The Increasing Importance of Operational Risk in Enterprise Risk Management

Russell Walker, Ph.D.[1]

Abstract

Enterprise Risk Management, as a corporate undertaking, has its deepest roots in financial services. Historically, for banks and insurance firms, the focus within enterprise risk has largely been credit and market risk. The Great Recession of 2008 showed us that liquidity risk and the interplay between a firm and capital markets were also important to consider. Now that sufficient time has passed since the Great Recession, we see that credit and market risk were not the sole causes. Indeed, critical operations and processes at many lending institutions failed. Underwriting procedures, loan processing, and the like were subject to little if any confirmation and oversight, leading to larger and higher credit risk positions than anticipated. Operational risk had reared its ugly head. The wave of regulation that has overtaken the financial services industry since then is largely driven by concerns over processes and procedures that caused harm to customers. The impact of processes and policies has never been greater. There are drivers at work to suggest that operational risk is still increasing, and that in particular, firms should be mindful of certain risk drivers, in the context of enterprise risk management, such as Increasingly Complex Operations, Development of New and Untested Products, Automation and Digitization, Increasing Reputational Impact from Operational Risk, New Focus of Regulators on the Treatment of Customers as Victims, and lastly, Cyber Risk. The disturbing and uncomfortable reality is that operational risk is unintended and, in theory, should not happen, if critical processes are well designed. Operational risk is self-inflicted, or if not self-inflicted, it is the result of unexpected errors or mistakes, all proving to be much more costly and dangerous than initially anticipated. Therefore, this leads firms to pay specific focus on operational risk management as part of enterprise risk management.

Keywords: Operational Risk, Enterprise Risk, Banking, Financial Services, Cyber Risk

[1] *Clinical Associate Professor, Managerial Economics and Decision Sciences. Kellogg School of Management Northwestern University, Evanston, IL USA. E-mail: russell-walker@kellogg.northwestern.edu*
Web: http://www.kellogg.northwestern.edu/faculty/directory/walker_russell.aspx

1. Origin of operational risk

The origins and notions behind the word "risk" have a heritage rooted in operational risk and specifically the perils and uncertainty of sea commerce in Mediterranean culture. The losses from sea transit were deemed a risk and related to the unpredictable nature of the sea, but also the experience of the captain and the soundness of the ship in question. Risk, and operational risk in particular, were focused on the externalities and the internal processes, decisions, and defenses to guard against those threats. So, not surprisingly, the word risk first appeared in the English language as part of insurance and shipping terms: shippers and receivers had to bear the "risk" of lost cargo in transit, much like the brave seamen before them. Previous to that focus on the operational losses from sea commerce, the concept of risk and the word risk are not seen in any language. Risk thus developed as a concept in commerce that could account for acts of God, force majeure, and the general danger and peril related to the loss of goods in transit. This is perhaps best preserved in the current Spanish phrase, "*por su cuenta y riesgo*," which is literally "by one's cost and risk," or more familiarly, "at your own risk." [Walker (2013)] It reminds us that risk, and in particular operational risk, has a cost. This undesirable operational risk proved too much for some in commerce. The aversion of risk by merchants gave rise to a highly profitable industry: shipping insurance.

These early notions of risk focused on loss that could not be separated from the act of conducting some commerce. It was operational risk that first challenged risk managers and risk takers, giving us the concept of risk. The operational risk of shipping goods was embedded in the operations of commerce. Frank Knight (1921) pointed out that risk is an economic concept at work in business decisions, owing to the inherent existence of known and unknown factors. Operational risk often involves a great deal of uncertainty. Invoking Frank Knight is all the more appropriate because he highlighted that immeasurable uncertainty is most dangerous. [Knight (1921)] So, it seems appropriate that we examine operational risk and its impact on enterprise risk management.

2. Focus on Operational Risk

The Great Recession of 2008 showed that risks are intertwined. We have learned that what appeared to be credit risk with mortgages was conflated with the operational risk of missing and incomplete loan documentation and even misrepresentations of personal financial details by borrowers. In many ways, the operational risk of the underwriting process used by mortgage originators led to more credit risk than was expected. Other industries have also showed mega

loses in operational risk. The BP crisis in the Gulf of Mexico shows us that critical operational failures can indeed lead to catastrophe for a firm and many others [Walker (2013)]. The challenges at Toyota and GM in manufacturing vehicles remind us that the public expects products be manufactured that are safe to use. Toyota and GM struggled to meet this expectation of surety, and their operational shortcomings showed through in their early response to these challenges. Operations that can impact customers and other sensitive constituents are especially critical and worthy of examination.

