Toward a Decision Support System for Measuring and Managing Cybersecurity Risk in Supply Chains

Wade Henderson Baker

Dissertation submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
In
Business Information Technology

Loren Paul Rees, Chairman

Deborah F. Cook

Lance A. Matheson

Cliff T. Ragsdale

Linda G. Wallace

January 27, 2017
Blacksburg, VA

Keywords: cybersecurity, cyber security, information security, cyber risk, information risk, risk modeling, risk management, security metrics, decision support systems, supply chain management, supply chain risk, supply chain information sharing

Toward a Decision Support System for Measuring and Managing Cybersecurity Risk in Supply Chains

Wade Henderson Baker

ABSTRACT

Much of the confusion about the effectiveness of information security programs concerns not only *how* to measure, but also *what* to measure – an issue of equivocality. Thus, to lower uncertainty for improved decision-making, it is first essential to reduce equivocality by defining, expanding, and clarifying risk factors so that metrics, the "necessary measures," can be unambiguously applied. We formulate a system that (1) allows threats to be accurately measured and tracked, (2) enables the impacts and costs of successful threats to be determined, and (3) aids in evaluating the effectiveness and return on investment of countermeasures. We then examine the quality of controls implemented to mitigate cyber risk and study how effectively they reduce the likelihood of security incidents. Improved control quality was shown to reduce the likelihood of security incidents, yet the results indicate that investing in maximum quality is not necessarily the most efficient use of resources. The next manuscript expands the discussion of cyber risk management beyond single organizations by surveying perceptions and experiences of risk factors related to 3rd parties. To validate and these findings, we undertake in an in-depth investigation of nearly 1000 real-world data breaches occurring over a ten-year period. It provides a robust data model and rich database required by a decision support system for cyber risk in the extended enterprise. To our knowledge, it is the most comprehensive field study ever conducted on the subject. Finally, we incorporate these insights, data, and factors into a simulation model that enables us study the transfer of cyber risk across different supply chain configurations and draw important managerial implications.

Toward a Decision Support System for Measuring and Managing Cybersecurity Risk in Supply Chains

Wade Henderson Baker

GENERAL AUDIENCE ABSTRACT

This dissertation comprises several manuscripts exploring various topics under the overall theme of cybersecurity risk in supply chains. The first topic presents the difficulties involved in measuring risk in the cybersecurity domain and discusses how this hinders firms in making justified decisions and taking appropriate actions to manage risk. We then examine the quality of controls implemented to mitigate cyber risk and study how effectively they reduce the likelihood of security incidents. Next, we survey firms to explore perspectives and experiences related to security incidents involving their supply chain partners. To validate these perspectives, we then analyze data collected from over 900 forensic investigations of real-world breaches. This provides excellent visibility into how 3rd parties cause and contribute to incidents in supply chains and key risk factors. Finally, we incorporate these insights, data, and factors into a simulation model that enables us study the transfer of cyber risk across different supply chain configurations and draw important managerial implications.

ACKNOWLEDGEMENTS

Thoughts of and work on this dissertation began in the fall of 2003 and continued—through doldrums of varying sorts and lengths—until my defense in January of 2017. I cannot begin to recount all those who have contributed to it and supported me over the years. But I feel the need to at least make an attempt, so here goes:

I thank God for opening doors that I could have never budged and granting me success far beyond my abilities.

Thanks to my parents (directs and steps), who gave me everything I needed (and more) and convinced me early on that I could succeed at anything I put my mind to.

My incredible wife has been supportive of this effort to a measure that is beyond words. She tolerated my absence on many nights and weekends and trusted me when I said that I would need to quit working for several months in order to get it done. Emiley—I don't know what we'll do with all the extra time now, but I sure look forward to it!

To my five children—all of whom have been born since I started this dissertation—you guys slowed me down a bit, but you build me up everyday. Let's go play.

I absolutely must call out Dr. Loren Rees for going WAY above and beyond in his patience, guidance, wisdom, friendship, encouragement, and support over the years. Same goes for Dr. Cliff Ragsdale, whose invaluable support started even before my doctoral program began when he helped me move stuff into a storage unit for the summer. People (and professors) like them are in short supply. There's no way I'm typing this today without them. I sincerely thank you both.

Thanks to my committee for not forgetting who I am or giving up on me between my proposal defense and final defense.

Few doctoral students have the opportunity to blend their academic and professional careers to the extent that I have done. That all began when Peter Tippett, then Chief Technology Officer of TruSecure, answered an unsolicited email from a lowly grad student looking for real-world data to use in his dissertation. When I consider all that has come about in the wake of that kind act, it is rather amazing. Thank you, Peter.

Last but not least, thanks to all the many colleagues and professors who have contributed in innumerable ways to my research and work in the field of information security. Dave, Chris, Marc, Alex, and Jay – you all deserve special mention, but unfortunately, I'm out of space to recount all the reasons why. I owe you one (or many).

TABLE OF CONTENTS

Chapter 1: Introduction

Over the last few decades, organizations have sought to become more efficient and productive through the rapid adoption of information and communication technologies (ICTs). As ICTs become more common, the intrinsic value of these systems becomes dwarfed by the mission-critical functions they support (Saydjari, 2004). This intimate relationship between technology and business functionality has proven to be an incubator for a dramatic rise in costly ICT-related incidents and failures leading to increasingly costly impacts. In light of this, organizations are more aware of the growing risk and the need to take appropriate action, but struggle to identify what those actions should be, how to prioritize them, and how to measure their effectiveness.

Seeking to protect the confidentiality, integrity and availability of business functions supported by ICTs, the information security industry now boasts an extremely large and diverse set of products, services, tools, processes, and policies. Leveraging this array of controls, many organizations have begun formal security management programs to protect themselves, their partners, and their customers. The high cost of time and money associated with the implementation and maintenance of these controls places pressure on security leaders to distinguish between those that are necessary and those that are less critical. Moreover, identifying the optimal level at which each individual control should be implemented is a delicate balance of risk reduction, cost efficiency, and business enablement. Although the security industry has taken steps toward this goal, across-the-board products lack important features necessary for true management decision support for investing in and deploying information security products and practices.

Information Security Management

The predominant tactics against cyber threats and vulnerabilities have historically relied on technological innovations. New security products were purchased and deployed in hopes of locking down network infrastructure, thereby allowing a safe perimeter in which to conduct business. This seems entirely reasonable given that the assets being protected are highly technical themselves. When used correctly, these techniques can go a long way to reduce the risk of security incidents within the enterprise. As successful and sophisticated as these solutions have become, the problem of information security has not been solved using technical

approaches alone. There are many reasons for this, but the foundation of the problem has been sluggish recognition of the integral relationship between solid security strategies and overall business objectives. In an environment of uncertainty and risk, businesses and IT architectures and processes are far from working in harmony and thus often perform well below their capabilities. META Group analyst Louis Boyle says: "A large percentage of organizations do not yet have this holistic view of IT spending…business units do not work together, and thus are prevented from fully leveraging their investments. In contrast, leading organizations do have a unified technology portfolio investment strategy that is driven by top-down from senior management (Lynn, 2003)."

As it has matured, the information security industry has steadily spread from mostly technical solutions to encompass more recent trends that recognize the importance of a holistic approach to securing assets on an enterprise scale. Companies are now using proven business strategies in combination with technologies and devices to provide a strong, well planned enterprise-wide security posture. Current implementations of these systems have a great deal of functionality and incorporate all levels of the organization. Automated security management solutions have been rolled out from the big names in the security industry, most utilizing a combination of hardware and software that constantly monitors activity across the environment.

Nevertheless, key functionality essential to management decision making has not yet been developed. And although many of these solutions claim to have predictive capabilities, these claims merely reference an ability to recognize vulnerabilities present in the network infrastructure and to 'predict' where problems will occur if left unchecked. Most solutions allow business and IT management to assign values to assets based on their importance to the enterprise and these considerations are then combined with sensors configured to alert IT staff to the presence of known vulnerabilities within these assets. These tools often incorporate some form of risk assessment and provide security staff with valuable insights. Management can then generate summary reports that aid in strategic planning.

Economic Models for Information Security

Approaches like those described above do indeed represent forward progress in intrusion prevention and asset management, yet security incidents continue to drain resources. As funds become tighter, strategic allocation and purchasing of technology products depends on the ability

to separate essential investments from those that are discretionary, superfluous or counterproductive (Carr, 2003). Because of this trend, the primary challenge is not technical advancement as much as finding the optimal balance between security investments, risk tolerance, and business needs. There is a growing base of literature focused on economic modeling and risk analysis in information security, including work by Gordon and Loeb (2001 and 2002) on economic models, a game theoretic approach by Cavusoglu, et al. (2004), and Jaisingh and Rees' (2001) work using Value at Risk. The basic premise of this stream of research concerns leveraging various models to locate the point at which "the most security bang for the buck" is achieved.

The difficulty in doing this, however is that these cost-benefit analyses in security depend on being able to accurately assess information security risk and assign numerical values to the benefits achieved (Geer, 2001). To date, there is widespread disagreement around the many approaches and calculations to evaluate this, which effectively creates a road block to any methodology depending on such assessments (Ozier, 2003). A survey by Network Computing corroborates the need for such research; managers cited limited budgets and unclear return on investment as the top two impediments to implementing new technology (Joachim, 2003).

Due to a lack of reliable and accessible data, analyses of information security risk and return on security investments (ROSI) have been weighted toward qualitative processes to date (Blakely, 2001). Although qualitative analysis can provide some level of value, it falls far short of supporting the complex decisions security leaders must make. Bruce Claflin, then President and CEO of 3Com, states (Clarifin, 2001):

> "I believe ROI analysis of security is possible and I demand it for all security spending…Quantification of risk avoidance is essential. In some instances, the investment is clear, but the tangible benefit of cost avoidance is undefined. When someone in the organization waves their arms and cries 'We're at risk!' but doesn't clearly define the results or attempt to quantify that risk, the argument loses momentum."

When paralysis stemming from uncertainty is combined with the already volatile status of the threat landscape, a recipe for disaster has been prepared. For these reasons, a system must be devised that provides managers with the capability to confidently direct their security programs amid a highly technical business climate that allows little room for mistakes.

Decision Support for Information Security

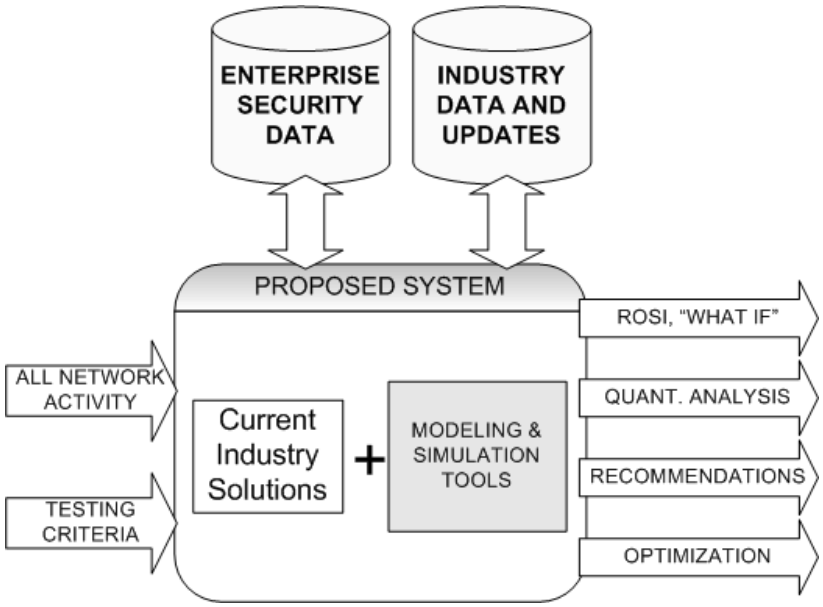
An ideal information security decision support system (DSS) would offer all the functionality and scope of existing operational security tools plus the added ability to fully support strategic analysis and planning applications for senior management. While admittedly such a prescription seems obvious, it should be noted that a solution of this magnitude is nonexistent. Not only is this concept theoretically ideal, it is practically attainable. Security companies have produced very powerful tools for monitoring and managing information assets, and they are perfectly suited for collecting the data necessary to support quantitative modeling and analysis. The advantage of access to data gathered in this way over generic industry data – even if it were available – is that it provides a customized picture of enterprise security activity over time. The longer the system is monitoring and logging information, the larger and more reliable the data set, thus opening the door for actuarial techniques to be applied to information security. Managers are thus supplied with the factors needed to measure risk, prioritize security initiatives, simulate outcomes, optimize investments, evaluate ROI, and other heretofore elusive types of analysis.

