flash** updates most common lure used by cyber-criminals.

Victims exposed to the Angler Exploit Kit, used in the past in such campaigns to deliver CryptoWall ransomware or effect click fraud.

"Malvertising is a silent killer because malicious ads **do not** require any type of user interaction in order to execute their payload.

The mere fact of browsing to a website that has adverts (and most sites, if not all, do) is enough to start the infection chain."

Latest Vulnerabilities, Threats, & Risk Mitigation…

HAMMERTOSS

APT29

FireEye. Special Report. (July 2015). HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group.

Introducing HAMMERTOSS
Five Stages of HAMMERTOSS

Stage 1: The Communication Process Begins with Twitter
Figure 1: HAMMERTOSS calls out to a Twitter handle

Stage 2: Tweeting a URL, Minimum File Size of an Image, and Part of an Encryption Key
Figure 2: Learning the URL, image size, and encryption key
Figure 3: Twitter page for d3109c83e07dd5d7fe032dc80c581d08

Stage 3: Visiting GitHub to Download an Image
Figure 4: The active Twitter account in our sample contained a GitHub URL and a related GitHub page with image containing encrypted data

Stage 4: APT29 Employs Basic Steganography
Figure 5: Encrypted data appended beyond the FF D9 JPEG End of File marker

Stage 5: Executing Commands and Uploading Victim Data
Figure 6: Executing Commands and Removing Data

Conclusion
Difficulty Identifying Accounts, Discerning Legitimate and Malicious Traffic, and Predicting the Payload

APT29: An Adaptive and Disciplined Threat Group

"Using a variety of techniques—from creating an algorithm that generates daily Twitter handles to embedding pictures with commands— it undermines detection of the malware by adding layers of obfuscation and mimicking the behavior of legitimate users…"

Latest Vulnerabilities, Threats, & Risk Mitigation…

2015

Trust is at the breaking point:
The idea of a Cryptoapocapyse is far from science fiction. Heartbleed was just a taste of what this could look like. Could a website be trusted? How many keys were compromised? Could an organization be trusted online? The era of cloud computing, parallel processing, and GPUs are being used to test these attacks. The cost to compromise a MD5-signed digital certificate is now $0.65[17] in Amazon AWS, down from $200,000 in less than two years.[18]

MOST ALARMING THREATS
(IN ORDER OF CONCERN)

1. WEAK CRYPTOGRAPHIC EXPLOIT
2. MOBILE CERTIFICATE MISUSE
3. CODE-SIGNING CERTIFICATE MISUSE
4. MALICIOUS MITM CERTIFICATES
5. SSH KEY MISUSE
6. SERVER CERTIFICATE MISUSE

2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point, Ponemon Institute, 2015.

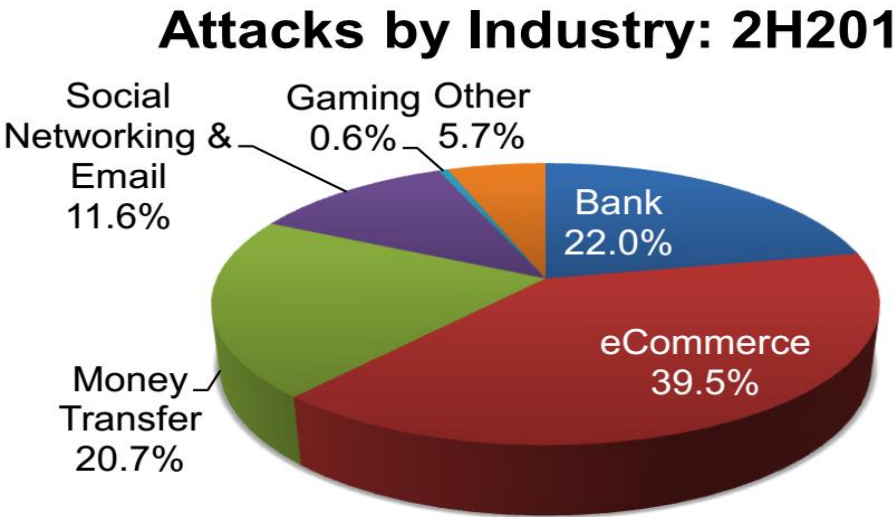
Latest Vulnerabilities, Threats, & Risk Mitigation…

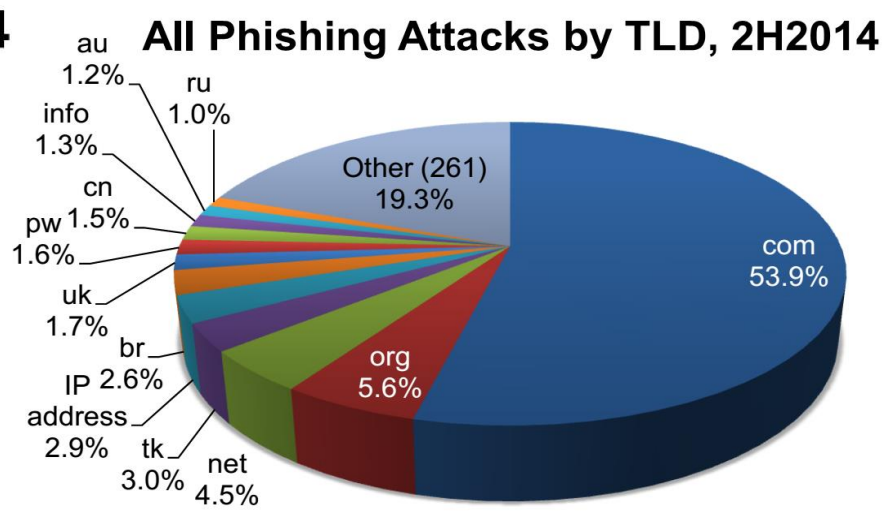
	Description of Attack Type	Example of Real-world Attack
Server Certificate Misuse	To impersonate public websites and decrypt encrypted traffic, attackers steal keys and certificates.	The theft of data on 4.5M healthcare patients in 2014 started with the exploit of Heartbleed to steal an SSL/TLS key and certificate that encrypted sensitive data.[4]
Code-signing Certificate Misuse	Attackers digitally sign malicious code to have it trusted and run.	The $1B theft by Carbanak operators was enabled by signed malware that looked like trusted software.[5]
SSH Key Misuse	Bad guys seeking to gain access to the most sensitive systems and data compromise SSH credentials.	APT operators like The Mask stole SSH keys and used their privileged access to compromise networks for over seven years.[6]
Man-in-the-middle (MITM) Attack	Cybercriminals compromise Certificate Authorities (CAs) or forge new certificates to trick users and monitor communications.	APT operators like Dark Hotel used a malicious CA and website certificates to get in and target executive communications.[7]
Weak Cryptographic Exploit	Adversaries target weak cryptography to create trusted keys and certificates.	As part of the Flame malware, Microsoft's software update service was spoofed by exploiting MD5-based signatures.[8]
Enterprise Mobility Certificate Misuse	Misuse of these credentials provides access to WiFi, VPN, or data protected by MDM/EMM systems.	An emerging threat that security professionals believe needs to be watched closely.

"The Ponemon Institute's 2015 *Cost of Failed Trust* Report reveals most organizations believe the trust established by cryptographic keys and digital certificates, which they require for their businesses to operate, is in jeopardy…"

2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point, Ponemon Institute, 2015.

Latest Vulnerabilities, Threats, & Risk Mitigation…

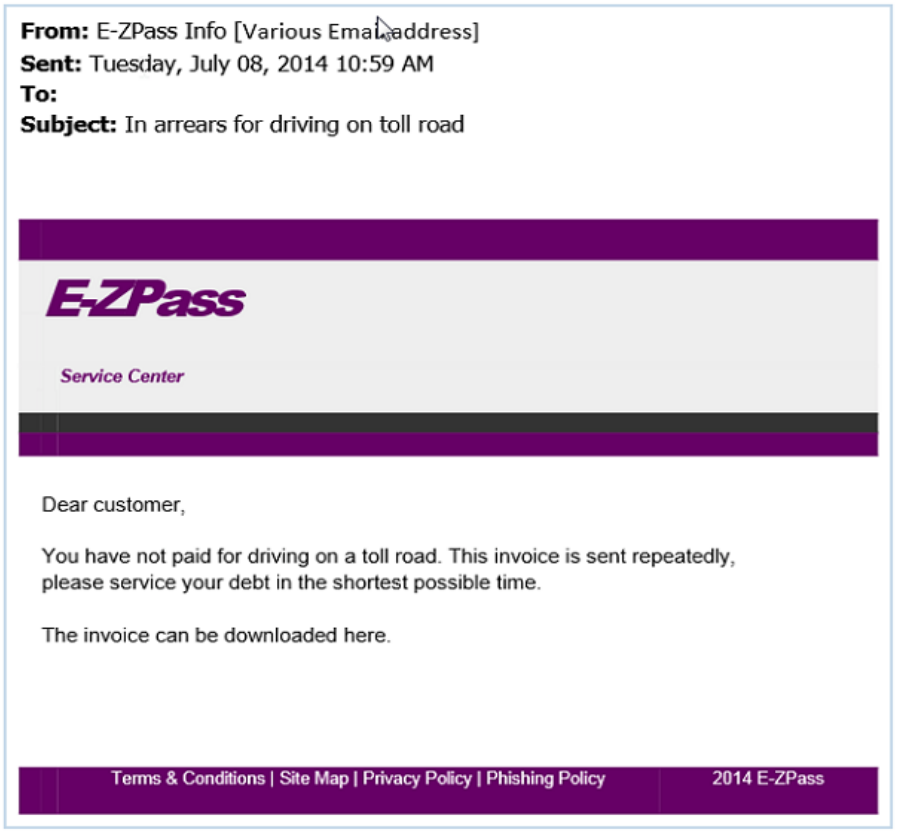




The majority of phishing continues to be concentrated in just a few namespaces. Most phishing takes place on compromised domain names, and so distribution by TLD has roughly paralleled TLD market share.

An APWG Industry Advisory. (Anti-Phishing Working Group, www.apwg.org). (27 May 2015). Global Phishing Survey: Trends and Domain Name Use in 2H2014: Unifying the Global Response To Cybercrime.

Latest Vulnerabilities, Threats, & Risk Mitigation…



From: E-ZPass Info [Various Email address]
Sent: Tuesday, July 08, 2014 10:59 AM
To:
Subject: In arrears for driving on toll road

E-ZPass

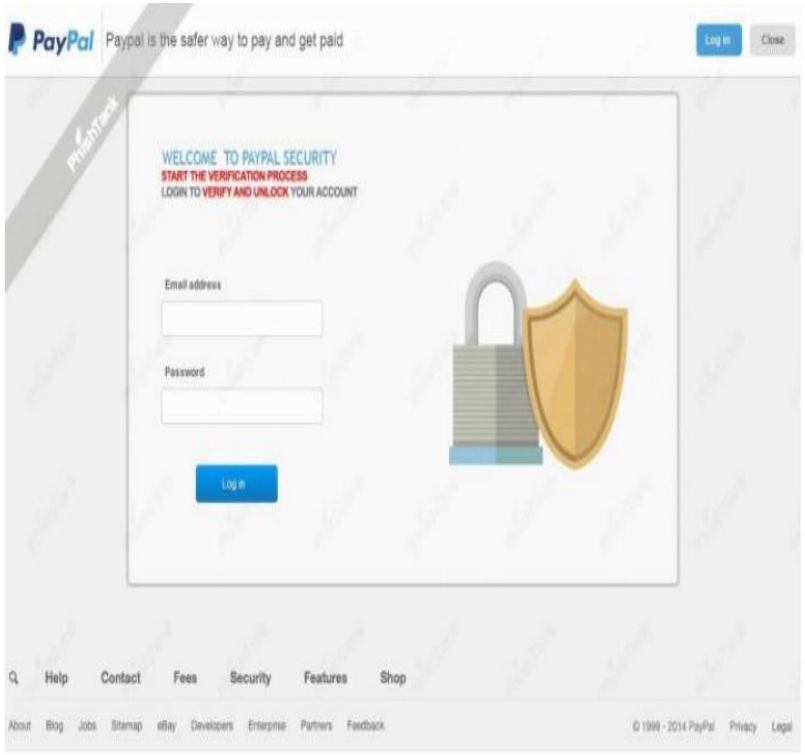
Service Center

Dear customer,

You have not paid for driving on a toll road. This invoice is sent repeatedly, please service your debt in the shortest possible time.

The invoice can be downloaded here.

Terms & Conditions | Site Map | Privacy Policy | Phishing Policy 2014 E-ZPass



A phishing lure e-mail targeting E-ZPass

An APWG Industry Advisory. (Anti-Phishing Working Group, www.apwg.org). (27 May 2015). Global Phishing Survey: Trends and Domain Name Use in 2H2014: Unifying the Global Response To Cybercrime.

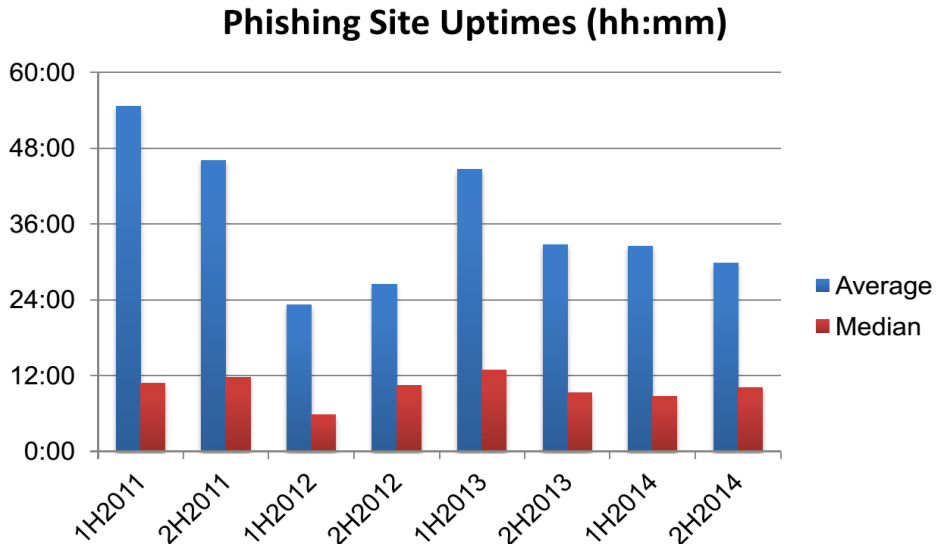
Latest Vulnerabilities, Threats, & Risk Mitigation…

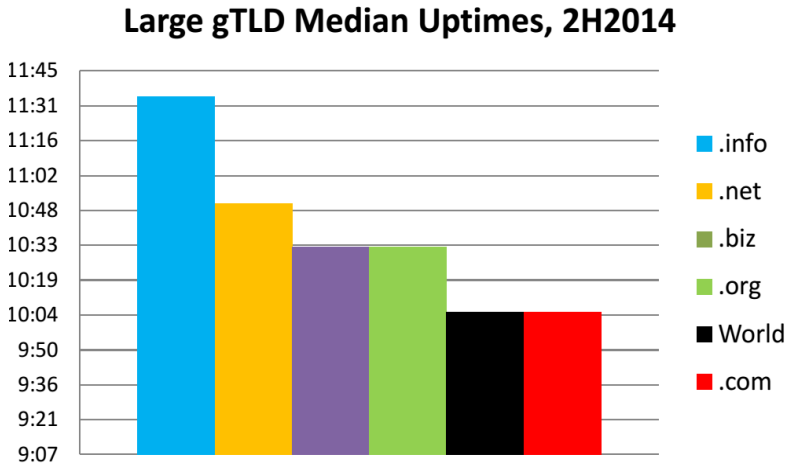
These show criminals seeking the credentials of consumers in places where consumers may least expect it. Phishers target wide-ranging targets for several reasons. One is to perform credit card theft, and hitting new targets may lull consumers into a false sense of security.
The phishers can also monetize stolen data through reshipping fraud, a tactic that remains popular. Phishers also steal usernames and passwords from one site in order to try those credential on other sites. Many **consumers re-use usernames and passwords**, and this poor habit can be costly.

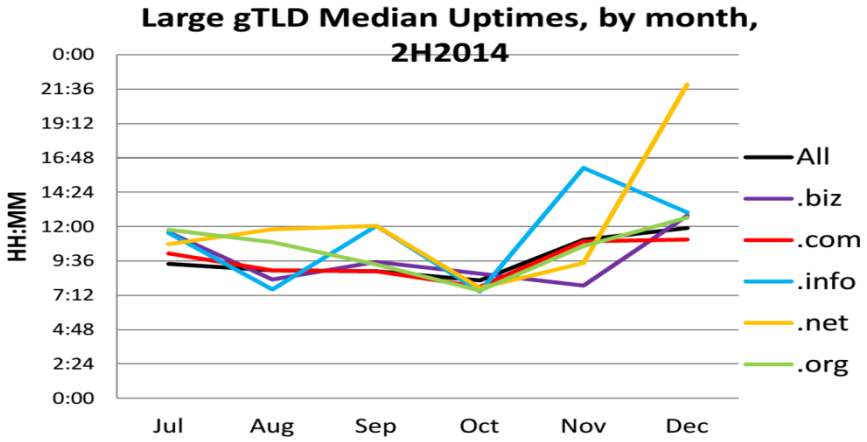
The "**uptimes**" or "**live**" times of phishing attacks are a vital measure of how damaging phishing attacks are, and are a metric of the success of mitigation efforts. The first day of a phishing attack is the most lucrative for the phisher, so quick takedowns are essential.

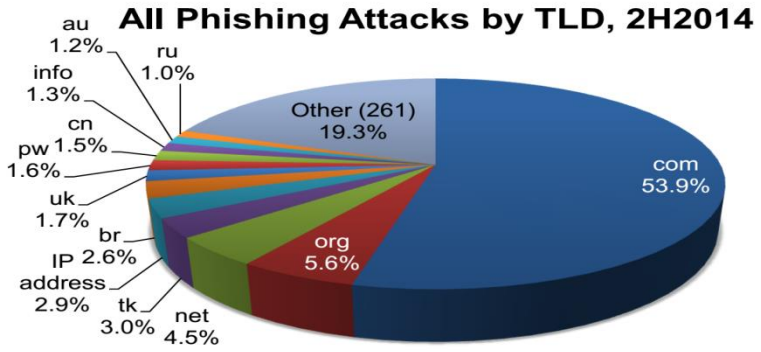
An APWG Industry Advisory. (Anti-Phishing Working Group, www.apwg.org). (27 May 2015). Global Phishing Survey: Trends and Domain Name Use in 2H2014: Unifying the Global Response To Cybercrime.

Latest Vulnerabilities, Threats, & Risk Mitigation…









An APWG Industry Advisory. (Anti-Phishing Working Group, www.apwg.org). (27 May 2015). Global Phishing Survey: Trends and Domain Name Use in 2H2014: Unifying the Global Response To Cybercrime.

Latest Vulnerabilities, Threats, & Risk Mitigation…

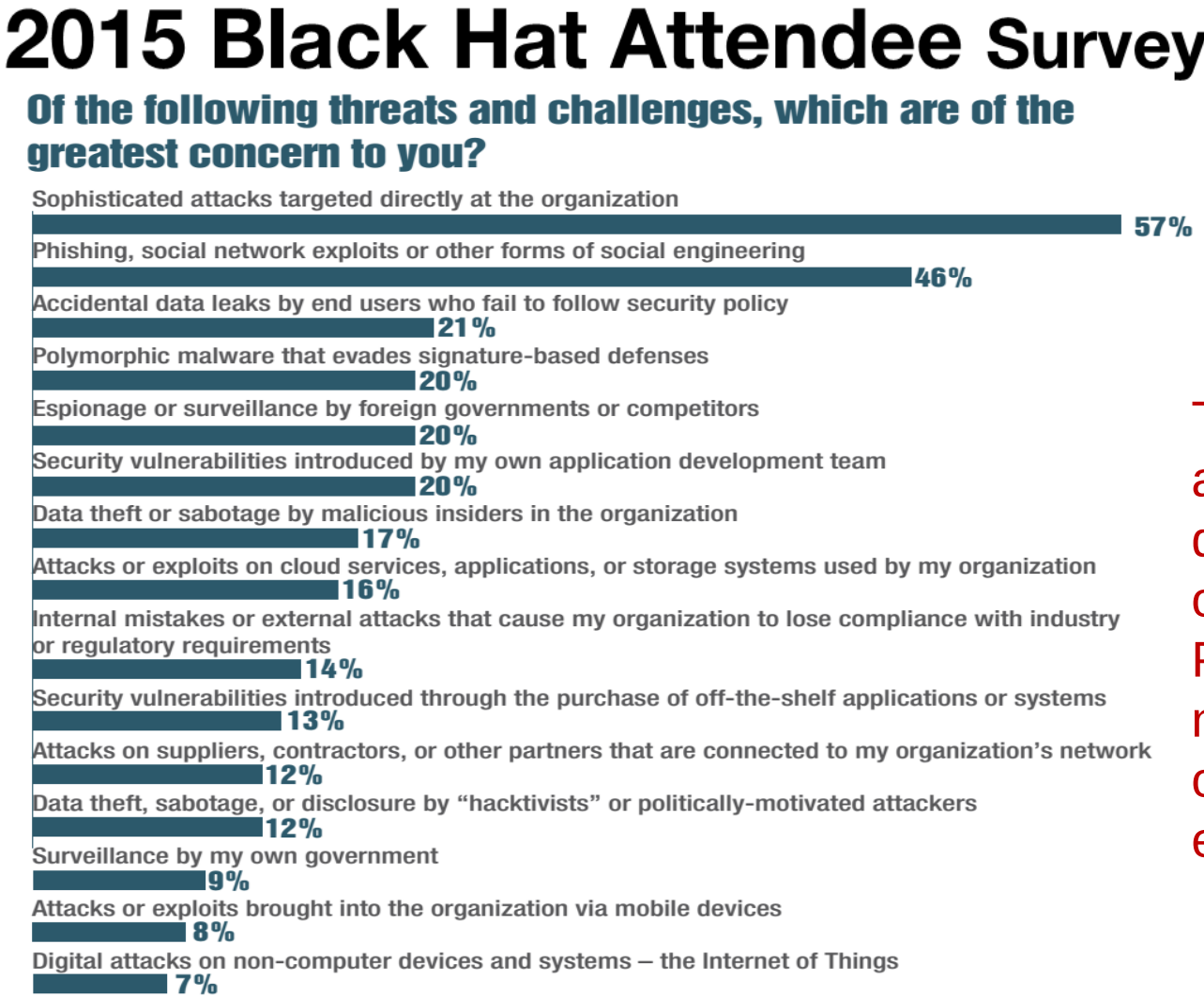
More than half **(54%) phishing attacks targeted just three brands** Apple, Paypal, and Chinese marketplace Taobao were hit by 20,000 unique phishing attacks each, while the **top ten brands accounted for over 75% of all phishing** and many of these saw more than 1000 separate attacks per month.

A high level of churn is seen in the smaller brands targeted, with well over half of those being hit in the first half of 2014 absent from the latest batch of stats.

One reason for going after smaller accounts is to catch victims unawares, access data like card information using the **logins acquired for smaller target sites**, and then trying the same access codes elsewhere in the hopes of **finding people indulging in password reuse**.

nakedsecurity. (June 1, 2015). Phishing study finds major brands heavily targeted, niche sites also at risk.

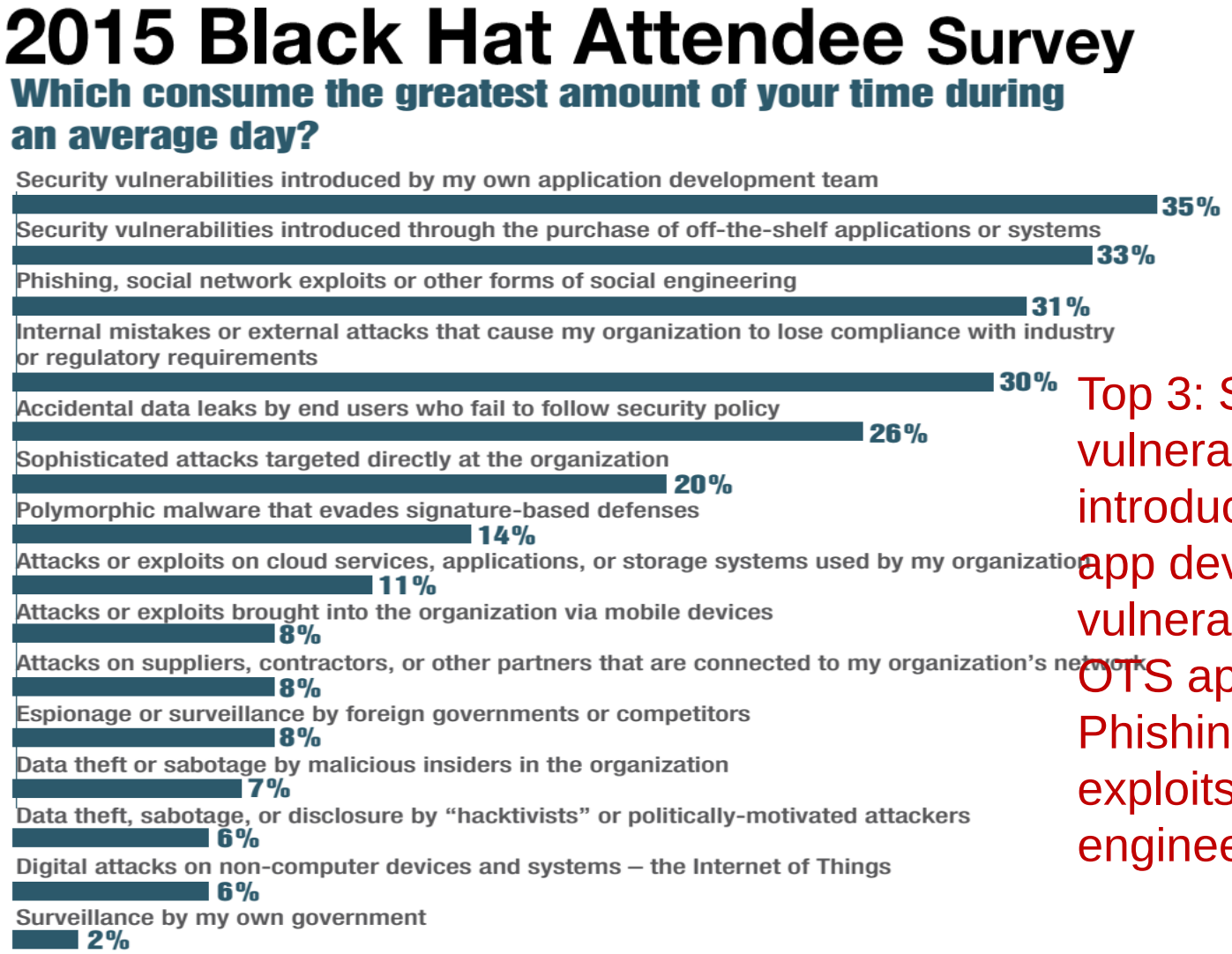
Latest Vulnerabilities, Threats, & Risk Mitigation…



Top 2: Sophisticated attacks targeted directly at the organization; Phishing, social network exploits or other forms of social engineering.

2015 Black Hat Attendee Survey (July 2015). 2015: Time to Rethink Enterprise IT Security.

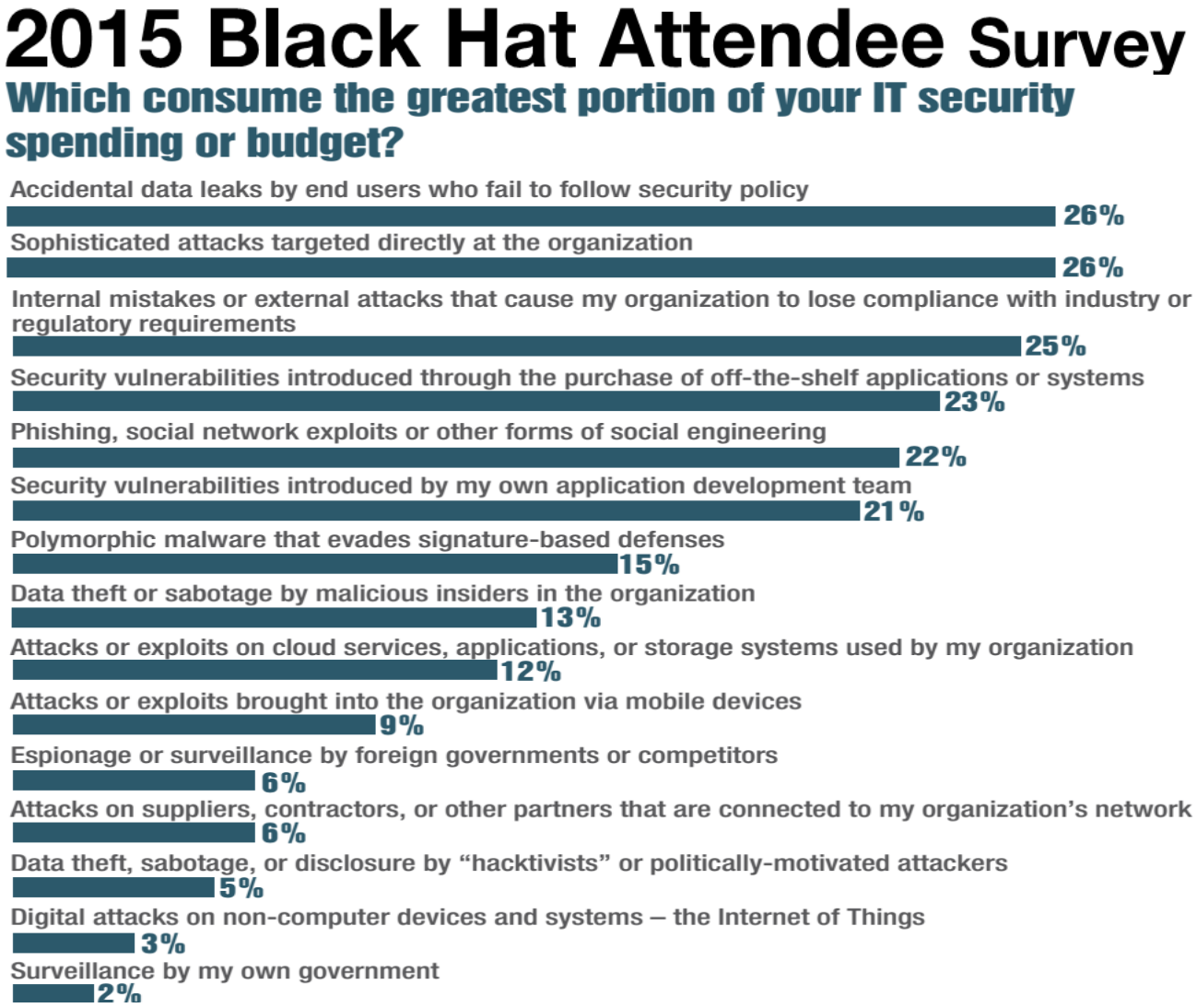
Latest Vulnerabilities, Threats, & Risk Mitigation…



Top 3: Security vulnerabilities introduced by my own app dev team; Security vulnerabilities through OTS apps or systems; Phishing, social network exploits, and social engineering.

2015 Black Hat Attendee Survey (July 2015). 2015: Time to Rethink Enterprise IT Security.

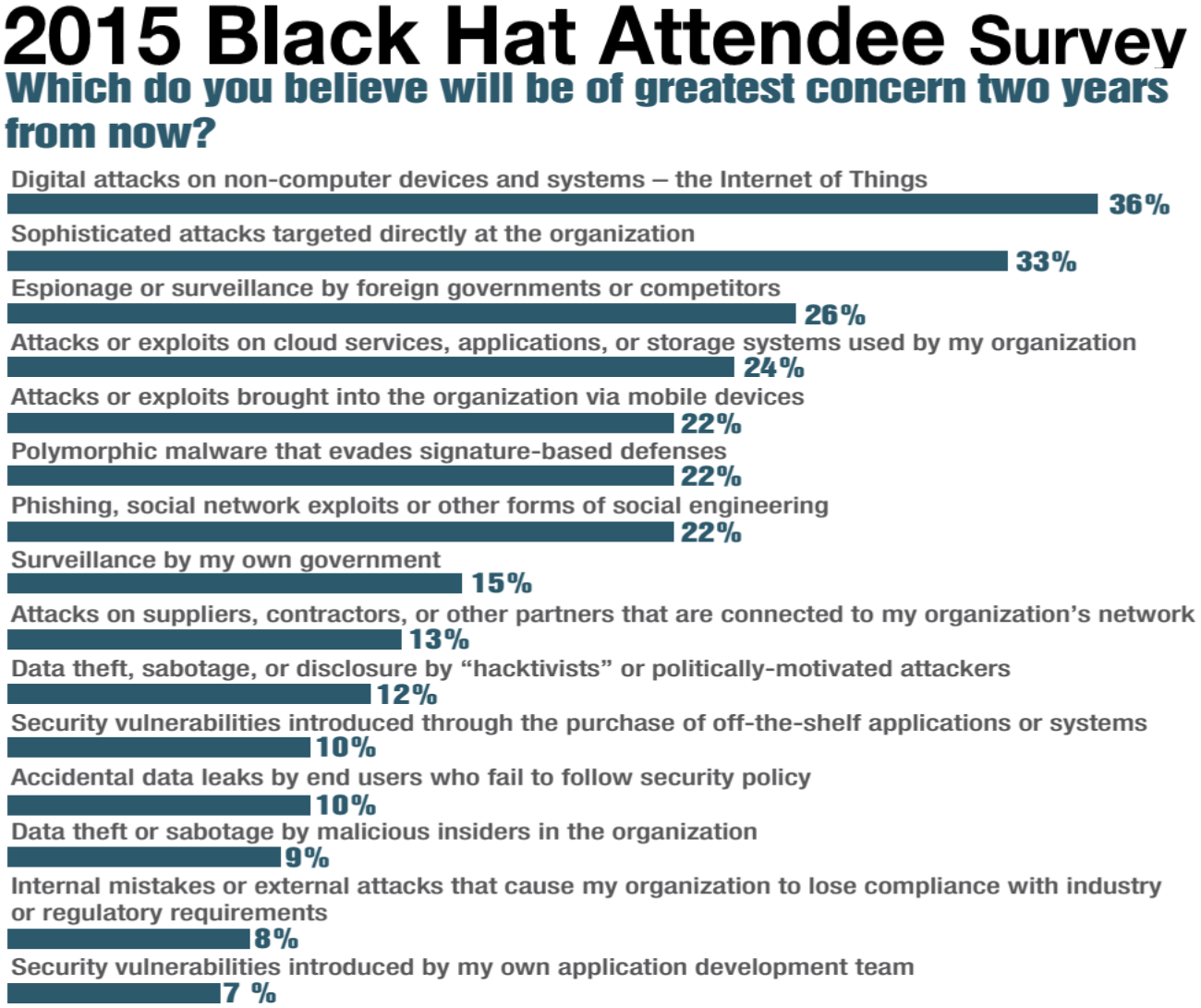
Latest Vulnerabilities, Threats, & Risk Mitigation…



Top 2: Accidental data leaks by end users who fail to follow security policy; Sophisticated attacks targeted directly at the organization.