During the Great Recession of 2008, operational risk resulted in economic shocks, while today, the most newsworthy operational risk involves large data breaches triggered by external attacks. In both examples, it appears that a series of process failures occurred, compounding the risk such that what appears to be an external event is actually a product of many poor or failed internal processes. It means one risk can lead to another. That phenomena, although troublesome to the business, is a form of contagion, and requires an approach to ensure containment. Most susceptible to contagion are operations that impact customers. New regulation, the emphasis on consumer advocacy, and the increased role of governments in the financial industry have led to countless lawsuits, large fines, and a new climate for reputational danger to financial firms. These new perils do not come from credit or market exposure directly, but rather stem from how firms conducted business and impacted customers. This is operational risk at work, and firms that are better at handling it are increasingly at an advantage.

Operational risk does not involve a direct capital deployment with the opportunity of an investment gain. Losses from operational risk are not due to bad loans or to holding volatile assets. The risk occurs because something undesirable resulted in an expense, fine, judgment, or other loss to the firm. Furthermore, there is no market or counterparty in operational risk, the loss cannot be renegotiated, and payment cannot be prolonged. In fact, operational risks are often detected long after issues emerge, and such issues are frequently intertwined and correlated, meaning that one form of operational risk increases the exposure to more risk.

Operational risk is at its core, a mistake, error, or hazard. Operational risk is embedded in how the enterprise functions, and are often driven by people and IT systems that do produce errors [Cruz (2002)]. Operational risk is not strictly the product of an internal decision process. But rather it is manifested through the complex web of employees, products, clients, systems, legal judgments, regulation, and fines. Operational risk is never really anticipated, but firms must be prepared for it as part of an enterprise risk management strategy. Perhaps the most challenging feature of operational risk is that it is not necessarily easy to identify once it has happened. Decisions that involve the implicit acceptance of operational risk may not clearly expose the

operational risk involved. Lastly and perhaps the most important reason to focus on operational risk is that it remains a material cost to the enterprise. It directly impacts profitability and needed capital.

3. Operational Risk in Financial Services

In the banking and financial services industry, the Basel Accords define operational risk as that risk coming from "inadequate or failed internal processes, people and systems, or from external events." In many ways, this broad definition does not focus on the causes of operational risk or even the ways to avoid or prevent it. Operational risk is driven by the firm's operations, not the firm's investments or other deliberate deployments of capital to seek a profit. Operational risk is often said, "*to be the cost of doing business*" or simply a byproduct of business activity. In many ways that is true. It is not separable from the act of doing business, as it is also embedded in other activities undertaken by the enterprise. This is especially dangerous, as a business manager does not explicitly take on operational risk, as he or she would do for market risk or credit risk. Instead it shows up in how the business is executed. Operational risk also can lead to additional regulatory and reputational harm, meaning that operational risk shows the dangerous feature of contagion. It gives rise to new or additional risks. This is especially true when the operational risk in question is left unattended by management.

3.1. Operational Risk in Market Risk – Trading and Fulfillment Processes are Critical

Market risk is related to the action of taking a position in an asset. The actions of purchasing that asset, managing that asset, and then liquidating that asset are full of operational risk. This is most critical for investment banks and similar firms that trade client money, or other brokers and custodians that execute trades. Such processes require critical systems to settle and fulfill trades. Holding assets like real estate or even patents can involve many managerial decisions – all ripe with possible errors or other mistakes that can result in losses. In general, operational risk that is lurking in the processes of market risk is seen as market losses that are unanticipated. Consider a trade that is execute a few minutes (or even micro seconds) late. The error in this can be from one of many operational challenges. The delayed trade can result in the asset being traded at a lower than anticipated price, resulting in a divergence from the actual market gain from the anticipated market gain. Investment banks and brokerage firms are well aware of the critical trading processes that must be in place to execute trades as promised. Such processes are now highly automated and driven by algorithms, bringing

higher scale and leverage to operational failures, as an algorithm or process may in fact touch millions of customers or trades. In short, operational risk can hide as unexpected or deviant losses in market risk. Identifying it as operational risk requires understanding small deviations that can come from trading processes. Without that definition and inquiry, operational risk in such activities may result in trade losses or perhaps result in a lawsuit from a client alleging poor execution of trading decisions.