Computer simulation capabilities are not offered in current security solutions, but they are not unheard of in the security arena. Several industry tools provide extensive architecture mapping and configuration combined with the ability to simulate attack events, purchase and deploy equipment and conduct "what-if" scenarios. Some of the applications falling in this genre represent the closest manifestation of successfully blending powerful managerial support functions with simulation abilities for information security, but still fall short of a holistic security solution. Most of these simulation packages are inherently focused on network-level security rather than taking into account enterprise-level assets and business processes. Though they are missing from simulation tools, it is important to note that these features are available in security management systems discussed previously from popular security solution providers, etc.

The perfect security solution therefore will combine benefits from current packages that include enterprise security monitoring, intrusion prevention, policy enforcement, employee management, and report generation with powerful features available in computer simulation packages. Tools from both camps are getting more sophisticated, but need to be pulled into one unifying solution to adequately combat the information security problem and to supply management with tools to optimize enterprise security posture. Figure 1 illustrates the

components and processes of a full-featured security DSS following the principles discussed to this point. All enterprise security activities and incidents are constantly monitored and logged.

Figure 1. A conceptual DSS framework for information security management.



There are many advantages to such a system. It would bridge the "Real-time" and "historical" abilities of security packages with the "uncertain" and "future" scope of simulation packages. Another possibility is the creation of an industry-wide, web-based knowledge pool that could be used by all organizations using the system. Naturally, data submitted by individual organizations would be stripped of sensitive content, before being uploaded. Information and testing results about new security products could be downloaded as an update feature to the system, simulating the effect of their integration before actually doing so. ROI procedures in which time periods would be simulated and effects on the bottom line evaluated is a very powerful option. As management proposes changes in business processes, procedures and policies that potentially affect information security could be analyzed before they go into effect. The system itself would be able to recommend changes that it sees as being advantageous and could back these recommendations with ROI estimates and improvements in security posture. Probing capabilities could utilize optimization techniques to detect redundant systems and inefficient configurations. Changes to network infrastructure, operating systems, patches and applications are all within the scope of such a security solution.

The information security industry is beginning to embrace the concept that successful security must permeate an organization's assets, people, goals, etc. Even processes that are seemingly disconnected from the security realm must be evaluated on their potential impacts on an organization's security posture. The cost of uninformed and unsupported decisions is simply too great. If reliable ROI cannot be meaningfully performed in security purchasing and deployment decisions, then pitiable investments, poor configurations, and liability issues will drive many companies out of business during the next few decades. Hard-line quantitative analysis and modeling of information technology and security within the context of enterprise business are essential components of a security DSS.

Statement of the Problem and Research Contribution

As mentioned, information security risk has increased dramatically over the last few years. The management of information security risk has been hampered by poorly-understood risk factors, unavailability of quality data driving those factors, and a lack of rigorous metrics and quantitative models. Consequently, the risk has not been satisfactorily measured or mitigated in either private firms or public sector agencies—not to mention the additional problems introduced when multiple organizations are connected in a supply chain.

This dissertation addresses these concerns by first developing an approach that will make the measurement of risk less equivocal. This is done by defining, expanding, and clarifying risk factors so that metrics can be unambiguously applied. This dissertation formulates a system that (1) allows threats to be accurately measured and tracked, (2) enables the impacts and costs of successful threats to be determined, and (3) aids in evaluating the effectiveness and return on investment of countermeasures.

With a measurement scheme in place, the dissertation next studies how varying levels of investments in security controls affect the likelihood of security incidents. This is a key aspect of risk modeling and decision-making because it demonstrates that countermeasure effectiveness behaves differently as implementation quality increases. This supports the need to optimize security investments to reduce risk because continued spending beyond certain levels will achieve very little additional benefit to the firm.

The third component of the dissertation examines the management of information security risk in the larger context of a supply chain. Even with an individual firm optimally

controlling its own risk, IT interconnectivity with both downstream suppliers and upstream distributors subjects the firm or agency to previously unforeseen levels and types of risk. This research defines the issues pertaining to supply chain information security risk and surveys firms to establish a link between supply chain collaboration and security incidents.

To validate survey findings with real-world observations, the fourth section of the dissertation examines forensic evidence from nearly 1000 data breach investigations over a ten-year period. The findings identify key risk patterns and factors contributing to data breaches in both individual firms and supply chains. Also introduced is a database schema ideal for information risk management and decision-making.

Finally, this dissertation proposes a theory and model of cyber risk in supply chains. Simulation is used to measure the impact of supply chain collaboration and configuration on cyber risk for all firms. Important managerial implications are discussed and recommendations made for future research and practice.

Research Methodology

The research tools in addressing the problems defined above are fairly eclectic, given the ambitious scope of this project. Proper definition of metrics (chapter 2) leverages expert insight and public sources of security data. Control effectiveness (chapter 3) and supply-chain considerations (chapter 4) are facilitated by questionnaires to industry professionals and managers. Analysis of data breaches (chapter 5) pulls from empirical data collected from forensic investigations. Simulation analyses (chapter 6) leverage data from all previous chapters to construct and validate a model of cyber risk in supply chains.

Scope and Limitations

The scope of this study encompasses both the private and public sectors. It addresses the managerial aspects of risk management, but does not speak to the technological issues involved, such as design of firewalls or antivirus software. There are several types of limitations to this work. Because of its seminal nature, only a “first-cut” could be made at metric definitions, model development, and specification of interfaces needed by management. Consequently, models are first-generation, do not include all possible threats, etc. Similarly, the extension of models to

supply-chain considerations is admittedly broad-brush, as the work reported here is essentially the first on information-security risk in this environment.

A second type of limitation is inherent in the methodologies employed. Though random sampling was used to select participants for the various surveys described in this work, the invitation was sent via email, thereby introducing the potential for self-selection bias. The pool of responding organizations is not a representative sample, and survey results – though considered informative – cannot be considered generalizable. The data collected from breach investigations, while quite possibly the most comprehensive ever amassed on the subject, is nevertheless biased in several ways. Namely, it consists of breaches that a) were discovered, b) required 3rd party investigation, and c) were investigated by Verizon. However, comparisons to public breach datasets and other private sources show many parallels that strengthen the claim of relevancy and usefulness of the data for this work.

Plan of Presentation

This dissertation, upon the insistence of my advisor, Dr. Rees, has been written as a series of manuscripts all under the thematic umbrella of the management of cybersecurity risk supply chains. This chapter has served as an introduction to information security risk. It has identified a need for the management of this risk. Chapter 2 defines risk factors so metrics can be unambiguously applied. With this accomplished, a risk model for a firm is outlined. Chapter 3 studies the quality of security controls within firms and the effectiveness of said controls on the likelihood of security incidents. Chapter 4 examines perceptions and experiences related to information security risk in supply chains. In particular, this research presents analysis of an industry survey conducted to empirically examine factors affecting information security risk in supply chains. Chapter 5 presents empirical findings from nearly 1000 data breach investigations. It identifies important factors contributing to breaches for individual firms and supply chains. Chapter 6 proposes a theory of cybersecurity risk in the supply chain and builds a simulation model to explore the impact of collaboration on individual firms and the overall supply chain. Future work is outlined in Chapter 7 of the dissertation.

Chapters 2, 3, and 4 are formatted as journal articles and are meant to stand on their own. Each has its own title page, abstract, and references. Chapter 5 stands on its own as well, but is not in the traditional article form because there is no plan to publish separately. Chapter 6

follows in this mold but will be further developed as an article for publication. References from each chapter have been alphabetically compiled at the end of the dissertation.

References

1. Blakely, B., "An Imprecise but Necessary Calculation," Secure Business Quarterly, Volume 1, Issue 2, Fourth Quarter 2001.

2. Carr, N., "IT Doesn't Matter," Harvard Business Review, 41-49, May 2003.

3. Cavusoglu, H., B. Mishra, S. Raghunathan, "A Model for Evaluating IT Security Investments," Communications of ACM, 47,7 (July 2004), 87-92.

4. Clarifin, B., "Information Risk Management at 3Com," Secure Business Quarterly, Volume 1, Issue 2, Fourth Quarter 2001.

5. Geer, D., "Making Choices to Show ROI," Secure Business Quarterly, Volume 1, Issue 2, Fourth Quarter 2001.

6. Gordon, L. and M. Loeb., "The Economics of Information Security Investment," ACM Transactions on Information and Systems Security, Vol. 5, No. 4, Pages 438 – 457, November 2002.

7. Jaisingh, J. and Rees, J. "Value at Risk: A methodology for Information Security Risk Assessment," in the Proceedings of The 6th INFORMS Conference on Information Systems and Technology (CIST-2001), Miami Beach, Florida, November 2001.

8. Joachim, D., "2nd Annual Survey…We Asked, You Told," Network Computing, pages 35-47 October, 2003.

9. Lynn, D, et al., "2004 IT Budgets: Battling for the Basics," META Group report, October, 2003.

10. Ozier, W., "Risk Metrics Needed for IT Security," Security Pro News, August, 2003.

11. Saydjari, O.S. Multilevel Security: Reprise. IEEE Security & Privacy, 2 (5). 64-67, 2004.

Chapter 2: Necessary Measures: Metric-Driven Information Security Risk Assessment and Decision-Making

Wade Baker
Loren Rees
Peter Tippett
Russ Cooper

Manuscript published in *Communications of the ACM*, October 2007, Vol. 50, No. 10.

Abstract
Much of the confusion about the effectiveness of information security programs concerns not only *how* to measure, but also *what* to measure – an issue of equivocality. Therefore, in order to generate data, and thereby lower uncertainty for improved security-related decision-making, it is first essential to reduce equivocality by defining, expanding, and clarifying risk factors so that metrics, the "necessary measures," can be unambiguously applied. This paper formulates a system that (1) allows threats to be accurately measured and tracked, (2) enables the impacts and costs of successful threats to be determined, and (3) aids in evaluating the effectiveness and return on investment of countermeasures.

1. Introduction

Information technology (IT) is now essential to the modern business environment. Managers are increasingly faced with the balancing act of leveraging the full potential of IT while protecting corporate assets made more vulnerable through it. Following this trend, security incidents have resulted in significant and consistently rising financial losses for many organizations. This is true despite the fact that organizations are spending large amounts of money on security technologies and staff, and despite growing stacks of policy documents, improved practices, training, and certifications. Furthermore, evidence exists that there is often no correlation between increased spending on such initiatives and actual improvements to the overall security record [1]. Personal experience with business leaders around the world suggests that many feel frustration at their inability to identify the highest impact strategies for reducing organizational loss expectancy. Moreover, though there is no shortage of security standards and research, managers often admit that they have no proven and reliable methodology for measuring the effectiveness of their security initiatives or collecting data needed for making strategic decisions and assessing the monetary value of their efforts. Fittingly, the U.S. Department of

Homeland Security recently named a lack of real-world data on risk factors as one of the most pressing information security research problems [11].