2015 Black Hat Attendee Survey (July 2015). 2015: Time to Rethink Enterprise IT Security.

Latest Vulnerabilities, Threats, & Risk Mitigation…



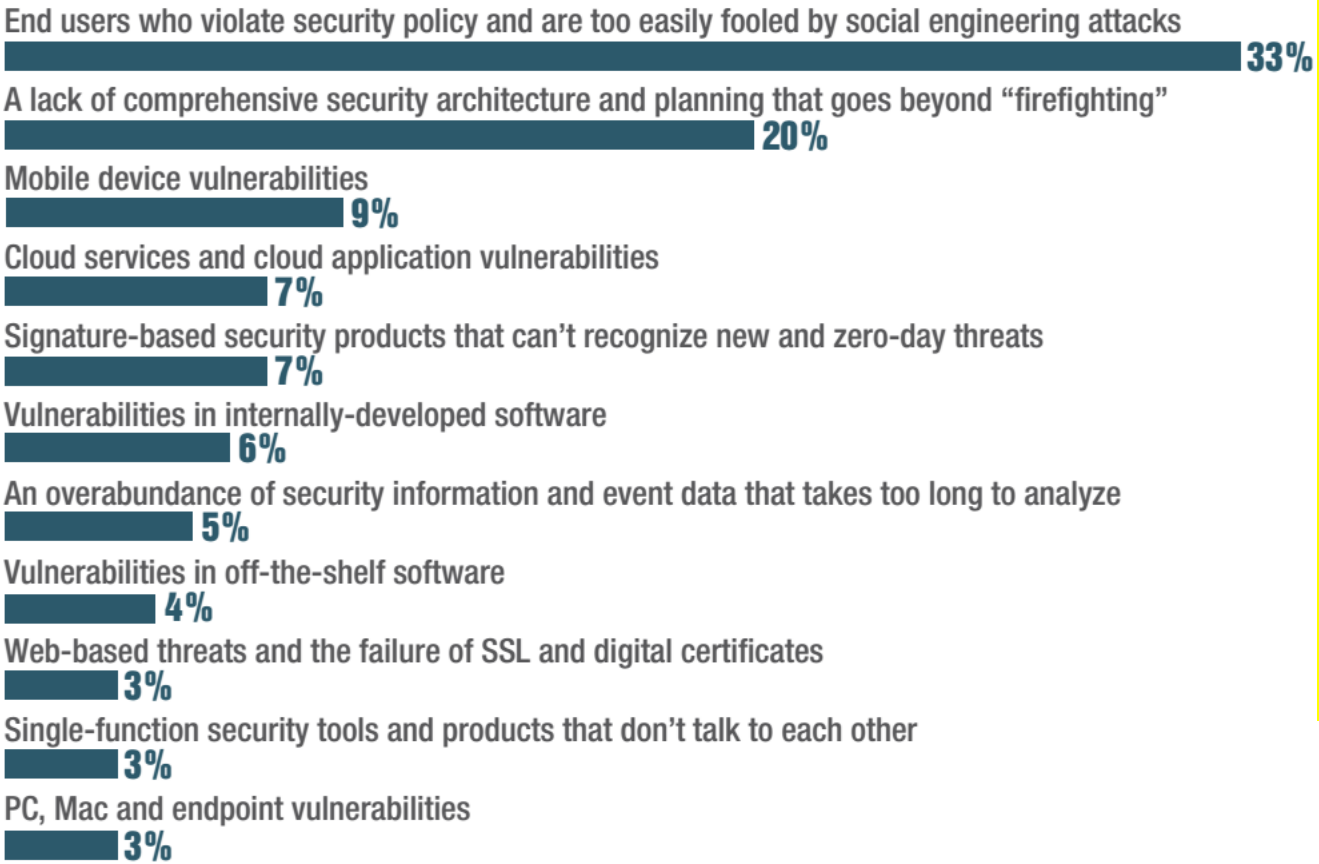
Top 3: Digital attacks on non-computer devices and systems – IOTs; Sophisticated attacks targeted directly at the organization; Espionage or surveillance by foreign governments and competitors.

2015 Black Hat Attendee Survey (July 2015). 2015: Time to Rethink Enterprise IT Security.

Latest Vulnerabilities, Threats, & Risk Mitigation…

2015 Black Hat Attendee Survey

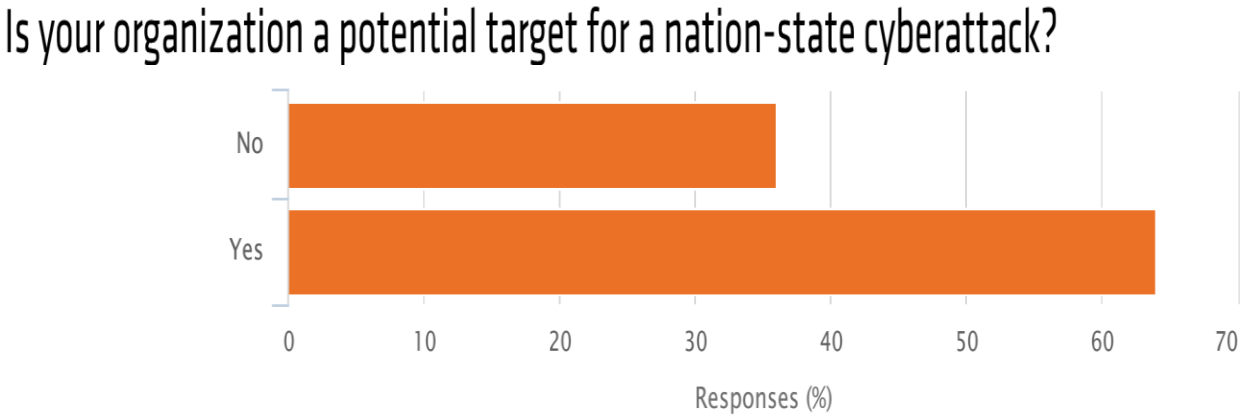
What is the weakest link in today's enterprise IT defenses?

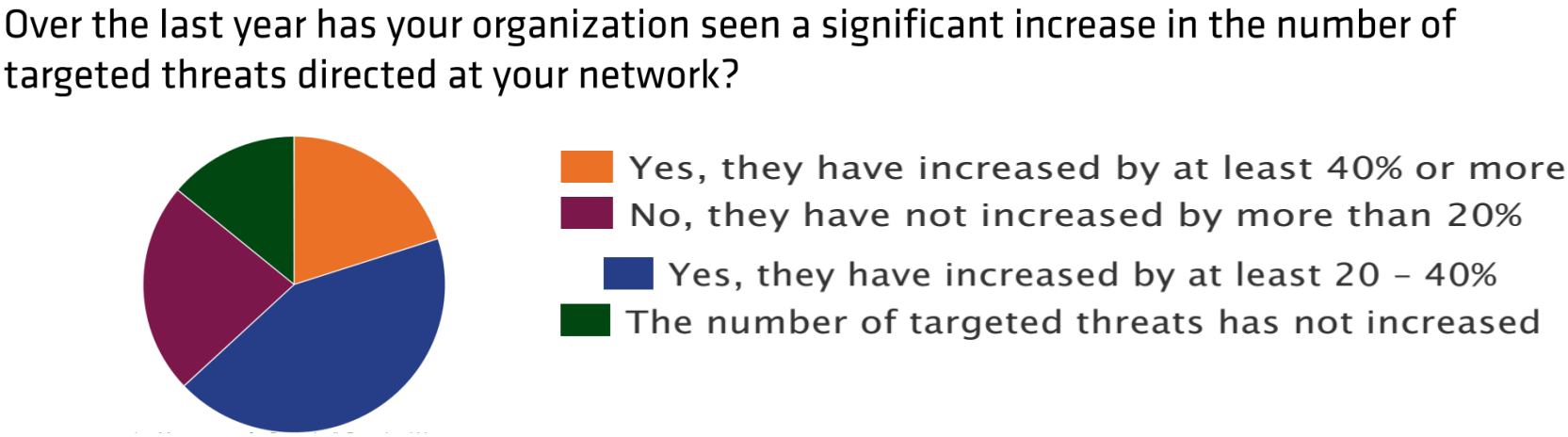


Top 2: End users who violate security policy and are **too easily fooled by social engineering attacks**; A lack of comprehensive security architecture and planning that goes beyond "firefighting."

2015 Black Hat Attendee Survey (July 2015). 2015: Time to Rethink Enterprise IT Security.

Latest Vulnerabilities, Threats, & Risk Mitigation…





Tripwire (2015). Black Hat 2015 Survey.

Latest Vulnerabilities, Threats, & Risk Mitigation…

PRINCIPLE 1 Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue. 7

PRINCIPLE 2 Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances. 9

PRINCIPLE 3 Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda. 11

PRINCIPLE 4 Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework. 13

PRINCIPLE 5 Board-management discussion of cyber risks should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach. 14

A rapidly evolving cyber-threat landscape… Balancing cybersecurity with profitability

National Association of Corporate Directors (2014). Cyber-Risk Oversight Director's Handbook Series.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Managing Cyber Risk: Are Companies Safeguarding Their Assets? 1st Qtr. 2015

Figure 1

To what extent do you agree or disagree with these statements related to your company's IT risk oversight?

	Agree	Somewhat Agree	Somewhat Disagree	Disagree	Unsure
Our company has IT risk very well under control with regard to the possibility of a cyber breach.	20.77%	58.45%	10.14%	5.80%	4.83%
To make sound decisions related to IT risk oversight, it is necessary for companies today to have at least one board member with a specific IT background.	24.64%	33.82%	25.60%	14.98%	0.97%
Our board has one or more members who do not have the skills and understanding of IT risk to provide effective oversight in this area.	32.20%	28.29%	18.54%	17.07%	3.90%

58%: **Somewhat Agree** that their company has IT risk very well under control…

Scally, Deborah. (1st Quarter 2015). Managing Cyber Risk: Are Companies Safeguarding Their Assets? NYSE Governance Services: Corporate Board Member Magazine.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Managing Cyber Risk: Are Companies Safeguarding Their Assets? 1st Qtr. 2015

Figure 2
Which of the following present challenges for your board's oversight of IT risk? *(Select all that apply.)*

83%: The sources of IT risk are constantly changing.

Scally, Deborah. (1st Quarter 2015). Managing Cyber Risk: Are Companies Safeguarding Their Assets? NYSE Governance Services: Corporate Board Member Magazine.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Managing Cyber Risk: Are Companies Safeguarding Their Assets? 1st Qtr. 2015

67%: **Somewhat confident** in management's ability to respond to cyber threats.

57%: Board **somewhat effective** in holding management accountable

Figure 3

How confident are you in your management's ability to respond to and mitigate the scope of IT/cyber threats in the current environment?

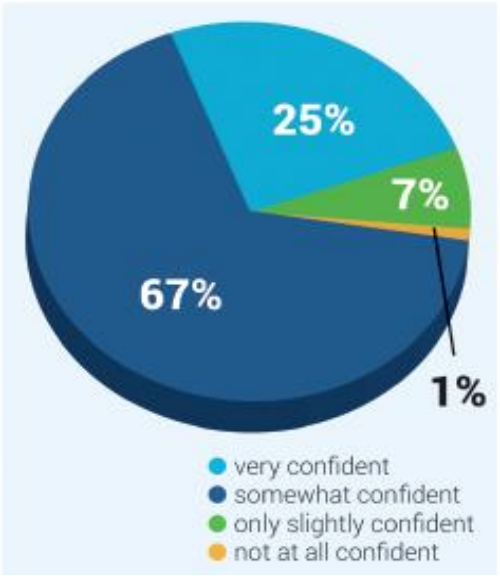
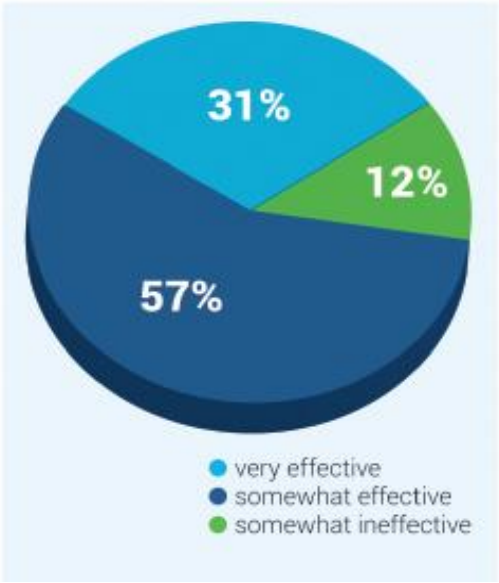


Figure 4

How effective is your board at holding management accountable for managing cyber security risk?



Scally, Deborah. (1st Quarter 2015). Managing Cyber Risk: Are Companies Safeguarding Their Assets? NYSE Governance Services: Corporate Board Member Magazine.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Managing Cyber Risk: Are Companies Safeguarding Their Assets? 1st Qtr. 2015

Figure 6

How often does your board discuss the following topics to oversee risk and enhance enterprise value?

	Regularly	Occasionally	Never
Cyber/IT security	54.85%	41.75%	3.4%
Emerging technologies	35.44%	54.37%	10.19%
Post-merger transaction integration	46.19%	36.55%	17.26%
Operational technology	53.40%	42.72%	3.88%
Compliance systems	71.84%	26.21%	1.94%
Social media	16.99%	65.63%	17.48%

17%: believe their Board discusses Social Media Regularly.

Scally, Deborah. (1st Quarter 2015). Managing Cyber Risk: Are Companies Safeguarding Their Assets? NYSE Governance Services: Corporate Board Member Magazine.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Cyber Smart: Building a Cyber Resilient Organization (Malhotra, 2015)

"Cyber Risk Management is the coordinated management of Strategies, Tactics, Operations, &, Intelligence to effectively manage an organization's digital assets and to minimize the potential for adverse consequences…"

"It includes processes by which an information-enabled enterprise protects its critical digital assets including reputational assets from external and internal threats… "

"Hence, cyber risk management should be considered as an integral aspect of business strategy, tactics, operations, and intelligence, as well as assessing, managing, and controlling related business risks."

Latest Vulnerabilities, Threats, & Risk Mitigation…

Cyber risk is more than an IT issue; it's a *business* issue. - PwC

- Have we performed a cyber business risk assessment to identify our key business risks?
- How do we know where to invest to reduce our cyber risks?
- What would be the disruption to our business from a cyber attack? How would it affect our business, brand, and reputation?
- How much revenue would we lose if our business processes were impacted by a cyber event?
- Have we identified our most critical business assets and do we understand their value to our adversaries?
- Have we looked at the value of these assets and business processes through the lens of the various threat actors?
- Do we have a cyber incident capability that will allow us to quickly respond to a cyber attack?
- How do we establish cyber risk tolerance to the organization?
- How do we communicate about cyber risk to the board and other stakeholders?
- Is my business resilient enough to survive a cyber attack?

PricewaterhouseCoopers LLP (2014 Oct.). Threat Smart: Building a Cyber Resilient Financial Institution.

Latest Vulnerabilities, Threats, & Risk Mitigation…

The Cyber-Finance-Trust ™ Framework

While many financial institutions have processes and controls in place to manage day-to-day risks, they often do not address cyber risks...

These two types of risk share similar traits; both are hard to quantify, seem remote, and have a low probability of occurring…

Typically, data-security systems are designed to meet just minimum levels of regulatory or industry compliance, rather than to identify the risks to the business and implement appropriate safeguards…

Such institutions are ill-prepared to **anticipate** cyber threats and prepare a response in advance. They can only react. - PwC

http://www.FutureOfFinance.org/

PDC x TS ➡ (EEO) ➡ F ⟷ C

PricewaterhouseCoopers LLP (2014 Oct.). Threat Smart: Building a Cyber Resilient Financial Institution.

Latest Vulnerabilities, Threats, & Risk Mitigation…

The Cyber-Finance-Trust ™ Framework

Can Help Firms Recognize the Following Limitations

- Cyber threats viewed solely as an IT issue rather than a business issue
- Inability to look at the big picture
- Lack of common processes and methodologies
- Reluctance to share cyber security intelligence
- Cyber risk flying below the radar
- Taking a one-size-fits-all approach

http://www.FutureOfFinance.org/

PDC x TS ➡ (EEO) ➡ F ⟷ C

PricewaterhouseCoopers LLP (2014 Oct.). Threat Smart: Building a Cyber Resilient Financial Institution.

Latest Vulnerabilities, Threats, & Risk Mitigation…

The Cyber-Finance-Trust ™ Framework

Can Help Firms in Achieving the following Goals

1. *Establish cyber risk governance.*
2. *Understand your cyber organizational boundary.*
3. *Identify your critical business processes and assets.*
4. *Identify cyber threats.*
5. *Improve your collection, analysis, and reporting of information.*
6. *Plan and respond. This step includes developing playbooks, improving cyber intelligence gathering techniques, leveraging cyber insurance options, and upgrading cyber security technologies.*

PricewaterhouseCoopers LLP (2014 Oct.). Threat Smart: Building a Cyber Resilient Financial Institution.

Latest Vulnerabilities, Threats, & Risk Mitigation…

2015 Information Security Breaches Survey

1. The number of security breaches has increased, the scale and cost has nearly doubled. Eleven percent of respondents changed the nature of their business as a result of their worst breach.
2. Not as many organisations increased their spending in information security, and fewer organisations than in previous years expect to spend more in the future.
3. Nearly 9 out of 10 large organisations surveyed now suffer some form of security breach – suggesting that these incidents are now a near certainty. Businesses should ensure they are managing the risk accordingly.
4. Despite the increase in staff awareness training, people are as likely to cause a breach as viruses and other types of malicious software.
5. When looking at drivers for information security expenditure, 'Protecting customer information' and 'Protecting the organisation's reputation' account for over half of the responses.
6. The trend in outsourcing certain security functions and the use of 'Cloud computing and storage' continue to rise.

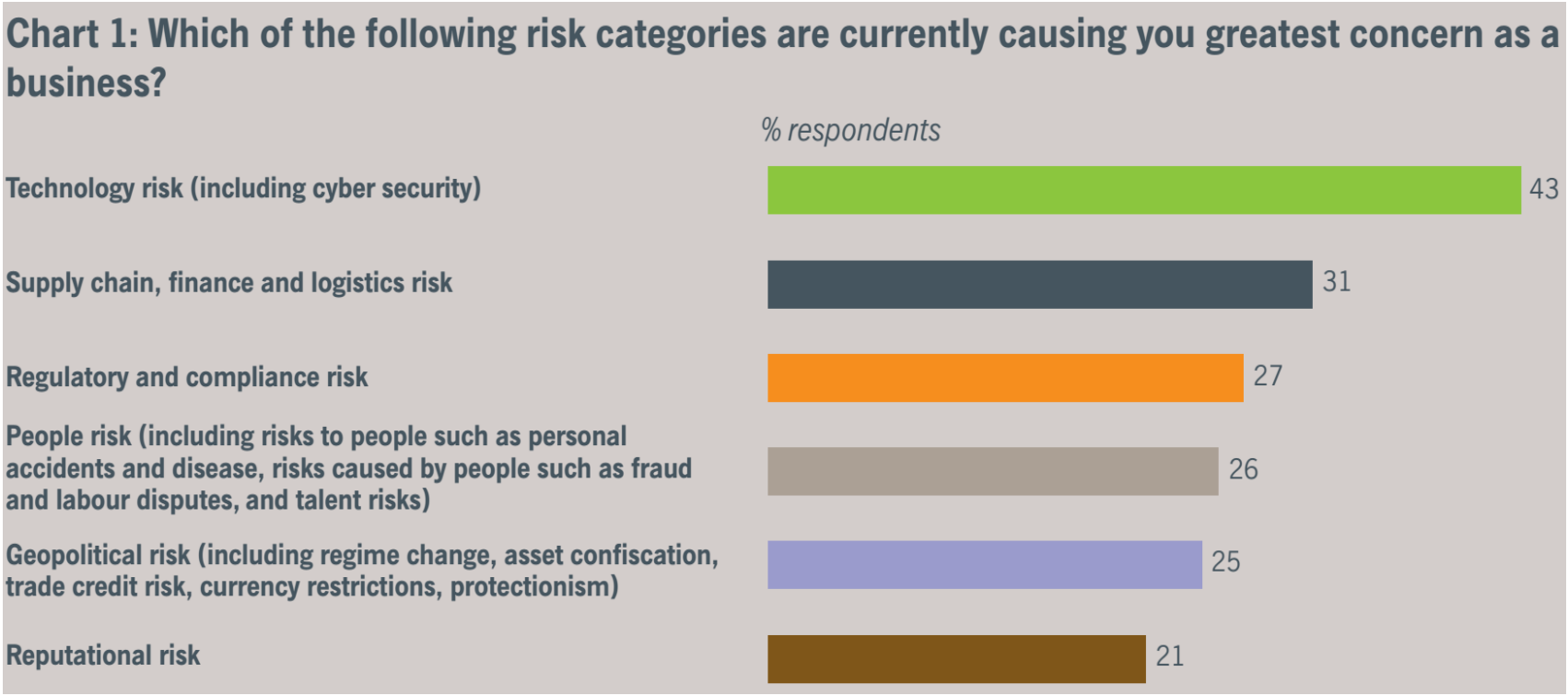
90% of **large organisations** reported that they had suffered a security breach, up from 81% in 2014.

Small organisations recorded a similar picture, with nearly **75%** reporting a security breach; this is an increase on the 2014 and 2013 figures.

HM Government (2015). 2015 Information Security Breaches Survey. (By PwC). HM Government, UK.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Emerging Risks Barometer 2015

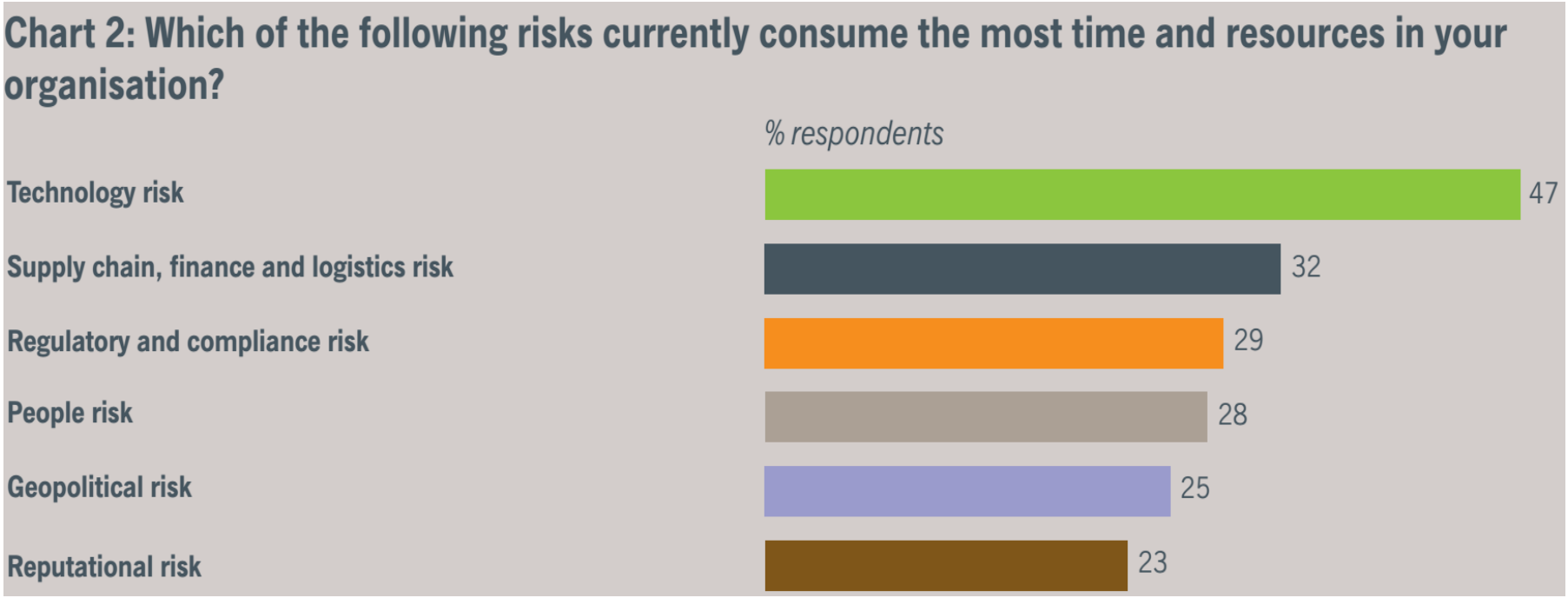


One of the consequences of **globalised and technology enabled growth** is a new wave of **complex**, **interrelated** and **fast-changing** risks.

ACE Limited. (2015). Emerging Risks Barometer: 2015 ACE European Risk Briefing.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Emerging Risks Barometer 2015

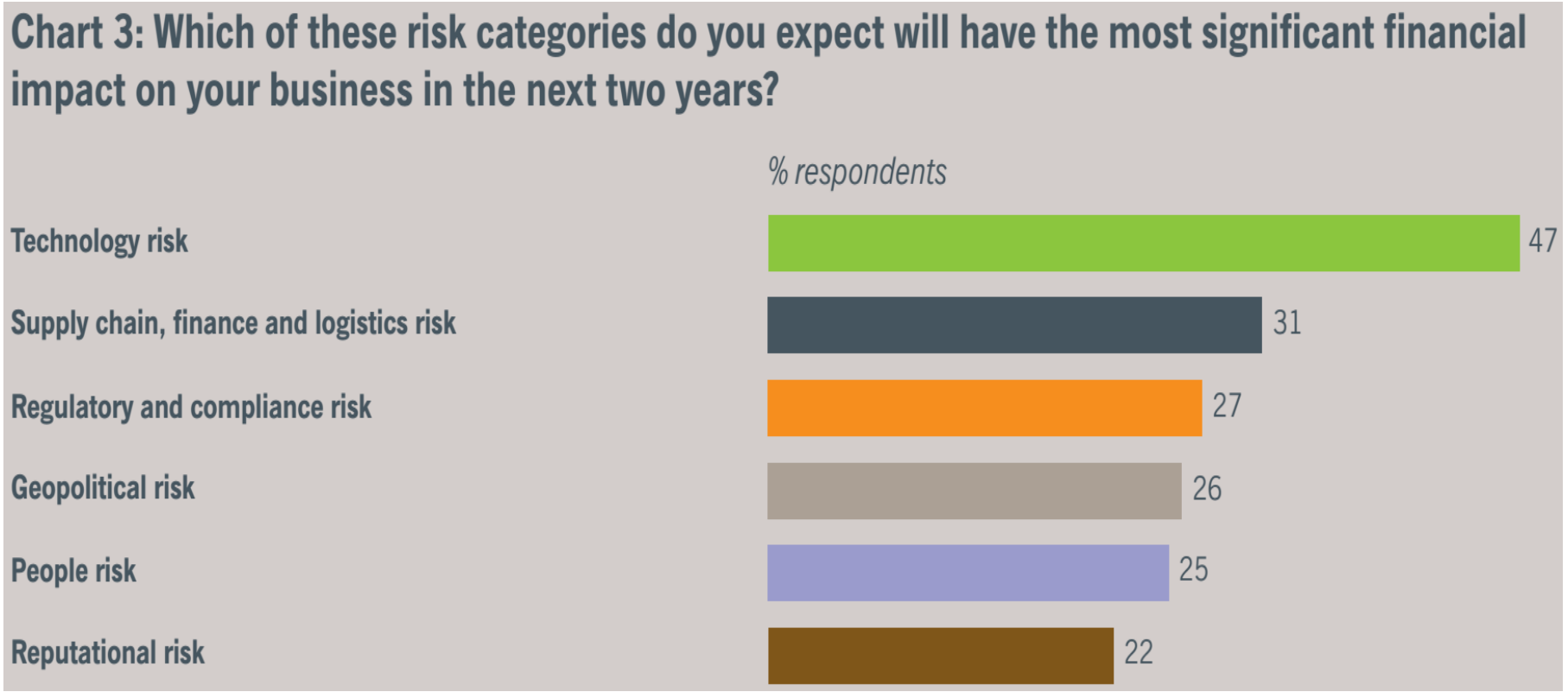


Verizon's 2015 Data Breach Investigations Report found **that internal workers ultimately caused** around **90% of data breach** incidents – whether through **basic error**, **allowing their devices to become infected**, **behaving irresponsibly online** or **losing their equipment**.

ACE Limited. (2015). Emerging Risks Barometer: 2015 ACE European Risk Briefing.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Emerging Risks Barometer 2015



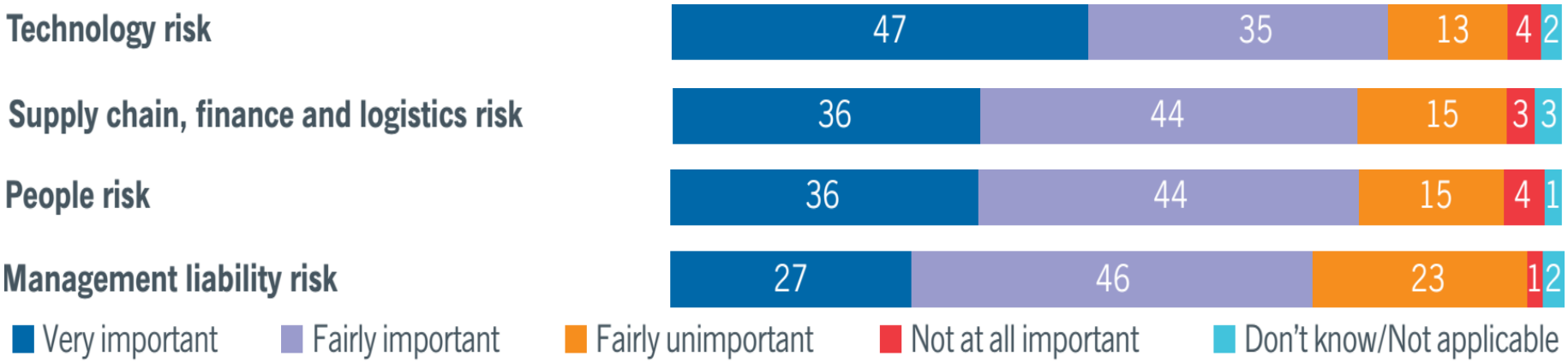
One of the consequences of **globalised and technology enabled growth** is a new wave of **complex**, **interrelated** and **fast-changing** risks.

ACE Limited. (2015). Emerging Risks Barometer: 2015 ACE European Risk Briefing.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Emerging Risks Barometer 2015

Chart 4: How important is insurance as part of your strategy to manage the following risks?



- Technology risk is most likely to be among risk managers' greatest concerns
- Risk managers expect this risk to have the greatest financial impact on their businesses
- It consumes the most time and resources of any emerging risk

- It is the risk area where insurance is of highest importance
- It is also the area where the market most needs to improve

One of the consequences of **globalised and technology enabled growth** is a new wave of **complex**, **interrelated** and **fast-changing** risks.

ACE Limited. (2015). Emerging Risks Barometer: 2015 ACE European Risk Briefing.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Emerging Risks Barometer 2015

Chart 5: Which of the following aspects of technology risk currently cause you the greatest concern?

33%
Hacking/denial-of-service attacks

30%
Systems failure

29%
Advances in digital technology threatening existing business model

27%
Deliberate introduction of malware/viruses

24%
Data theft by third parties

23%
Data theft by staff

23%
Violation of customer privacy/data security breach

19%
Business interruption (e.g. loss of key business applications)

18%
Theft of intellectual property

ACE Limited. (2015). Emerging Risks Barometer: 2015 ACE European Risk Briefing.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Bank of England Systemic Risk Survey

And finally, the **perceived risk of cyber attack** increased markedly (+20 percentage points to 30%) and is now at its **highest recorded level**.

The seven risks most frequently cited in the 2015 H1 survey were (**Chart 5**):

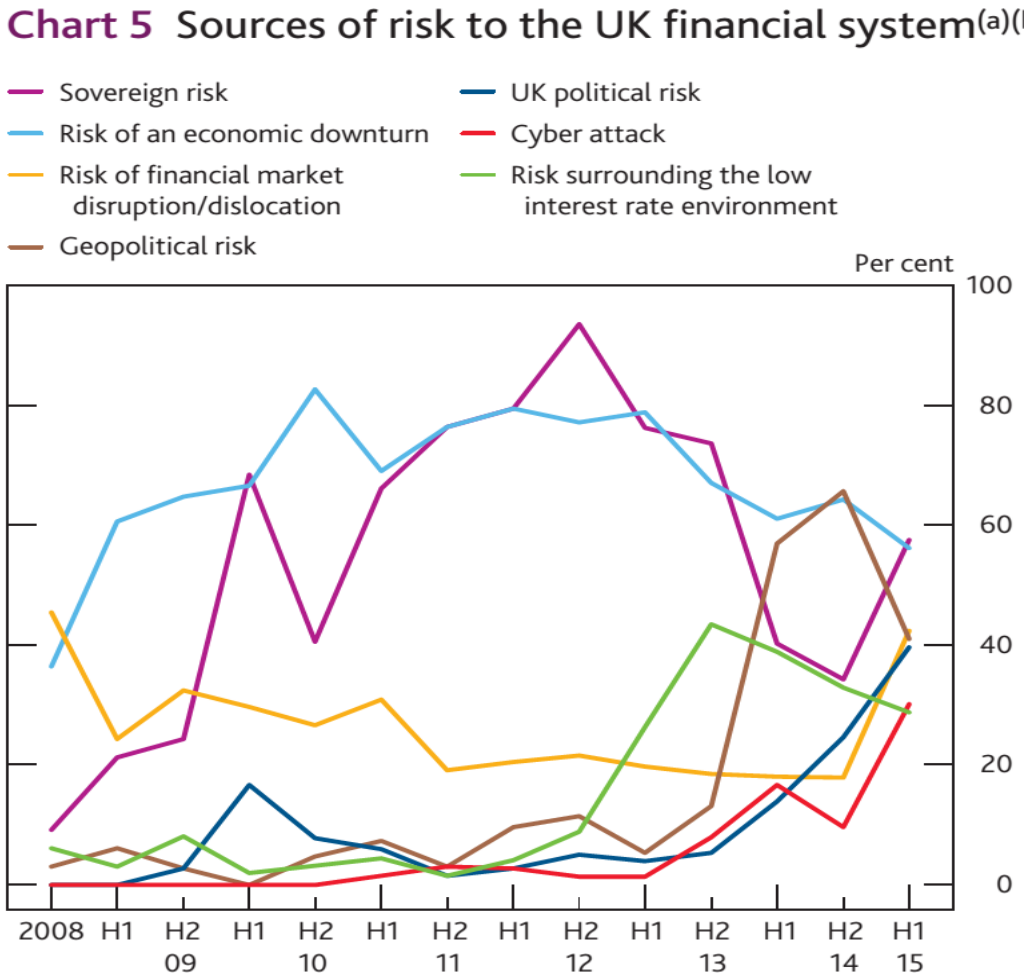
- Sovereign risk (cited by 58% of respondents)
- Risk of an economic downturn (56%)
- Risk of financial market disruption/dislocation (42%)
- Geopolitical risk (41%)
- UK political risk (40%)
- Cyber attack (30%)
- Risk surrounding the low interest rate environment (29%)

Cyber attack is now classified as an individual category, where as **previously it was predominantly captured by operational risk**. Applying this to the 2014 H2 results means operational risk no longer appears in the top seven risks.