3.2. Operational Risk in Credit Risk – Processes for Loans are Critical

For banks, credit risk also involves an investment. It involves transferring cash into a future receivable. The selection of the loan and its terms are therefore paramount to the banking business. The process of selecting a credit risk is generally contained by a lending policy and ensured by an underwriting procedure. In such critical processes, a bank or lender looks to data about the borrower, applies economic models to determine the credit risk under economically stressful conditions, and perhaps even puts in place conveyances on the borrower to further control the credit risk. In all of these processes, we find operational risk lurking.

Consider a bank that issues mortgages and forgets to confirm borrower income or disregards the confirmation of the borrower income during the loan application. This form of operational risk occurred during the real estate boom leading up to the Great Recession. The missing information meant that credit information was subject to error and misrepresentation. The error was not due to a credit policy but rather to an operational failure to confirm data. This is a process failure and is clearly an operational risk: the bank experiences increased loan default. The loss and impact from this error is not easily identified as an operational cost. Rather, it is manifested in higher loan delinquencies than the bank predicted at the time of loan origination. The signs of increased credit risk may be in the form of late loan payments or no payments at all, which may be an early-warning sign of default. Managing the credit risk does not fix this missing data problem of the delinquent loans. Nor does fixing the problem in this mortgage example come from changing the credit policy, but rather it is fully resolved by changing the process for confirmation of a borrowers' income. This confluence of risks makes operational risk detection even more difficult. The impact of such an operational risk is seen as negative performance, relative to pre-issuance credit expectations. More dangerously, the impact of the error may not be seen for years or decades, making detection challenging, if not impossible, to separate from the credit risks of the product.

Indeed, the challenge that we see in the postmortem of the Great Recession is that firms might have had sound credit risk policies in principle, but poor data about the borrower and poor

processes for executing the credit policy. Some define this as model risk, but in reality, the processes for confirming borrower data were not in place, and/or follow-up surveillance on the borrower was not conducted. These are critical process failures and indeed operational risk. Operational risk in a credit book does not jump up and announce itself. Instead, operational risk in a portfolio of loans means that the bank has accepted credit risk that was unintended. It might be accepting more loans that anticipated or loans of a true credit quality that was not otherwise detectable. The losses seen from these failed processes are, therefore, seen as larger credit losses than anticipated or losses that occur more quickly than anticipated. For the insurance industry, the operational risk embedded in the product formulation is known ahead of time, and larger claims than anticipated can be especially problematic for insurance firms seeking asset-liability matches in the future.

4. Operational Risk – Causes and Sources

Excellence in managing operational risk requires revealing the risks embedded in business decisions. For banks, this means that managing operational risk brings greater focus to the credit and market risk functions, as unexplained or unexpected credit and market losses are reduced. As mentioned before, unlike credit and market risk, operational risk is not measured by looking at a borrower or a market, or by relying on economic assumptions. Instead, operational risk is tied to a failure that results in a cost to the firm. There is a challenge in managing operational risk because for many firms, the measurement of the means remains less important than the measurement of the ends. Operational risk requires understanding the means and the path to the outcome. This, therefore, relegates operational risk to a poorly understood form of risk, even though it is largely embedded in every business decision and possesses a threat to the enterprise overall.

With the Basel framework in place, financial service firms calculate the needed economic capital for operational risk, but look at risk types across various lines of business. The operational risk loss types are outlined in the following table [BCBS (2006)].

Types of operational risk	Examples
Internal fraud	-Unauthorized transaction resulting in monetary loss -Embezzlement of funds
External fraud	-Branch robbery -Hacking damage (systems security)
Employment practices and workplace safety	-Employee discrimination issues -Inadequate employee health or safety rules
Clients, products, and business practices	-Money laundering -Lender liability from disclosure violations or aggressive sales -Disagreements with clients -Poor product execution
Damage to physical assets	-Natural disasters, e.g. earthquakes -Terrorist activities
Business disruption and system failures	-Utility outage (e.g. blackout)
Execution, delivery, and process management	-Data entry error -Incomplete or missing legal documents -Disputes with vendors/outsourcing

Table 1: Types of operational risk in the Basel framework (Source: BCBS, 2006, "International convergence of capital measurement and capital standards," Basel Committee on Banking Supervision.)