Although managers frequently cite confusion about how to measure the effectiveness of their security efforts, it is our belief that confusion about *how* to measure and gather data is also the result of confusion about *what* to measure – an issue of equivocality. In organizational theory, equivocality stems from the existence of ambiguity and conflicting interpretations, whereas uncertainty is the result of a lack of information [4]. In terms of organizational security programs, equivocality results from ambiguity about *what* to measure while uncertainty exists because managers are unsure of *how* to measure it, the combination of which creates a debilitating lack of information about the factors driving information security risk. Therefore, in order to generate data, and thereby lower uncertainty for improved decision-making, it is first essential to reduce equivocality by defining, expanding, and clarifying risk factors so that metrics, the "necessary measures" of management, can be unambiguously applied.

This research addresses equivocality as follows. We start with the basic premise that a firm's goal is to minimize loss expectancy, or risk, by maximizing the efficiency of mitigation efforts. There is substantial research on this topic, including applications of systems risk [8], economic models [5], game theory [3] and value at risk [7]. Though varied in form and terminology, in general, models sharing this purpose define risk as the product of three main factors, namely the frequency of threats/attacks (Threat), their likelihood of success (Vulnerability), and their organizational impact (Cost). The authors have used such models while successfully implementing information risk management programs for years and can attest to their effectiveness. However, we have discovered that although this approach provides an adequate superstructure for decision-making, there remains a high degree of confusion across, and even within, companies about how threat, vulnerability, and cost are individually measured and modeled. Current approaches traditionally recommend and employ estimates for critical factors like attack frequencies and countermeasure effectiveness because there exists no clear and accepted framework of what real-world measurements are needed to drive risk models or how they are to be collected. With the goal of reducing equivocality surrounding risk-based decision models, this paper formulates a system that (1) allows threats to be accurately measured and tracked, (2) enables the impacts and costs of successful threats to be determined, and (3) aids in evaluating the effectiveness and return on investment of countermeasures. With reduced

equivocality, uncertainty can then be addressed and current risk models made useable, as we illustrate through a managerial decision scenario. We begin by introducing a system of classifying threat that provides a foundation for risk modeling and the collection of reliable metrics.

2. Threat Classification

If management is to take systematic action to reduce risk [8], one of its primary tasks is to identify and understand the threats facing the organization [12]. Numerous taxonomies using varied techniques have been proposed in years past to classify and systematize threats to information security [6]. However, these classification systems have tended to either be geared toward security professionals or to such purposes as trending and surveys and, in our opinion, are not suitable for managerial decision-making. In order to maximize decision-making capabilities, a threat taxonomy should be focused on two main purposes: (1) using metrics to quantify risk factors, and (2) identifying efficient risk reduction strategies. We now propose such a system.

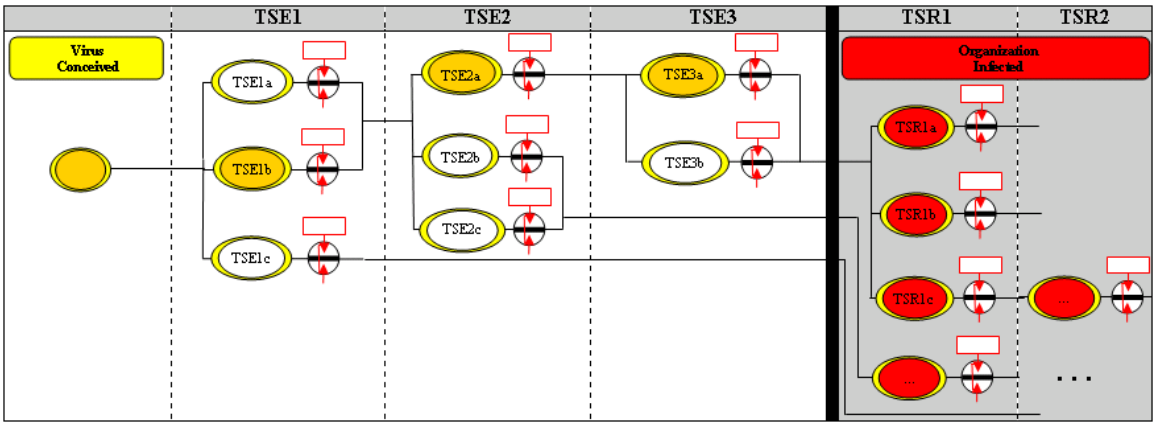
We find Howard and Longstaff's [1998] *Computer Security Incident Information Taxonomy* to be principally sound and agree that threat taxonomies must be mutually exclusive, exhaustive, unambiguous, repeatable, acceptable, and useful. However, to optimally satisfy the two purposes identified in the preceding paragraph, we extend their overall taxonomy requirements as follows. In our system, all possible threats are categorized into a manageable number of *threat scenarios* in which individual threats can be grouped together if they share a similar: (1) source, (2) channel or mode of attack, (3) target, (4) frequency of occurrence, (5) impact and cost, and (6) set of countermeasures with a similar mitigation value. Several previous taxonomies include categories such as "viruses" or "hacking" and make no allowance for the fact that there are many types of each, all requiring different metrics to be effectively utilized in decision models. For instance, malicious code (malcode) can infect an organization through email, Usenet, P2P applications, web surfing, etc. Each enters the organization via different channels, occurs at highly varied frequencies, results in diverse impacts to the organization, and requires different countermeasures to mitigate them. These threats clearly violate our requirements 1-6 above and therefore cannot be classified as one threat scenario, though previous taxonomies have grouped them.

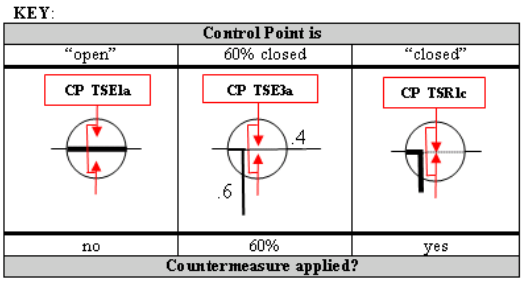
Additionally, and most importantly, threat scenarios are described within the context of our system as a chain of events from conception to resultant financial impacts on the organization. In so doing, we emphasize that security threats are not simple and one-dimensional events (i.e. "viruses"), but rather are very complex, often combining data, devices, and people to achieve success. Failing to identify, measure, and incorporate these complexities greatly reduces the ability of management to quantify risk factors for decision models. Constructing the entire event chain for threat scenarios also allows variations of a threat, such as those mentioned for malcode, to be accurately represented. In Figure 1, a few common malcode variations are modeled according to our taxonomy. Descriptions of events and results are included in Table 1. The event chain for a malicious executable email attachment, such as "Netsky," is shaded. Though we are using malcode to highlight the characteristics of our system, it is important to note that all information security threats, from hacking to employee theft can be modeled similarly as well. Classifying threat scenarios in this manner is not just an exercise in theory, but rather has very practical implications for data collection and decision models. Because every link represents a distinct, and therefore measurable, stage of progression, the application of metrics to threat scenarios becomes a much less equivocal endeavor.

3. From Threats To Cost, As A Bottom Line

Quantifying the frequency and cost of threats as well as determining the mitigation power of various security countermeasures are essential in building decision models for reducing risk. However, this process, as stated previously, is greatly misapplied in many security management programs and confusion exists concerning what it is about these factors that should be measured and quantified. We hold that organizations can accurately accomplish this with consistently obtained and rationally applied metrics. However, additional distinctions must be defined beyond those already described above for threats if one is to remove equivocality surrounding security-related decisions.

Figure 1. Example of event chaining for common malcode threat scenarios.
(Note: All possible chains are not shown.)





The first point to note is that threats themselves do not *directly* cause financial loss. Rather, it is more precise and helpful to recognize that successful threats cause any number of business-level undesirable results, which we term "bad outcomes." For example, in Figure 1, the event chain TSE1b-2a-3a causes the firm to become infected, which in turn causes several bad outcomes, including those shown in TSR1a, 1b, and 1c. Within the organization, each of these outcomes has a distinct cost which must be assessed and quantified separately.

We observe that many attempting to quantify costs for risk models incorrectly ask the question "How much does a virus incident cost?" when it is more appropriate to ask "What *bad outcomes* does a virus incident cause an organization and its assets, and how much do those individual outcomes cost?" Therefore, the primary task is to identify and model all possible outcomes caused by a threat scenario and later turn to assessing the associated financial losses.

Table I. Description of Threat Scenario Events and Results of Figure 1.

Threat Scenario Events (TSEs)	
TSE1a	Malcode seeded in Usenet, collected by victim's NNTP server, and made available to mail client software
TSE1b	Malcode sent via email, processed by victim's SMTP server, and delivered to mail client software
TSE1c	Internet worm (e.g., Blaster, Sasser, ...)
...	
TSE2a	Email entices user to click executable attachment (e.g., Netsky.D, MyDoom, ...)
TSE2b	Mail client software automatically invokes malcode, which exploits an OS vulnerability (e.g., Netsky.P, ...)
TSE2c	Mail client software automatically invokes malcode, which exploits an application vulnerability
...	
TSE3a	Malcode is successfully executed (now a program running on system)
TSE3b	Malcode exploits an OS vulnerability
...	
Threat Scenario Results (TSRs)	
TSR1a	Malcode installs backdoor. Cost incurred from theft of sensitive information & from regulatory penalties
TSR1b	Malcode replicates to all mail contacts or network shares. Productivity costs incurred from high utilization of system & network resources
TSR1c	System files corrupted. Cost incurred from cleanup and recovery efforts
...	
TSR2a	...
...	

Care must also be exercised when transforming threats to bad outcomes and then to costs to keep units consistent. We propose measuring threats as *rates*, say per year, and transforming threat rates into outcomes by specifying the number or extent per threat. For example, we conducted a study of 1500 organizations to quantify specific outcomes resulting from the MyDoom worm of January 2004, and found that organizations spent an average of 44 person-hours on clean-up and recovery following infection. Another study found that compromised firms lost an average 2.1% of their market value in the days surrounding an incident [2]. Thus, threat rates are changed into bad outcome rates. When the cost of each outcome is factored into the equation, a firm can more accurately calculate its exposure, or expected loss for any threat scenario, which is essential to prioritize mitigation efforts. A numerical example will follow momentarily.

Along with enabling the quantification of threat frequency and bad outcomes, modeling threat scenario chains has powerful implications for evaluating countermeasures that reduce organizational risk. Note that to impact the organization a threat scenario must be successful at each stage of the event chain. If the chain is broken at any link, the threat will be effectively mitigated. Management's task then becomes to identify and evaluate the many possible countermeasures that could be deployed to impede threat scenarios as they progress along the event chain. Straub and Welke [1998] proposed a countermeasure matrix in which the effectiveness of a countermeasure to mitigate threats is expressed as a fraction between zero and one (inclusive). This value is typically an estimate, the accuracy of which is often diminished because of poorly defined threats and other complications involving implementation quality. We adopt Straub and Welke's concepts to countermeasures applied at any stage of a threat scenario in order to more accurately calculate risk reductions, as will be seen.

First note that the precision we have insisted on here provides significant elimination of equivocality. Because every link in our threat scenario is a distinct channel and target, it is far less ambiguous to evaluate the effectiveness of countermeasures independently at specific links rather than attempting to do this for broad categories like "viruses." For example, it is possible to actually test the probability that anti-virus software will stop malcode entering TSE2a in Figure 1 rather than estimate this value for the threat as a whole. (Anti-virus software is typically tested at 100% effectiveness against recognized signatures, but is ineffective against new variations appearing since the last update, hinting that the ratio of "new" to "old" malcode and anti-virus update frequency are important metrics.) Additionally, training initiatives that educate users about the risks of opening strange email attachments could break the threat scenario if it is dependent on segment TSE2a, but this countermeasure would be ineffective at mitigating variations TSE2b, and TSE2c. In this manner, the synergistic value of "defense-in-depth" approaches to security management can be visualized and modeled.