Bank of England (2015). Systemic Risk Survey: Survey results | 2015 H1.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Bank of England Systemic Risk Survey

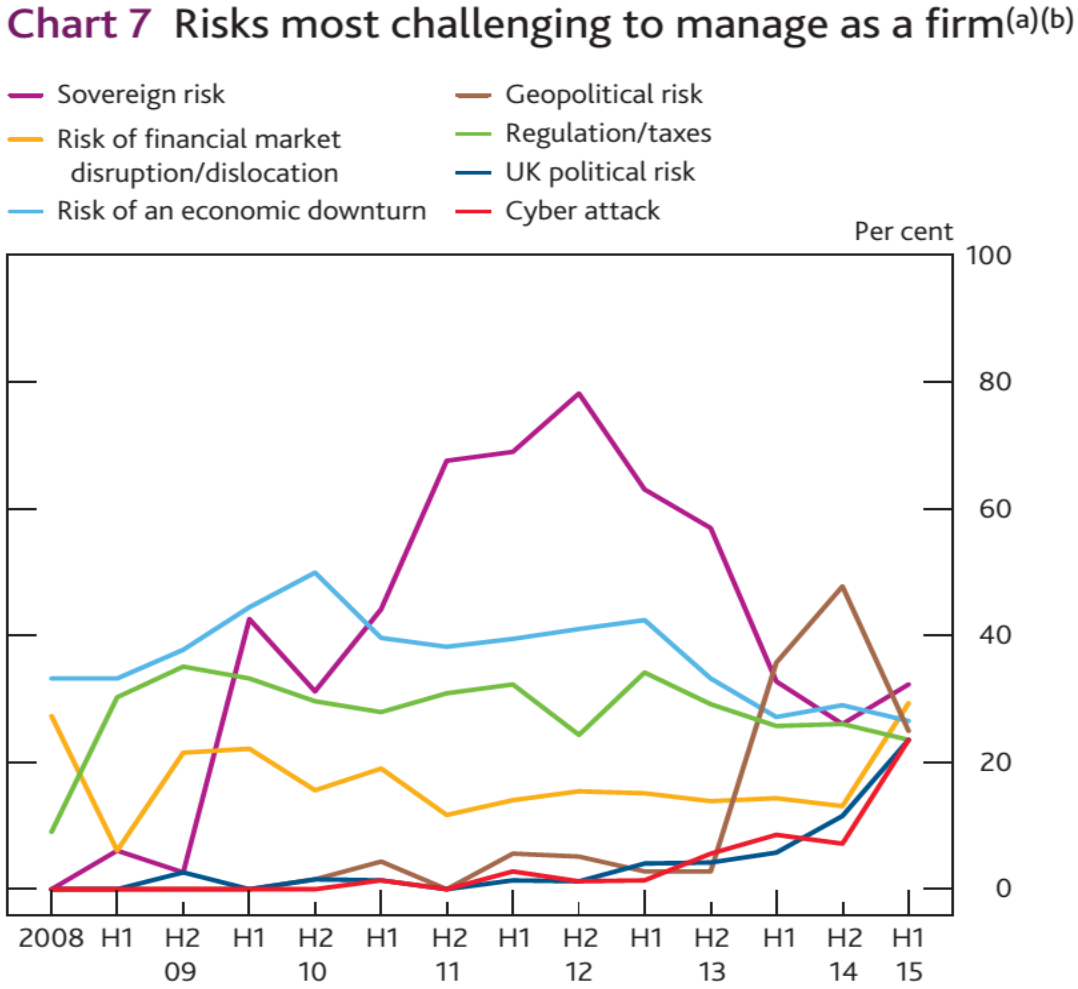


Given the increased proportion of respondents citing cyber attacks as a perceived risk, a **new source of risk category** was introduced — **cyber attack**. This new category was **one of the seven most commonly cited risks** in the 2015 H1 survey.

Bank of England (2015). Systemic Risk Survey: Survey results | 2015 H1.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Bank of England Systemic Risk Survey



Given the increased proportion of respondents citing cyber attacks as a perceived risk, a **new source of risk category** was introduced — **cyber attack**. This new category was **one of the seven most commonly cited risks** in the 2015 H1 survey.

Bank of England (2015). Systemic Risk Survey: Survey results | 2015 H1.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Mobile Threat Assessment

WE FOUND THE FOLLOWING THREATS TO ANDROID DEVICES:

MALWARE

We found millions of mobile malware samples—and that number is growing by the week. Ninety-six percent of malware targets Android. KorBanker, which stole users' bank login credentials, is one example.

VULNERABILITIES

5 billion

More than five billion downloaded Android apps are vulnerable to remote attacks. One especially risky vulnerability is known as JavaScript-Binding-Over-HTTP (JBOH).

AGGRESSIVE ADWARE

5.61%

Aggressive ad libraries can leak personal data over the network— sometimes in plain text. Burstly is one of the most popular. It's used in more than 300,000 apps, including 5.61 percent of the 500 most-downloaded ones.

World Population is ~ 7 Billion

More than 5 billion downloaded Android apps are vulnerable to remote attacks.

FireEye (February 2015). Special Report: Out Of Pocket: A Comprehensive Mobile Threat Assessment of 7 Million iOS and Android Apps.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Mobile Threat Assessment

WE FOUND THE FOLLOWING THREATS TO IOS DEVICES:

VULNERABILITIES

UXSS

In particular, SSL/TLS misuse and other crypto-related vulnerabilities are common to apps. Attackers are also more often exploiting Universal Cross-Site Scripting (UXSS) vulnerabilities.

ENPUBLIC APPS

1400

These apps bypass Apple's strict review process by hijacking a process normally used to install custom enterprise apps. Many EnPublic apps invoke risky private APIs. In the wrong hands, these APIs threaten user privacy and introduce many vulnerabilities. We found only 1,400 EnPublic apps, a relatively low number. But this poses an intriguing avenue for attackers in the future.

MALWARE

Although uncommon, attackers are looking closely at this attack vector. They're eager to compromise devices that have not been "jailbroken." Attackers have started to use enterprise/ad-hoc provisioning to deliver iOS malware to non-jailbroken devices through trusted USB connections and over-the-air delivery.

Mobile app usage accounts for 86% of time spent on mobile devices, up six percent in just one year.

FireEye (February 2015). Special Report: Out Of Pocket: A Comprehensive Mobile Threat Assessment of 7 Million iOS and Android Apps.

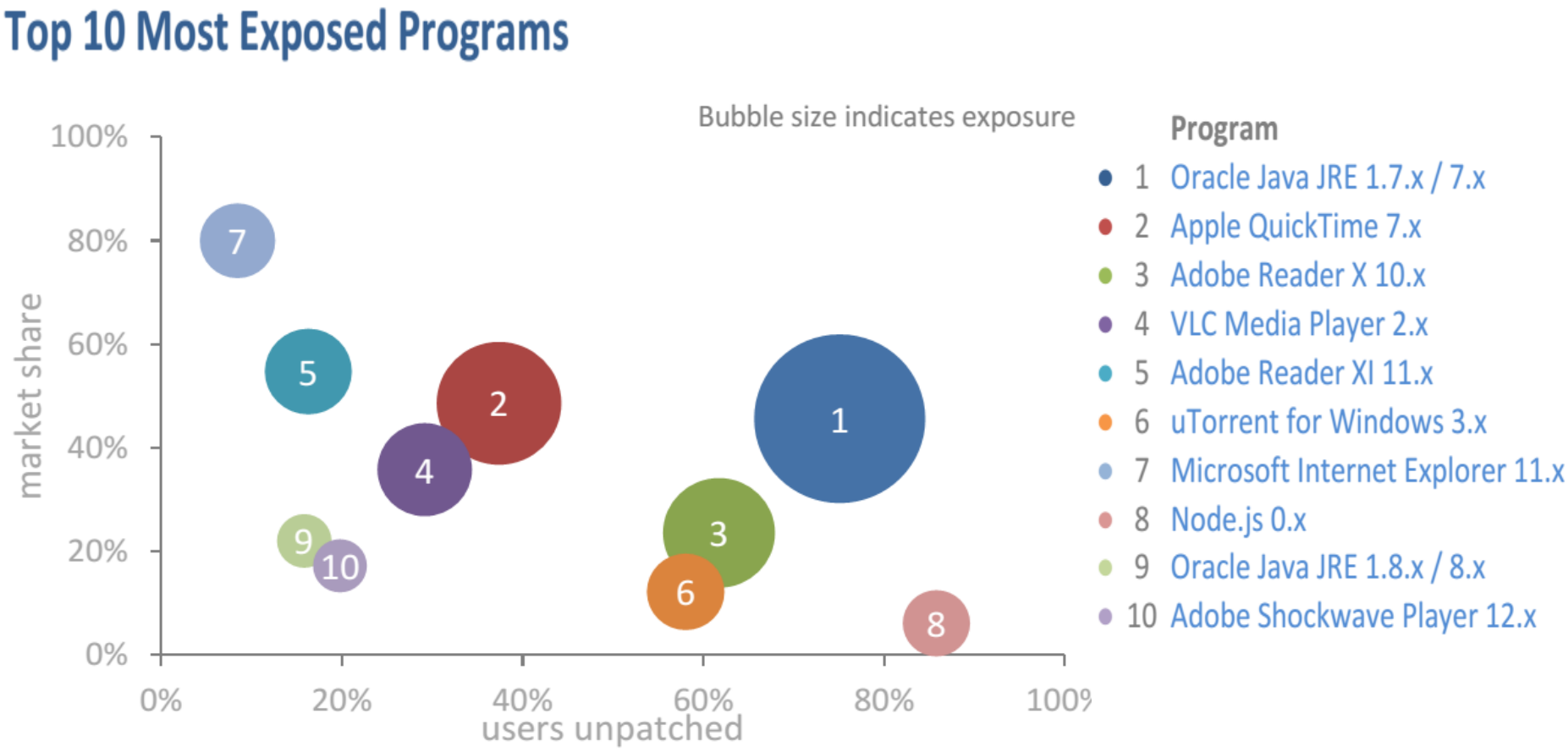
Latest Vulnerabilities, Threats, & Risk Mitigation…

Top 10 Most Exposed Programs

	Program	Unpatched	Market share	Vulns
1	Oracle Java JRE 1.7.x / 7.x	75%	46%	101
2	Apple QuickTime 7.x	37%	49%	4
3	Adobe Reader X 10.x	62%	24%	39
4	VLC Media Player 2.x	29%	36%	6
5	Adobe Reader XI 11.x	16%	55%	40
6	uTorrent for Windows 3.x	58%	12%	1
7	Microsoft Internet Explorer 11.x	8%	80%	258
8	Node.js 0.x	86%	6%	23
9	Oracle Java JRE 1.8.x / 8.x	16%	22%	101
10	Adobe Shockwave Player 12.x	20%	17%	0

Secunia (2015). Secunia PSI Country Report - Q1 2015, United Kingdom.

Latest Vulnerabilities, Threats, & Risk Mitigation…



Secunia (2015). Secunia PSI Country Report - Q1 2015, United Kingdom.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Top 10 End-of-life (EOL) Programs

#	Program	Market share
1	Adobe Flash Player 16.x	81%
2	Microsoft XML Core Services (MSXML) 4.x	62%
3	Google Chrome 40.x	47%
4	Mozilla Firefox 35.x	28%
5	Google Chrome 39.x	25%
6	Oracle Java JRE 1.6.x / 6.x	19%
7	Adobe AIR 3.x	15%
8	Apple iTunes 11.x	14%
9	Mozilla Firefox 34.x	14%
10	Adobe AIR 15.x	13%

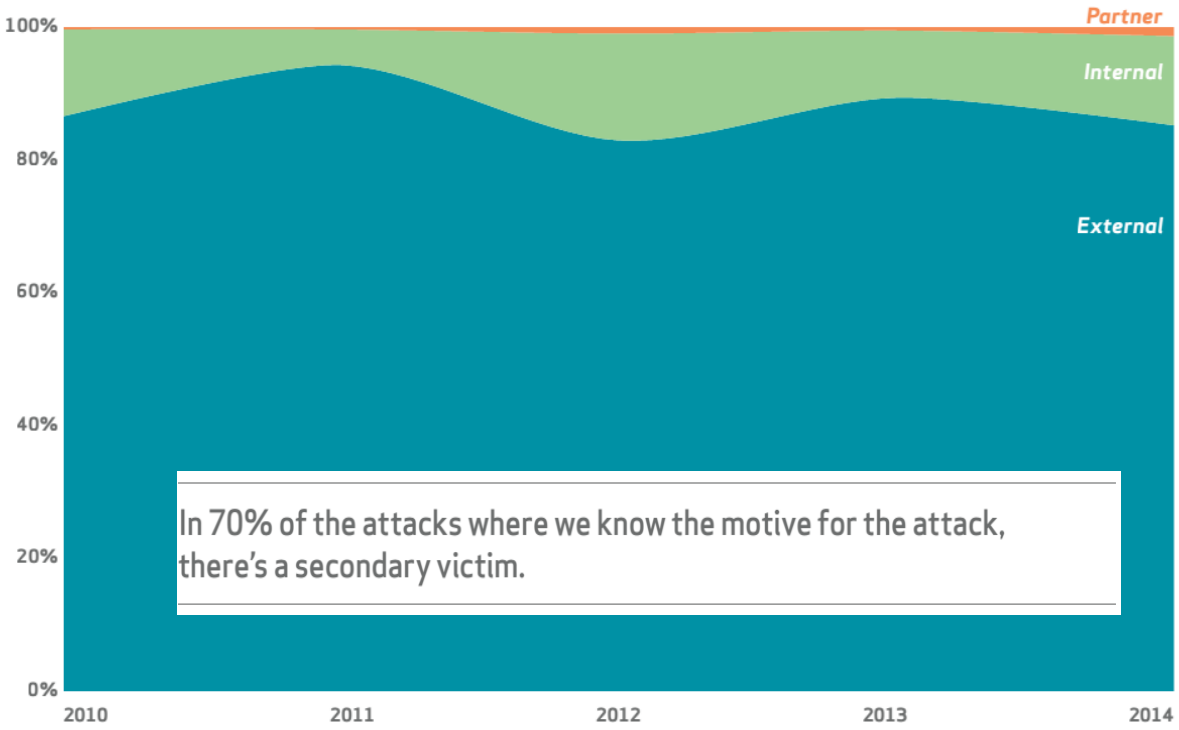
Secunia (2015). Secunia PSI Country Report - Q1 2015, United Kingdom.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Verizon 2015 Data Breach Investigations Report

THREAT ACTORS

Though the number of breaches per threat actor changes rather dramatically each year as we add new partners and more data, the overall proportion attributed to external, internal, and partner actors stays roughly the same. The stream plot for Figure 3 demonstrates this well and shows that overall trends in the threat actors haven't shifted much over the last five years.



INCIDENTS VS. BREACHES

This report uses the following definitions:

Security incident: Any event that compromises the confidentiality, integrity, or availability of an information asset.

Data breach: An incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party. We use this term interchangeably with "data compromise" in this report.

Verizon (2015). 2015 Data Breach Investigations Report.

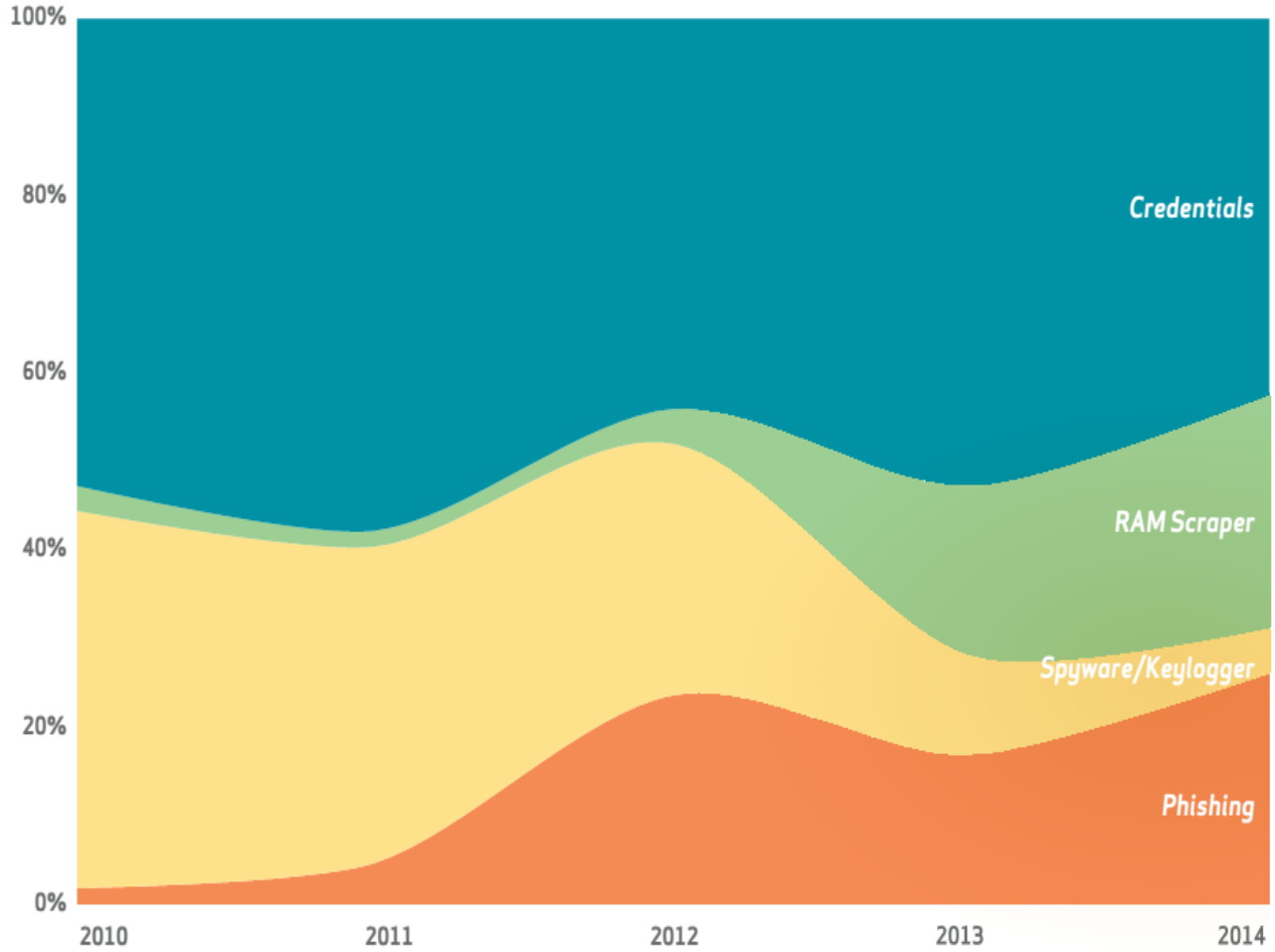
Latest Vulnerabilities, Threats, & Risk Mitigation…

Verizon 2015 Data Breach Investigations Report

	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31–33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44–45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48–49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

Latest Vulnerabilities, Threats, & Risk Mitigation…

Verizon 2015 Data Breach Investigations Report



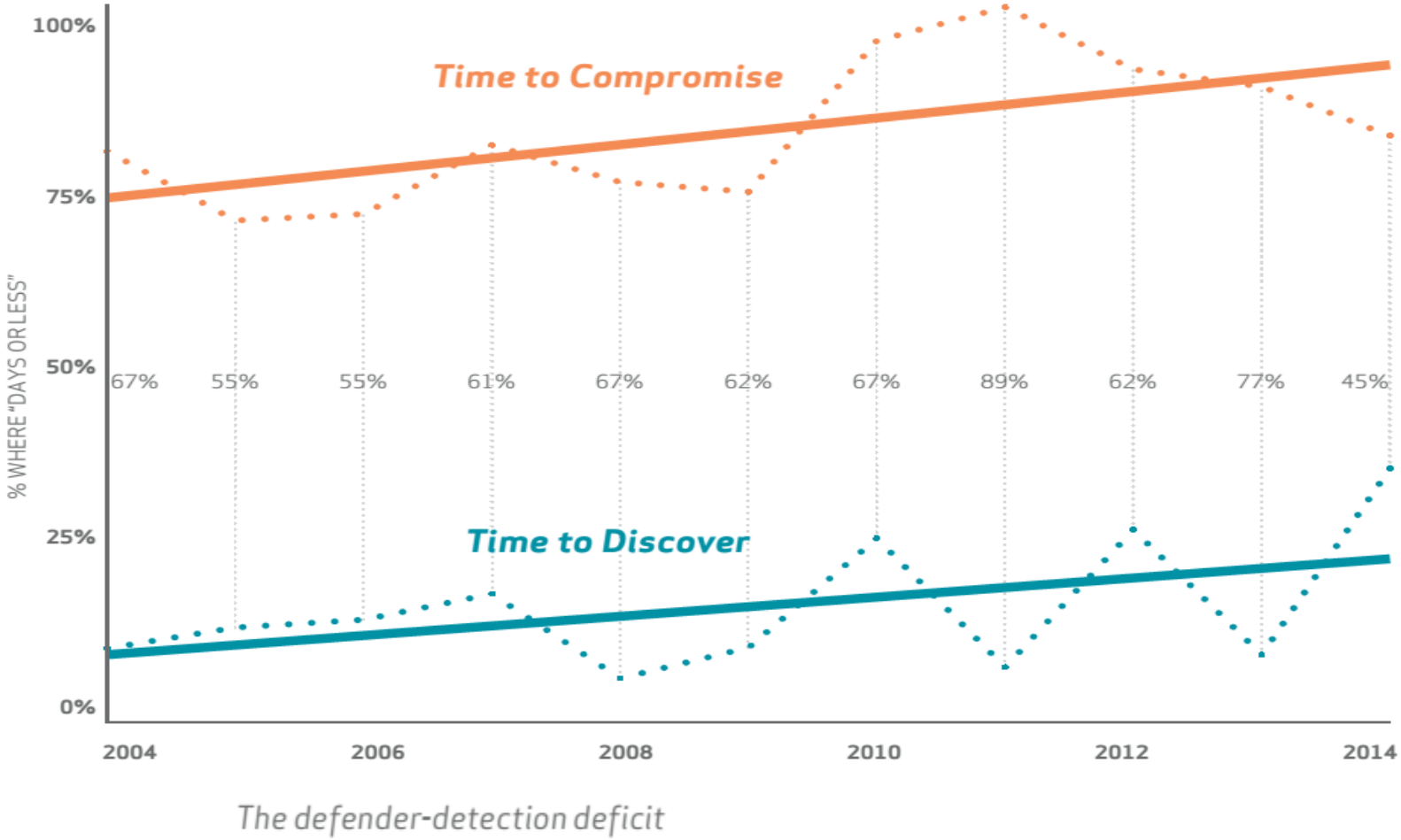
RAM scraping has grown in a big way. This type of malware was present in some of the most high-profile retail breaches.

1. Use strong passwords to access POS devices
2. Keep POS software up to date
3. Use firewalls to isolate the POS production network
4. Employ antivirus tools
5. Limit access to the Internet from production network
6. Disable all remote access to POS systems.

Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…

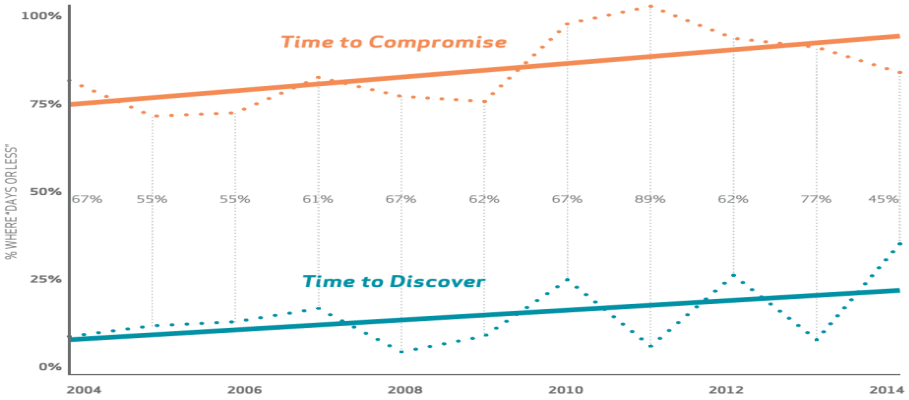
Verizon 2015 Data Breach Investigations Report



Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Verizon 2015 Data Breach Investigations Report



The defender-detection deficit

60%

IN 60% OF CASES, ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

Figure 5 offers a new twist on one of our favorite charts from the 2014 DBIR. It contrasts how often attackers are able to compromise a victim in days or less (orange line) with how often defenders detect compromises within that same time frame (teal line). Unfortunately, the proportion of breaches discovered within days still falls well below that of time to compromise. Even worse, the two lines are diverging over the last decade, indicating a growing "detection deficit" between attackers and defenders. We think it highlights one of the primary challenges to the security industry.

Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Verizon 2015 Data Breach Investigations Report

23%

OF RECIPIENTS NOW OPEN PHISHING MESSAGES AND 11% CLICK ON ATTACHMENTS.

50%

NEARLY 50% OPEN E-MAILS AND CLICK ON PHISHING LINKS WITHIN THE FIRST HOUR.

PHISHING

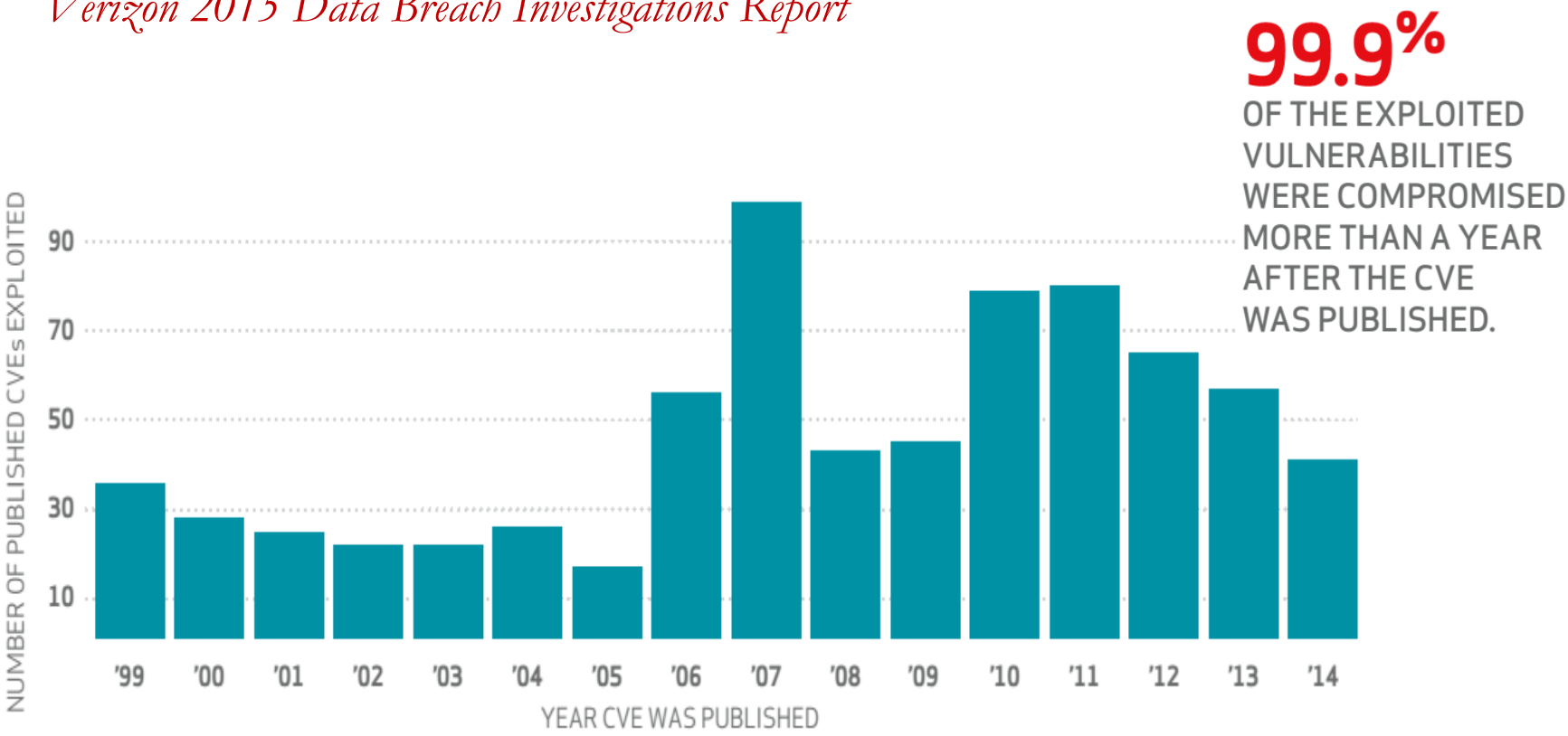
DOING MORE WITH LESS

The payload for these phishing messages has to come from somewhere. Data from the Anti-Phishing Working Group (APWG)[10] suggests that the infrastructure being used is quite extensive (over 9,000 domains and nearly 50,000 phishing URLs tracked each month across the Group's members). The charts in Figure 9 also show that the attackers have finally learned a thing or two from the bounty of their enterprise breaches and may even have adopted a Lean Six Sigma approach to optimize operations.

Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…

Verizon 2015 Data Breach Investigations Report

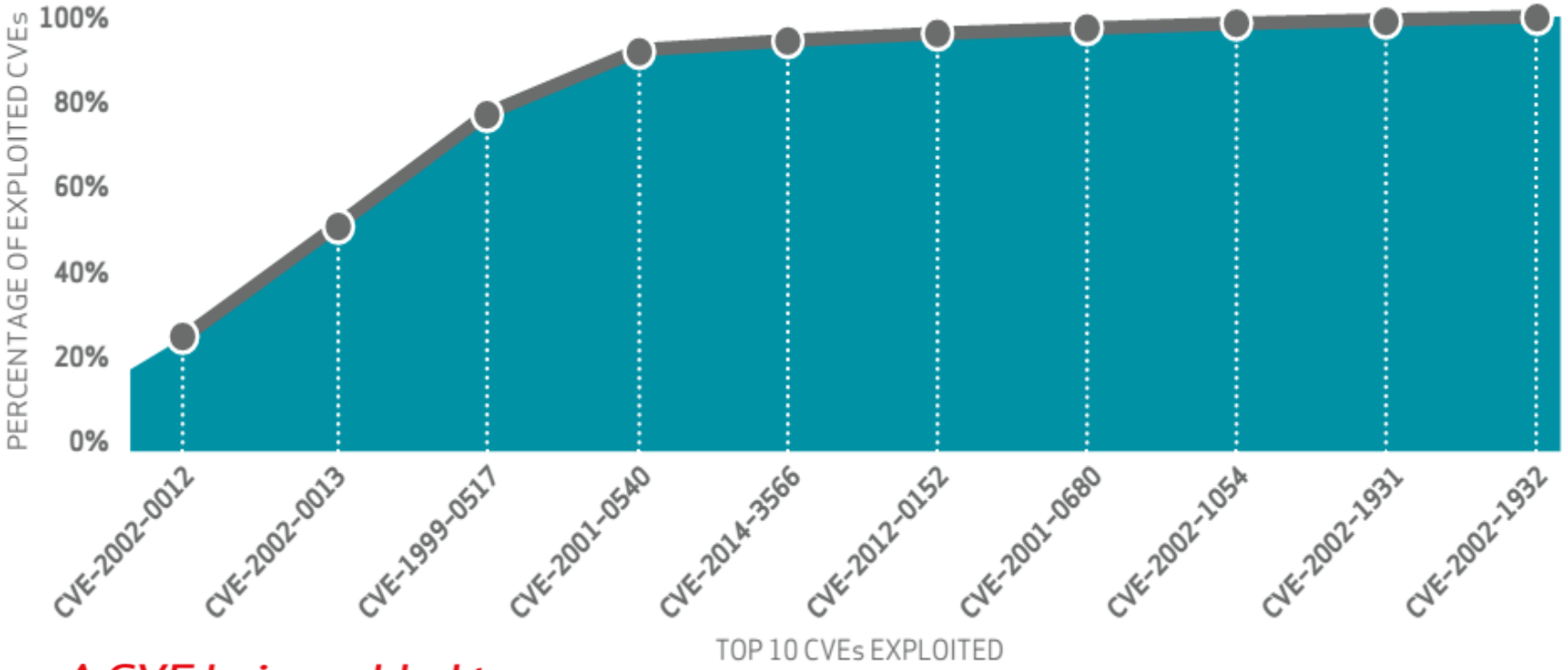


Count of exploited CVEs in 2014 by CVE publish date

Common Vulnerabilities and Exposures (CVE) is "a dictionary of publicly known information security vulnerabilities and exposures."—cve.mitre.org

Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…



A CVE being added to Metasploit is probably the single most reliable predictor of exploitation in the wild.

About half of the CVEs exploited in 2014 went from publish to pwn in less than a month.

Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…

CVSS attributes across classes of CVEs

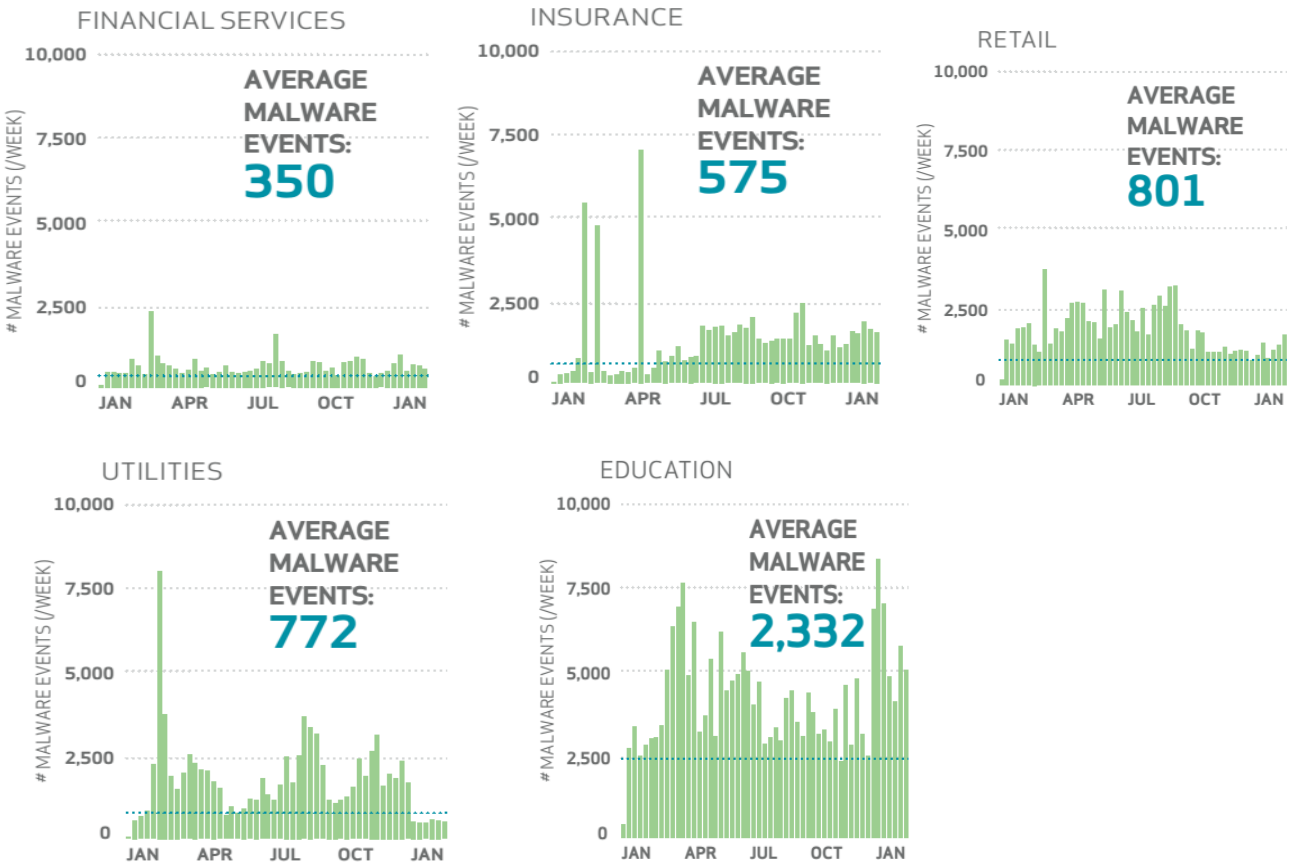
Common Vulnerability Scoring System (CVSS) is designed to provide an open and standardized method for rating IT vulnerabilities.

https://nvd.nist.gov/cvss.cfm

Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…

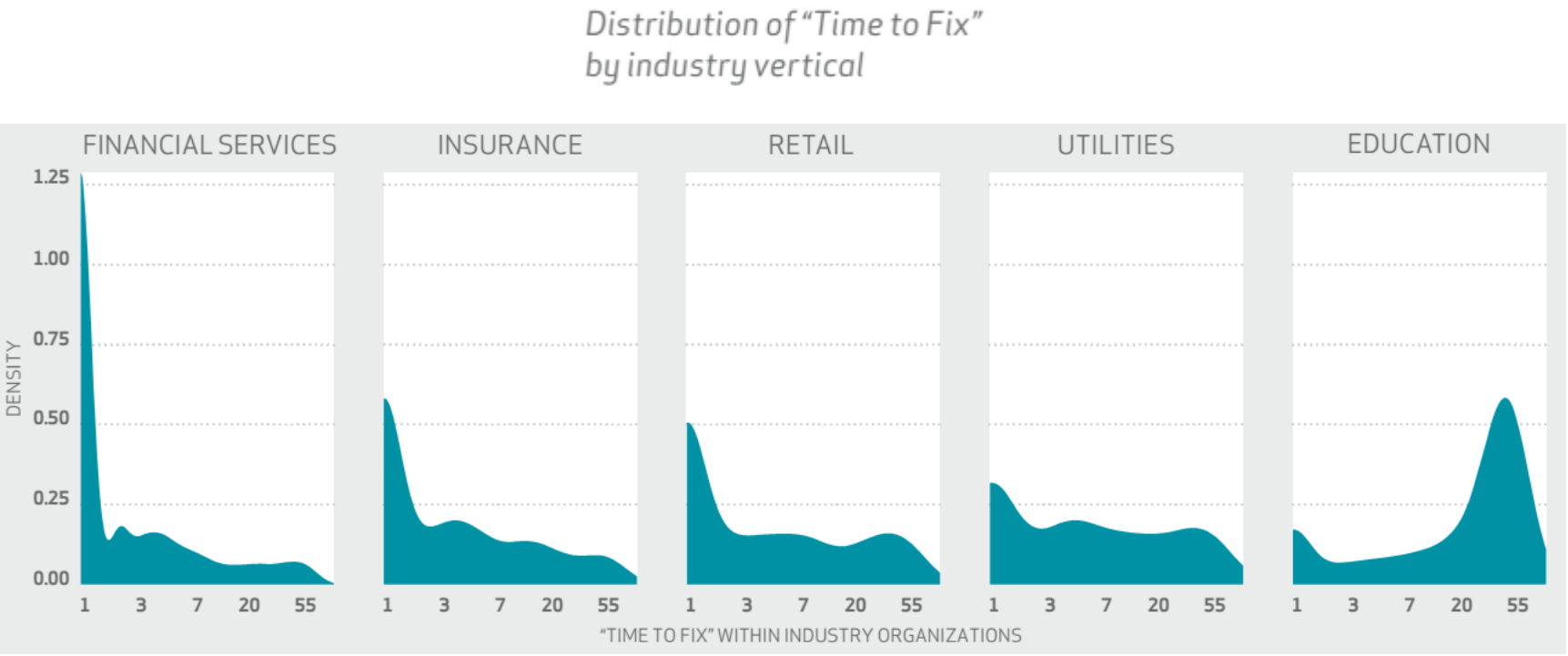
Figure 17 shows the weekly average number of malware events for five industries: Financial Services, Insurance, Retail, Utilities, and Education.



The key differences between the malcode of 2005 and malware of 2014 are that the older viruses were noisy e-mail worms with varying backdoor capabilities, whereas the common components of the 2014 "top seven" involve stealthy command-and-control botnet membership, credential theft, and some form of fraud (clickfraud or bitcoin mining).

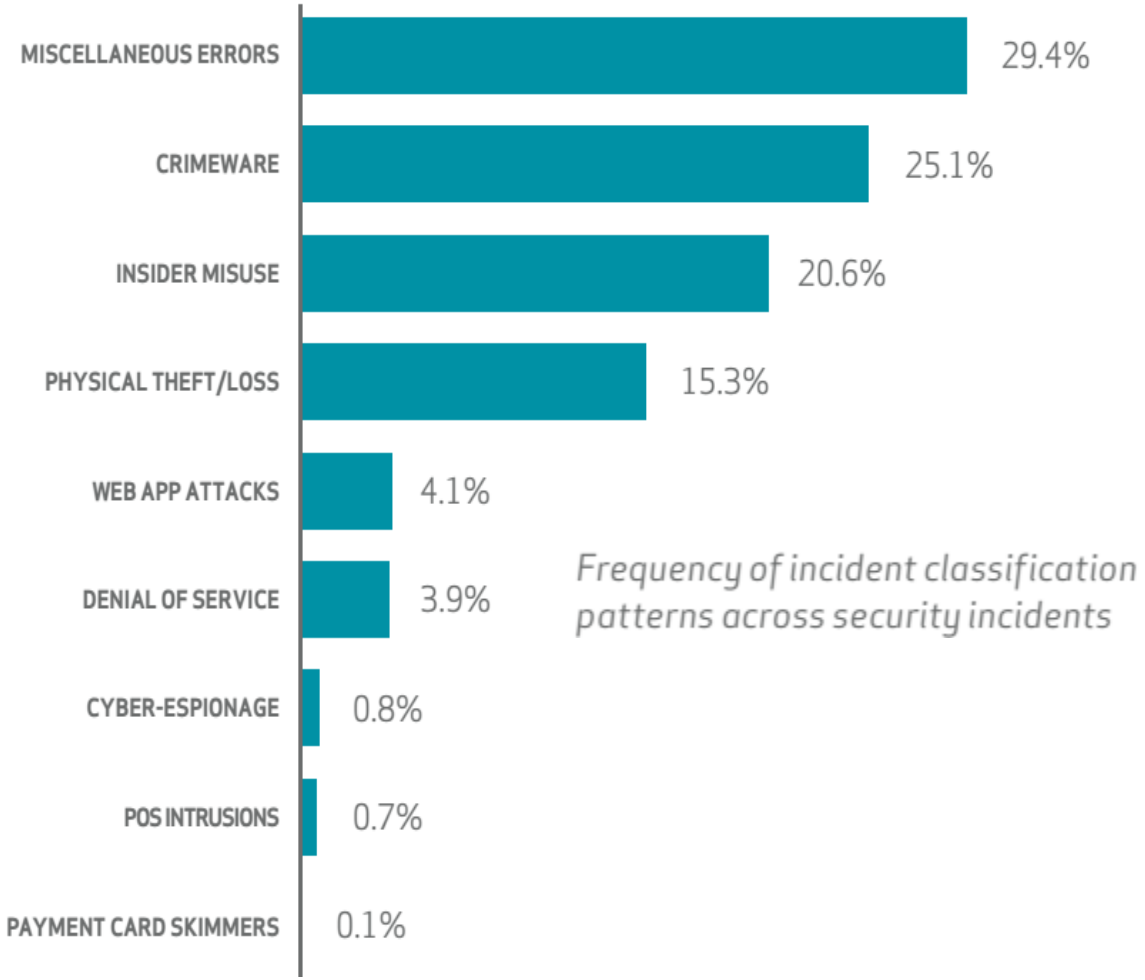
Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…



Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…

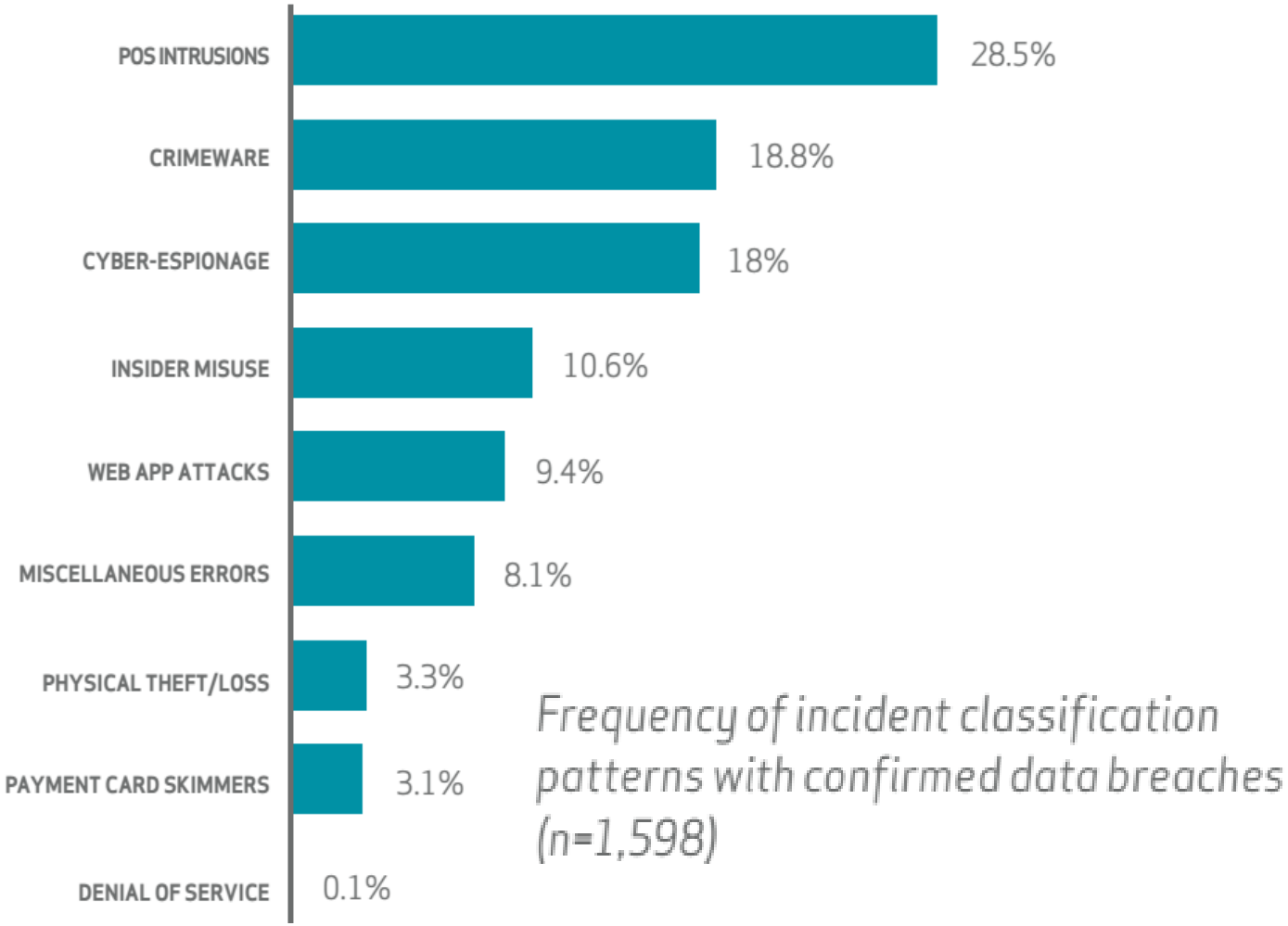


96%

WHILE WE SAW MANY CHANGES IN THE THREAT LANDSCAPE IN THE LAST 12 MONTHS, THESE PATTERNS STILL COVERED THE VAST MAJORITY OF INCIDENTS (96%).

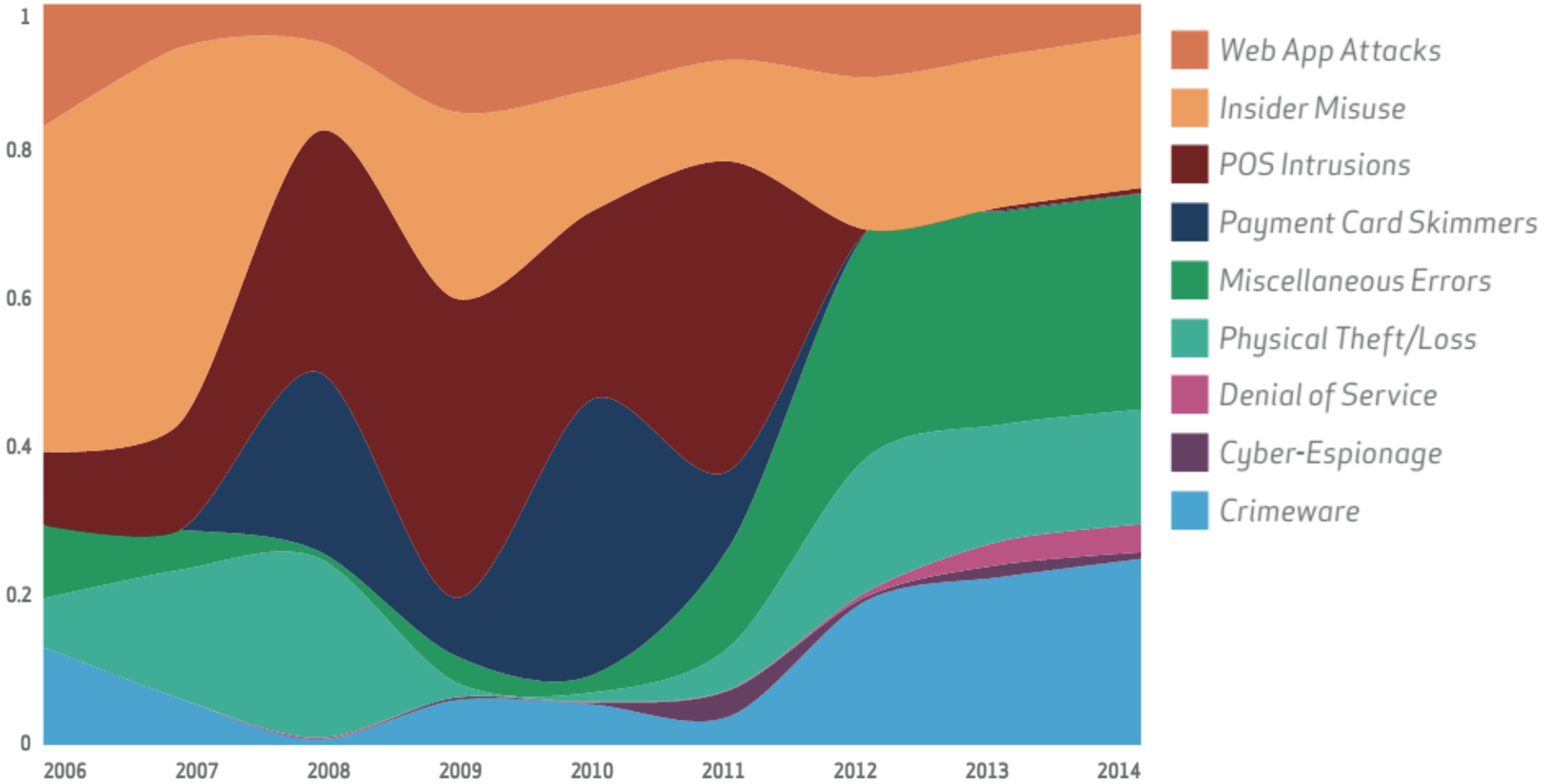
Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…



Verizon (2015). 2015 Data Breach Investigations Report.

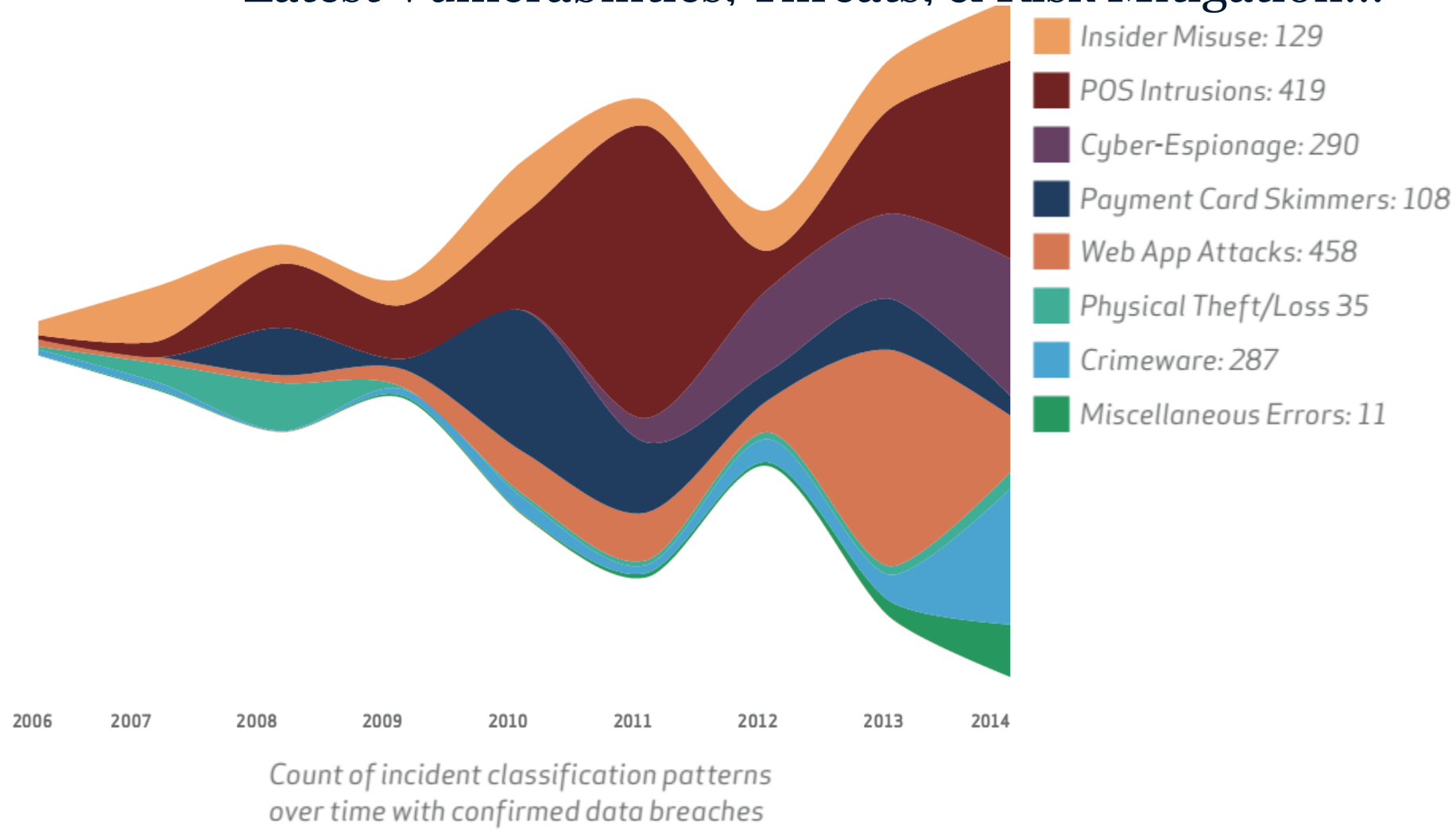
Latest Vulnerabilities, Threats, & Risk Mitigation…



Frequency of incident classification patterns over time across security incidents

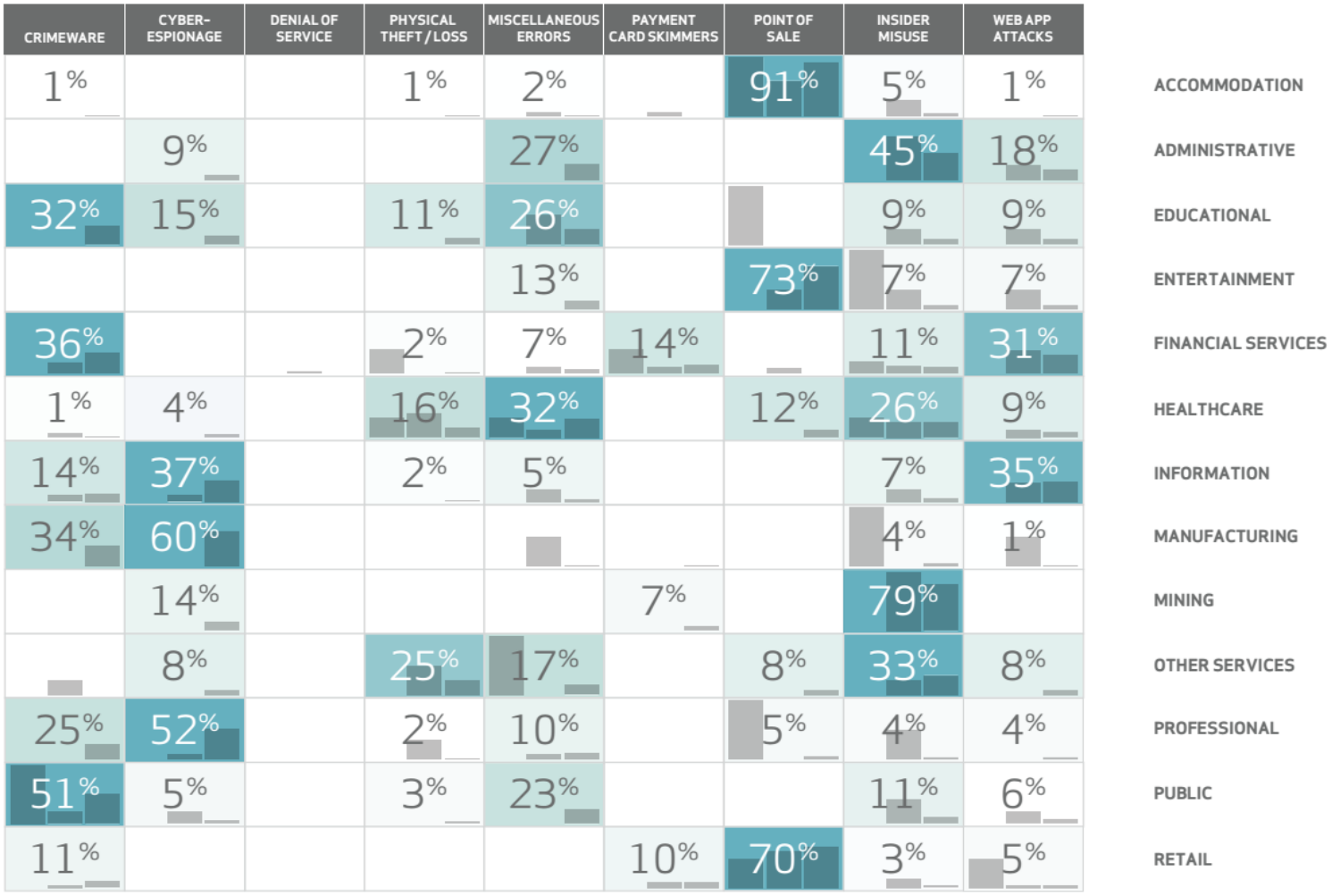
Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…



Verizon (2015). 2015 Data Breach Investigations Report.

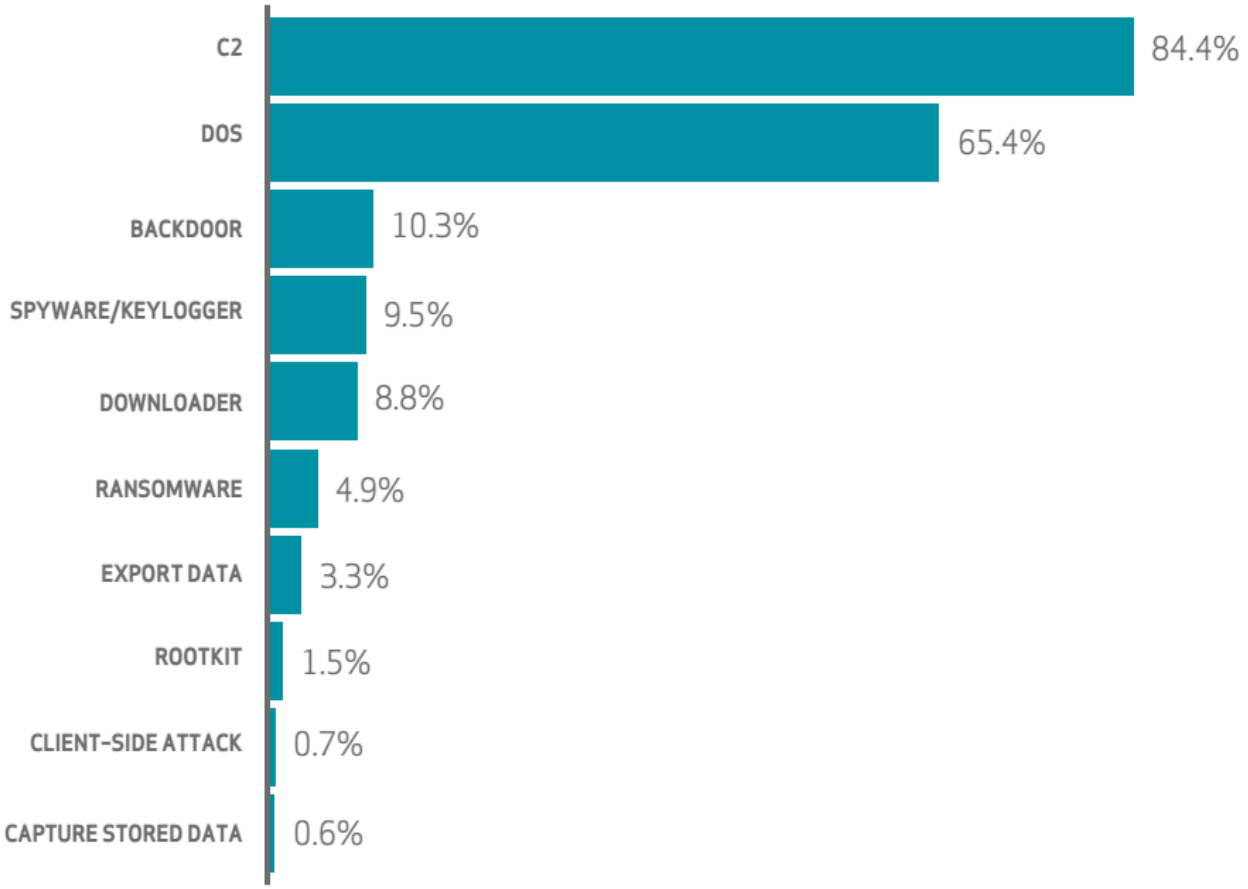
Latest Vulnerabilities, Threats, & Risk Mitigation…



Frequency of data disclosures by incident patterns and victim industry

Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…



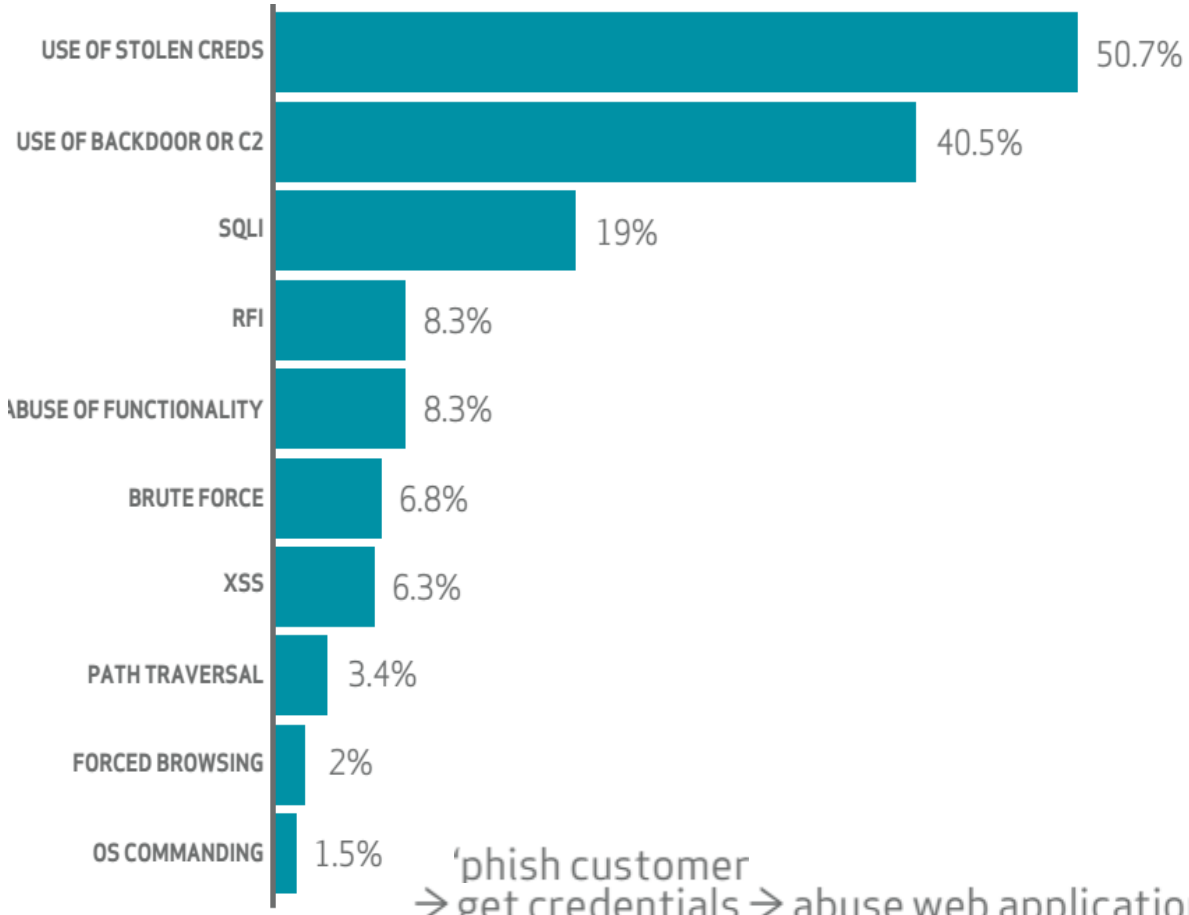
Variety of malware within Crimeware pattern (n=2,545)

Malware used to launch DoS attacks jumped from #8 to #2 in threat action variety, while command and control remains at #1.

Larger breaches tend to be a multi-step attack with some secondary system being breached before attacking the POS system.

Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…



Most affected industries: Information, Financial Services, and Public

95%

OF THESE INCIDENTS INVOLVE HARVESTING CREDENTIALS STOLEN FROM CUSTOMER DEVICES, THEN LOGGING INTO WEB APPLICATIONS WITH THEM.

'phish customer → get credentials → abuse web application → empty bank/bitcoin account

This year, organized crime became the most frequently seen threat actor for Web App Attacks.

Verizon (2015). 2015 Data Breach Investigations Report.

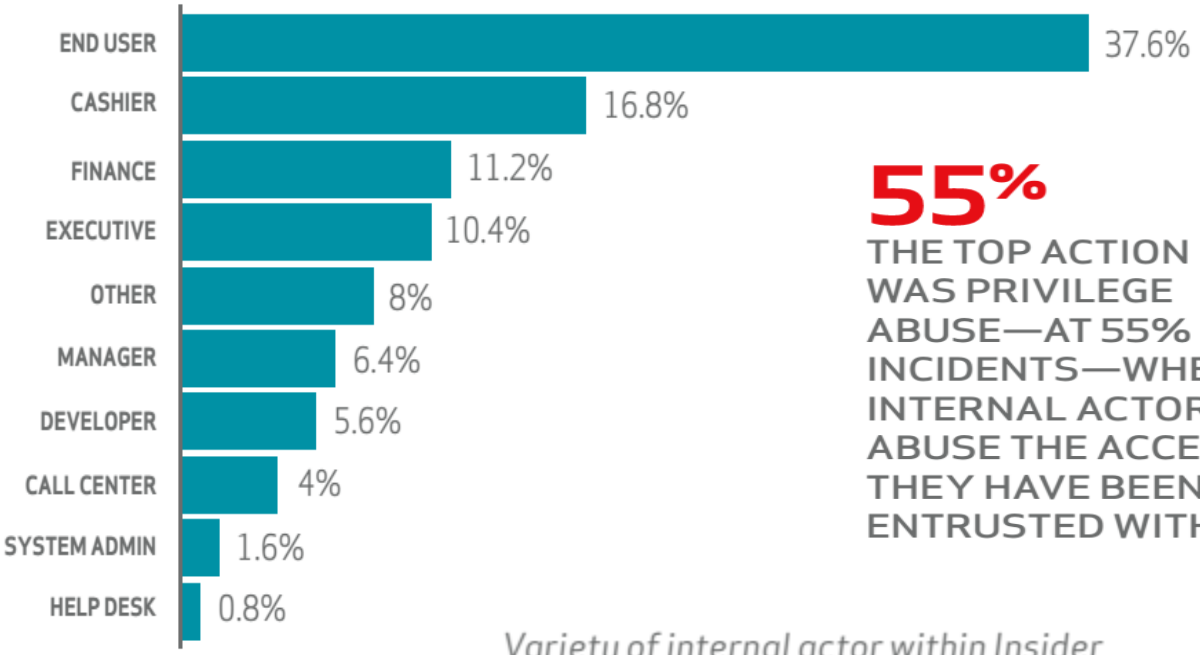
Latest Vulnerabilities, Threats, & Risk Mitigation…

INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	140	0	80	60
Administrative (56)	164	0	1	163
Agriculture (11)	0	0	0	0
Construction (23)	0	0	0	0
Educational (61)	10	0	0	10
Entertainment (71)	1	0	0	1
Financial Services (52)	184	1	17	166
Healthcare (62)	17	3	1	13
Information (51)	72	16	8	48
Management (55)	2	0	1	1
Manufacturing (31–33)	157	2	22	133
Mining (21)	3	0	0	3
Other Services (81)	11	3	0	8
Professional (54)	161	4	1	156
Public (92)	435	0	245	190
Real Estate (53)	0	0	0	0
Retail (44–45)	207	1	3	203
Trade (42)	6	6	0	0
Transportation (48–49)	3	0	0	3
Utilities (22)	2	0	0	2
Unknown	860	0	0	860
TOTAL	2,435	36	379	2,020

Number of DDoS attacks by victim industry and organization size (small is < 1,000 employees)

Verizon (2015). 2015 Data Breach Investigations Report.