Of these loss types defined by Basel, one is worthy of special attention, given its broad reach and importance to customer-facing interactions: *Clients, Products, and Business Practices.*

Clients, Products, and Business Practices: In the operations of a financial services firm, there are many opportunities for product misuse, client requests, and business practices to pose risks. Moreover, the interpretation of product terms, the enforcement of product terms, and the action by banks and insurers against customers are all grounds for disagreement and litigation. The foreclosure processes of many banks in the wake of the Great Recession are perfect examples. Many lawsuits ensued. In total, these risks are typically seen through lawsuits against the firm, or may be enforced by regulatory action too. Product policies can be viewed after issuance, with a new lens on what is appropriate to the customer, causing new risks to the firm. Clients, too, may pose unique risks, such as conducting money laundering or transfers that put the firm at risk of regulatory or accounting inquiry. For both banks and insurers, as research by Cummins et al (2004) shows, *Clients, Products, and Business Practices* is the predominant form of operational risk.

The most advanced forms of calculating economic capital for operational risk look to historical data on firm losses from operational risk and other industry loss events to provide a basis for

predicting the level of operational risk in the future. Indeed, such data is used to map operational risks to economic capital calculations that build on the Value-at-Risk concept used in market and credit risk management. It appears that this is more a move to consistency and convenience rather than one to formally reduce and remove operational risk. Indeed, the process of calculating economic capital for operational risk does not provide an explanation for the operational risk, leaving the path to the error undefined, and the ability of the firm to remove the operational risk weakened.

In recent years, we have seen operational risk increase in financial service firms [FRS (2005)]. The losses are not generally attributed to the attention-grabbing and scandalous rogue trading cases that we can all name. Instead, operational risk in banks and insurers is highly tied to the interaction with clients and the execution of products (as from the Basel-defined loss type). In research by Cummins et al. (2004) and Cummins et al (2007), the manifestation of operational risk in U.S. insurers is almost entirely in the 'Clients, Products' category. In Figure 1, actual operational loss data from U.S. insurers was examined. The category of 'Clients, Products' dominates in both frequency and severity, indicating that for insurers, operational risk is highly dependent on interfacing with customers.

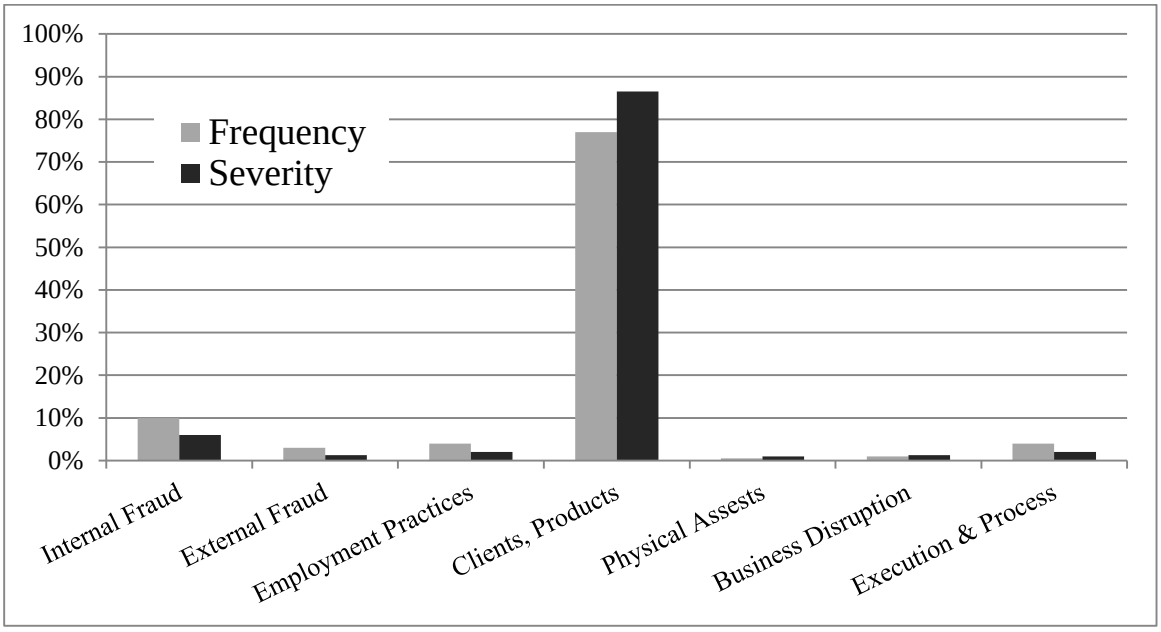

Figure 1: Operational risk event by event type: U.S. insurers [Cummins et al (2004)]