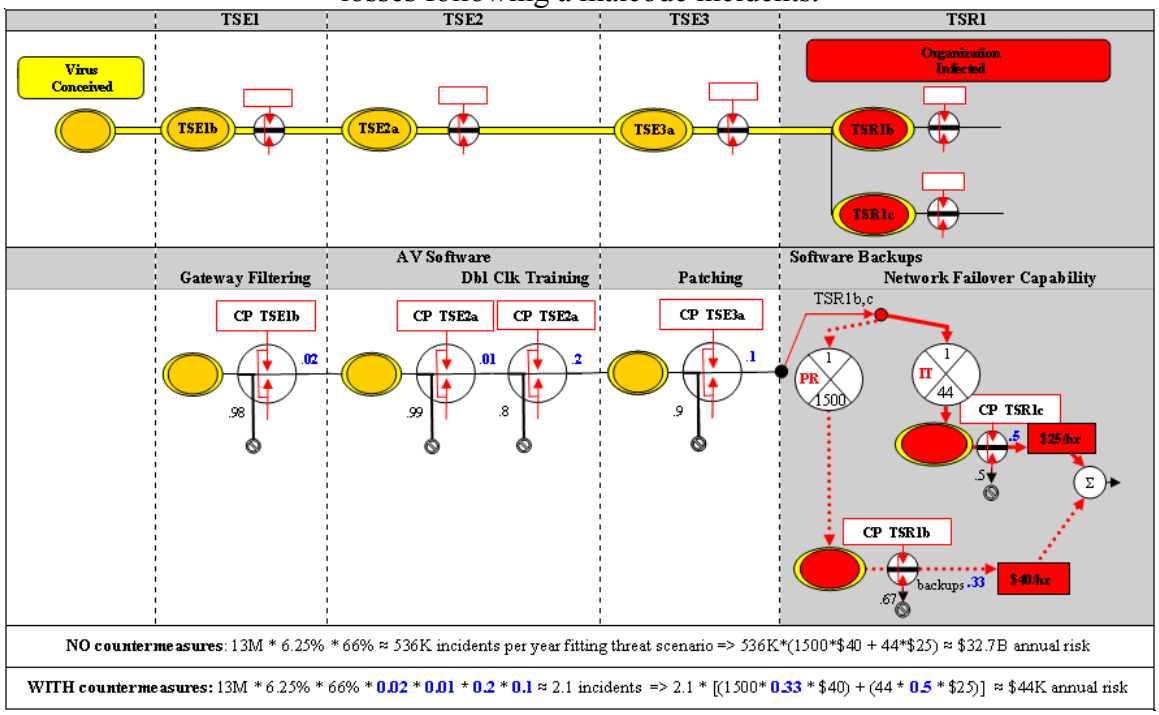
Second observe that threat scenarios may either be broken along the event chain prior to impacting the organization or subsequently. In the former case, deterrent and protective countermeasures act to lower the probability of a threat's occurrence or success. When the extent of bad outcomes is decreased, and thus incident costs lowered, countermeasures assume a detection and recovery role. Figure 2 shows the TSE1b-2a-3a->TSR1b-1c chain of threats from

Figure 1 with four deter-and-protect countermeasures and two detect-and-recover countermeasures applied.

4. Implications To Risk Assessment And Decision-Making

We now expand the example of email-based malcode in Figure 1 for two purposes. The first is to demonstrate *how* measures of frequency, cost, and countermeasure effectiveness can be derived through metrics to lower uncertainty and build actionable intelligence for any organization. Secondly, we make the point that since event chains for each threat scenario are modeled from conception through financial impacts it becomes clear precisely what should be measured at each step. Throughout 2004, we monitored traffic from 40 organizations, collecting metrics necessary to demonstrate the risk calculation process for the threat scenario depicted in Figures 1 and 2. Averages for relevant metrics collected in the study are presented in Tables 2 and 3 along with their sources.

Figure 2. Threats, countermeasures, and costs: An example of sources and impacts of financial losses following a malcode incidents.



Note from Figure 2 that by listing the complete chain of events, our system makes it possible to derive an initial threat frequency and then revise it through the use of metrics at each

successive intersection of the event chain. The bottom of Figure 2 demonstrates how organizational risk for the threat scenario is calculated using the data in Tables 2 and III. The first calculation depicts the loss expectancy of a firm having no security measures, though the figure is absurd as such a firm could not maintain operations while connected to the Internet. However, the calculation is pedagogically valuable as it shows the proper transformation of threat rates into financial costs. Since all firms have at least some security controls, a more realistic example is shown in the second calculation where six common countermeasures have been applied along with their effectiveness at each stage of the threat scenario. Using the data from Tables 2 and 3, the example shows that the firm can reduce the risk from the threat scenario to approximately $44,000 annually.

So, what should a firm wishing to mitigate its IT security risk do? There are four categories of data mentioned above for a firm to collect: expected threat frequency; countermeasure-effectiveness data; threat-to-bad-outcome transitions; and bad-outcome cost data. During the risk assessment process, an organization has numerous options relating to metric sources. For example, Tables 2 and 3 includes metrics collected from internal logs, public sources/databases, and internal/expert analysis. Deciding which sources to use depends on availability, internal resources and the maturity of the risk assessment program, among other things. For a more detailed discussion of security metrics, refer to [9]. In general, companies will find that the further to the right in Figures 1 and 2 one collects metrics, the more important it is to develop firm-specific numbers rather than employ national averages. For example, costs to the firm for loss of productivity will vary widely across companies and industries, as opposed to the effectiveness of (say) antivirus software as a countermeasure, or the threat rate of malcode (both further left in the figures).

Table 2. Threat and Countermeasure Metrics Relevant to Figure 2

Description	Value	Possible Source
Threat frequency data		
# of emails expected/year	13,000,000	Internal Logs
% of email infected with malcode	6.25%	Internal Logs or Public source*
% of email-based malcode of type TSE2a	66%	Internal Analysis
Countermeasure effectiveness data (deter and protect)		
Gateway filtering – % of emails *not* blocked	2%	Independent testing lab**
Anti-virus software – % of infected emails *not* blocked	1%	Independent testing lab**
Employee training – % of infected emails still executed by employees after training	20%	Estimate or Internal testing
Patching at 90 day intervals - % of malcode exploits not patched	10%	Internal Analysis
Countermeasure effectiveness data (detect and recover)		
Network failover capability - % of downtime reduced (assumes network is restorable within 2 hours of incident)	67%	Internal testing
Software backups - % of reduced system reinstallation and reconfiguration time	50%	Estimate or Internal testing
*e.g., Messagelabs - http://www.messagelabs.com		
**e.g., ICSA Labs - http://www.icsalabs.com		

Table 3. Impact and Cost Metrics Relevant to Figure 2

Description	Value	Possible Source
Threat-to-bad-outcome data		
Number of hours of lost worker productivity from network downtime (assumes 25% of 1000 employees require network access to perform their duties)	1500	Historical company data
IT person-hours required for clean-up and restoration	44	Public Data/Studies (e.g. our MyDoom study)
Note: Other threat impacts not shown for pedagogical reasons (could include lost sales, reputation damage, regulatory and legal fees, etc.)		
Bad-outcome cost data		
Average employee wage (includes overhead) per hour	$40	Company data
Average IT professional wage (includes overhead) per hour	$25	Company data

The ability to calculate risk using real-world metrics as prescribed in this paper has far-reaching implications for managerial decisions. An obvious extension lies in evaluating the return on investment of proposed security initiatives. To illustrate this, data from the study described previously revealed a nearly threefold increase in malcode activity during the first half of 2004. Noting this, a manager might decide to patch systems monthly instead of quarterly in order to reduce those system vulnerabilities often exploited by malcode. This reasoning is flawed for several reasons, all of which would have been clear if the proper metrics were available: 1) We estimate that testing and deploying patches in a 1000-system company can easily reach $73,000/push, or approximately $584,000 annually for the proposed eight additional patch deployments. Therefore, it would be impossible for the firm to regain its investment regardless of the level of benefit realized from additional patching. 2) Our metrics showed only a third of email-based malcode exploited vulnerabilities, suggesting that patching would be ineffective anyway. 3) Furthermore, malcode that did exploit vulnerabilities, targeted a vulnerability for which a patch had been released nearly three years prior – the quarterly patching cycle would have been more than sufficient. Though this illustration is hypothetical, in reality increased patching, although adopted by many organizations, is often an inefficient mitigation strategy against malcode; the example shows how firms with inadequate data are prone to waste security dollars.

A second implication of this research is also very pragmatic. For the past five years, following these methods, thousands of metrics for global threat, vulnerability, and cost have been collected for threat scenarios on a monthly basis to create the Cybertrust Index. Similar in function to other economic indices, the index tracks changes in the relative risk of conducting business over time for Internet-connected organizations. When localized, it allows any organization to measure and score the efficacy of their risk management program and to conduct comparisons across divisions and partners. Readers interested in this line of research may wish to read [10].

5. Conclusion

The old axiom “you can’t manage what you can’t measure” appropriately describes the fundamental issue confronting today’s business leaders concerning the security of their organizations. Current risk models, and the decisions made using them, are only as good as the

data upon which they are based. As such, this paper calls for a new, more reasoned approach to measuring and modeling security factors, including careful delineation of threats; collecting threat-to-bad-outcome data; gathering cost data; and calculating countermeasure vulnerability reductions. If these approaches are not consistently pursued, managerial decision-making will continue to be plagued by uncertainty, inevitably resulting in overspending, loss of boardroom credibility, poor security configurations, increased incidents, and costly regulatory penalties. If, however, the "necessary measures" are taken, improved analysis and decision-making can rightfully follow.

References

1. Berinato, S. 2003. The State of Information Security 2003. *CIO Magazine,* October, 2003.

2. Cavusoglu, H., Mishra, B., And Raghunathan, S. The Effect of Information Security Breach Announcements on Shareholder Wealth: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*. Forthcoming.

3. Cavusoglu, H., Mishra, B., And Raghunathan, S. 2004. A Model for Evaluating IT Security Investments. *Communications of the ACM, 47*, 7, 87-92.

4. Daft, R. and Lengel, R. 1986. Organizational Information Requirements, Media Richness and Structural Design. *Management Science, 32*, 4, 554-569.

5. Gordon, L. and M. Loeb. 2002. The Economics of Information Security Investment. *ACM Transactions on Information and Systems Security, 5*, 4, 438 – 457.

6. Howard J. and Longstaff T. 1998. A Common Language for Computer Security Incidents. Sandia Laboratories Report, SAND98-8667, October 1998.

7. Jaisingh, J. and Rees, J. 2001. Value at Risk: A Methodology for Information Security Risk Assessment. In *Proceedings of the INFORMS Conference on Information Systems and Technology*, Miami, Florida, November 2001, 3-4.

8. Straub, D.W., and Welke, R.J. 1998. Coping with Systems Risk: Security Planning Models for Management Decision-Making. *MIS Quarterly, 22*, 4, 441 – 470.

9. Swanson, M., et al. 2003. Security Metrics Guide for Information Technology Systems. *NIST Special Publication 800-55*, July 2003.

10. Tippett, P.S. 2005. The Cybertrust Index: Measuring Information Risk in Corporations and Society. *A Cybertrust whitepaper*, http://www.cybertrust.com/intelligence/research_library.html.

11. Verton, D. 2004. DHS Seeks Real-World Data on Security Breaches, *Computerworld*, September 20, 2004.

12. Whitman, M. E. 2003. Enemy and the Gate: Threats to Information Security. *Communications of the ACM*, 46, 8, 91-95.

Chapter 3: Is Information Security Under Control? Investigating Quality in Information Security Management

Wade Baker
Linda Wallace

Manuscript published in *IEEE Security & Privacy*, vol. 5, no. 1, pp. 36-44, January/February 2007.