Latest Vulnerabilities, Threats, & Risk Mitigation…



55%
THE TOP ACTION WAS PRIVILEGE ABUSE—AT 55% OF INCIDENTS—WHERE INTERNAL ACTORS ABUSE THE ACCESS THEY HAVE BEEN ENTRUSTED WITH.

Most affected industries: Public, Healthcare, and Financial Services

60%
OF INCIDENTS WERE ATTRIBUTED TO ERRORS MADE BY SYSTEM ADMINISTRATORS—PRIME ACTORS RESPONSIBLE FOR A SIGNIFICANT VOLUME OF BREACHES AND RECORDS.

Variety of internal actor within Insider Misuse pattern (n=125)

INSIDER MISUSE

Verizon (2015). 2015 Data Breach Investigations Report.

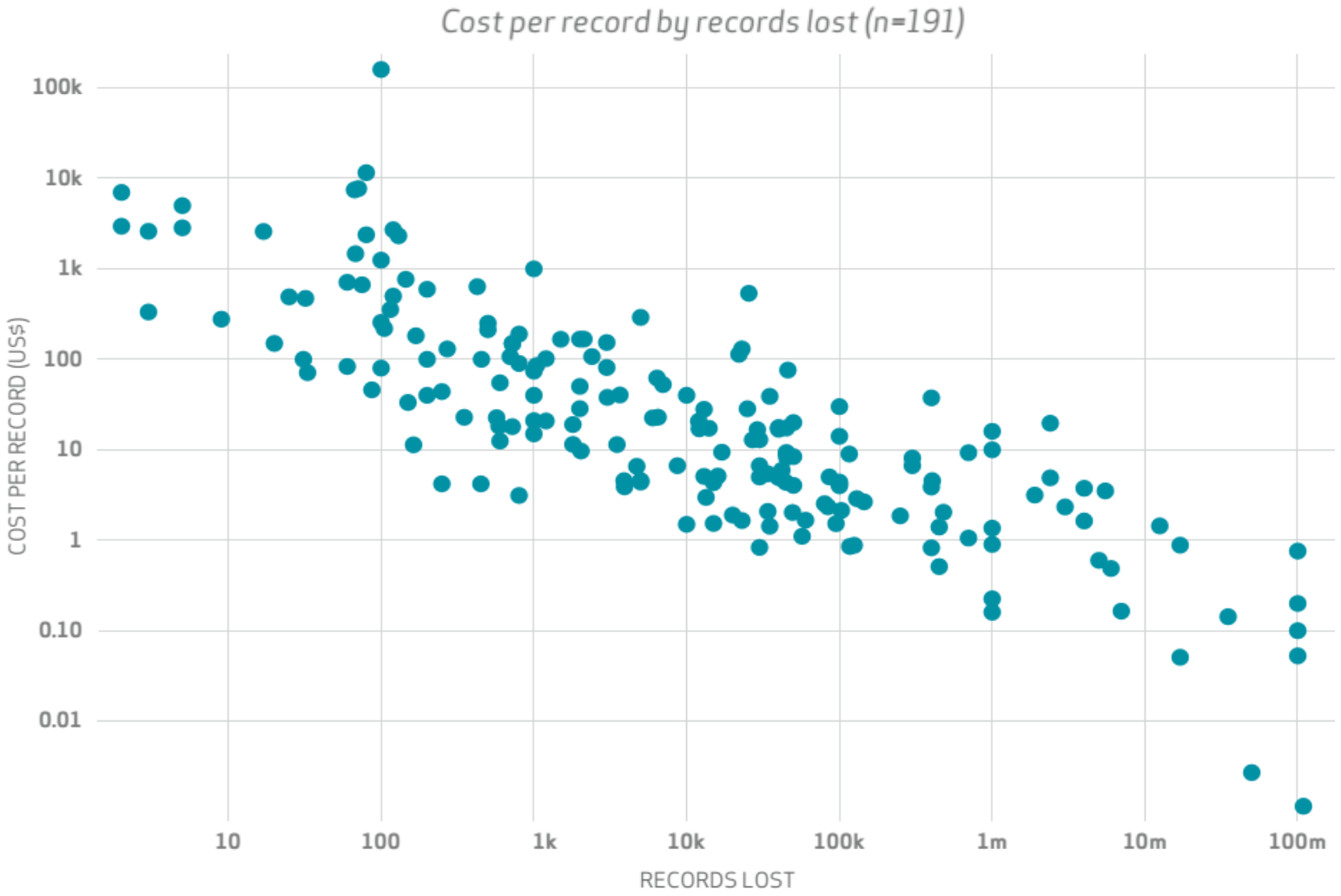
Latest Vulnerabilities, Threats, & Risk Mitigation…

CSC	DESCRIPTION	PERCENTAGE	CATEGORY
13-7	2FA	24%	Visibility/Attribution
6-1	Patching web services	24%	Quick Win
11-5	Verify need for Internet-facing devices	7%	Visibility/Attribution
13-6	Proxy outbound traffic	7%	Visibility/Attribution
6-4	Web application testing	7%	Visibility/Attribution
16-9	User lockout after multiple failed attempts	5%	Quick Win
17-13	Block known file transfer sites	5%	Advanced
5-5	Mail attachment filtering	5%	Quick Win
11-1	Limiting ports and services	2%	Quick Win
13-10	Segregation of networks	2%	Configuration/Hygiene
16-8	Password complexity	2%	Visibility/Attribution
3-3	Restrict ability to download software	2%	Quick Win
5-1	Anti-virus	2%	Quick Win
6-8	Vet security process of vendor	2%	Configuration/Hygiene

Critical security controls mapped to incident event chains (Verizon caseload only)

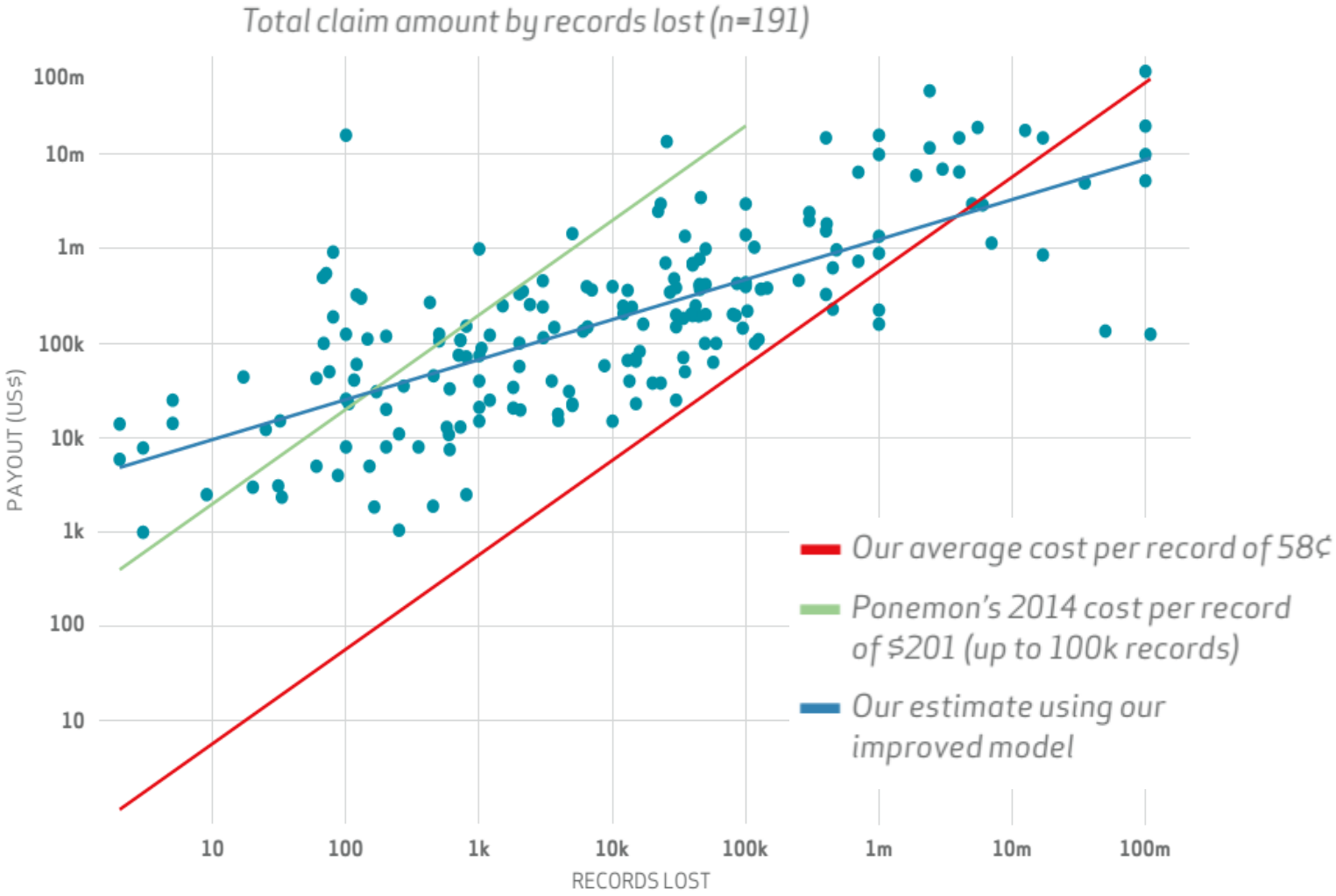
Verizon (2015). 2015 Data Breach Investigations Report.

Cyber Risk: Quantifying, Modeling, & Valuation…



Verizon (2015). 2015 Data Breach Investigations Report.

Cyber Risk: Quantifying, Modeling, & Valuation…



Verizon (2015). 2015 Data Breach Investigations Report.

Cyber Risk: Quantifying, Modeling, & Valuation…

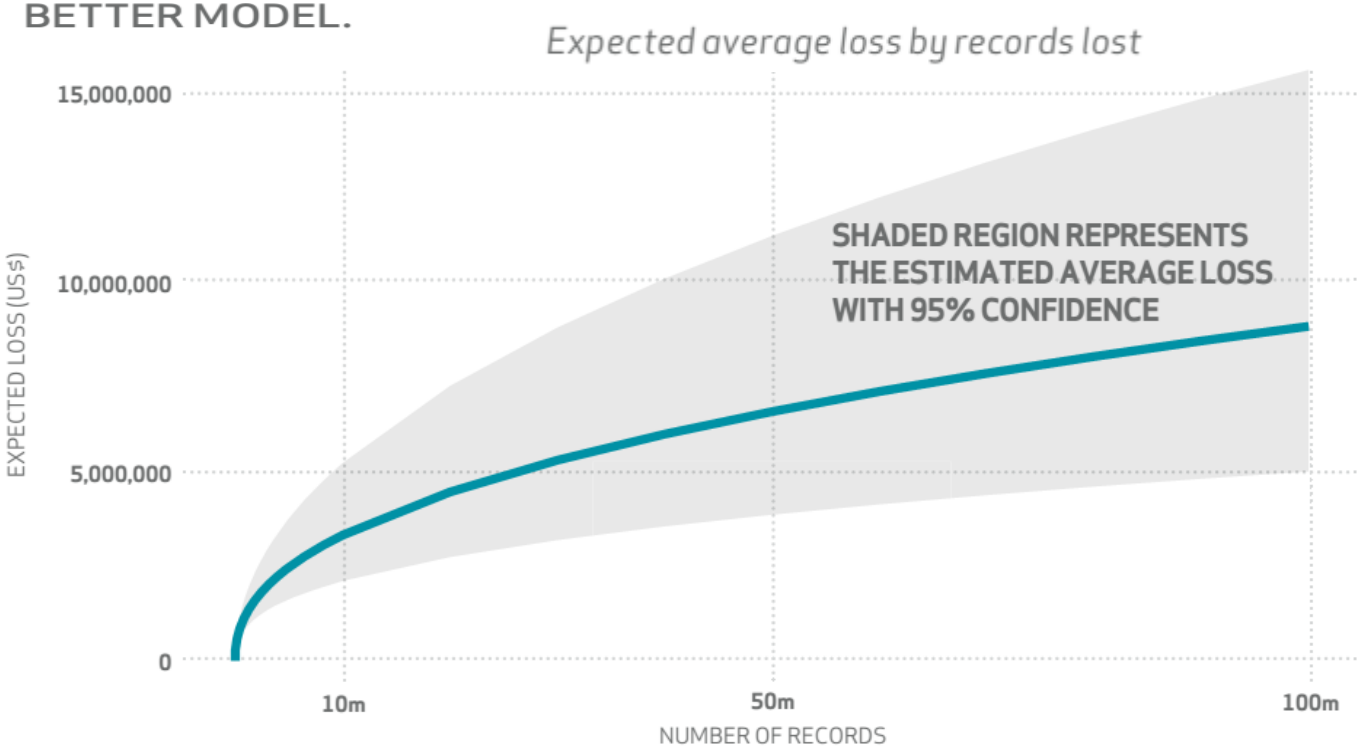
58¢

AVERAGE COST PER RECORD WAS 58¢, HOWEVER THIS IS A VERY POOR ESTIMATE OF LOSS, SO WE BUILT A BETTER MODEL.

RECORDS TELL ONLY HALF THE STORY

Our new breach-cost model accounts for the uncertainty as record volume increases.

Larger organizations have higher losses per breach, but they typically lose more records and have higher overall costs.



Verizon (2015). 2015 Data Breach Investigations Report.

Cyber Risk: Quantifying, Modeling, & Valuation…

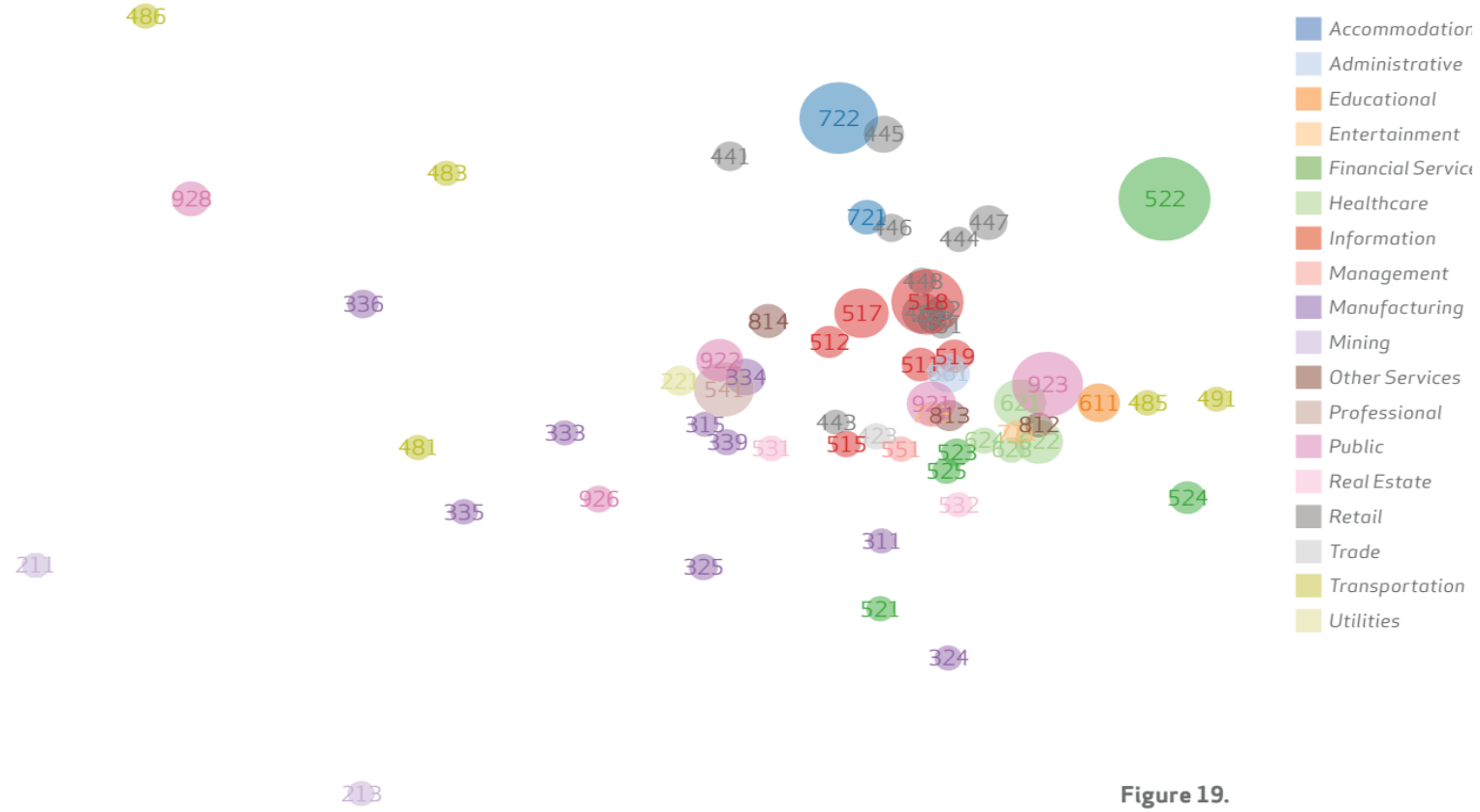


Figure 19.

Clustering on breach data across industries

28 To look up the three-digit NAICS codes, visit: census.gov/eos/www/naics/index.html

Verizon (2015). 2015 Data Breach Investigations Report.

It's Better to be **Approximately Right** than being **Precisely Wrong**!

Cyber Risk: Quantifying, Modeling, & Valuation…

RECORDS	PREDICTION (LOWER)	AVERAGE (LOWER)	EXPECTED	AVERAGE (UPPER)	PREDICTION (UPPER)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

Ranges of expected loss by number of records

Verizon (2015). 2015 Data Breach Investigations Report.

Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Cyber Risk

Cyber Risk Loss

Cyber Insurance

Cyber Risk Models

Beyond VaR to

ES, EVT, Power Laws

FINANCE

CYBER

Cyber-Finance Risk Management

From 'Prediction' to "Anticipation of Surprise"

From Risk Modeling to Uncertainty Management

Threat & Vulnerability Analysis

Risk Mitigation

Risk Transfer

Risk Acceptance

Enterprise Risk Management

Finance ⟷ **C**yber

PDC x **T**S ➡ (**E**EO) ➡ **F** ⟷ **C**

Production **D**istribution **C**onsumption Across **T**ime and **S**pace
Efficiency **E**ffectiveness **O**ptimization

ASSESS Risk

Quantitative

Qualitative

- **Pen** Testing

Deterministic

Stochastic

Non-Deterministic

- Scenarios

MANAGE Risk

Cybersecurity & Cyber-Finance Risk Management Strategies, Tactics, Operations, &, Intelligence

Enterprise Risk Management to Model Risk Management

Understanding Vulnerabilities, Threats, & Risk Mitigation

Four Parts: Intuition, Data, Humans, Models

Part 3: Humans: The Human Factor

1. The Cyber-Finance-Trust ™ Framework, 1993-2015
2. Latest Vulnerabilities, Threats, & Risk Mitigation…
3. The Human Factor: The Non-Deterministic 'Variable'
4. Cyber Risk: Quantifying, Modeling, & Valuation

"In physics you're playing against God, and He doesn't change His laws very often. In finance you're playing against God's creatures, agents who value assets based on their ephemeral opinions."

- Dr. Emanuel Derman

Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Cyber Risk

Cyber Risk Loss

Cyber Insurance

Cyber Risk Models

Beyond VaR to

ES, EVT, Power Laws

FINANCE

CYBER

Cyber-Finance Risk Management

From 'Prediction' to "Anticipation of Surprise"

From Risk Modeling to Uncertainty Management

Threat & Vulnerability Analysis

Risk Mitigation

Risk Transfer

Risk Acceptance

Enterprise Risk Management

Finance ⟷ **C**yber

PDC x **T**S ➡ (**E**EO) ➡ **F** ⟷ **C**

Production **D**istribution **C**onsumption Across **T**ime and **S**pace
Efficiency **E**ffectiveness **O**ptimization

ASSESS Risk

Quantitative

Qualitative

- **Pen** Testing

Deterministic

Stochastic

Non-Deterministic

- Scenarios

MANAGE Risk

Proceedings of the 32nd Hawaii International Conference on System Sciences - 1999

~ 700 Citations in Google Scholar

Malhotra, Y., and, Galletta, D.F., Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation. **Proceedings of the Hawaii International Conference on System Sciences (HICSS 32)**, 6-19, January, 1999, IEEE, Hawaii. http://brint.org/technologyacceptance.pdf

Figure 1 (a). Technology Acceptance Model (TAM)
(Based on Davis et al. 1989)

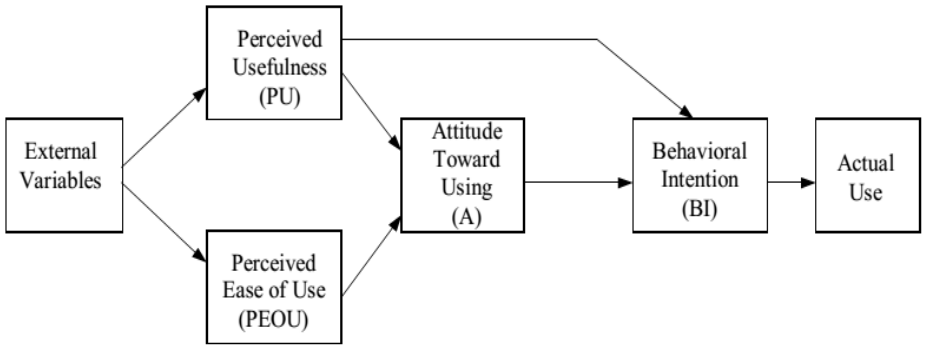
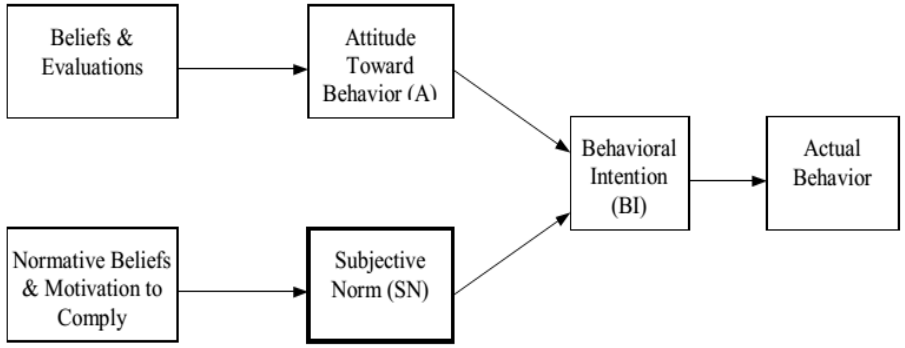


Figure 1 (b). Theory of Reasoned Action (TRA)
(Based on Fishbein & Ajzen 1975).



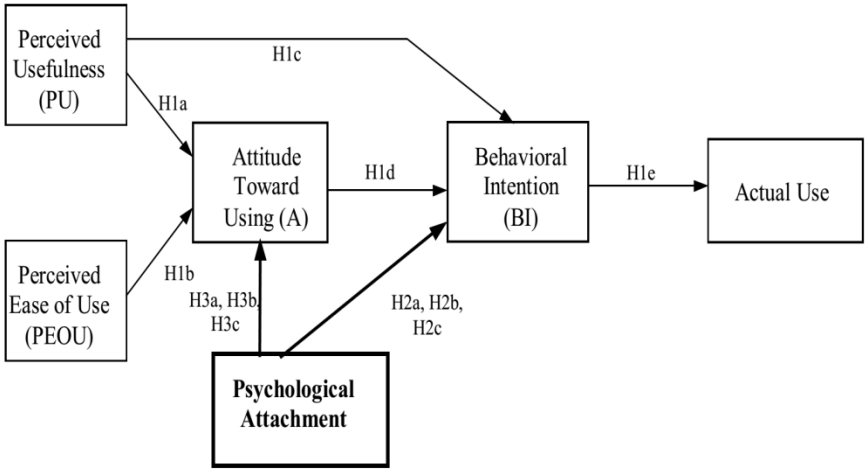


Figure 2. Research Model: TAM Extended to Account for Social Influences

Digital Change Management and Innovation Adoption Models were incomplete in one important respect: they didn't account for social influences in the adoption and utilization of new innovations.

An Early AI, Expert Systems, and, Machine Learning Paper

PERGAMON

Expert Systems with Applications 20 (2001) 7–16

Expert Systems with Applications

www.elsevier.com/locate/eswa

Expert systems for knowledge management: crossing the chasm between information processing and sense making

Y. Malhotra*

Abstract

Based on insights from research in information systems, information science, business strategy and organization science, this paper develops the bases for advancing the paradigm of AI and expert systems technologies to account for two related issues: (a) dynamic radical discontinuous change impacting organizational performance; and (b) human sense-making processes that can complement the machine learning capabilities for designing and implementing more effective knowledge management systems.

Keywords: Expert systems; Artificial intelligence; Knowledge management; Information systems; Information science; Business strategy; Discontinuous change; Sense making; Information processing

Missing Human Factors in IT/MIS/IS/Economics Research
'MEANING' and 'SENSE-MAKING'
Result: ~ 80%-90% Systems Implementation Failures

Personal Communication with Dr. John H. Holland, the pioneer of Genetic Algorithms and Professor of **Psychology** and Professor of **Electrical Engineering and Computer Science** at the University of Michigan, Ann Arbor, then situated at Santa Fe Institute, New Mexico.

"There has been an over-concentration on Shannon's definition of information in terms of uncertainty (a very good definition for the original purposes) with little attempt to understand how MEANING directs a message in a network. This, combined with a concentration on end-points (equilibria) rather than properties of the trajectory (move sequence) in games has lead to a very unsatisfactory treatment of the dynamics of organizations." — John H. Holland (personal communication, June 21, 1995)[1]

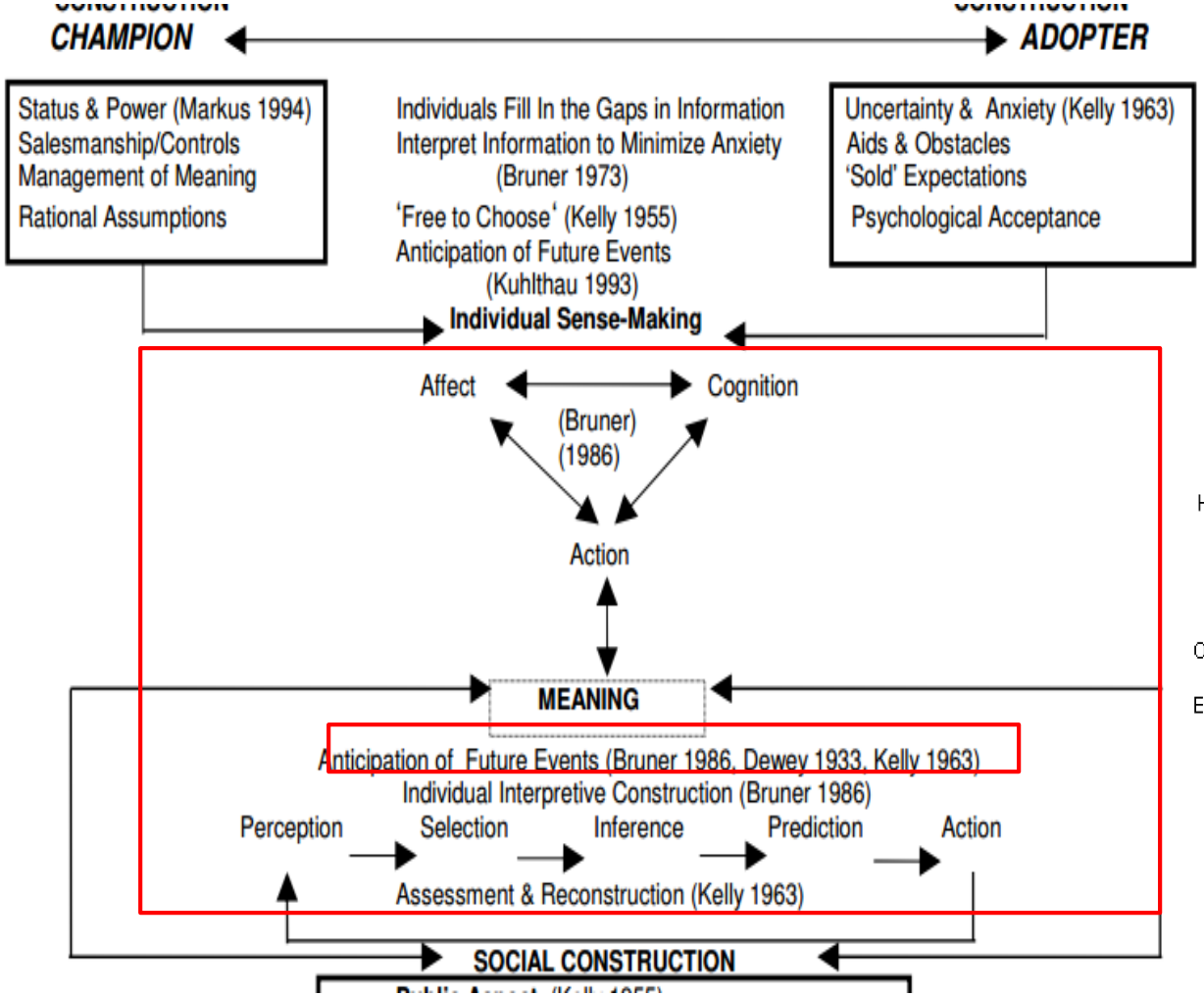
1. Introduction

The narrative cited above as an observation by the noted psychologist and computer scientist John Holland was in response to my query to him regarding the possibility of using intelligent information technologies for devising self-adaptive organizations. As meaning seems to be a crucial construct in understanding how humans convert *information* into *action* [and consequently *performance*], it is evident that information-processing based fields of artificial intelligence and expert systems could benefit from understanding how humans translate *information* into *meanings* that guide their *actions*. In essence, this issue is relevant to the design of both human- and machine-based knowledge management systems. Most such systems had been tradi-

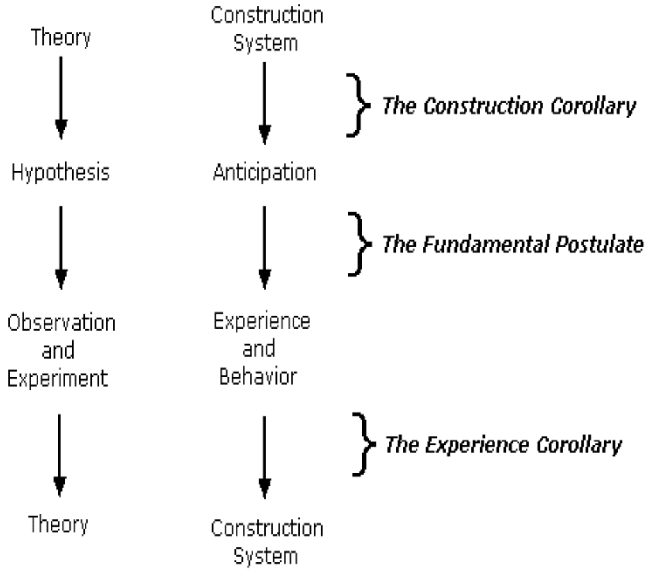
*Expert Systems for Knowledge Management: Crossing The Chasm Between **Information Processing** and **Sense Making**. Journal of Expert Systems with Applications (Malhotra, 2001).*

http://www.brint.org/expertsystems.pdf

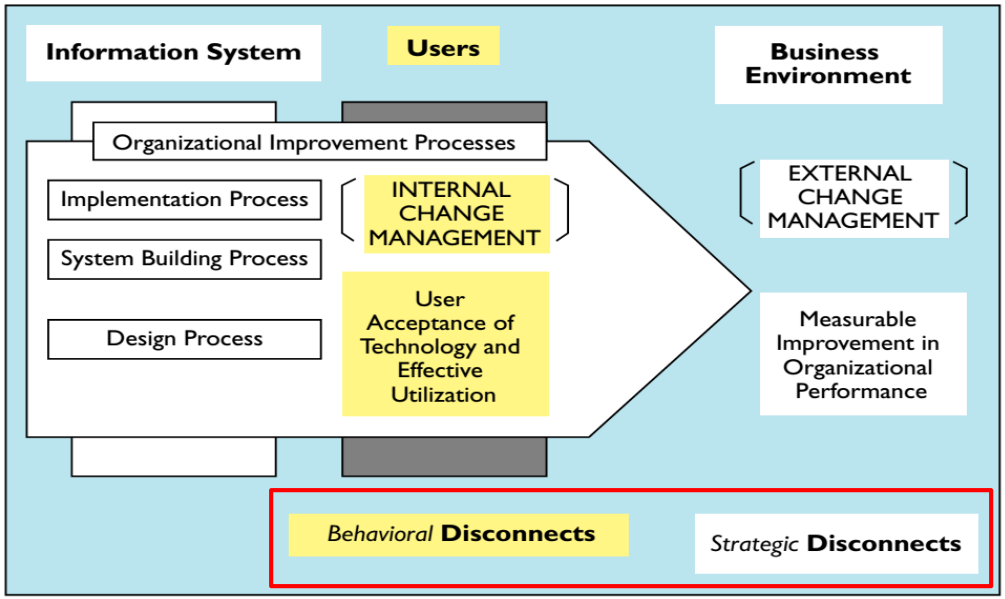
'MEANING' and 'SENSE-MAKING'

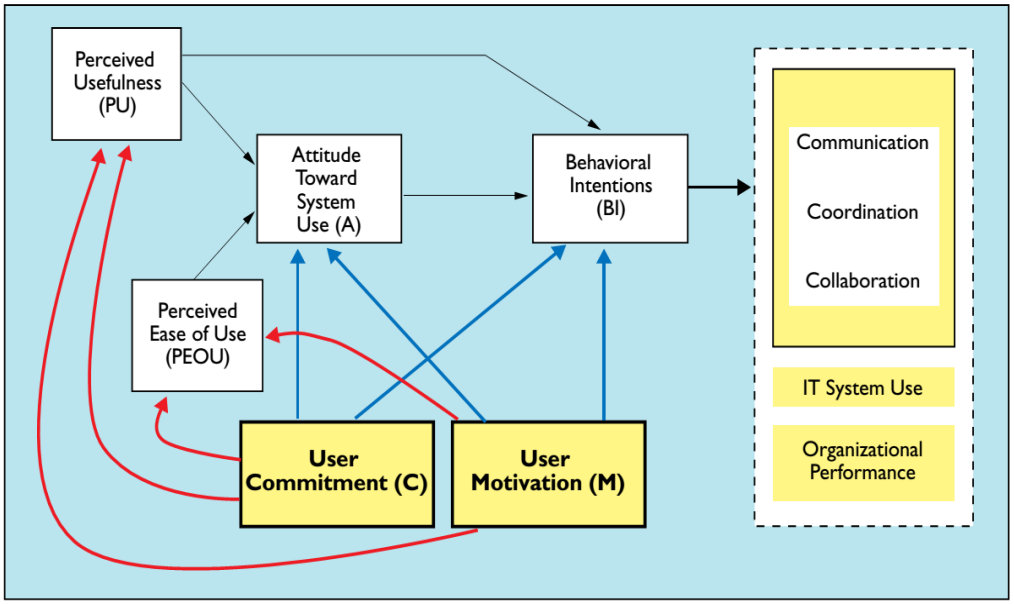


Based upon
Personal Construct Psychology
Developed by
George Kelly:
Geometrician Turned Psychologist :
Model of "Human as Scientist"



Malhotra, Y., Bringing the Adopter Back Into the Adoption Process: A Personal Construction Framework of Information Technology Adoption. **Journal of High Technology Management Research**, 10(1), 1999, 79-104. http://brint.org/PersonalConstructionsofMeaningPaper.pdf





Behavioral and *Strategic* Disconnects in Digital Change Management Practices

Fundamental Gaps in Human Commitment and Motivation as applied to adoption of change, new ideas, innovation, information, and information and decision systems and models…

Resulting in Fundamental **Gaps in Risk Management, Controls, and, Compliance Models & Practices**!