The concentration of the occurrence of operational risk differs between insurers and banks. For banks, 'Clients, Products' also produce the largest form of operational risk, however, 'Internal Fraud' generates a much higher risk in banks than in insurers. Specifically, operational risk stemming from 'Clients, Products' comprise about 60 percent in frequency and severity, while 'Internal Fraud' comprises approximately 25 percent in frequency and severity at banks.

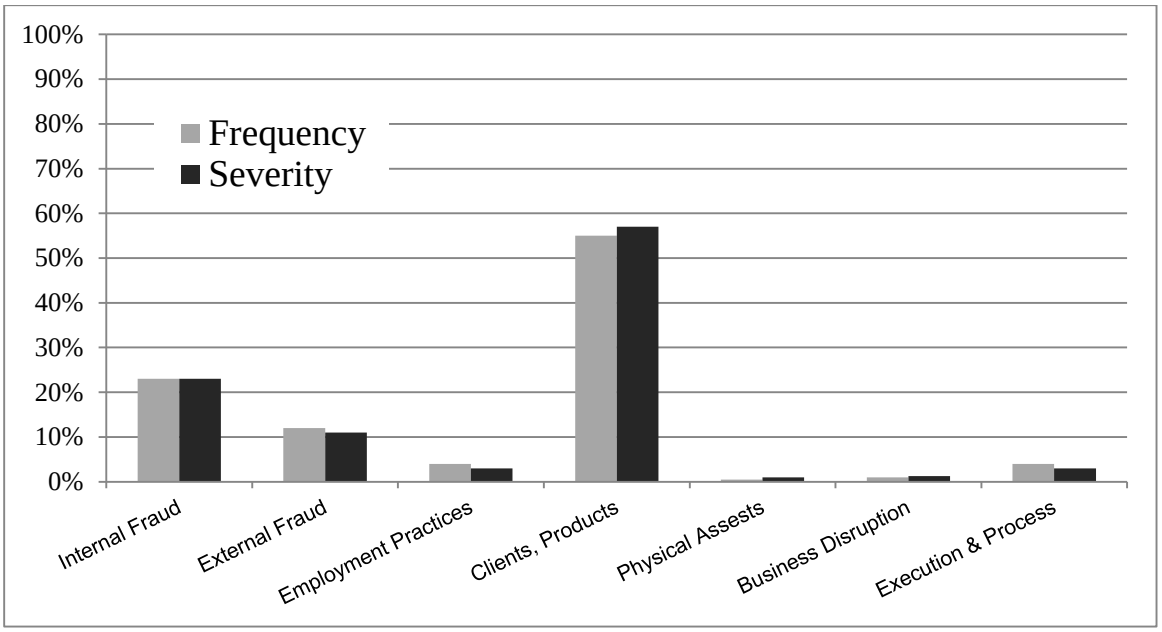

Figure 2: Operational risk event by event type: U.S. banks [Cummins et al (2004)]

For insurers, risk from 'internal fraud' is less than 10 percent in severity and frequency (Figure 1). These differences between banks and insurers are because of the more active trading role found in banks (especially investment banks) and the ability for bank employees to trade in large sums. Many risk managers would point to the fraud cases of Barings Bank and Société Générale as prime examples of this point [Walker (2013)]. The research by Cummins et al is even more telling in that operational losses highly occur in business lines that are tied to customer interactions. Figure 3 shows the operational losses by line of business, where retail banking and retail brokerage show some of the greatest operational risk levels.