Abstract
The purpose of this paper is to present the findings of a recent survey conducted to examine how organizations are managing information security through the implementation of security controls. Rather than assessing the presence or absence of controls, the survey was designed to investigate the quality, or thoroughness, of implementation. Results show that implementation quality varies significantly by organizational size as well as industry. Many organizations are focusing heavily on technical controls while neglecting important operational and management procedures such as security policies. Those organizations which did maintain strong policies exhibited higher levels of implementation quality in related controls. Improved control quality was shown to reduce the likelihood of security incidents, yet the results indicate that investing in maximum quality is not necessarily the most efficient use of resources. These findings establish a foundation whereby organizations can begin to properly pursue strategies to efficiently and effectively control information security risk.

Introduction

Over the last decade, organizations have sought to become more efficient and productive through the rapid adoption of information and communication technologies (ICTs). As ICTs become more common, the intrinsic value of these systems becomes dwarfed by the mission-critical functions they support [1]. This intimate relationship between technology and business functionality has proven to be an incubator for a dramatic increase in costly information security incidents and failures leading to substantial revenue losses. In light of this, organizations are more aware of information security risks and the need to take appropriate action. However, with so many security options available, many organizations are struggling to identify the best ways to counteract the threats they are facing.

Seeking to protect the confidentiality, integrity and availability of business functions supported by ICTs, the information security industry now boasts an extremely large and diverse set of products, services, tools, processes and policies ranging from complex mathematical encryption algorithms to human resource management and federal legislation. Leveraging this array of controls, many organizations have begun formal information security management programs in an effort to protect themselves, their partners and their customers. With the high cost of time and money associated with the implementation and maintenance of security controls, however, managers are under increasing pressure to distinguish between controls that are necessary within their organizations and those that are less critical or superfluous. Moreover, identifying the optimal level at which each individual control should be implemented is a delicate balance of risk reduction and cost efficiency.

Unfortunately, for many of these programs, managing security risk has become more about quantity than quality. Because they are unsure of the best controls for their situation, managers are often deploying as many controls as possible, checking them off from a list without regard to the quality or effectiveness of the implementation. In some instances controls are being used to correct security deficiencies but have the reverse effect of actually adding more deficiencies to the system [2]. Information security management would do well to take a lesson from the long-established paradigm of quality management; incidents are indicative of defects in the organization's security program. The essence of the challenge, therefore, is to increase quality by rationally implementing the controls necessary to minimize defects and ensure continued and efficient business functionality. Amid numerous vulnerabilities, complex threats,

greater regulation and shrinking budgets, the payoff for meeting the challenge is clear; when organizations are able to identify the appropriate controls for their situation and implement them efficiently, risks to information security can be effectively managed [3].

The purpose of this paper is to present the findings of a recent survey designed as an initial step toward meeting this challenge by benchmarking how organizations are managing information security through the implementation of various controls. Though security surveys are nothing new, the method we used is atypical of previous studies in that it was designed to: 1) foster greater insight into specific details of control implementation and 2) focus on the quality, or thoroughness, of implementation. Analysis of this caliber is necessary for more accurate inference concerning information security in organizations where small details matter a great deal and varying levels of quality can make the difference between success and failure. By obtaining a more precise understanding of current practices, information security management can begin to properly pursue efficient and effective strategies to improve quality and lower risk.

The paper is organized as follows: The first section provides some general information about security controls and discusses shortcomings in other security studies that have limited their ability to offer organizations new perspectives toward improving their security programs. We then discuss the data collection procedures and explain how the survey was designed to provide a greater degree of detail than other publicly-available reports. This is followed by our analysis of the survey's results along with some conclusions and implications.

Information Security Controls

Many of the first efforts to develop information security programs relied heavily on technological innovations. New security products were purchased and deployed to lock down networked resources, thereby allowing a safe perimeter in which to conduct business. This approach was reasonable given that many of the assets requiring protection were highly technical themselves. When used correctly, these techniques go a long way toward reducing security incidents within the enterprise. However, as successful and sophisticated as these technologies have become, security problems have not been solved through technical approaches alone for the simple reason that information security is not merely a technical problem; it is also a social and organizational problem [4]. As it has matured, the information security discipline has progressed

to recognize the importance of a holistic approach to securing technology, processes, people and other organizational factors on an enterprise scale.

The National Institute of Standards and Technology (NIST) classifies information security controls into three categories: technical, operational and management [5]. Technical controls traditionally include products and processes such as firewalls, anti-virus software, intrusion detection and encryption techniques which are mainly focused on protecting the organization's ICTs and the information flowing across and stored within them. Operational controls include enforcement mechanisms and methods of correcting operational deficiencies that could be exploited by various threats. Physical access controls, backup capabilities and protection from environmental hazards are all examples of operational controls. Finally, management controls such as usage policies, employee training and business continuity planning, target the non-technical areas of information security. For the purposes of this study, we adopt the NIST categorization system and designate controls as belonging to one of these three categories. This distinction is important because the type and quality of control categories utilized by an organization are key indicators of the maturity of the overall security management program. It will also allow us to determine if organizations are focusing on technical and operational controls to the detriment of management controls or vice versa. Given the evolution of security controls from a technical background we would suspect that many security programs are still drawn to technical and operational practices and overlook management controls, such as policy development.

Microsoft Vice President Dave Thompson has said "Security is a journey, not a destination [2]." With the evolving nature of security controls it stands to reason that consistent research aimed at discovering where organizations are along this journey is highly beneficial. As a result, the adoption of security controls by organizations around the world has been the focus of several studies during the last 10 years. One of the more long-running and well-known studies is the CSI/FBI Computer Crime and Security Survey, which is administered on a regular basis to identify and establish trends [6]. Though the CSI/FBI and other similar studies reveal important changes in organizational security practices over time, the real value and insight gained from them has been limited because of several key issues.

First, although it is common for surveys to ask about the use of various controls such as anti-virus software and backup procedures, they do not ask questions at the level of detail which

could reveal critical limitations in the effectiveness of the controls. For instance, knowing that an organization uses anti-virus software is of minor importance compared to uncovering specific details about which systems have anti-virus software installed, whether the anti-virus software is enabled for full-time protection, or how often virus definitions are updated [7].

Secondly, because questions on previous surveys have tended to be binary (Yes/No) in nature, the implementation quality of the controls that are being implemented, for the most part, remains unknown. In fact, we are unaware of any surveys in the security domain that target the important dimension of control quality. Most security professionals would agree that the full effectiveness of a firewall, for instance, is not achieved by simply plugging it into the network. Once installed, simple variations in rulesets, location and administration contribute greatly to the device's quality. One might answer "yes" to a survey asking if they use anti-virus software when in reality the software may be poorly configured, inadequately maintained and installed on only a few systems, thus limiting (and often compromising) any benefits normally afforded by the control. A clearer picture of the state of information security management could be achieved if studies were to focus on the comprehensiveness of control implementation rather than simply whether a control is used or not.

Finally, because of security and privacy concerns, organizations are often (rightly) reluctant to divulge specific or complete descriptions of their security practices to outsiders, making the collection of quality information a difficult process [8]. The following section describes the methodology we used to address these limitations and obtain a clearer picture of the implementation levels of a wide variety of detailed security controls from a large number of organizations.

Survey Methodology

To better understand how organizations are using controls to manage information security risk, we created a web-based survey addressing 80 specific security practices in 16 general security domains (see Table 1 for the list of domains). The controls included in the survey constitute a well-balanced information security management program and represent a cross-section of controls found in several international standards including British Standard 7799, NIST Special Publication 800-53, the Graham-Leach-Bliley Act of 1999 and NERC's Urgent Action Standard 1200. A group of ten security experts from industry and academia assisted with the process of identifying the 80 controls used in our survey.

Table 1. Major security domains and number of controls addressed in each.

General Security Control Domains	# of Controls
Anti-Virus (AV) Software	4
Backup and Recovery	5
Business Continuity/Incident Response	5
Employee Training and Awareness	6
Help Desk/IT Support Training	4
Hiring/Termination	4
Monitoring and Logging	4
Network Auditing and Logging	6
Network Security Management	6
Passwords and Access Control	4
Physical Security	9
Remote Access Security	4
Sensitive Data Handling and Protection	6
System-level Security	4
Technical Documentation	4
Testing and Review	5
	80

Survey participants were solicited from a listserv of security practitioners via an email invitation that described the nature of the study and offered access to the results as an incentive for participation. Subsequent follow-ups and reminders were also sent during the two weeks the survey was active. The 349 respondents were located in North America (71%), Europe (18%), Asia-Pacific (10%) and South America (1%). 34% of the organizations represented by the participants had less than 100 computer systems while 38% had between 101 and 1000 and the remaining 28% reported more than 1000 systems. Respondents selected from a list of 30 industries, which we grouped into Services (27%), Information Technology (20%), Government (14%), Production (14%), Education (11%) and Finance (13%) for analysis purposes. We created the survey to be anonymous in order to gain trust from the participants and made it clear to them that there would be no way of tracking responses to an individual respondent or to the organization they represent. To further provide credibility and encourage participation [8], the study was conducted in cooperation with Cybertrust, a global security services company.

Information security executives, managers and technical specialists were asked to rate the quality of the current implementation for each of the 80 practices according to the scale described below. An “unsure” option was available if they were unfamiliar with their organization’s adherence to a particular control.

0 = Not Implemented: The practice is not implemented at all.
1 = Poor: The control is poorly implemented. Although there is possibly some benefit from the practice, it is incomplete, of low quality and not rationalized.
2 = Below Average: Less than adequate implementation. Does not meet all requirements or does not meet them well.
3 = Average: Average implementation. Could be a "work in progress" or simply of mediocre quality.
4 = Above Average: Fairly well implemented, possibly some enforcement and documentation.
5 = Advanced: Mostly to fully implemented, at least some enforcement and documentation.
6 = Comprehensive - Fully implemented, well thought-out, strictly enforced and thoroughly documented.

The value of this approach over previous surveys is demonstrated in Figure 1, in which the responses concerning two of the practices involving anti-virus (AV) software are summarized. In comparison, the 2004 CSI/FBI survey is substantially less descriptive, only reporting that AV software usage was 99% [6]. Our results indicate that the CSI/FBI number may be a little misleading because in reality there are several issues surrounding the use of AV controls that are important (e.g., the percentage of desktops covered and whether there is a policy to mandate AV software use) and each control is not always implemented at the highest quality level. For example, we found that only 67% of the respondents comprehensively implemented AV software and about 30% of them rated their AV policy as below average or worse. The following sections highlight some of the more interesting and noteworthy findings of the study.