Malhotra, Y. and Galletta, D.F., Building Systems that Users Want to Use, **Communications of the ACM**, 47, 12, December 2004, 89-94. http://www.kmnetwork.com/ITUseCACM.pdf

Malhotra, Y. and Galletta, D.F., A Multidimensional Commitment Model of Volitional Systems Adoption and Usage Behavior, **Journal of Management Information Systems**, Summer 2005, Vol. 22, No. 1; 117-151. http://www.brint.org/JMIS.pdf

A Multidimensional Commitment Model of Volitional Systems Adoption and Usage Behavior

YOGESH MALHOTRA AND DENNIS GALLETTA

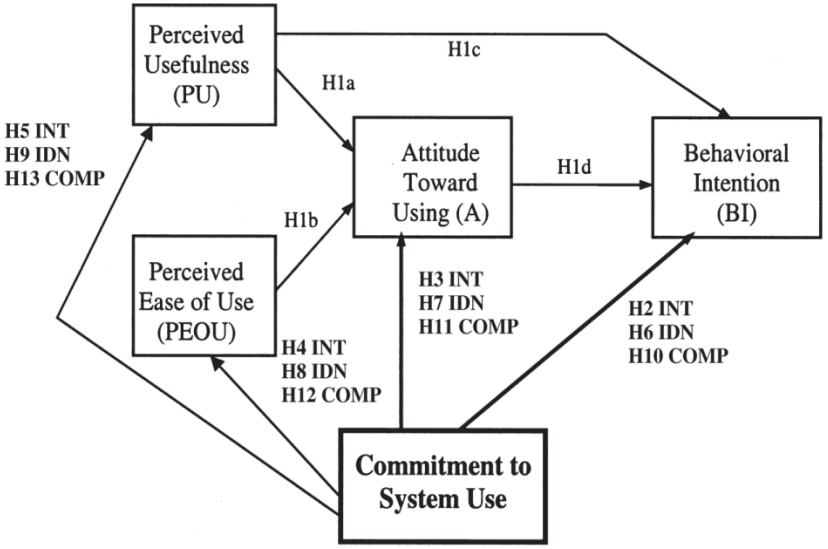


Figure 1. The Psychological Attachment Model: The Multidimensional Commitment Model of Volitional System Adoption and Use

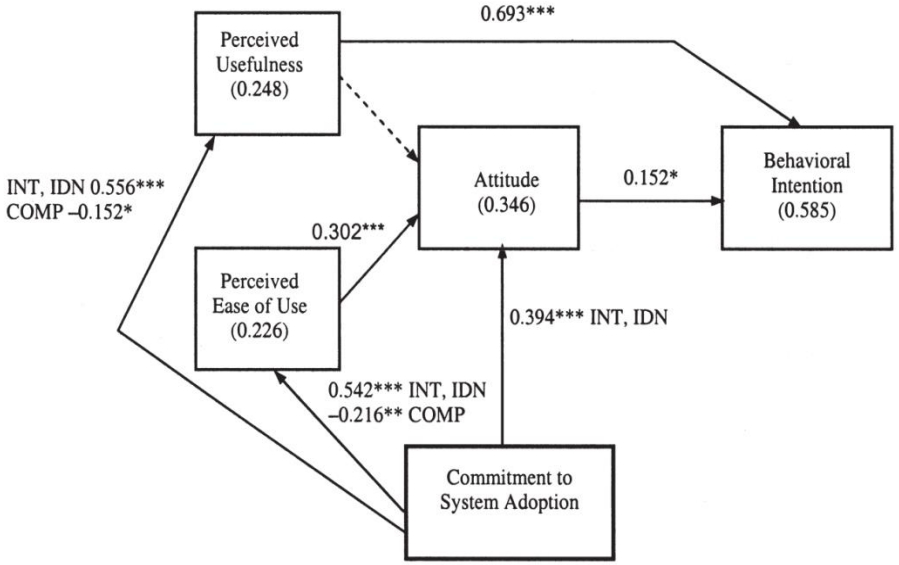


Figure 2. The Multidimensional Commitment Model of Volitional System Adoption
Notes: Only significant relationships are shown. Numbers represent standardized regression coefficients. Variance explained in dependent variables is shown in parentheses. * significant at $p < 0.05$; ** significant at $p < 0.01$; *** significant at $p < 0.001$.

Advancing upon Research of Harvard Psychologist Herbert C. Kelman: Determined that modeling of **Human Commitment** in Digital Change Management contexts is **Incomplete**!

High Risk resulting from Naïve understanding of Human Behaviors published in IT/MIS/IS/Economics Systems and Models Research!

Malhotra, Y., Galletta, D.F., and, Kirsch, L.J. How Endogenous Motivations Influence User Intentions: Beyond the Dichotomy of Extrinsic and Intrinsic User Motivations, **Journal of Management Information Systems**, Summer 2008, Vol. 25, No. 1, 267-299. http://www.brint.org/JMIS2.pdf

How Endogenous Motivations Influence User Intentions: Beyond the Dichotomy of Extrinsic and Intrinsic User Motivations

YOGESH MALHOTRA, DENNIS F. GALLETTA, AND LAURIE J. KIRSCH

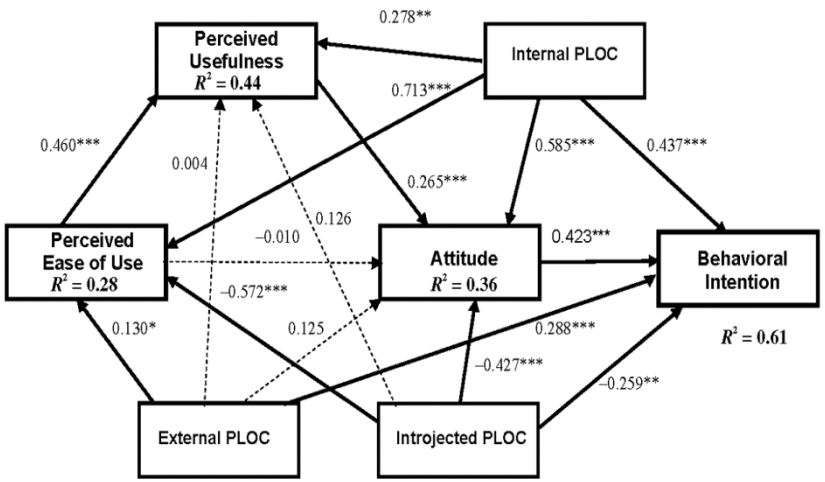


Figure 3. Model Results: Standardized Path Coefficients: Initial Adoption
Notes: Solid arrows show significant paths, dashed arrows show nonsignificant paths.
*** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$.

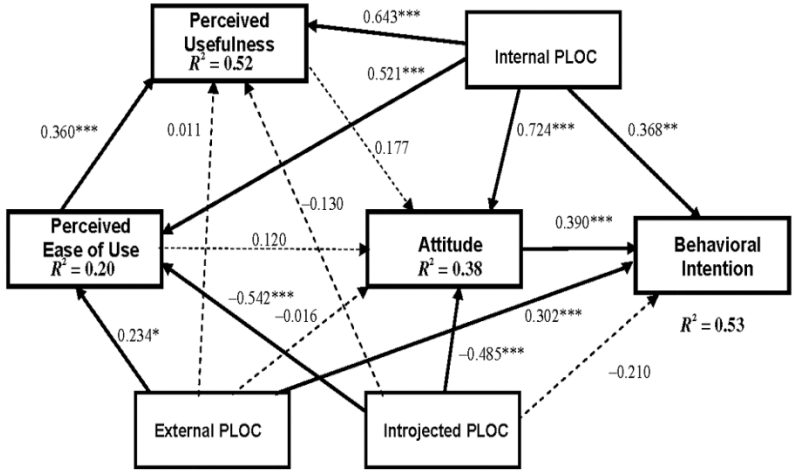


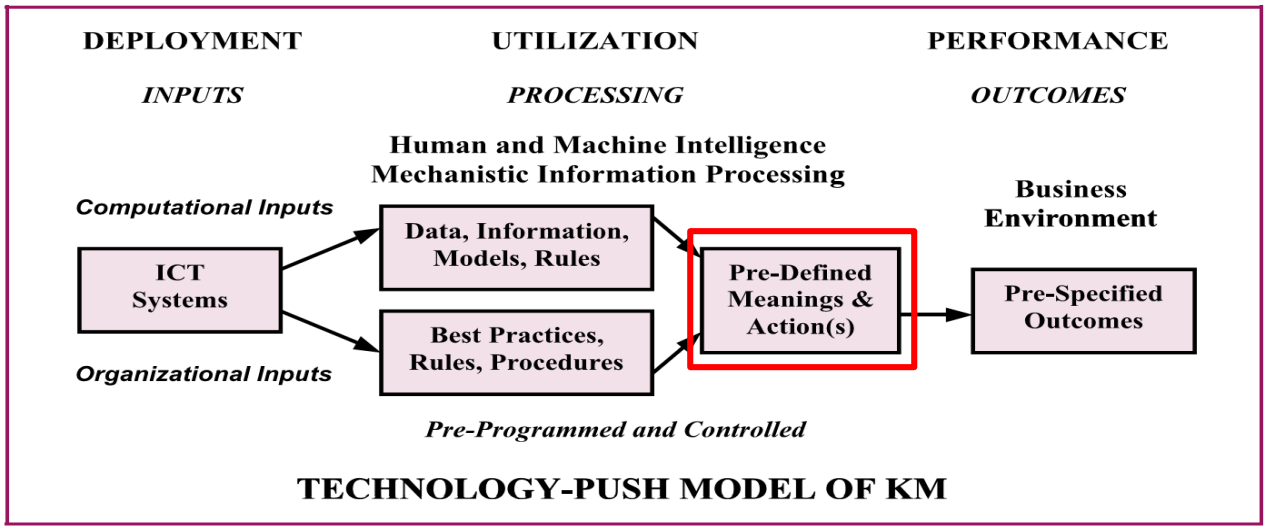
Figure 4. Model Results: Standardized Path Coefficients: Experienced Use
Notes: Solid arrows show significant paths, dashed arrows show nonsignificant paths.
*** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$.

Advancing upon Research of Rochester Psychologists Deci & Ryan: Determined that modeling of **Human Motivation** in Digital Change Management contexts is **Incomplete**!

High Risk resulting from Naïve understanding of Human Behaviors published in IT/MIS/IS/Economics Systems and Models Research!

Malhotra, Y., Integrating Knowledge Management Technologies in Organizational Business Processes: Getting Real Time Enterprises to Deliver Real Business Performance, **Journal of Knowledge Management**, Vol. 9, Issue 1, April 2005, 7-28. http://www.kmnetwork.com/RealTime.pdf

Figure 1 How ICT systems drive and constrain strategic execution

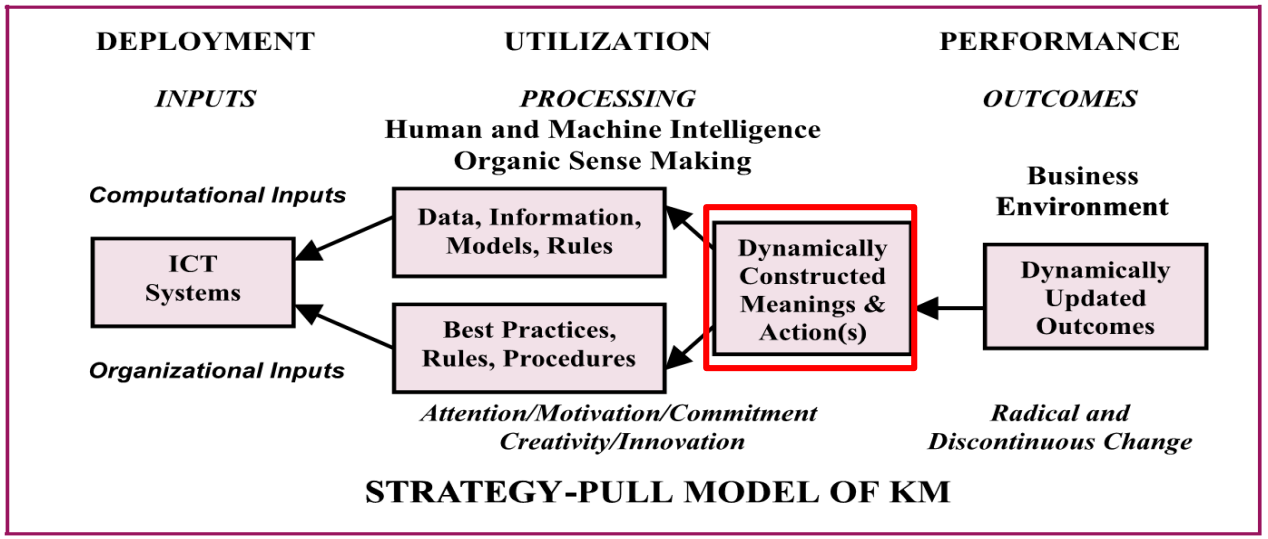


Real Time Enterprise Business Models

'Doing the Thing Right'

Efficiency vs. Effectiveness

Figure 2 Strategic execution – the primary enabler of the RTE business model



'Doing the Right Thing'

Malhotra, Y., Why Knowledge Management Systems Fail? Enablers and Constraints of Knowledge Management in Human Enterprises. In Holsapple, C.W. (Ed.), Handbook on Knowledge Management 1, Springer-Verlag, 2002. (**CNET Corporate Computing Award, 2002, Most Influential Paper**.) http://www.kmnetwork.com/RealTime.pdf

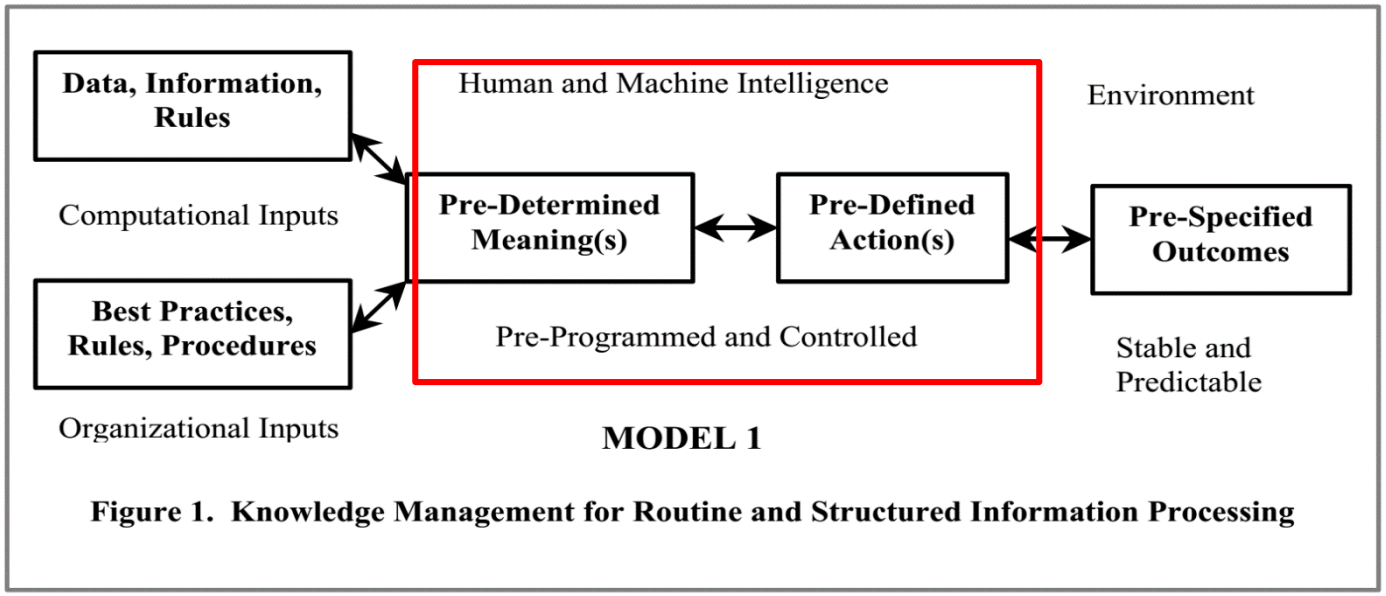


Figure 1. Knowledge Management for Routine and Structured Information Processing

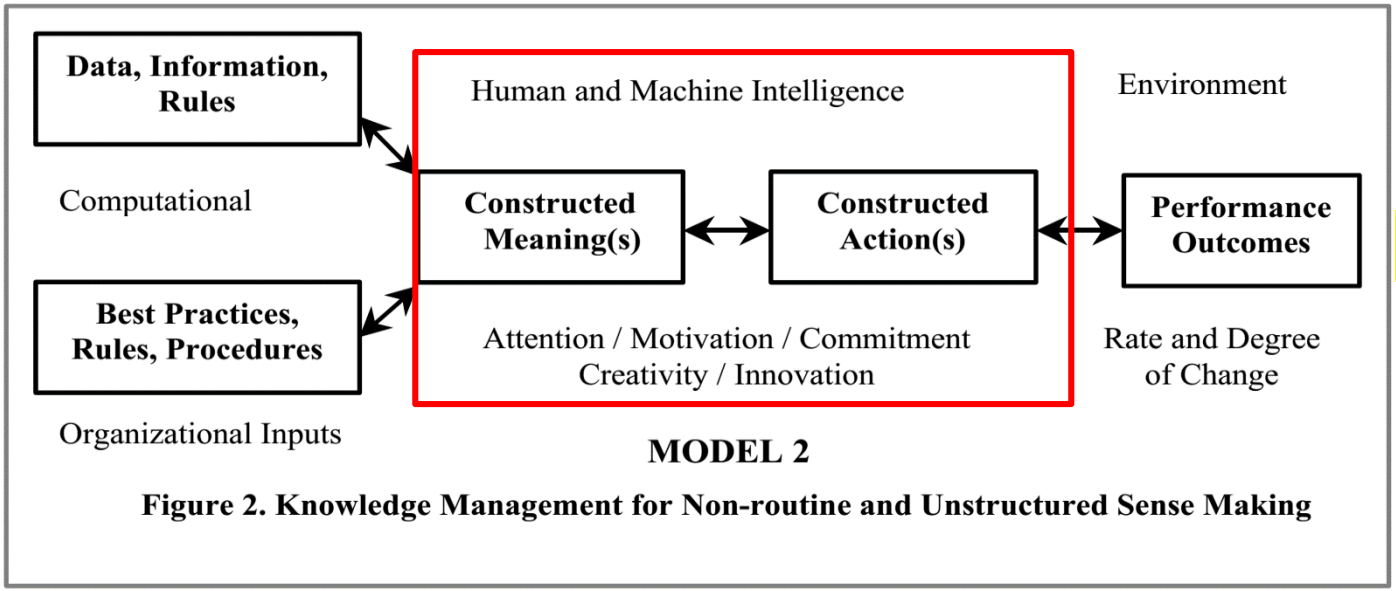


Figure 2. Knowledge Management for Non-routine and Unstructured Sense Making

Anticipation of Surprise Business Models

'Doing the Thing Right'

Efficiency vs. Effectiveness

'Doing the Right Thing'

Later… Global Financial Crisis… 2008

New York Times:

"In Modeling Risk, the Human Factor Was Left Out"

http://www.nytimes.com/2008/11/05/business/05risk.html

HOME PAGE | MY TIMES | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

SUBSCRIBE NOW | Log In | Register Now

The New York Times

Business

Search All NYTimes.com

Go

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS | STYLE | TRAVEL | JOBS | REAL ESTATE | AUTOS

Search Business

Go

Financial Tools

Select a Financial Tool

More in Business »

World Business | Markets | Economy | DealBook | Media & Advertising | Small Business | Your Money

In Modeling Risk, the Human Factor Was Left Out

Illustration by The New York Times

By STEVE LOHR
Published: November 4, 2008

Today's economic turmoil, it seems, is an implicit indictment of the arcane field of financial engineering — a blend of mathematics, statistics and computing. Its practitioners devised not only the exotic, mortgage-backed securities that proved so troublesome, but also the mathematical models of risk that suggested these securities were safe.

TWITTER
LINKEDIN
SIGN IN TO E-MAIL OR SAVE THIS
PRINT
REPRINTS

More Articles in Business »

MOST POPULAR - BUSINESS

EMAILED | VIEWED

1. High-Tech Lights to Help Baby Sleep, or Students Stay Alert
2. Retiring: For Widows, Social Security System Can Provide Rude Shocks
3. Walt Disney, a Visionary Who Was Crazy Like a Mouse
4. Automakers Will Make Automatic Braking Systems Standard in New Cars
5. Your Money: Simpler, Less Expensive 401(k) Options Emerge for Small Businesses
6. Wealth Matters: When Family Members Run Foundations, Scrutiny Never Ends
7. The Fedâ€™s Policy Mechanics Retool for a Rise in Interest Rates
8. Your Money Adviser: Health Savings Accounts Growing, Especially Among the Better Paid
9. Banks to Settle With Investors in Suit Over Financial Crisis
10. Report Finds Vulnerabilities in Guardrails Lining U.S. Roads

Go to Complete List Â»

Dr. Emanuel Derman, Managing Director, Goldman Sachs, Head of Quantitative Strategies Group until 2002

"To confuse the model with the world is to embrace a future disaster driven by the belief that humans obey mathematical rules."

Models are at bottom tools for **approximate thinking**; they serve to transform your **intuition** about the future into a price for a security today... The **most important question about any financial model is how wrong it is likely to be**, and **how useful it is** despite its assumptions. You must start with **models** and then overlay them with **common sense** and **experience**…

WILMOTT
SERVING THE QUANTITATIVE FINANCE COMMUNITY

Emanuel Derman and Paul Wilmott January 7 2009

Emanuel Derman's Blog

The Financial Modelers' Manifesto

Posted At : January 8, 2009 3:14 PM | Posted By : Emanuel Derman
Related Categories: Models

The Financial Modelers' Manifesto

Bloomberg Business | News | Markets | Insights | Video

Magazine

Financial Models Must Be Clean and Simple

December 30, 2008

Preface

A spectre is haunting Markets - the spectre of illiquidity, frozen credit, and the failure of financial models.

Beginning with the 2007 collapse in subprime mortgages, financial markets have shifted to new regimes characterized by violent movements, epidemics of contagion from market to market, and almost unimaginable anomalies (who would have ever thought that swap spreads to Treasuries could go negative?). Familiar valuation models have become increasingly unreliable. Where is the risk manager that has not ascribed his losses to a once-in-a-century tsunami?

To this end, we have assembled in New York City and written the following manifesto.

Manifesto

Many academics imagine that one beautiful day we will find the 'right' model. But **there is no right model**, because the world changes in response to the ones we use. Markets change and newer models become necessary. Simple clear models with **explicit assumptions** about small numbers of variables are therefore the best way to **leverage your intuition** without deluding yourself.

The Financial Modelers' Manifesto

Posted At : January 8, 2009 3:14 PM | Posted By : Emanuel Derman

We do need models and mathematics - you cannot think about finance and economics without them - but one must never forget that models are not the world. Whenever we make a model of something involving human beings, we are trying to force the ugly stepsister's foot into Cinderella's pretty glass slipper. It doesn't fit without cutting off some essential parts. And in cutting off parts for the sake of beauty and precision, models inevitably mask the true risk rather than exposing it. The most important question about any financial model is how wrong it is likely to be, and how useful it is despite its assumptions. You must start with models and then overlay them with common sense and experience.

Building financial models is challenging and worthwhile: you need to combine the qualitative and the quantitative, imagination and observation, art and science, all in the service of finding approximate patterns in the behavior of markets and securities. The greatest danger is the age-old sin of idolatry. Financial markets are alive but a model, however beautiful, is an artifice. No matter how hard you try, you will not be able to breathe life into it. To confuse the model with the world is to embrace a future disaster driven by the belief that humans obey mathematical rules.

Emanuel Derman and Paul Wilmott January 7 2009

“The similarity of physics and finance lies more in their syntax than their semantics. In physics you’re playing against God, and He doesn’t change His laws very often. In finance you’re playing against God’s creatures, agents who value assets based on their ephemeral opinions.”

Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Cyber Risk

Cyber Risk Loss

Cyber Insurance

Cyber Risk Models

Beyond VaR to

ES, EVT, Power Laws

FINANCE

CYBER

Cyber-Finance Risk Management

From 'Prediction' to "Anticipation of Surprise"

From Risk Modeling to Uncertainty Management

Threat & Vulnerability Analysis

Risk Mitigation

Risk Transfer

Risk Acceptance

Enterprise Risk Management

Finance ⟷ **C**yber

PDC x **T**S ➡ (**E**EO) ➡ **F** ⟷ **C**

Production **D**istribution **C**onsumption Across **T**ime and **S**pace
Efficiency **E**ffectiveness **O**ptimization

ASSESS Risk

Quantitative

Qualitative

- **Pen** Testing

Deterministic

Stochastic

Non-Deterministic

- Scenarios

MANAGE Risk

Cybersecurity & Cyber-Finance Risk Management Strategies, Tactics, Operations, &, Intelligence

Enterprise Risk Management to Model Risk Management

Understanding Vulnerabilities, Threats, & Risk Mitigation

Four Parts: Intuition, Data, Humans, Models

Part 4: Linking Intuition & Models

1. The Cyber-Finance-Trust ™ Framework, 1993-2015
2. Latest Vulnerabilities, Threats, & Risk Mitigation…
3. The Human Factor: The Non-Deterministic 'Variable'
4. Cyber Risk: Quantifying, Modeling, & Valuation

"When creating a mathematical proof, the mind does not see the cold, ordered arguments which one reads in texts, but rather it perceives an idea or a scheme which when properly formulated constitutes deductive proof. The formal proof, so to speak, merely sanctions the conquest already made by the intuition."

- Dr. Morris Kline in *Mathematics for the Non-mathematician*

Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Cyber Risk

Cyber Risk Loss

Cyber Insurance

Cyber Risk Models

Beyond VaR to

ES, EVT, Power Laws

FINANCE

CYBER

Cyber-Finance Risk Management

From 'Prediction' to "Anticipation of Surprise"

From Risk Modeling to Uncertainty Management

Threat & Vulnerability Analysis

Risk Mitigation

Risk Transfer

Risk Acceptance

Enterprise Risk Management

Finance ⟷ **C**yber

PDC x **T**S ➡ (**E**EO) ➡ **F** ⟷ **C**

Production **D**istribution **C**onsumption Across **T**ime and **S**pace
Efficiency **E**ffectiveness **O**ptimization

ASSESS Risk

Quantitative

Qualitative

- **Pen** Testing

Deterministic

Stochastic

Non-Deterministic

- Scenarios

MANAGE Risk

Dr. Yogesh Malhotra: RISK, UNCERTAINTY & PROFIT FOR THE DIGITAL AGE™
Bayesian VaR Models Advancing Beyond VaR Model Risks Exposed by the Global Financial Crisis of 2008-2009

"The only Constant used to be Change... Even it is not Constant anymore...."
- Dr. Yogesh Malhotra, circa 2011 based on published research circa 1993-2008.

http://www.yogeshmalhotra.com/risk.html

Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management: How to Manage Risk (After Risk Management Has Failed).
Alternative Download Source of Above Article

"Given critical systemic risk related limitations of VaR market risk models underlying the recent financial crisis known to the Basel Committee as early as 2001, financial institutions must advance beyond traditional VaR models to more robust spectral risk measures."
-- **Yogesh Malhotra** in **Measuring & Managing Financial Risks with Improved Alternatives Beyond Value-At-Risk (VaR)** at Midtown Manhattan presentation at Fordham University, **January 26, 2012**.

http://ssrn.com/abstract=2594859

"A review of trading book capital rules, due to be launched in March by the Basel Committee on Banking Supervision, will consider ditching value-at-risk as the main measure on which market risk capital is calculated, sources say - but it may not be easy to find a replacement."
-- **Goodbye VaR? Basel to Consider Other Risk Metrics**, **Risk.Net**, **28 Feb 2012**.

The Story of VaR…
Danielsson et al. 2001…
January 26, 2012…
28 Feb 2012…
May 2012…

BANK FOR INTERNATIONAL SETTLEMENTS

-- **Basel Committee Proposes Switch from VaR to Expected Shortfall to Better Capture 'Tail Risk'**, **Bank for International Settlements (BIS)**, **May 2012**.

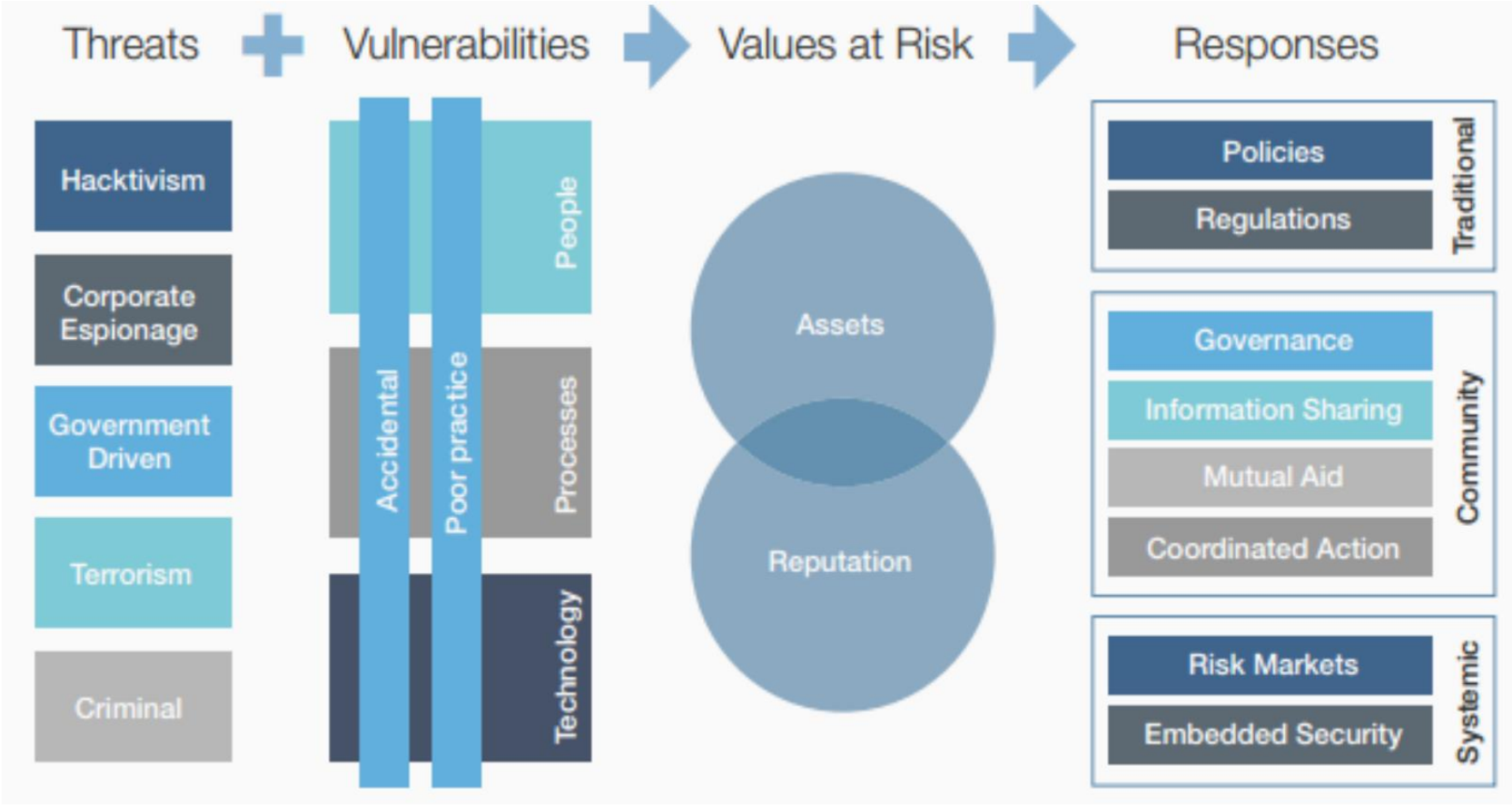
Advancing Beyond 'Normal' VaR for Managing Risk & Uncertainty

Dr. Yogesh Malhotra's Market Risk presentation of January 26, 2012, in which he strongly recommended market risk analysts to start looking beyond VaR and seriously considering Expected Shortfall models preceded subsequent "revelation" on February 28, 2012, by Risk.net that the Basel Committee was considering ditching VaR as a means of calculating market risk capital. Risk.Net reports about its February 28, 2012, article that their "February 2012 article broke the news that the Basel Committee was considering ditching VaR as a means of calculating market risk capital in favour of expected shortfall."