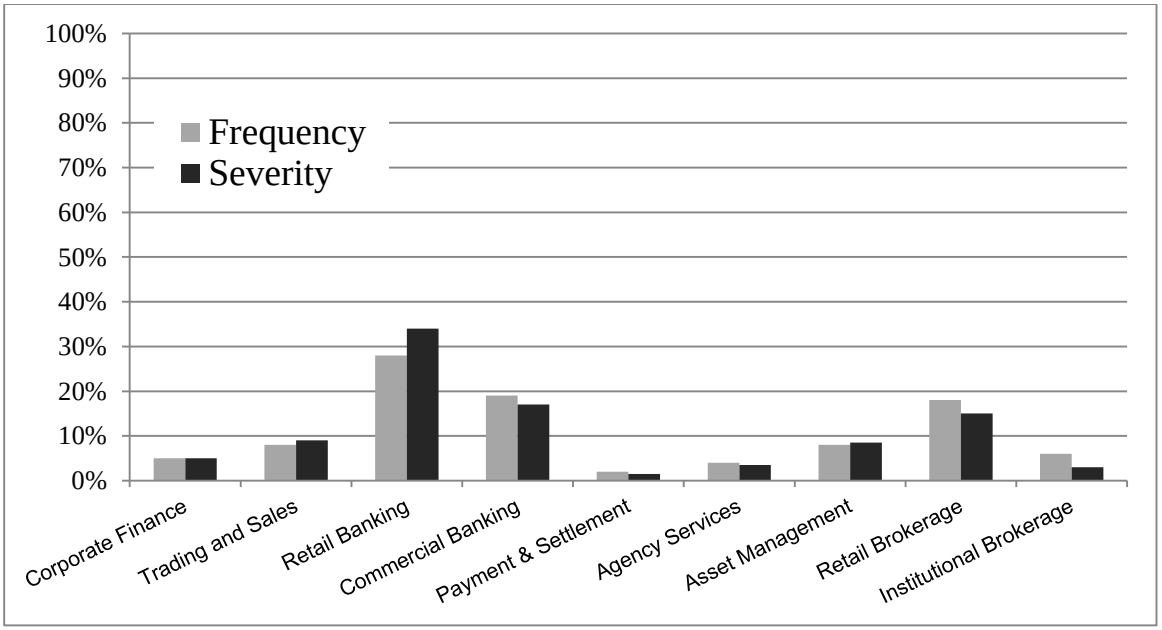

Figure 3: Operational loss events by line of business [Cummins et al (2004)]

5. Increasing Drivers of Operational Risk

Operational risk is increasing in frequency and severity [Cummins et al (2004), De Fontnouvelle et al (2006), and FRS (2005)]. Recent losses and the increased regulatory attention in both the US and Europe suggest that operational risk loss events through fines and penalties have never been greater. The drivers behind this increase in operational risk, include: Increasingly Complex Operations, Development of New and Untested Products, Automation and Digitization, Increasing Reputational Impact from Operational Risk, New Focus of Regulators on the Treatment of Customers as Victims, and lastly, Cyber Risk.

5.1. Increasingly Complex Operations

Operational risk is inherent in the firm's selection of a client, country, technology, or system. Operational risk increases as systems and processes become more complex and less understood. Today, financial service firms have more complex IT operations, reliance on outsourcers, new products in mobile and Internet banking, all which are drivers to increased complexity and trends which are expected to continue.

Modeling the complexity of a system requires an understanding of how it fails. Since operational risk is often the result of an unpredictable or a not-fully understood failure mechanism, predicting operational risk remains a challenge.

Managing operational risk requires an engineering-like understanding of systems, processes, and failure mechanisms. Sadly, most businesses do not invest enough to understand processes and systems in such a granular level, especially when the systems and processes are secondary to the business models or goals. This is at the core of cyber risks and data breaches. For most firms, the security of data is a secondary process to running a bank or retailer. As we have seen, the details and complexity in managing data assets is of grater importance than ever. Cyber risk, in particular, is an operational risk that is full of complexity and rooted not just in the capabilities of an external fraudster but the internal processes and defenses of a firm.