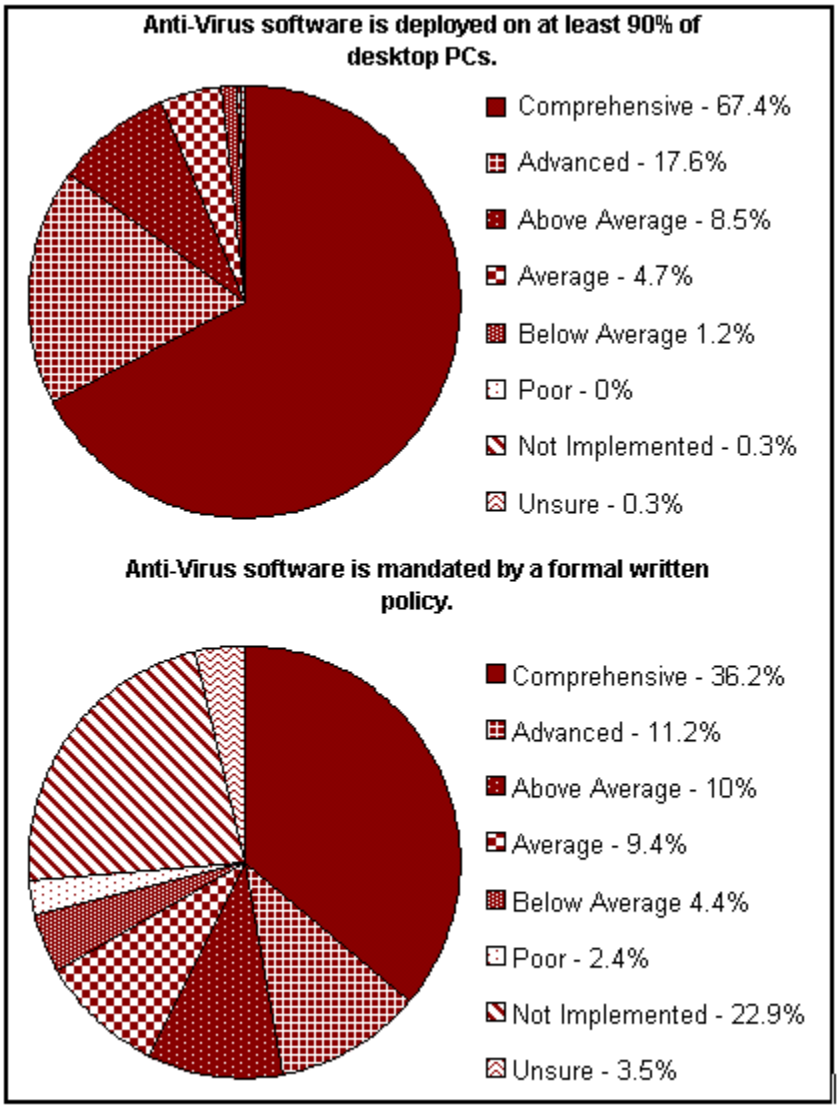


Figure 1. Breakdown of quality ratings for two questions relating to anti-virus controls

Results of Analysis

Controls with highest and lowest implementation quality

Our first goal was to identify the controls that, on average, are implemented comprehensively (a 6 rating) versus those that are poorly implemented (a 1 rating). Table 2 shows the ten controls that were rated the highest by our respondents in terms of implementation quality. Not surprisingly, anti-virus practices occupy the top three spots and are the only controls with an average quality rating of 5 (Advanced) or above. Viruses and malicious code represent some of the more obvious and persistent security risks and therefore most organizations are

diligent in mitigating the threats posed by them. Two other well-known controls, backups and system patching, received the next highest scores although there was more variation in quality than exhibited by the anti-virus controls, as can be seen in the stacked bar graphs of Table 2. Organizations also appear to be focusing on the importance of technical documentation, at least in the areas of network characteristics and critical device administration. Outside the top ten, the picture of implementation quality is somewhat less optimistic. Only one additional control was rated above 4 (Above Average), a fact that we found both surprising and disturbing.

Of the 80 controls included in the study, those listed in Table 3 were rated by participants as being of the lowest quality. In light of the rapid growth of the mobile workforce and remote connections, we would not have expected the identification and tracking of modem connections to be the lowest rated control in the survey. These connections often provide direct access to critical systems and are a significant source of risk that should not be neglected. Another poorly implemented control involves training personnel on how to prevent social engineering attacks. All employees, especially those with access to or knowledge of systems containing sensitive information, are choice targets of social engineering tactics and it appears that organizations may not be adequately preparing their employees to counter these threats. It is also imperative that organizations are able to detect an incident and remedy its impact [4], yet business continuity/incident response controls appear frequently in Table 3, with three of the five control practices in this domain included in the list of the bottom ten.

Table 2. Controls with the highest implementation quality rating

NIST Category	Not Impl / Poor / Below Avg / Avg / Above Avg / Advcd / Comp / Unsure	Average Rating
Tech	Anti-Virus software is updated with current signatures monthly (or more frequently)	5.48
Tech	Anti-Virus software is deployed on at least 90% of desktop PCs	5.45
Tech	Anti-Virus software is configured with full-time automatic protection enabled	5.4
Oper	Backup and Recovery procedures ensure that critical systems are backed up at intervals appropriate to their criticality	4.58
Tech	System-level Security procedures include deploying OS/application/system updates and patches on all Internet-facing devices within 90 days of availability	4.33
Oper	Physical Security Controls include effective locking mechanisms for every means of entrance to the facility	4.16
Mgmt	Accessible Technical Documentation includes contact information for all administrators of critical devices	4.15
Tech	Password and Access Control procedures on all local and remote systems include account lockout restrictions after no more than 5 bad logon attempts	4.07
Tech	Remote Access Security procedures include operational firewalls and AV software on each system accessing organizational assets	4.06
Mgmt	Accessible Technical Documentation exists relating to important network characteristics (topology, address ranges, devices, etc)	4.04

*Note: The first few words of each control relate it to one of the sixteen major security domains shown in Table 1.

It is also surprising to see inferior quality for real-time alerting in the event of a security breach since organizations surveyed in other security studies have reported high usage of intrusion detection systems. Organizations that have detection systems without real-time alerts are like houses filled with smoke detectors which have no alarm mechanisms. It once again demonstrates that some of the other security studies may not be asking questions at a detailed enough level to detect subtle differences that could prove to be critical to the success of the security program.

Table 3. Controls with the lowest implementation quality rating

NIST Category	Not Impl / Poor / Below Avg / Avg / Above Avg / Advcd / Comp / Unsure	Average Rating
Tech	Testing and Review procedures include a "war dial" of inbound phone lines to identify active modems	1.4
Mgmt	Help Desk/IT Support Training includes annual (or more frequent) training on how to prevent social engineering attacks	1.99
Mgmt	Business Continuity/Incident Response procedures include annual (or more frequent) testing of the response plan	2.15
Mgmt	Business Continuity/Incident Response procedures include a formal written policy addressing requirements for responding to all security incidents	2.18
Mgmt	Physical Security Controls include a formal written policy detailing all aspects of site security	2.33
Oper	Monitoring and Logging procedures include tracking the removal of any device from the business premises	2.5
Mgmt	Business Continuity/Incident Response procedures include training on response procedures for members of the response team	2.51
Tech	Network Auditing and Logging procedures include real-time alerting of appropriate personnel in the event of a security breach	2.52
Tech	Protection for all Sensitive Informational assets including the encryption of data in transit and in storage	2.58
Mgmt	Backup and Recovery procedures ensure that trial restorations from system backups are performed at least every 6 months	2.61

Management controls: the role of policy in quality

An analysis of the NIST control categories represented in Tables 2 and 3 reveals an important trend: only two of the top ten are management controls (and even these have a strong technical focus), while six management controls appear in the bottom ten. Extending this line of analysis beyond controls listed in Tables 2 and 3, we found that of all 80 practices surveyed, management controls had substantially lower implementation ratings than controls in the technical and operational categories. These findings are not without real-world relevance since many management controls serve to define what 'security' means in the context of the organization's mission and clarify the activities and procedures that are and are not allowed [9].

Organizations must realize that a large proportion of information security problems extend far beyond technology [4], and learn to appreciate the role that less-technical controls, such as policy development, play in minimizing the impact of security breaches to mission-critical operations.

Differences in perceptions of the value of policies and other management controls may explain some of the substantial disparity in control quality among organizations in our study. To empirically assess the value added by management controls, we conducted a test of the statistical relationship between security polices and the implementation level of related controls in the four security domains that contained a policy-related question[1]. To accomplish this, we compared organizations rating the quality of their security policies as below average with those rating their policies as above average. The results of the analysis of variance (ANOVA) tests to check for differences between the two groups are included in Table 4.

As evident in Table 4, organizations had a significantly higher quality rating for all non-policy controls when the implementation of the governing policy was rated above average. This correlation suggests that strong policies foster improved quality and that management controls can play a vital role in an organization's commitment to security. Furthermore, it demonstrates how one-dimensional approaches may be detrimental and helps to strengthen the argument for a holistic approach to security. We should mention that our survey was not designed to prove causality between security policies and improved control quality so the possibility exists that other factors were responsible for the correlation that we were not able to uncover. Policies have no innate capabilities for improving the implementation of technical controls and it is likely that the effects observed in Table 4 are partially a result of organizations having mechanisms in place to enforce these policies. In any event, the results in Table 4 are compelling and certainly warrant future research.

[1] The fact that we examine policies for only 4 of the 16 security domains is not an attempt to claim that policy is not needed in other areas.

Table 4. The effect of policy on control quality ratings*

Average control rating when policy quality was rated as:	Below Average	Above Average
Anti-Virus (AV) Software		
90% deployment	6.07	6.64
Updated monthly	6.09	6.71
Full-time protection	5.97	6.64
Business Continuity/Incident Response		
Assessing device criticality	3.44	5.87
Delineation of responsibility	2.84	5.81
Training for response team members	2.53	5.35
Testing of response plan	2.05	5.29
Physical Security		
Locking mechanisms on entrances	4.44	6.32
Access control to critical areas	3.14	5.75
Monitoring activities in facility	2.82	5.70
Restriction of ingress via infrastructure	2.76	5.69
Protection from environmental hazards	3.19	5.76
Preventing access to infrastructure	3.07	5.61
Equipment locked in racks and cabinets	2.92	5.58
Alerts in event of physical breach/failure	2.72	5.49
Sensitive Data Handling and Protection		
Training on use/handling of sensitive data	2.49	5.36
Labeling of all system outputs	2.70	4.80
Disposal of sensitive information	2.96	5.48
Review of applicable laws/regulations	2.65	5.37
Encryption of data in transit/storage	2.39	5.05

*Note: The p-values for all ANOVA tests were highly significant with levels less than .0001.

Variation by Size

Numerous surveys have shown that the adoption of certain security controls may be affected by organizational size. These findings seem reasonable, given that larger organizations likely have a larger budget for information security-related expenses. On the other hand, it is also expected that the difficulty of implementation would increase as well, potentially lowering control quality. Therefore, we examined how implementation quality differed according to the size of the organization. In doing so, we divided respondents into 3 categories based on the number of computers within the organization. Small organizations were those with 100 or fewer computers. Medium organizations had 101-1000 computers and large organizations had over 1000 computers.

In almost every case, our results showed that controls had a higher quality of implementation within larger organizations. However, the difference was statistically significant for only about 25% of the controls. The security practices that varied the most by organizational size are included in Figure 2. It is worth noting that these differences were predominately limited to two major domains: network security management and physical security. Given that the complexity of networks and the square footage of the physical location are likely to increase along with an organization's size, it makes sense that large firms would exert more diligence in protecting these assets.