His research on managing the risks of black swan like events has been applied by worldwide firms and governments for more than a decade before the term 'black swan' became fashionable among analysts. His research is advancing the execution of SR11-7 and OCC 2011-12 Model Risk Management Guidance of OCC and US Federal Reserve System such as 'anticipation of risks' by 'effective challenge of models'. His presentation also highlighted critical systemic risk concerns about VaR underlying the financial crisis that were plausibly known to the Basel Committee for Banking Supervision as early as 2001

Cyber Risk: Quantifying, Modeling, & Valuation

Towards the Quantification of Cyber Threats, World Economic Forum, **January 2015**



World Economic Forum. (2015). Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats, World Economic Forum, In collaboration with Deloitte. January 2015

Cyber Risk: Quantifying, Modeling, & Valuation

Towards the Quantification of Cyber Threats, World Economic Forum, January 2015

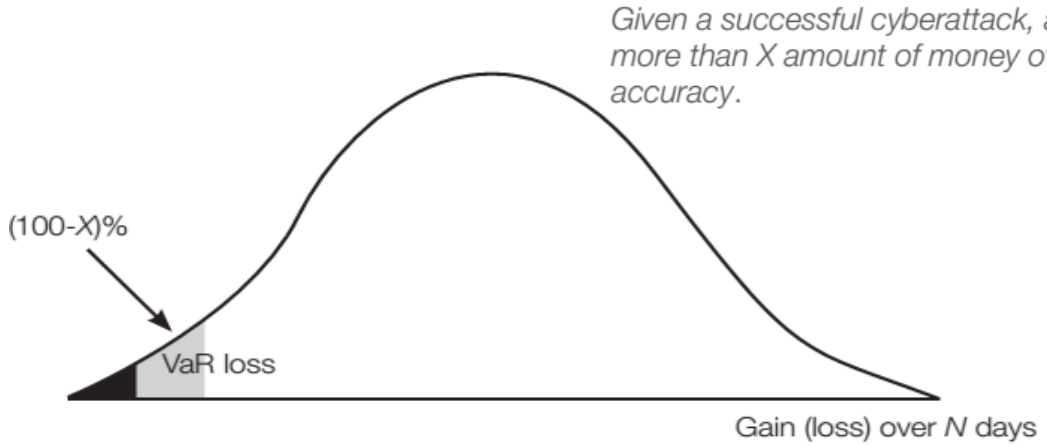
Figure 1. Optimal cyber resilience investment

World Economic Forum. (2015). Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats, World Economic Forum, In collaboration with Deloitte. January 2015

Cyber Risk: Quantifying, Modeling, & Valuation…

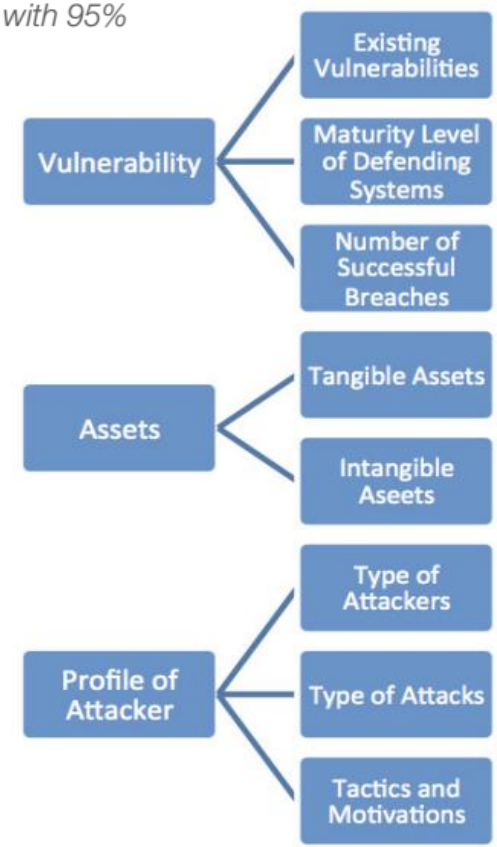
Towards the Quantification of Cyber Threats, World Economic Forum, January 2015

Figure 2. VaR curve



The concept of cyber value-at-risk is based on the notion of value at risk, widely used in the financial services industry. In finance, VaR is a risk measure for a given portfolio and time horizon defined as a threshold loss value. Specifically given a probability X, VaR expresses the threshold value such that the probability of the loss exceeding the VaR value is X. In figure 2, the curve is the normal distribution of the risk, N days is the time horizon, the X axis is the performance of the portfolio and X represents the VaR threshold. (100 – X)% is the probability of not exceeding the VaR value

Figure 3. Cyber value-at-risk components



World Economic Forum. (2015). Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats, World Economic Forum, In collaboration with Deloitte. January 2015

Cyber Risk: Quantifying, Modeling, & Valuation
However, Cyber Risk… A Different Kind of Risk!

Post-Doc Research on Cyber Risk Quantification, Modeling, Valuation:

"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 ICTs and standard computing network protocols."

PDC x TS ➡(EEO) ➡ F⟷C

http://www.FutureOfFinance.org/

Malhotra, Yogesh. Jan. 2015. **Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance & Advanced Analytics**.
Post-Doctoral Thesis. Thesis Committee: Distinguished Computer Scientists and Cybersecurity Specialists, **Air Force Research Lab**, **New York State Cyber Research Institute**, **New York State.**

Original Contributions of Post-Doc Research
Cyber Risk & Cyber Risk Insurance Modeling

1. First known Trust Computing Framework for Cyber Risk Insurance modeling
   - Analyze how Finance risk entangled with Cyber risk
   - Exacerbates the *systemic*, *interdependent*, and *correlated* character of Cyber risks.
2. First known Model Risk Management Framework for Cyber Risk Insurance modeling
   - Model risk management has received sparse attention in Cyber risk assessment and Cyber Insurance modeling.
3. First Known Review of Quantitative Models in Cyber Risk Insurance modeling
   - First known analysis: extreme *model risks*, *tail risks*, and, *systemic risks* related to predominant models in use.

Malhotra, Yogesh. Jan. 2015. **Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance & Advanced Analytics.** http://www.FutureOfFinance.org/

Original Contributions of Post-Doc Research
Cyber Risk & Cyber Risk Insurance Modeling

4. Empirical Study of VaR and Bayesian Statistical Inference Methodologies
   - Specific guidance for containing model risks relevant to their adoption from Finance for Cyber risk assessment and Cyber Insurance modeling.
5. Markov Chain Monte Carlo Models, Gibbs Sampling, Metropolis-Hastings Algorithms
   - Enabling Bayesian statistical inference methodologies to minimize model risk.
6. First known Portfolio Theory based Framework for Cyber Risk Insurance Modeling
   - Guidance to minimize model risks, tail risks, and systemic risks inherent in models in commercial Cyber risk insurance modeling.

US National Focus on Cyber-Finance

*"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.*

New York State Focus on Cyber-Finance

*"**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.

US Banking Focus on Cyber-Finance

"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.

2/3rd US Households Impacted in Just One Breach!

Overview of Cyber Risk & Cyber Risk Insurance

We define **cyber risk** as "risk having consequences affecting the confidentiality, availability, integrity, authentication, non-repudiation, or accessibility of information."

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.

If the risk relates to "cyber", short for cyberspace, it is cyber risk.

Cyber risk in fact subsumes many other risks!

Overview of Cyber Risk & Cyber Risk Insurance

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*.

"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." - Bruce Schneier

Overview of Cyber Risk & Cyber Risk Insurance

- Categories of Cyber Risk Consistent: **CERT**, **Basel II**, and **Solvency II**
  - Peoples, Systems, Technology, Processes, Events
- Aegis London: **cyberattacks will be the 'new normal'** in 2015
  - Destructive attacks linked to **on-going global conflicts**
- Investments: **$120Bn** by 2017 growing 11% annually
- Risk Exposure: **$9Tn** to **$21Tn** of economic-value creation
- Cyber risk loss data **sparse**: '**non material**' SEC public filings.
- No data to empirically '**back test**' models or check **analytical** results.
- VaR: current predominant model of choice in applied practice.

Another 'Formula That Killed Wall Street…'?

- How is VaR exactly applied in its native empirical real world context of measuring portfolio loss by real world Finance trading desks using VaR models?
- 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?
- 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 CRI modeling?

Another 'Formula That Killed Wall Street…'?

- **How Cyber domain's exponentially greater interconnectedness, interdependence, and correlations in case of Cyber risks contribute to the above risks related to VaR?**
- How can cyber risk assessment and CRI modeling applications and practices minimize the above model risks, tail risks, and systemic risks?
- What alternative models can cyber risk assessment and CRI modeling applications use to further minimize the above model risks, tail risks, and systemic risks?

Trust Troika: Cyber-Finance-Trust ™ Framework

- Macroeconomic context of most recent trends and developments
- *Cyber* context frames cyber risk and cyberattacks as *economic games* that influence *economic value*.
- *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.**
- *Finance* (and Economics) *scoreboards* of *economic value* in which the economic costs of cyber risks, cyberattacks, 'wins', and 'losses' are accounted for.

Trust Troika: Cyber-Finance-Trust ™ Framework

- **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.**
- Cyber, Trust, and Finance contexts together defines cyber risk and its economic assessment in terms of models such as Value-at-Risk (VaR).
- It is in the application of specific economic risk assessment models such as VaR that model risk and model risk management need to be applied.

Cyber War Games and Economic Value Creation, Exchange, Transfer, and Destruction

- Cyberattacks most severely impact most information intensive firms
- Banking & Finance: most of its products and services, processes, as well as channels of distribution and consumption are all digital.
- **Common shared platforms, HW, SW, Exchanges, Networks (FIX/FAST, SWIFT): greater probability of correlated cyber risk.**
- Sophisticated global cyber-attacks: 'the new normal'
- **"Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems."**

Cyber War *Games* and *Economic Value* Creation, Exchange, Transfer, and Destruction

"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." "Unprecedented in the history of corporate cyberhacks"

"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*... *destructive nature of this attack, coupled with its coercive nature*, sets it apart… intended to inflict *significant harm on a U.S. business…* undermine the *economic and social prosperity* of our citizens"

Cyber War *Games* and *Economic Value* Creation, Exchange, Transfer, and Destruction

"A *nonkinetic* attack (i.e., destructive malware, destructive computer network attack) that causes just as much damage 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."

"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."

Sony hack: visibility of financial economic dimensions… of **data**.

However, it should *not* be *really* a surprise as:

"Cyberwarfare is underway all of the time…"

- Former NATO Commander & US Presidential Candidate

Cyber War *Games* and *Economic Value* Creation, Exchange, Transfer, and Destruction

"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..."

Nation state cyber offensive capabilities including the ability of incapacitating an adversary country's power grids as early as 1994…

Nation state capability to disable another nation's complete national critical information infrastructure including banking, railroads, airlines, sewage, water and electric power since 1999…

In *Trust Relationships*, Every Entity a Plausible Target, Accessory, Source of Attack

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.

***More significant cyber risk is in vulnerabilities* in the enabling *medium* such as O/S, Networking S/W & Protocols.**

Vulnerabilities inherent in the medium can be exploited resulting in cyber risk regardless of the user's actions or inactions…

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.

In *Trust Relationships*, Every Entity a Plausible Target, Accessory, Source of Attack

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.

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.

In *Trust Relationships*, Every Entity a Plausible Target, Accessory, Source of Attack

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.

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'.

In *Trust Relationships*, Every Entity a Plausible Target, Accessory, Source of Attack

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 of all other risks.

Zero trust approach… traditional perimeter based security *will* be breached, including all defense-in-depth security layers…

Valuable data and assets: protect from inside-out… encryption, data cloaking, data masking… at-rest and in-transmission…

Adaptive perimeter… minimize attack surface… by wrapping mobile apps and authenticated secure communities of interest.

Financial Markets as *Scoreboards* of *Economic Value* at Various Units of Analysis

Cyber context of *economic games* that influence *economic value*…

Trust context that frames the contrast between the Finance and Cyber domains as well as the inter-relationships between the two…

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*…

Cyber Finance* (*information based Finance*), or, *virtual Finance [whenever the interface is digital and not physical] – pretty much most of post-WWW *contemporary Finance* – For most purposes of *actual* production, processing, and distribution, Finance is more or less… Cyber.

Financial Markets as *Scoreboards* of *Economic Value* at Various Units of Analysis

Scores of the online cyber game of Finance… global and national economic indicators, stock prices, AUMs, and, ultra-rich net worth indicators.

In the **Cyber** context, the Trust relationships are through the interactions of the *message* and the *medium* as discussed earlier.

In the **Finance** context, the Trust relationships are through the interactions of *economic scores* and economic well-being.

Troika of **Cyber-Finance-Trust**, **complex interweaving web of entangled *economic 'trust relationships'* inter-relates to *cyber 'trust relationships'*.**

***Interacting web of cyber and economic trust relationships* relevant to examining and understanding diverse vectors of cyber threats and cyber-attacks, as well as potential targets, accessories and sources of cyberattacks.**

Financial Markets as *Scoreboards* of *Economic Value* at Various Units of Analysis

In Finance score-keeping, Value-at-Risk (VaR) of interest as a statistical model and methodology of measuring economic risk of expected loss.

In Troika of Cyber-Finance-Trust, analyze VaR adoption from Finance into Cyber domain for measuring economic risk of expected loss.

Finance-Cyber Interact:
***No Cyber Risk Score*: 'Non Material' SEC Filings**

"*Depending on the severity and impact* of the cybersecurity attacks, ***disclosure is either required or not***."

"Disclosure guidance 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]"… "*avoid generic risk factor disclosure*."

Using 'Value at Risk' (VaR) to Measure and Model Financial Risk and Cyber Risk

Scarcity of financial loss disclosure… while investors, shareholders, and public officials pressing for requiring such cyber risk disclosures.

Scarcity of available, reliable data hampers objective and reliable quantification of cyber risk and modeling of cyber risk insurance.

In absence of data to test **any** model, VaR from Finance has emerged as the predominant model for commercial cyber risk insurance modeling.

VaR is essentially a point estimate measure of risk used in Finance for modeling market risk, credit risk, and [increasingly] operational risk.

Model Risk Management of VaR in Modeling Cyber Risk and Cyber Risk Insurance

It is *critical* to understand the *compatibility* of Finance and Cyber contexts when *transplanting* VaR from Finance to Cyber domain. Without compatibility, the *model* is bound to fail… *Model Risk*

Model Risk Management Ensures that the application of the model is consistent and compatible with the assumptions, boundaries, and limitations of the model

OUR PRIMARY FOCUS: Model risk management of VaR in cyber risk and cyber risk insurance (CRI) modeling.

Model Risk Management of VaR in Modeling Cyber Risk and Cyber Risk Insurance

Model risk management of VaR is critically important:

- Predominant use in Cyber Risk Insurance Modeling.
- Central role in the Global Financial Crisis.
- Neglects modeling of Systemic Risks.
  - Interdependencies and Correlations.
- Even more critical in Cyber Risk Modeling
  - Systemic risks much more extreme.
- Will result in significant Model Risk in Cyber.
  - **Much more extreme than in Finance**.

Model Risk Management of VaR in Modeling Cyber Risk and Cyber Risk Insurance

- How is VaR exactly applied in its native empirical real world context of measuring portfolio loss by real world Finance trading desks using VaR models?
- 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?
- 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 CRI modeling?

Model Risk Management of VaR in Modeling Cyber Risk and Cyber Risk Insurance

- How Cyber domain's exponentially greater interconnectedness, interdependence, and correlations in case of Cyber risks contribute to the above risks related to VaR?
- How can cyber risk assessment and CRI modeling applications and practices minimize the above model risks, tail risks, and systemic risks?
- What alternative models can cyber risk assessment and CRI modeling applications use to further minimize the above model risks, tail risks, and systemic risks?

Model Risks and Model Risk Management

"it may be more damaging to apply a model that really doesn't apply than realizing that there isn't one"

Finance Practice: Quantitative Risk Strategies Group at Goldman Sachs

Dr. Emanuel Derman, Columbia University, Financial Engineering Program

"assumptions and risks involved in using models"

"reliance on models to handle risk carries its own risks."

"*even the finest model is just a model*, and *not the real thing*"

Assumptions, Logic, Data, Sampling Windows: *Model vs. Real World*

Analytic Solutions Need to be Validated Using Real Data.

Models Need to be Tested with Different Parameters and Methods.

Natural Science (Physics) versus Sociotechnical (Finance, Cyber)

Overwhelming Unknown in Finance is UNCERTAINTY

Cyber in comparison to Finance GREATER UNCERTAINTY, COMPLEXITY

Cyber Attack Losses: $10mn vs. $300mn; $171mn vs. $1Bn

Model Risks and Model Risk Management

Finance Regulation: US Federal Reserve, Comptroller of Currency

Supervisory Guidance on Model Risk Management SR11-7/OCC 2011-12 *

"*Model Risk* *arises from the potential adverse consequences* (including financial loss) *of making decisions based on incorrect or misused model outputs and reports, leading to financial loss, poor business decision making, or reputational damage*."

"Those *consequences* should be addressed by active management of model risk."

"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*."

* http://www.yogeshmalhotra.com/blackswans.html

Model Risks and Model Risk Management

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 in Finance.

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 CRI models and measures being applied in commercial practice.

Cyber Risk Insurance & Cyber Risk Models

Review of such models applied for cyber risk and CRI modeling indicates VaR as the predominant model of choice.

"*cyber threats pose one of the gravest national security dangers*"

Yet, negligible disclosures of cyberattack related losses in public filings.

The companies don't do so because they are not *required* to do so.

Cyberattacks become *so common*, they are becoming *less material.*

"***Everybody's getting breached. With most companies, it's not a matter of if, but when, they get a data breach… The quantitative materiality of a data breach I do believe is deteriorating.***"

Cyber Risk Insurance & Cyber Risk Models

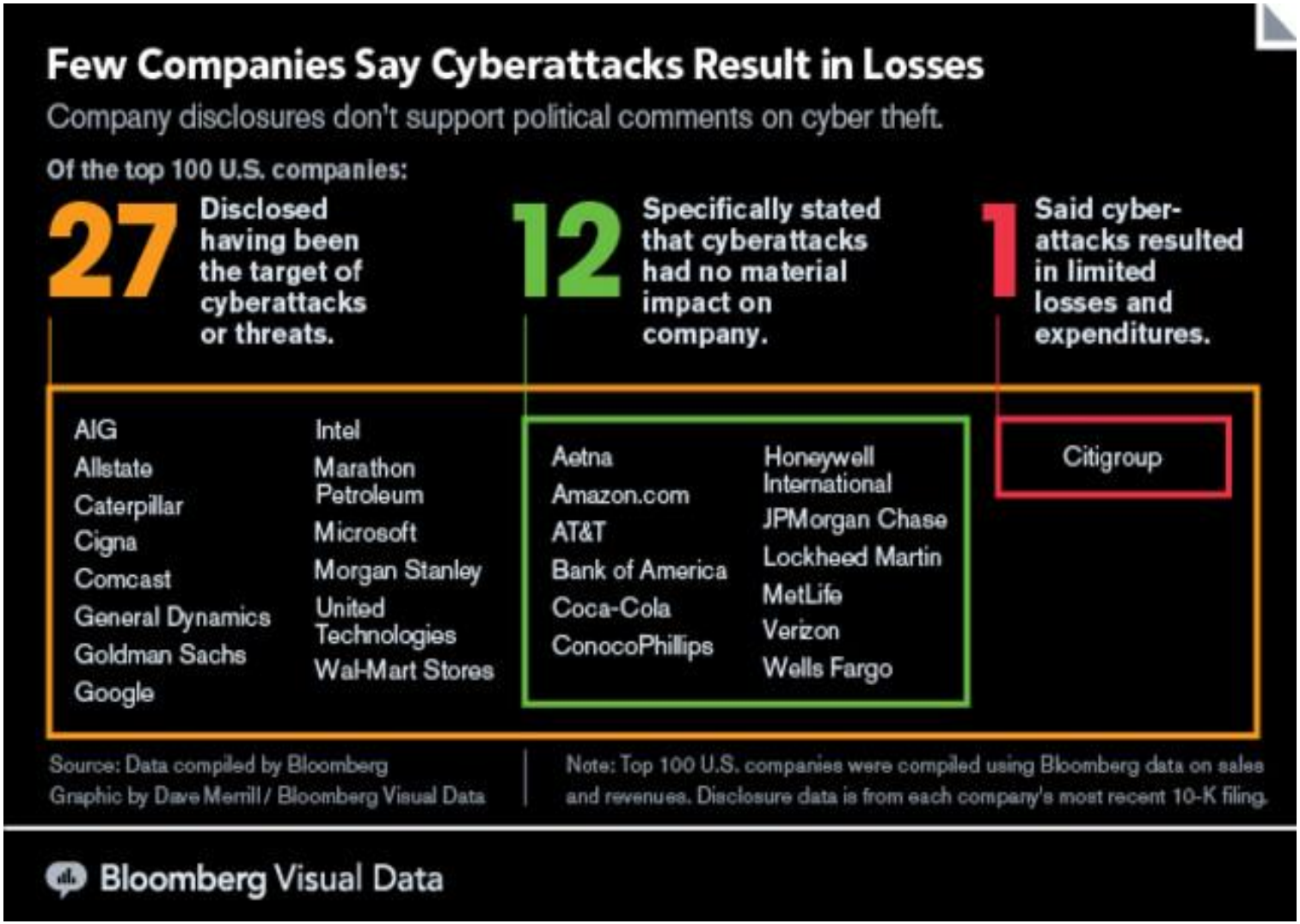
"We basically know that *companies don't measure these things*"

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."

Cyber Risk Insurance & Cyber Risk Models

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.

Cyber Risk Insurance & Cyber Risk Models



Cyber Risk Insurance & Cyber Risk Models

- No Data… make the task of finding valid models for assessing costs of cyber insurance all the more challenging
- any specific model validated in one context may require rethinking in another context given dynamics of the fast evolving context
- all models tentative approx. representations of fast changing reality
- regardless of the model applied, model risk management is all the more crucial in case of CRI modeling
- *asymmetric information*, *adverse selection* and *moral hazard*
- scarcity of reinsurance providers contributes to risks in CRI coverage

Cyber Risk Insurance & Cyber Risk Models

- Insurance underwriters must maintain a large enough **portfolio** of
  - **insured firms** represent risks that are ***independent*** and ***uncorrelated***.
- ***Model risk management*** *of central significance*
- unlike insurance of other tangibles and intangibles, *in case of cyber insurance, risks are interdependent* ***and*** *correlated*.
- '**Diversity** Is the Way to Avoid Cyber Collapse', "potential for a global *systemwide IT failure occurring simultaneously across many organisations* – a "*correlated loss*" as firms more interconnected."
- **CDOs**… used the Gaussian copula model to convince they didn't have any risk at all, in fact they just didn't have any risk 99 percent of the time… and that too theoretically speaking!

Cyber Risk Insurance & Cyber Risk Models

- Cyber risks, *highly interconnected, distributed, networked, and, universal contexts*, *embedded in the medium and the message*…
  - **most highly *interdependent* as well as most highly *correlated***
- *monoculture* in *installed operating systems, and, in…*
- *…software enabling underlying network and security protocols*
- *Ongoing patches…active* applications… *network layer protocols*
- *network layer protocols 'most universal' of all potential vulnerabilities*
- *monoculture transitioning: vendor specific* to *universal infrastructure*
- *epidemically huge damage*… *attacking all computers at same time*

Cyber Risk Insurance & Cyber Risk Models

- 'open source' software and its reliability as a 'public good'
- *intensely technical/human nature of cyberspace*
- *more susceptible and vulnerable to social engineering risk*
- universal reliance upon most universal public good
- current era of **exponentially increasing cyber risk**
- *'materiality': earthquakes and tsunamis* ***vs.*** *global cyberattacks*
- **Research**: All quantitative models for cyber risk modeling
- **Finding**: Most key cyber insurance players rely upon VaR.
  - Significantly underestimates and misestimates cyber risk

VaR Models in Use for Modeling Cyber Risk and Cyber Insurance

Representative Academic Research Studies in this domain

Catastrophe Modeling of Tail Risks Using EVT with VaR, T-VaR

Portfolio Modeling of Risk Optimization Using MVO with CVaR

Commercial Applications in the US cyber insurance industry

CyberV@R: A Model to Compute $ VaR of Loss to Cyber Attack

DoD Information Analysis Centers

McKinsey & Company

Visa

Wipro

PwC… need pervasive confidence and understanding

VaR Poses Significant Model Risk for Cyber Risk and Cyber Insurance Modeling

The Number That Killed Us: A Story of Modern Banking, Flawed Mathematics, and a Big Financial Crisis

Obvious caveat… ordinary VaR model doesn't account for the extreme risk in the tails which could lead to 'catastrophic economic losses.'

Lack of independence and correlations across diverse cyber risks can result in significant systemic risk that VaR doesn't account for.

VaR is being adopted as a 'black box' in this domain…

Commercial applications of VaR in CRI modeling did not consider model risks, tail risks, or systemic risks…

VaR Poses Significant Model Risk for Cyber Risk and Cyber Insurance Modeling

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**.

Recognize the impending cyber risk insurance crisis as well as *provide a solution by helping steer cyber risk assessment and cyber risk insurance modeling practice away from that crisis* by *judicious applications of model risk management related to the relevant quantitative models*

Empirical Finance VaR & Bayesian Modeling

- Model risk: because risk cannot be measured, but must be estimated.
- *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).
- Modeling of 'Bayesian priors' i.e. 'subjective judgment': challenge.
- Bayesian modeling relies on computing algorithms such as MCMC.
- *Hence, regardless of models being used, VaR or Bayesian, model risk management is necessary for minimizing risk management failures.*

Empirical Finance VaR & Bayesian Modeling

Bayes' rule is based on *conditional probability*, the probability of one event given that we know that the other event is true.

Sophistication and complexity of models: two-edged sword.

Simple models are always preferred *if they help understand assumptions and limits of their scope: helps manage model risk.* ***Complex and sophisticated models*** *may increase the model risk if they obfuscate such understanding and clarity.*

Evaluation of complex integrals over high dimensional parameter space major challenge for actual use of Bayesian analysis.

Malhotra, Yogesh, Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management: How to Manage Risk (After Risk Management Has Failed) for Hedge Funds (December 4, 2014). http://ssrn.com/abstract=2538401.
JP Morgan Private Bank *Quantitative Risk Modeling.*

Empirical Finance VaR & Bayesian Modeling

A key limitation of Bayesian inference is often attributed to the choice of the appropriate and reasonable prior distribution.

Bayesian analysis doesn't *rely* on *ad hoc subjective personal judgment*

But upon use of *priors that are agreeable to a skeptical audience.*

VaR quantifies how much at most can be lost with a given probability over a specific time horizon.

Worst expected loss over a given time horizon at a given confidence level under normal market conditions.

Malhotra, Yogesh, Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management: How to Manage Risk (After Risk Management Has Failed) for Hedge Funds (December 4, 2014). http://ssrn.com/abstract=2538401.
***JP Morgan Private Bank** Quantitative Risk Modeling.*

Empirical Finance VaR & Bayesian Modeling

VaR is just an *estimate* and not a uniquely defined value.

VaR does not provide any information on losses that exceed its value.

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.

VaR ***does not*** specify the ***amount of loss*** expected in excess of VaR.

Malhotra, Yogesh, Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management: How to Manage Risk (After Risk Management Has Failed) for Hedge Funds (December 4, 2014). http://ssrn.com/abstract=2538401.
JP Morgan Private Bank *Quantitative Risk Modeling.*

Empirical Finance VaR & Bayesian Modeling

- Historical Simulation is based upon actual data.
  - non-parametric: independent of assumptions about underlying statistical distribution or related parameters; does not assume normal distribution
  - disadvantage lie in its assumption that historical correlations will repeat
- Parametric Method uses the data only for generating the necessary parameters for specifying the distribution.
  - limitations: *normality* and *linearity* assumptions. (Non-linear: e.g. derivatives.)
- Monte Carlo generates data using simulation.
  - *stochastic* model typically based upon a *non-deterministic* component
  - probabilistically strong, mathematically complex, computation intensive

Empirical Finance VaR & Bayesian Modeling

Modified VaR: accounts for the higher (third and fourth) moments

- Modified by using the Cornish-Fisher expansion
- Gaussian $z_{\propto}$ into a non-Gaussian z_{cf}

Coherent Risk Measure

VaR not a *coherent risk measure*… primary drawback… not subadditive

Risk measure *R* that is a *coherent risk measure should satisfy*

Subadditivity (diversification) $R\ (L_1 + L_2) \leq\ R\ (L_1)\ +\ R(L_2)$

Positive homogeneity (scaling) $R\ (\lambda L) = \lambda R(L)$, for every $\lambda\ > 0$

Monotonicity $R\ (L_1) < R(L_2)$ if $L_1 < L_2$

Transition property $R\ (L + a) < R\ (L) - a$

Empirical Finance VaR & Bayesian Modeling

Expected Shortfall (ES), *Expected Tail Loss (ETL), T-VaR, Conditional VaR*

Average of all the losses greater than VaR

Conditional to going beyond VaR

VaR 99% confidence level => ES averages the worst 1% losses

Actual loss (and related risk), however, could be more **extreme**.

ES is a coherent measure as it is subadditive unlike VaR.

Expected value [severity of losses beyond $c = 1 - \alpha$]**.**

Markov Chain Monte Carlo for Bayesian

Bayesian inference based on posterior distributions with many parameters compounds the curse of dimensionality

- MCMC important role in advancing simulation-based Bayesian inference

MCMC… closer to the reality of the data generating process (DGP) in terms of analysis… well-suited for models based upon sparse data.

- Bayesian with MCMC natural way consider parameter & model uncertainty.

General quantitative methods to find approximate solutions to complex problems in polynomial time…

…Where outputs lack interpretability because of high-dimensionality and complex interactions in inputs

Finance Portfolio Theory Mapped to the Domain of Cyber Risk Insurance Modeling

- …Conversely, the higher the correlation of the cyber risk with other cyber risks, the higher the overall risk of the portfolio of cyber risks.
- Cyber risks are highly correlated to each other given intrinsic nature [compared to financial risks], cyber risks are much more risky as compared with financial risks.
- Most cyber risks will be positively and highly correlated and thus contribute to very high riskiness of the portfolio of cyber risks.
- **Unique character of cyber risks** is expected to result in 'portfolios' of extremely highly interdependent and highly correlated cyber risks.

VaR & Beyond VaR for Cyber Risk Insurance

VaR: Amount of loss *not* to be exceeded in a *given time frame* with a *certain probability*.

Maximum amount of money likely to be lost over a *specific time period*, at a *specific confidence level*.

Theoretical basis of VaR is the portfolio theory and MVO.

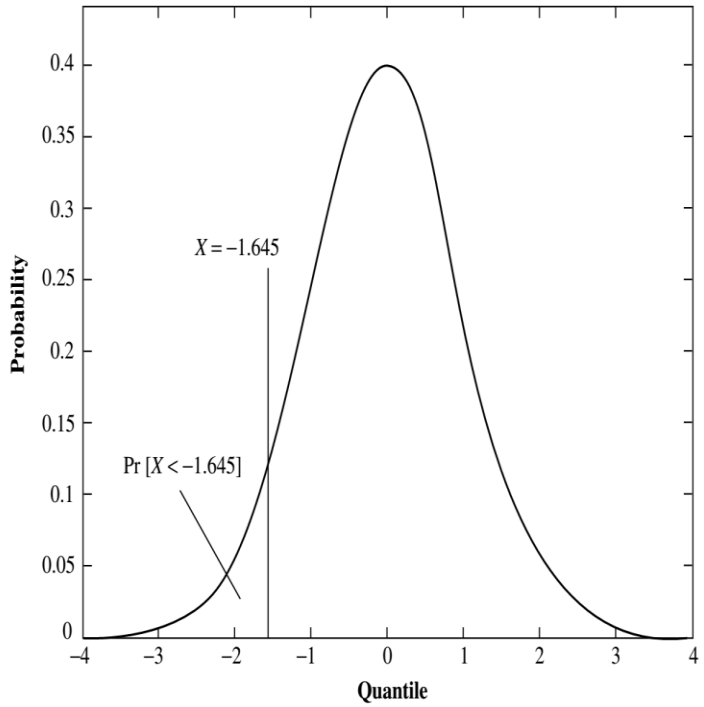
Mean Variance Framework for Measuring Cyber Risk Loss

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

Mean Variance Framework for Measuring Cyber Risk of Expected Financial Loss

Normal pdf with $\mu = 0$ and $\sigma = 1$ known as a *standard normal*

$$f(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2}$$



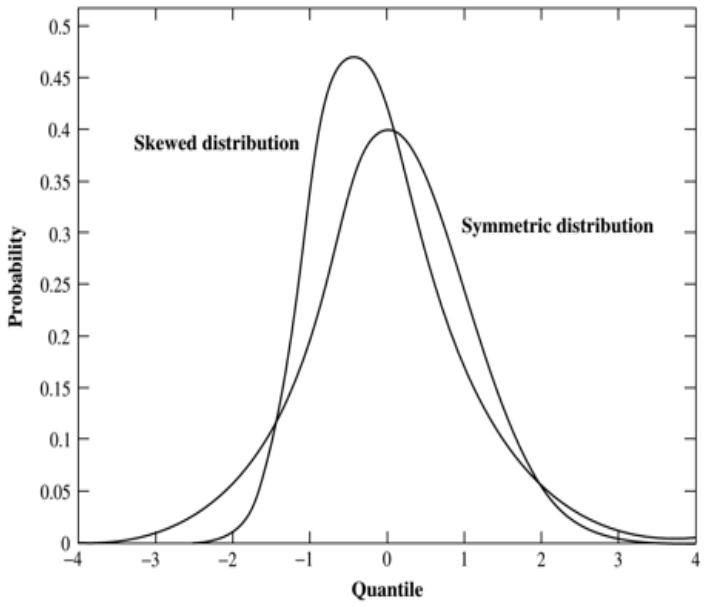
standard normal variate

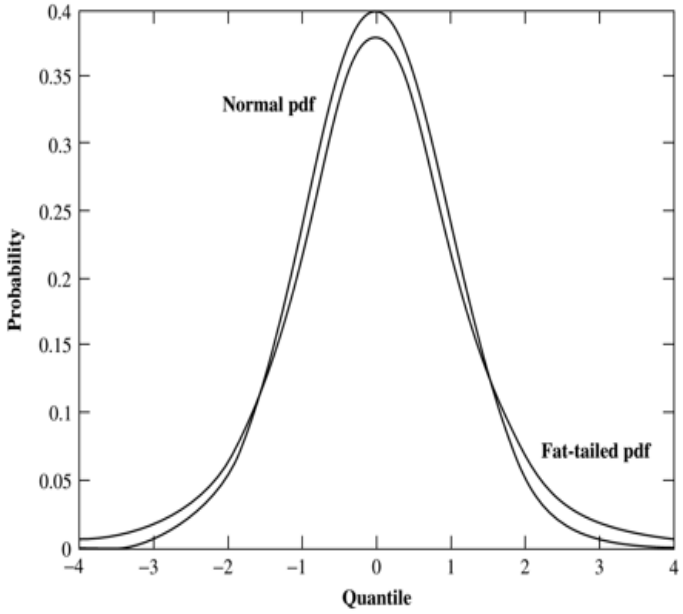
$$\alpha_{cl} = \frac{X_{cl} - \mu}{\sigma}$$

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

Dowd, K. (2007). Measuring Market Risk. John Wiley & Sons.