5.2. Development of New and Untested Products

The financial service industry has been highly innovative in bringing new products to market. In general, the proliferation of new loan instruments, derivatives, and payment mechanisms have brought advantages to users and the issuers. However, these products are not easily customer or market-tested. Most retail banks are now pressing to issue new mobile banking tools, more on-line capabilities, and a general reliance on banking services through digital

forms. This has many advantages such as cost reductions to both the user and banks. However, it increases fraud and errors that can be propagated across millions of accounts. Additionally, new consumer-focused bodies in the US, such as the Consumer Financial Protection Bureau, are reexamining the treatment of customers by financial institutions. At the core are the products and processes offered by banks. Operational risk in these areas become an increasing concern if limited or no testing occurs. Market pressures to innovate will push more institutions into offering products before the operational risk is fully understood.

5.3. Movement to Automation and Digitization

The Internet changed how we buy, shop and bank. Most customers expect to conduct all banking services online, including complex loan applications. For banks, this is the new norm. Customers rarely ever interact with a bank employee (and actually might not want to do so). Removing human discretion does remove error and therefore operational risk. So, automation and digitization should be good for reducing operational risk. In part, such movements do reduce the frequency of errors of operational risk. However, due to the implicit scale in using automation, millions of accounts can be impacted with the same error, making the severity of operational risk losses from automation much greater. This is at work in the fraud and data breach cases in recent years.

Additionally, the customer is empowered with the tools of the Internet and the high velocity of data transfer. With the advent of e-mail and social media, it has never been easier for a customer to spread his or her displeasure, discontent, and experience with other customers and to bring their experience to the attention of regulators. Additionally, the speed at which this can happen has never been greater. As more and more of the process of banking becomes automated and delivered by mobile devices, the importance of excellence in operations will surely increase.

5.4. Increasing Reputational Impact from Operational Risk

Operational loss events are largely ones that impact customers and the firm's ability to conduct business with the customer. When mentioning reputational risk, most firms worry over the potential loss of customer trust, which has been built over many years. Firms that have trust as their major assets are especially sensitive to reputational harm. This explains why the accusations against the audit and accounting firm Arthur Andersen proved so tumultuous. For the financial services industry, trust is paramount. Firms that violate that or have left distrust in the eyes of customers suffer reputational harm. In many ways, this harm is amplified because

customers may now broadcast their negative opinions through social media, and regulatory bodies are listening more than ever to such complaints.

Reputational risk is challenging to enumerate, because it is unclear which constituents will react negatively to the firm and to what degree they will do so. Consider the following definition of reputational risk: "Reputational risk is the potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions." Investment to overcome reputational harm is generally expensive and may indeed be impossible. Reputational risks linger over a long period of time and are implicit in the business operations of the firm. Reputational damages are not driven by credit risk or market risk, but rather by the customer's experience and opinion of how he or she was treated, which is related directly to internal processes and shows that operational risk is the often origin of reputational harm.

5.5. New Focus of Regulators on the Treatment of Customers as Victims

An unfortunate feature of risk contagion is that it often activates a risk that is driven by external forces. In the financial services industry, the inherent disagreements that arise between the firm and customer often lead to reputational and regulatory risks. The danger of this contagion is that operational risk (to the extent that it is driven by internal processes and systems) is controlled largely by the actions of the enterprise. Once the risks give rise to another risk driven externally through contagion, the control mechanism is lost. The fate of the firm is, to some regard, put in the hands of customers, regulators, investors, etc.

Preventing risk contagion is a key benefit of effective operational risk management in the insurance industry. As the research illustrates, most operational risk is due to 'Clients, Products' and is realized as legal or regulatory fines. Regulatory and reputational risks share an important and unfortunate similarity: they are often perpetuated by an offended or motivated agent (regulator or customer) seeking a judgment or penalty against the firm. Regulatory risks generally reference or involve customer harm. The economic impact of these risks means that firms must manage reputation and regulation through a series of on-going activities. These risks, when manifested, cannot be directly controlled by the firm through internal operations.

The recent movement by U.S. and European governments to consider new regulation in financial services and other consumer-facing industries has drawn new attention to the reality of regulatory risk. In many ways, regulatory risk can be viewed as a game changer in the industry in that it can help some market participants and harm others. Specifically, regulations

may not be objectively applied and may even be directed at specific market participants for political or economic reasons. Reversing regulation, while not impossible, is difficult and expensive as it often becomes ingrained in U.S. code. Regulatory risk may arise for many reasons, but it is more often caused by customer concerns about practices by a specific firm or an entire industry. The rise of the Consumer Finance Protection Bureau and provisions in Dodd-Frank, the Credit Card Act, and the general swing towards protecting consumers against financial service firms is unlikely to reverse anytime soon and is more likely to bring additional focus on the treatment of the customers by financial firms and the operational risks that are derived from those interactions.