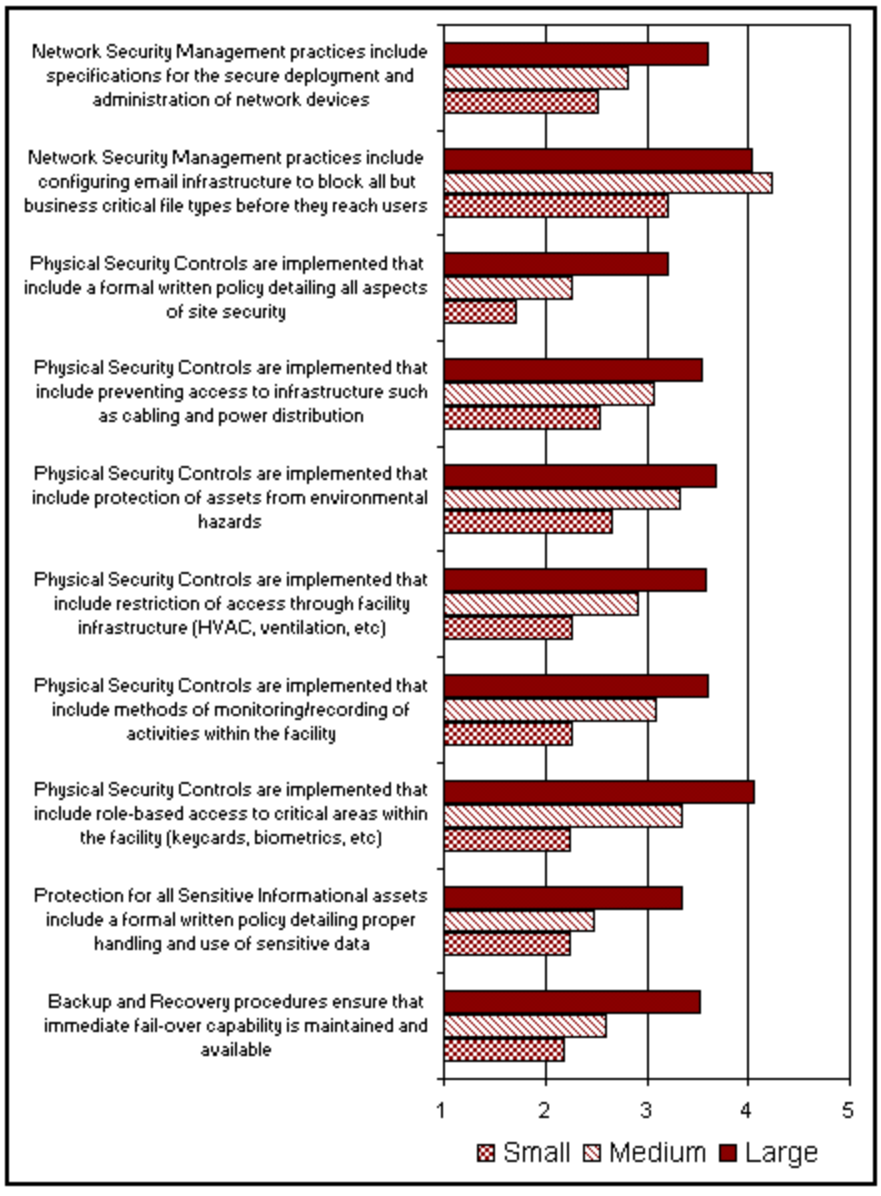


Figure 2. Controls exhibiting significant quality differences by organization size.

However, smaller organizations cannot afford lax security just because they have fewer resources and should assess whether their decreased attention to these areas is increasing their exposure to related threats. Another interesting finding is that of all 80 controls we surveyed, only one was found to have a higher implementation rating as organizational size decreased – reviewing network logs on a weekly basis. We interpret this result to be a reflection of the sheer difficulty of comprehensively and consistently auditing logs generated by increased traffic on larger networks.

Variation by Industry

In addition to organizational size, we would expect control quality to vary among the industries participating in our survey. At first glance, our results showed that the variation in implementation quality across industries was highly significant for many controls. Upon further review, it became apparent that only two of the industry groups were responsible for the disparity – education and finance. Although there was slight variation among the average control ratings among the service, production, government and information technology industry groups, none of the differences were statistically significant.

Without exception, the education industry reported lower scores than all other groups for each of the 80 controls surveyed while finance typically scored the highest. This trend is clearly demonstrated in Figure 3, which plots the implementation quality rating in the 16 major security domains for the six industry groups. As can be seen, 12 of the 16 security domains were rated below the 'Average' score of 3 in the education industry. In light of numerous major information security incidents reported within educational institutions in recent years [10] [11], we find these results to be extremely telling.

Although the free exchange of information and decentralization are staples of higher education, there must be comprehensive security programs in place that protect both the institutions themselves and the individuals within them. Individuals outside of academia may also be affected, as institutions of higher education are notorious staging grounds for malicious activity directed toward government or commercial organizations. Limited budgets, inadequate security staffs (often consisting of a few part-time graduate students) and departmental autonomy make security efforts all the more difficult. Conversely, financial institutions often have larger and highly trained security departments backed by ample budgets. Increased pressure from

customers, partners and regulatory agencies to secure their assets and processes likely provides additional impetus toward higher levels of control implementation.

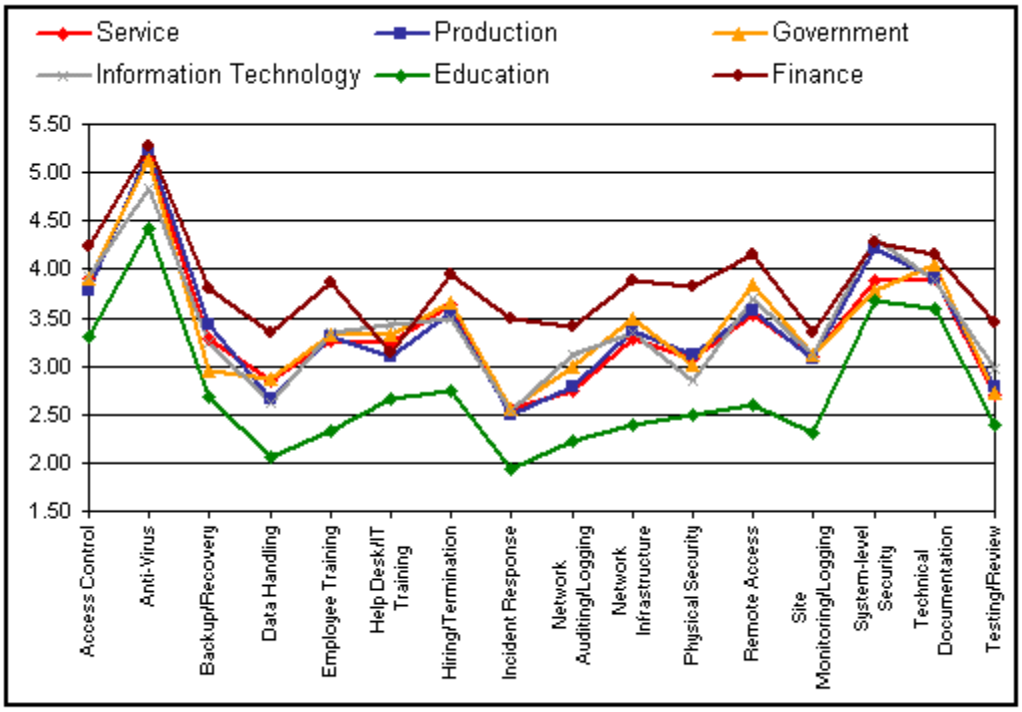


Figure 3. Control quality differences between industry groups.

It is also quite possible that the disparity exhibited in Figure 3 stems from the fact that each industry operates in a somewhat unique risk environment. Research has shown that attack rates, vulnerabilities and impact from security incidents vary among industries [12] [13]. It is logical to conclude therefore that security efforts are somewhat related to these factors and that organizations operating in riskier environments would exert more diligence to protecting themselves.

The Effect of Control Quality on Reported Incidents

A rather crucial line of analysis at this point involves whether there is any empirical evidence that quality matters in an information security program. To test the relationship between control quality and security incidents, we asked participants if their organization had been impacted by 10 common types of information security incidents during the year prior to the

survey. These responses were then compared to the implementation quality of their overall security program (the mean score of all 80 controls) and the results shown in Table 5.

Table 5. The effect of program quality on reported security incidents.

	% reporting incidents	
	Program Quality Score	
Type of Incident Reported:	**0-2**	**5-6**
Viruses & malicious code	85%	42%
Network intrusion by outsiders	67%	30%
Network denial of service attacks	31%	16%
Data theft via breach of network	62%	18%
Internet & Electronic Fraud	54%	33%
Network intrusion by insiders	67%	33%
Misuse/abuse of resources by insiders	85%	61%
Errors and omissions	92%	85%
Data theft via breach of premises	31%	13%
Physical denial of service	38%	27%

As is apparent from the table, organizations with poor implementation quality (a mean score of 0-2) were more likely to report incidents than those with advanced (a mean score of 5-6) security programs. Though it is possible that organizations reporting superior implementation scores simply under-reported incidents (or vice versa), these results suggest that higher quality controls lower the probability of security incidents. One should note that the improvement is substantial for some incident types (e.g., data theft via breach of network) yet less so for others (e.g., errors and omissions), hinting that benefits conferred through higher quality vary among control and threat combinations. Although it cannot be seen in Table 5, our data showed that organizations reporting high levels of technical controls but low levels of management and operational controls were more likely to report incidents than those with high scores across all three types of controls. This seems to support the notion that an unbalanced security program may not be as effective as a more balanced one, and offers further evidence in favor of holistic security measures.

Further analysis reveals that certain types of threats respond differently as the quality of the security program improves. We provide an example of this effect in Figure 4. As implementation quality increases progressively from poor to advanced, the percentage of organizations reporting virus and malicious code incidents drops sharply at first and then levels

out. Following the assumption that cost increases with control implementation, it would not appear beneficial for an organization desiring to reduce virus infections to achieve maximum quality. Alternatively, insider network intrusions exhibit a somewhat different behavior. The incident rate declines initially but shows almost no further reduction until implementation quality reaches advanced levels. In this case, the additional effort and expenditure to maximize quality may prove worthwhile for the organization.

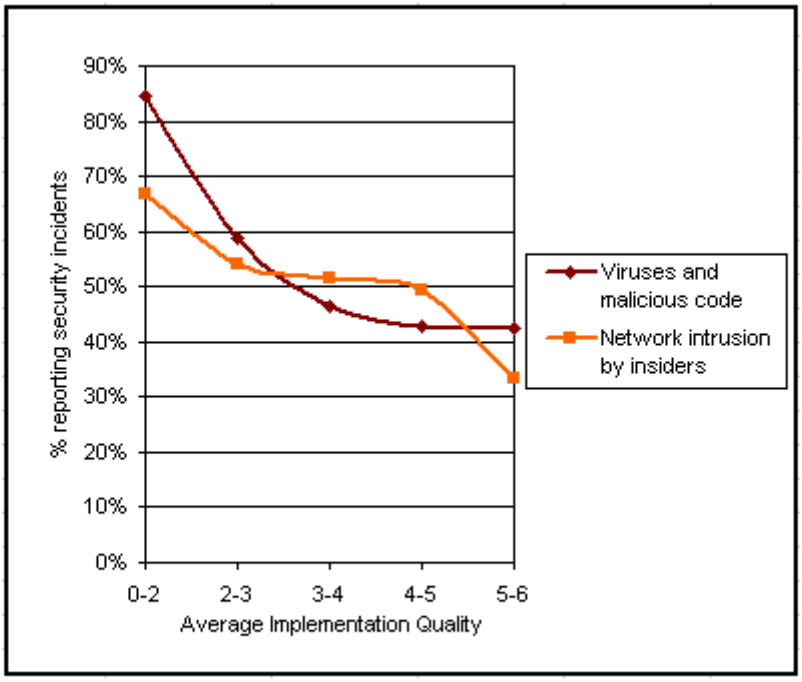


Figure 4. Incremental effect of program quality on reported security incidents

Along these lines, Gordon and Loeb point out that it is not an efficient use of resources to fully implement every available control and that an organization should invest in security only to the point where marginal benefit equals marginal cost. Though they apply this principle to the organization as a whole, it logically applies to individual controls as well. It may be possible, for instance, to optimize return on investment by implementing three controls at an 'average' level rather than a single control at a 'comprehensive' level. Feigenbaum's Four Costs of Quality [15], have been extensively used in the field of quality management to derive optimum quality levels in a system and potentially offer valuable insight for information security management as well.

Conclusions and Implications

Today's organizations appear to be actively seeking to control information security, but the approach taken by this survey to examine specific details and the quality of these efforts shows that there is significant variation in how they are going about this process. Overall, it seems that many organizations are managing security in a somewhat inconsistent and superficial manner. Rather than a calculated or rational approach, certain controls are heavily emphasized while others, though no less important, are poorly maintained.

Results indicate that larger organizations are maintaining higher levels of control quality than smaller ones, particularly when it comes to physical security and network security. Financial organizations exhibited the highest quality ratings of all industry groups in our study while educational institutions consistently reported the lowest. We suspect that the superior control quality reported by the finance industry is at least somewhat related to strict regulations and well-supplied security departments. Educational institutions, on the other hand, suffer from a lack of both but may be able to use the results of this study to justify additional expenditures to their superiors. In light of recent trends toward increased legislation and compliance requirements, we believe research directed at examining the effect of regulations on security program quality and success to be an intriguing area of future research.