Skewness and Kurtosis Characterize 'Tail Risks' in Non-Normal Distributions





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

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

Dowd, K. (2007). Measuring Market Risk. John Wiley & Sons.

cyber risks are highly correlated and highly interdependent

For cyber risk, negative skew with a *left long tail* indicating *greater concentration of risk of loss.*

For cyber risk, *left fat tail* indicating *extreme events* more likely inflicting large losses particularly relevant

Value-at-Risk (VaR) for Cyber Risk Assessment and Cyber Risk Insurance Modeling

VaR is the maximum likely loss over some target period at a specified probability level.

Broadly speaking, VaR can be applied in various ways:

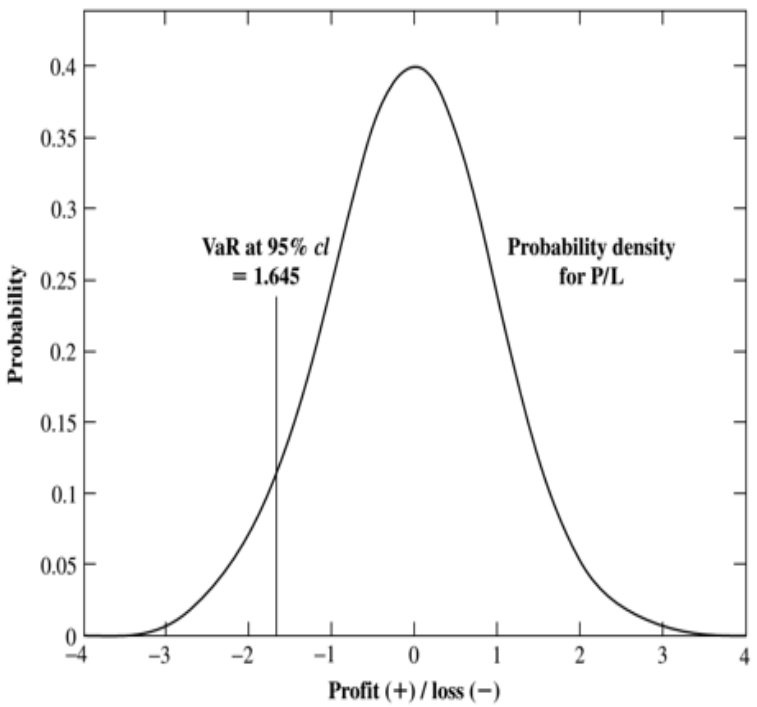
(a) as a point estimate measure of *maximum probabilistic loss*,

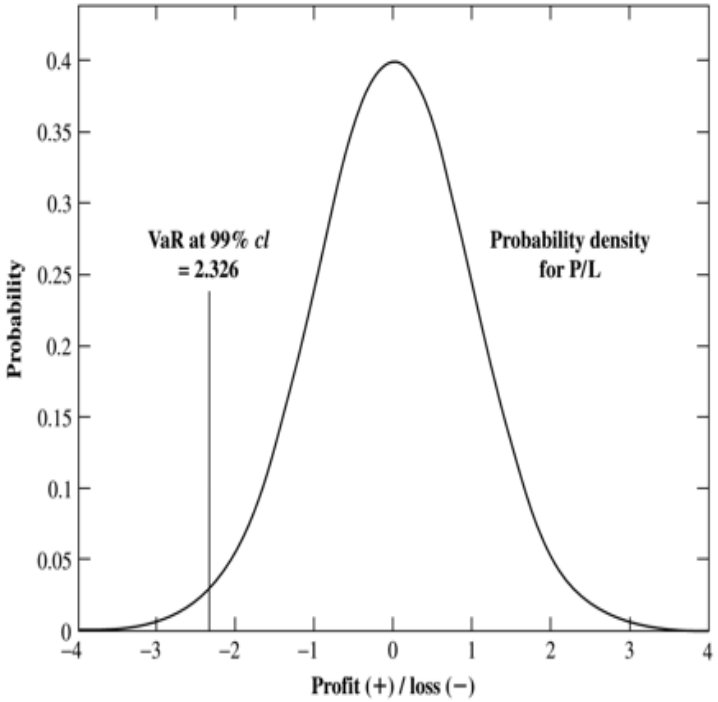
(b) as an *estimation procedure*,

(c) as a *methodology* that can estimate other risks as well, and,

(d) as an *approach to risk management* for strategic decision-making.

How Tail Risks Vary for Different Point Estimates of Normal VaR



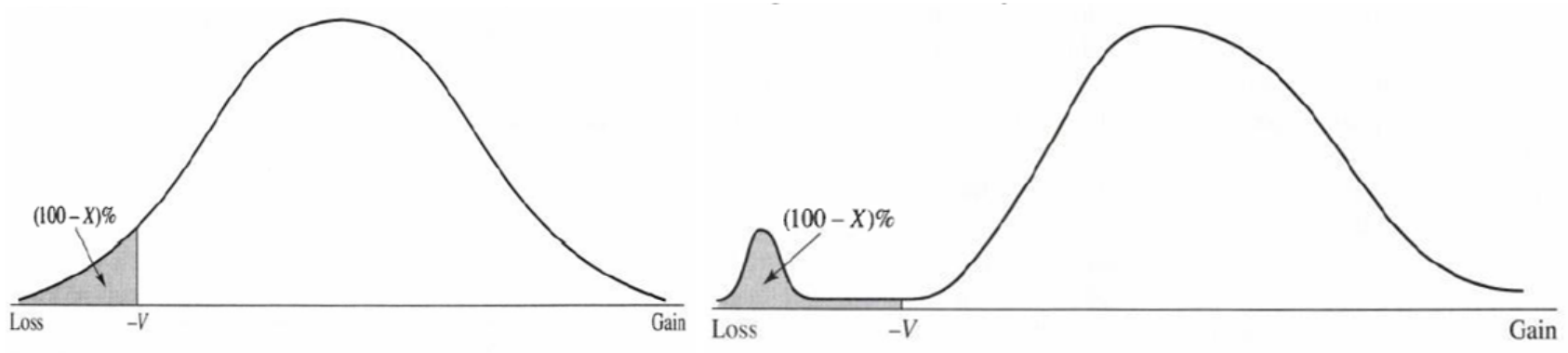


at the same confidence level, 5% of the time, the maximum cyber risk loss *can* exceed 1.645 σ

1% of the time, the maximum cyber risk loss *can* exceed 2.326 σ

Dowd, K. (2007). Measuring Market Risk. John Wiley & Sons.

Why VaR is unable to Account for *Tail Risk*? *Because it is not so designed*

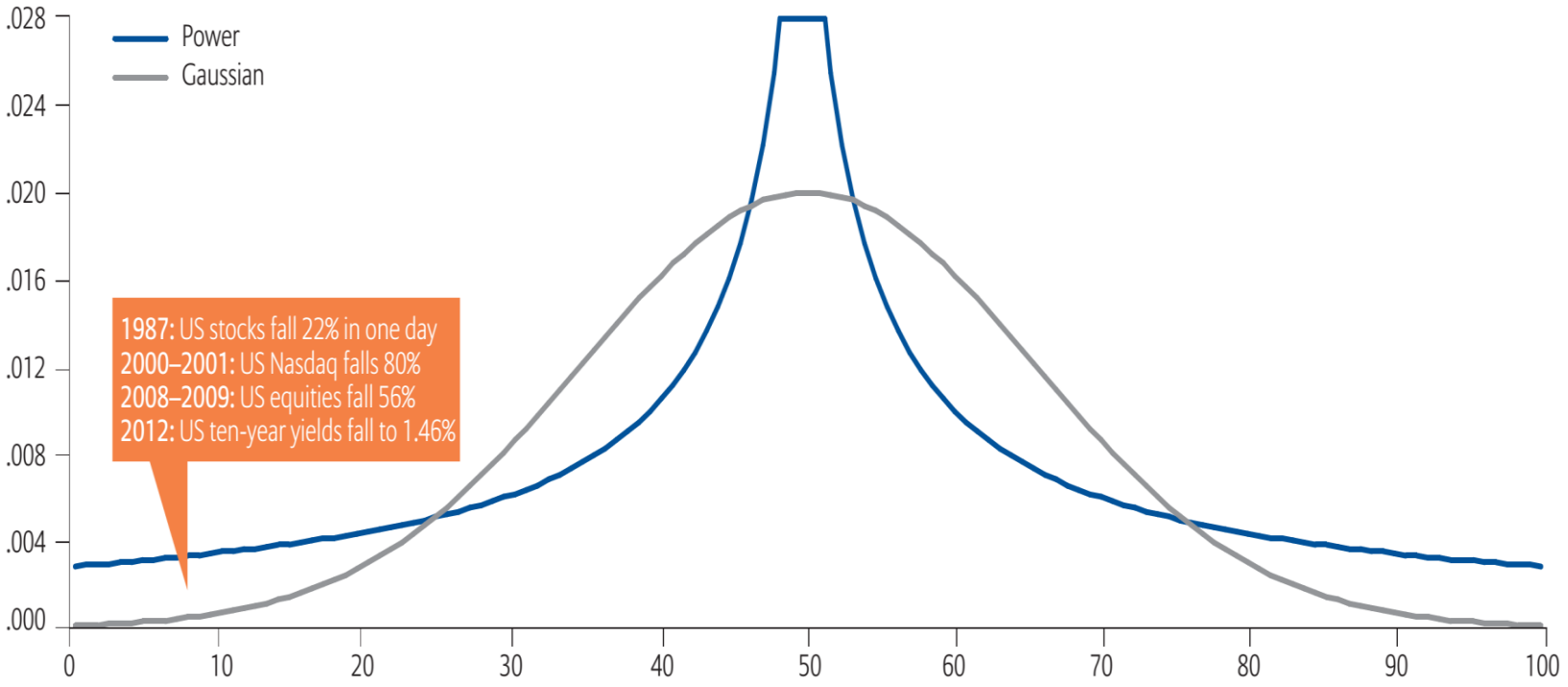


Left panel and the right panel both have the exact same VaR. However, the right panel shows *non-normality* in which the probability of risk is concentrated in the left tail, a *fat tail* resulting from a multimodal distribution.

Hull, J. (2012). Risk Management and Financial Institutions, John Wiley & Sons.

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 *endogenous* in nature.

Most of *Sociotechnical* World is *Non-Normal* and Governed by *Power Laws*



allianzgi.com

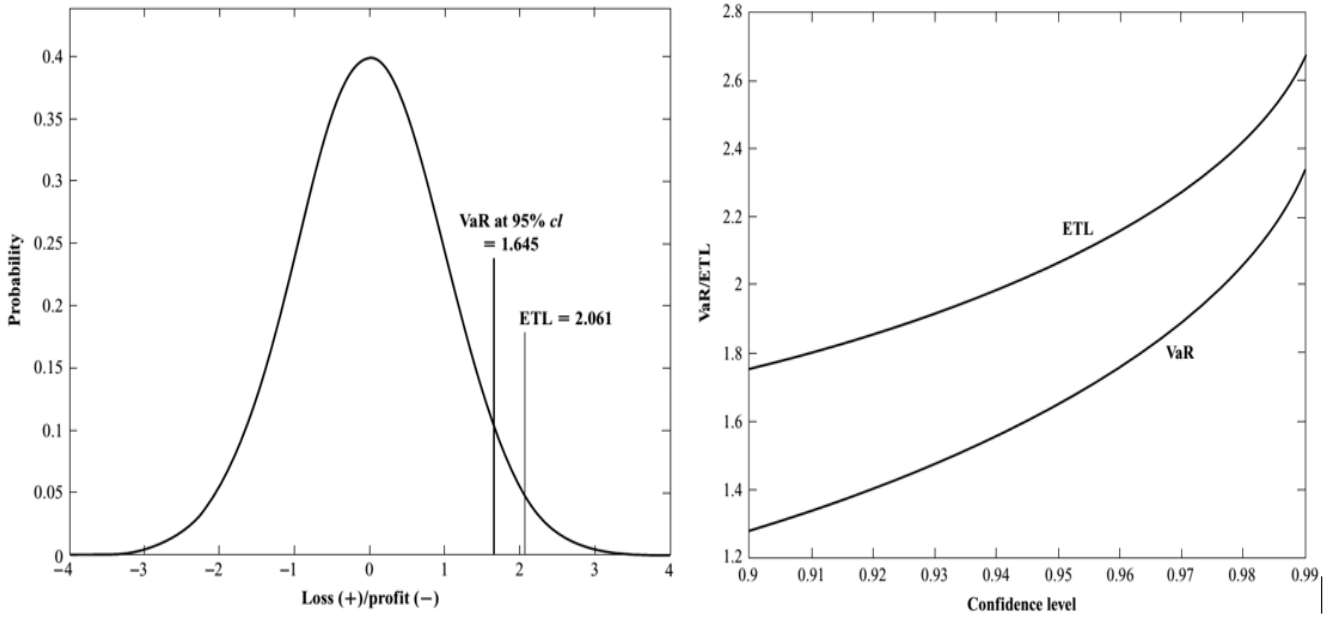
Improved Alternatives beyond VaR and Toward Coherent Risk Measures

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:

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

May 2014 Report on Cyber Security in the Banking Sector by the New York State Department of Financial Services: "The larger the institution, the more likely it appeared to experience **malware** *and* **phishing** attempts.

Expected Tail Loss (aka T-VaR and Expected Shortfall) as a Coherent Risk Measure

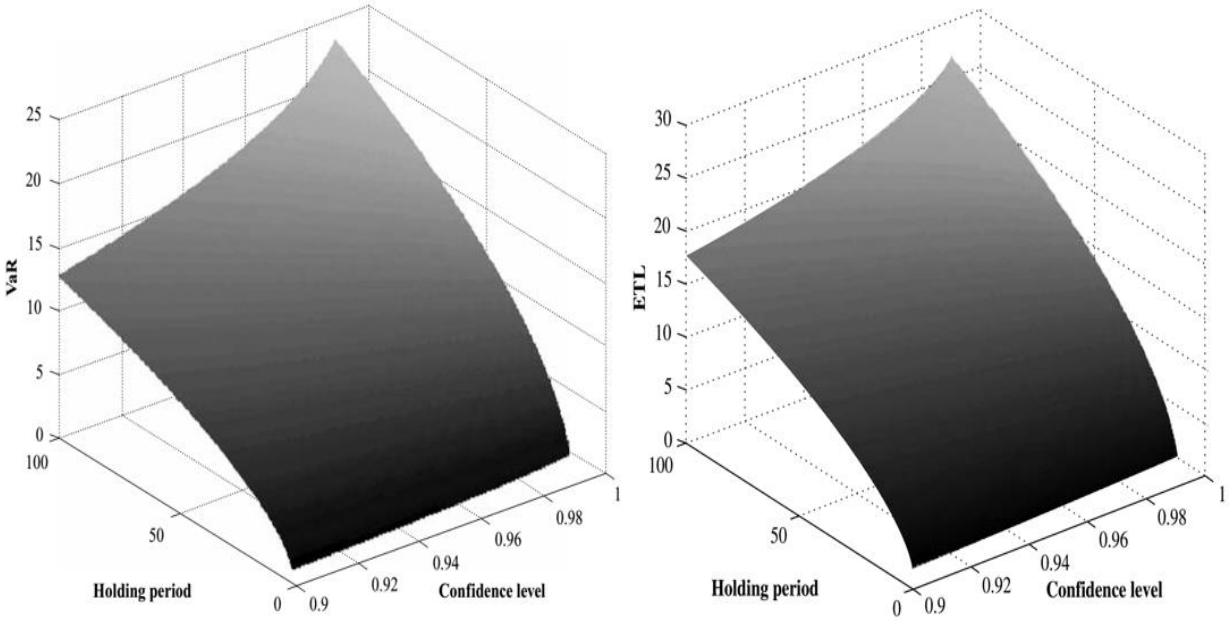


VaR measures the maximum expected loss if an extreme event i.e., 'tail,' *does not occur*, and the ETL measures expected loss *on average* if an extreme event i.e., 'tail,' *does occur*

In the real 'sociotechnical' world, tails are the norm!
Hence, must account for tail risks.

Dowd, K. (2007). Measuring Market Risk. John Wiley & Sons.

Comparison of How VaR and ETL vary with the Two Parameters

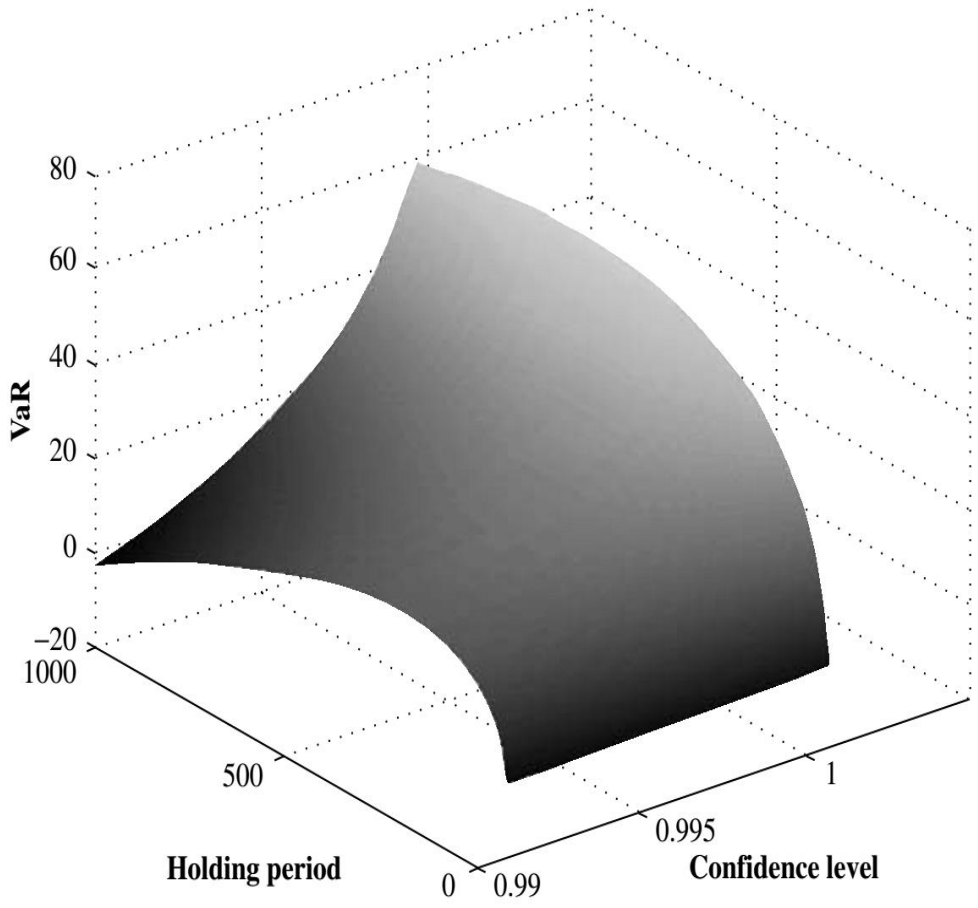


The actual loss (and related risk), however, could be more extreme than the average of the left tail risk. Hence, ETL does not provide any information about the severity of loss by which VaR is exceeded.

Dowd, K. (2007). Measuring Market Risk. John Wiley & Sons.

Need for Extreme Value Methods… and **Data**

$$\Pr\left\{\frac{M_n - b_n}{a_n} \leq x\right\} = F(a_n x + b_n)^n \to H(x)$$



$$H(x) = \exp(-e^{-x}), \text{ all } x \quad \text{(Gumbel)}$$

$$H(x) = \begin{cases} 0 & x < 0 \\ \exp(-x^{-\alpha}) & x > 0 \end{cases} \quad \text{(Fréchet)}$$

$$H(x) = \begin{cases} \exp(-|x|^{\alpha}) & x < 0 \\ 1 & x > 0 \end{cases} \quad \text{(Weibull)}$$

Dowd, K. (2007). Measuring Market Risk. John Wiley & Sons.

Planning for Catastrophic Risks of Extreme Events…

Extreme Value Theory (EVT): Theory of modelling and measuring extreme events, i.e., events which occur with very small probability.

- Example: Measurement of extreme losses i.e., left-tail, in P&L distribution.
- Extracts reliable measure of estimated loss given limited data for extreme event.

Block Maxima (BM) Method: Subdividing the time period of loss data into a set of equal blocks (sub-periods) and taking the **maximum loss in each block** gives the local block maxima. It can be used to characterize or fit a probability distribution and is often called **generalized extreme value (GED) distribution**.

Peaks Over Threshold (POT) Method: More widely used method based on choice of a numerical threshold which denotes **every loss over the threshold** as extreme loss. It can be used to characterize or fit a probability distribution and is often called **generalized Pareto distribution (GPD)**.

Planning for Catastrophic Risks of Extreme Events…

- **Extreme Value Theory (EVT)**

CDF $F(x) = P(X \leq x)$

CDF $F_u(y) = P(X - u \leq y \,|X > u)$

$y = X - u$, excess loss or exceedance over the threshold

for a reasonably high threshold, u, $F_u(y)$ ~ General Pareto Distribution (GPD)

$$G(X) = \begin{cases} 1 - \left(1 + \dfrac{\xi y}{\beta}\right)^{-1/\xi} & \textit{if } \xi \neq 0 \\ 1 - \exp\left(-\dfrac{y}{\beta}\right) & \textit{if } \xi = 0 \end{cases}$$

where $y = X - u$, $\xi = 1/\alpha$ shape parameter, α the tail index

β simple scaling parameter. **Parameters Estimation:**
maximum likelihood, elemental percentile method and the method of moments

Embrechts et al. Extreme Value Theory as a Risk Management Tool and Related Lecture Notes.

Planning for Catastrophic Risks of Extreme Events...

VaR using the GPD approach

$$VaR_{1-\alpha} = u + \frac{\beta}{\xi}\left(\left(\frac{N}{n_u}\alpha\right)^{-\xi} - 1\right)$$

where N is the total number of data points
n_u the number of data points
that exceed the threshold u.

expected shortfall $ES_{1-\alpha}$ $\quad ES_{1-\alpha} = \frac{VaR_{1-\alpha}}{1-\xi}\frac{\beta - \xi u}{1-\xi}$

if amount of data in the tail of the returns distribution small
it leads to broad confidence intervals and weak significance estimates.
Both the BM and POT method suffer from the problem of limited data
although it is possible to reduce the time division in the BM
or lower the threshold for the POT
to produce more data points to fit to the desired distribution.

Embrechts et al. Extreme Value Theory as a Risk Management Tool and Related Lecture Notes.

Planning for Catastrophic Risks of Extreme Events…

Generalized Pareto Distribution (GPD) for extreme tail of a wide range of distributions
EVT is concerned only with the tail of the distribution

As you let the threshold u go to infinity, distribution of observations beyond the threshold (call them y) converge to the $GPD(y;\xi,\beta)$, where

$$GPD(y;\xi,\beta) = \begin{cases} 1-(1+\xi y/\beta)^{-1/\xi} & \text{if } \xi > 0 \\ 1-\exp(-y/\beta) & \text{if } \xi = 0 \end{cases}$$

fat tails. Student's $t(d)$

normal distribution

with $\beta > 0$ and $y \geq u$.

We could use MLE to estimate the GPD distribution however, if $\xi > 0$

Hill estimator $F(y) = 1 - cy^{-1/\xi} \approx 1-(1+\xi y/\beta)^{-1/\xi} = GPD(y;\xi,\beta)$

conditional distribution $f(y|y>u) = f(y)/\Pr(y>u) = f(y)/(1-F(u))$, for $y > u$

$F(u) = 1 - cu^{-1/\xi}$

$$f(y) = \frac{\partial F(y)}{\partial y} = \frac{1}{\xi} c y^{-1/\xi - 1}$$

Embrechts et al. Extreme Value Theory as a Risk Management Tool and Related Lecture Notes.

Planning for Catastrophic Risks of Extreme Events...

construct the likelihood function for all observations y_i larger than the threshold, u

$$L = \prod_{i=1}^{T_u} f(y_i)/(1 - F(u)) = \prod_{i=1}^{T_u} \frac{1}{\xi} c y_i^{-1/\xi - 1} / (c u^{-1/\xi}), \quad \text{for } y_i > u$$

T_u is the number of observations y larger than u, rule of thumb set $T_u = 50$.

log-likelihood function is $$\ln L = \sum_{i=1}^{T_u} \left(-\ln(\xi) - (1/\xi + 1)\ln(y_i) + \frac{1}{\xi}\ln(u) \right)$$

Hill estimator Taking the derivative with respect to ξ and setting it to zero

$$\xi = \frac{1}{T_u} \sum_{i=1}^{T_u} \ln(y_i/u)$$

c parameter $F(u) = 1 - cu^{-1/\xi} = 1 - T_u/T$ Solving for c, $c = \frac{T_u}{T} u^{1/\xi}$

estimate of the cumulative density function for observations beyond u

$$F(y) = 1 - cy^{-1/\xi} = 1 - \frac{T_u}{T}(y/u)^{-1/\xi}$$

Embrechts et al. Extreme Value Theory as a Risk Management Tool and Related Lecture Notes.

… While Minimizing Catastrophic Risk of Model Risks

Dear Sir

The article "Of couples and copulas", published on 24 April 2009, suggests that David Li's formula is to blame for the current financial crisis. For me, this is akin to blaming Einstein's $E=mc^2$ formula for the destruction wreaked by the atomic bomb.

Feeling like a risk manager whose protestations of imminent danger were ignored, I wish to make clear that many well-respected academics have pointed out the limitations of the mathematical tools used in the finance industry, including Li's formula. However, these warnings were either ignored or dismissed with a desultory response: "It's academic".

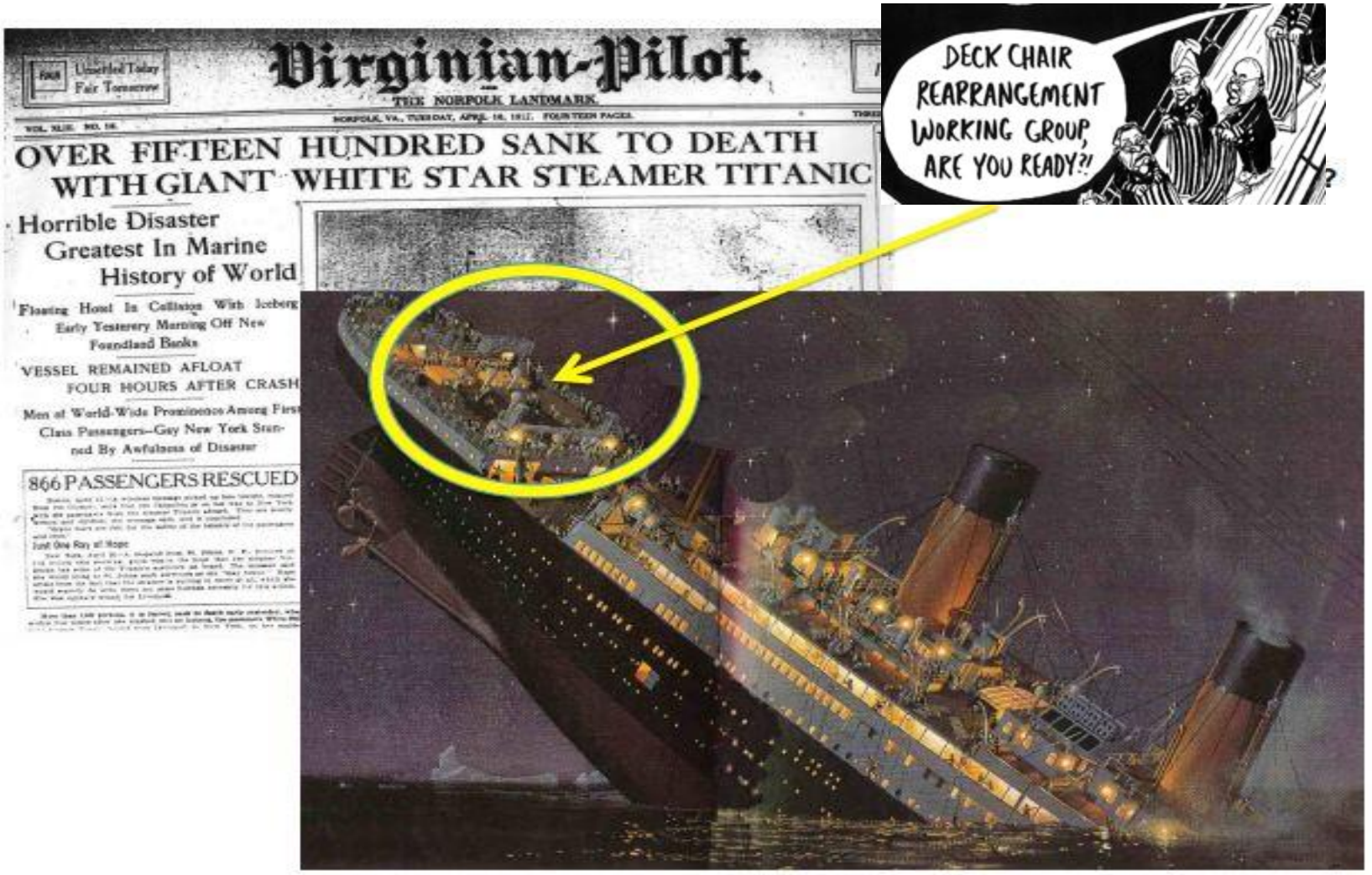
We hope that we are listened to in the future, rather than being made a convenient scapegoat.

Yours Faithfully,
Professor Paul Embrechts
Director of RiskLab
ETH Zurich

Also Harry Panjer

http://www.actuaries.org/ASTIN/Colloquia/Helsinki/Presentations/Embrechts.pdf

Many Quant Risk Management Groups…



Linking Intuition & Models

"Models are at bottom tools for **approximate thinking**; they serve to transform your **intuition** about the future into a price for a security today... The **most important question about any financial model is how wrong it is likely to be**, and **how useful it is** despite its assumptions. You must start with **models** and then overlay them with **common sense** and **experience**…Many academics imagine that one beautiful day we will find the 'right' model. But **there is no right model**, because the world changes in response to the ones we use. Markets change and newer models become necessary. Simple clear models with **explicit assumptions** about small numbers of variables are therefore the best way to **leverage your intuition** without deluding yourself."

Cyber Risk: Quantifying, Modeling, & Valuation
Hence, Cyber Risk… A Different Kind of Risk!

POST-DOCTORAL RESEARCH: http://www.FutureOfFinance.org/

"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 ICTs and standard computing network protocols."

Consistently, original post-doctoral research developed original holistic framework for understanding, analyzing, and, assessing cyber risk and modeling cyber risk insurance:

Malhotra, Yogesh. Jan. 2015. **Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance & Advanced Analytics**. Post-Doc Thesis.

Post-Doctoral Research: Overall Key Contributions

The Post-Doctoral research averted the impending national Cyber Risk and Cyber Risk Insurance disaster based upon large-scale commercial reliance upon [VaR] quantitative models with inherent model risks, tail risks, and systemic risks. Based upon first known critical analysis of the Cyber Risk Insurance Modeling loss assessment models applied in mainstream practice across industry, post-doctoral research determined that those models weren't suitable for the specific purpose of cyber risk loss assessment. Advancing upon quantitative risk modeling of risk of loss assessments from Quantitative Finance risk modeling research and practices, it further prescribed the application of alternative quantitative models such as Expected Shortfall models, Extreme Value Theory models, and, Power Laws models corresponding to the specific context of tail risks and systemic risks relevant to the specific cyber risk insurance modeling application contexts.

Original Contributions of Post-Doc Research
Cyber Risk & Cyber Risk Insurance Modeling

1. First known Trust Computing Framework for Cyber Risk Insurance modeling
   - Analyze how Finance risk entangled with Cyber risk
   - Exacerbates the *systemic*, *interdependent*, and *correlated* character of Cyber risks.
2. First known Model Risk Management Framework for Cyber Risk Insurance modeling
   - Model risk management has received sparse attention in Cyber risk assessment and Cyber Insurance modeling.
3. First Known Review of Quantitative Models in Cyber Risk Insurance modeling
   - First known analysis: extreme *model risks*, *tail risks*, and, *systemic risks* related to predominant models in use in industry applications.

Original Contributions of Post-Doc Research
Cyber Risk & Cyber Risk Insurance Modeling

4. Empirical Study of VaR and Bayesian Statistical Inference Methodologies
   - Specific guidance for containing model risks relevant to their adoption from Finance for Cyber risk assessment and Cyber Insurance modeling.
5. Markov Chain Monte Carlo Models, Gibbs Sampling, Metropolis-Hastings Algorithms
   - Enabling Bayesian statistical inference methodologies to minimize model risk.
6. First known Portfolio Theory based Framework for Cyber Risk Insurance Modeling
   - Guidance to minimize model risks, tail risks, and systemic risks inherent in models in commercial Cyber risk insurance modeling.

Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Four Parts: Intuition, Data, Humans, Models

1. The Cyber-Finance-Trust ™ Framework, 1993-2015
2. Latest Vulnerabilities, Threats, & Risk Mitigation…
3. The Human Factor: The Non-Deterministic 'Variable'
4. Cyber Risk: Quantifying, Modeling, & Valuation

Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Cyber Risk

Cyber Risk Loss

Cyber Insurance

Cyber Risk Models

Beyond VaR to

ES, EVT, Power Laws

FINANCE

CYBER

Cyber-Finance Risk Management

From 'Prediction' to "Anticipation of Surprise"

From Risk Modeling to Uncertainty Management

Threat & Vulnerability Analysis

Risk Mitigation

Risk Transfer

Risk Acceptance

Enterprise Risk Management

Finance ⟷ **C**yber

PDC x **T**S ➡ (**E**EO) ➡ **F** ⟷ **C**

Production **D**istribution **C**onsumption Across **T**ime and **S**pace
Efficiency **E**ffectiveness **O**ptimization

ASSESS Risk

Quantitative

Qualitative

- **Pen** Testing

Deterministic

Stochastic

Non-Deterministic

- Scenarios

MANAGE Risk

Cybersecurity & Cyber-Finance Risk Management
Strategies, Tactics, Operations, &, Intelligence
Enterprise Risk Management to Model Risk Management
Understanding Vulnerabilities, Threats, & Risk Mitigation

Yogi

Yogesh Malhotra, PhD
Global Risk Management Network, LLC
757 Warren Road, Cornell Business & Technology Park, Ithaca, NY 14852-4892
http://www.linkedin.com/in/yogeshmalhotra
dr.yogesh.malhotra@gmail.com

Presentation at the Cybersecurity Summit
Altria Group Inc. Headquarters,
6601 W Broad St, Richmond, VA

Tuesday, September 15, 2015