5.6. Cyber Risks

Recently, we have seen a wave of large-scale data breaches that have impacted firms of all sizes, and left most of us wondering if data breaches should be considered as the new normal. The large data breaches at Target and Home Depot, to name a few, have led us to question if retailers and other not data-centric firms are simply not prepared to handle the complexity of data breaches. Again, critical operations, such as credit card processing and the custodianship of credit card details can impact customers. It is an example of how seemingly small process failures can lead to large operational losses.

Cyber risk is complex. Understanding the pathways and vulnerabilities to a breach are many. Fraudsters are sophisticated and see and earn real value by stealing credit card numbers and other digital data assets. It will be an on-going battle. For many of the recent data breaches, a few troublesome similarities suggest that cyber risk had been underestimated. In the TJ Maxx company data breach (the largest credit card data breach before Target), a deliberate decision was made to not upgrade data security protocols, given the cost of doing so and the perceived low probability of a data breach [Walker (2013)]. In many of the cases, the hacker or fraudster entered by a means unanticipated or unknown to the firm. In the case of the Target, it appears that a vendor's access to the store's data system was the path for the hackers. Banks have experienced large-scale breaches, as in the data breach at JPMorgan Chase in which some 70 million passwords were compromised. Banks are also exposed to the operational risk at merchants, as full reimbursement for fraudulent charges stemming from a breach will be impossible for a bank to recover. For many firms, developing and maintaining a world-class data security team to match the capabilities of hackers is unattainable, suggesting a need for deploying best in class technologies.

6. Conclusion

Operational risk is increasing in importance, owing to its ability to impact a firm's reputation and its relationship with its many constituents (shareholders, customers, and regulators). Operational risk losses are increasing in frequency and magnitude, confirming that more operational risk is being realized. The processes and procedures that define the treatment of the customer and the interaction with the customer are ones that pose the greatest operational risk. Consumer lending and consumer brokerage show some of the highest operational risk levels and operational risk is greatest in Client, Products, and Business Practices. This reality of operational risk is most troubling as it can directly impact customers and lead to increased reputational harm and regulatory scrutiny. Needless to say, preventing and reducing operational risk directly improves a firms footing with reputational and regulatory risks.

The financial services industry relies on automation, digitization, and product innovation for growth and cost savings. These drivers and others are leading to increased operational risk, especially in the servicing of customers and the interaction with them on digital systems. Expect more operational risk to arise from Increasingly Complex Operations, Development of New and Untested Products, Automation and Digitization, Increasing Reputational Impact from Operational Risk, New Focus of Regulators on the Treatment of Customers as Victims, and Cyber Risk. All of this signals that the management of operational risk ultimately is tied to preventing reputational and regulatory harm and now assumes a greater position in the enterprise risk management of firms.

References

BCBS, 2001, “Working Paper on the Regulatory Treatment of Operational Risk.” Basel Committee on Banking Supervision

Basel Committee, Sound Practices for the Management and Supervision of Operational Risk," 2003. Bank for International Settlements

Cruz, M., 2002, *Modeling, measuring and hedging operational risk,* West Sussex: Wiley

Cummins, J. D., C. M. Lewis, and R. Wei, 2004, “The market value impact of operational risk events for U.S. banks and insurers,” Working paper, 23 December

Cummins, J. D., R. Wei, and X. Xie, 2007, “Financial sector integration and information spillovers: effects of operational risk events on U.S. banks and insurers,” working paper, 20 August

De Fontnouvelle, P., V. De Jesus-Rueff, J. S. Jordan, and E. S. Rosengren, 2006, “Capital and risk: new evidence on implications of large operational losses.” Journal of Money, Credit and Banking 38(7), 1819-1846

Federal Reserve System. Results of the 2004 Loss Data Collection Exercise for Operational Risk May 12, 2005

The Financial Crisis Inquiry Commission, 2011, “The Financial Crisis Inquiry Report, Authorized Edition: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States.”

Knight, Frank, 1921, *Risk, uncertainty and profit,* Cornell University Library

Walker, Russell, 2013, *Winning with Risk Management*, World Scientific Publishing Company