The most thoroughly implemented security measures across all sizes and industries are predominately technical controls, yet our analysis offers evidence that this disparity leads to a higher rate of security incidents. This is possibly related to our finding that stronger security policies correlate with better control implementation. Organizations focusing only on technical solutions should consider establishing management and operational controls in key areas to strengthen and enforce their security posture. This may also provide organizations with tight budgets (like educational institutions) a relatively low-cost way to improve security without investing in new technologies. This recommendation is doubly important because we have also shown that security policies foster higher quality control implementation and higher quality controls decrease the likelihood of incidents.

While this study gives a more accurate account of the current state of information security management than many previous studies, it cannot reveal if the less than impressive quality levels are the result of a predetermined effort on the part of organizations to optimally implement each control. However, we find it unlikely that most organizations can or are attempting to conduct such calculations. As a step toward remedying this situation, we

recommend that researchers and professionals move away from simplistic binary investigation and trending of security practices to a more analog view of controls. Organizations can use our survey to gain enhanced insight into the quality and efficacy of their security programs with very little additional effort or cost. Systems and compliance audits could have more of an eye toward quality when assessing controls. Future research should build upon this approach and develop improved metrics of control strength and cost-efficiency to optimize ROI. Further investigation should be made to examine the benefits offered by combining various levels of technical, management, and operational controls to achieve true holistic security against a diverse range of present and future risks. Though the findings of this study reveal some positive trends, there is still progress to be made before it can be said that organizations truly have information security "under control."

References

1. Saydjari, O.S. Multilevel Security: Reprise. IEEE Security & Privacy, 2 (5). 64-67.

2. Mercuri, R.T. Computer Security: Quality Rather than Quantity. Communications of the ACM, 45 (10). 12-14.

3. Straub, D.W. and Welke, R.J. Coping with Systems Risk: Security Planning Models for Management Decision-Making. MIS Quarterly, 22 (4). 441-470.

4. Dhillon, G. and Backhouse, J. Information Systems Security Management in the New Millennium. Communications of the ACM, 43 (7). 125-128.

5. Stoneburner, G., Goguen, A. and Feringa, A. Risk Management Guide for Information Technology Systems. Commerce, U.S.D.o. ed., National Institute of Standards and Technology, 2002.

6. Gordon, L., Loeb, M., Lucyshyn, W. and Richardson, R. Ninth Annual CSI/FBI Computer Crime and Survey Report, Computer Security Institute, 2004.

7. Whitman, M.E. Enemy at the Gate: Threats to Information Security. Communications of the ACM, 46 (8). 91-95.

8. Kotulic, A.G. and Clark, J.G. Why There Aren't More Information Security Research Studies. Information & Management, 41. 597-607.

9. Bishop, M. What is computer security. IEEE Security & Privacy, 1 (1). 67-69.

10. Meglio, F. D. A Hacker Break-In Scrambles Kellogg. Businessweek, APRIL 12, 2005.

11. Schaker, B. CMU says hacker broke into computers. Pittsburgh Post-Gazette, April 21, 2005.

12. Belchner, T., et al. Riptech Internet Security Threat Report, Riptech, 2002.

13. The Internet Business Disruptions Benchmark Report. Aberdeen Group, 2004.

14. Gordon, L.A. and Loeb, M.P. The Economics of Information Security Investment. ACM Transactions on Information and System Security, 5 (4). 438-457.

15. Feigenbaum, A.V. Total Quality Control. Harvard Business Review, 34 (6). 93.

Chapter 4: Exploring Information Security Issues in Supply Chain Collaboration

Introduction

As the scope and complexity of modern supply chains continue to grow, firms rely on collaborative activities to achieve substantial mutual benefits. This trend has accelerated in recent decades as firms increasingly leverage information technology (IT) to enhance supply chain collaboration. By eliminating traditional layers of internal and external separation which once formed a protective barrier around a firm's assets and processes, IT-facilitated collaboration has simultaneously improved the ability to satisfy customer needs while increasing vulnerability to an array of IT-specific risks. Thus, the intimate relationship between technology and revenue forces managers to balance often opposing goals: collaboration vs. security.

Though questions relating to this balance are considered to be among the most challenging and frequently asked of the day (Lee and Whang, 2000), research on the topic is surprisingly sparse. Therefore, the purpose of this article is an initial investigation into the nature of information security risk in supply chains. To that end, we conducted an industry survey of more than 200 firms spanning various supply chain functions.

The remainder of this paper is structured as follows. First, we present a short literature review of collaboration and IT in integrated supply chains. This is followed by a discussion of the survey methodology. Next, we discuss the results of the survey, focusing briefly on perceptions surrounding information security risk within supply chains and then a deeper analysis of factors influencing the probability of security incidents. We conclude with a discussion of managerial implications and limitations of current approaches.

Literature Review

The goal of supply chain management is to merge all value chain functions into a unified routine that stresses collaboration among partners. Collaboration, a mutual decision making process where partners share information, knowledge, risk and profits based on a foundation of trust and commitment (Mentzer, 2002), is the central principle in creating flexible supply chains (Narus and Anderson, 1996). The necessity of collaboration among supply chains has rapidly increased, so much so, that research has identified collaboration as possibly the single most

pressing need in supply chain management for process optimization (Ashayeri and Kampstra, 2005).

Collaboration enables supply chain partners to exceed simple operational-level interactions and increases their competitiveness (McLaren et al., 2002). Recent research suggests that collaboration among supply chain partners facilitated by integrating the flow of information produces significant benefits (Lee et al., 1997, Li, 2002, Frohlich and Westbrook, 2001, Metters, 1997). Numerous benefits such as revenue enhancement, cost reduction, and operational flexibility have been associated with collaboration (Simatupang and Sridharan, 2005). Although highly collaborative firms exhibit many common characteristics, literature repeatedly emphasizes the level or maturity of partner relationships, information sharing and IT integration.

The beneficial effects of collaboration stem from supply chain partners jointly gaining a clearer understanding of prospective demand and developing realistic plans which satisfy this demand (Sahay, 2003). This idea is validated by Corbett and Blackburn (Corbett and Blackburn, 1999) who state that as partnerships between companies and suppliers mature, the competitiveness of their supply chains improve.

Supply chain management is essentially information-driven with organizations recognizing that supply chains which share information for coordinated decision-making achieve maximum efficiency for all supply chain partners. This requires that supply chain partners embrace a new philosophy based on cooperation and trust, seeking to improve the performance of the overall system rather than individual processes or organizations within the chain. This acknowledges the new reality that competition is no longer between organizations, rather it is between competing supply chains. Facilitating this unified approach is IT, which has enabled integration of information flows between partners, thus diminishing uncertainty and risk. Gunasekaran and Ngai (Gunasekaran and Ngai, 2004) have argued that an efficient, competitive, and collaborative supply chain is an impossibility without IT.

As partners deepen relationships, integrate IT systems and share greater amounts of information, increased importance must be placed on information security. Though it has been suggested that supply chain information security demands more attention than it is currently receiving (Lee and Whang, 2000, Kolluru and Meredith, 2001, Gunasekaran and Ngai, 2004), relatively little research has actually been conducted in the area. In fact, at the time of this

writing the authors are aware of no empirical research focused on the effect of supply chain collaboration on information security risk.

Survey Methodology

While few researchers have conducted studies on information security in the context of supply chain management, Smith et al. (2007) have taken steps toward identifying and framing the inherent IT security risks between collaborative partners. Their work provides the theoretical foundation upon which the industry survey which is the subject of this paper is built. The survey is exploratory in nature, the purpose of which is an initial investigation toward isolating, analyzing and establishing an empirical relationship between supply chain collaboration and information security risk.

Conducting research involving information security programs has proven to be a challenging task. For obvious reasons, firms are often reluctant to divulge information about security practices and problems to outside parties. Prior research has, however, suggested that partnering with a trusted entity (i.e., government body or independent security company) when conducting information security research encourages participation and improves results (Kotulic and Clack, 2004). Based on this, the survey discussed in this paper was developed and conducted in cooperation with Cybertrust, the world's largest information security services company.

A web-based survey of approximately 20 questions was created for this study. The survey instrument evolved through several iterations of testing and refinement before final invitations were sent to the selected firms. The survey was organized around two main response variables: 1) perceived level of information security risk and 2) actual occurrence of security incidents.

In general, risk is defined in terms of an expected value measurement, a 'combination of probability, or frequency, of occurrence of a defined hazard and the magnitude of the consequences of the occurrence' (1992). Unfortunately, at this time measuring supply chain information security risk is highly problematic (Smith et al., 2007). Whereas many firms have data on security event frequencies and probabilities, the financial impact associated with these events is not easily measurable or available. Attempts to obtain this information often results in nothing more than mere conjecture of the likely financial impact incurred from a security event. Due to these circumstances, we did not attempt to measure and quantify risk in its entirety (probability x consequences). Rather, as a measure of probability, we asked participants if their

organization suffered an information security incident directly related to a supply chain partner. It is logical that firms having a higher likelihood of security incidents also have higher risk. We believe this to be the most feasible method of obtaining a realistic "measure" of risk at the current time.

Numerous exposure variables were used in the study including collaborative activities, security practices, partner assessments and managerial involvement. As these variables present are qualitative, we constructed cross tabulation tables and calculated Chi-square values as a measure of statistical association. In addition, to evaluate sufficiently the nature of the data and relationships, we also include Gamma, Sommer's d, Kendall's tau-c, Spearman and Pearson's R in our analysis of ordinal variables (Kang, 1973).

Due to the nature of the survey, the authors felt that the ideal target sample was individuals with knowledge or responsibility for IT, security and operational functions within the firm. Such individuals likely have an intimate and realistic knowledge of IT in their firms and the technological risks associated with collaboration and integration with supply chain partners. Individuals fitting this description were randomly selected from a proprietary list of firms maintained by a third-party organization and invited to participate via email. Because the survey involved highly sensitive information, it was conducted anonymously to promote trust and honest responses. As an incentive, participants were offered a full report of results. Two rounds of follow-up emails were sent to non-respondents to further encourage participation.

In total, 206 firms completed the survey. Of those, 18 were eliminated from the final analysis due to non-existent or insignificant supply chain relationships. The 188 firms remaining represented various supply chain functions from manufacturing to retail. Firms of all sizes, ranging from fewer than 50 to greater than 100,000 employees, participated in the study. Further, respondents described their role in the firm as IT administration (39%), IT management (20%), Non-IT/Operations management (32%) and senior management (9%). The following sections highlight some of the more interesting and noteworthy findings of the study.

Survey Results

Collaboration and Perception of Risk

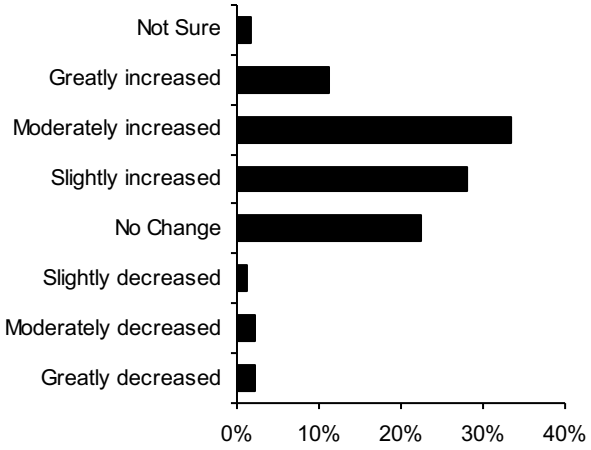
Questions with regard to perceived risk were included in the survey to test what factors and activities related to supply chain collaboration contributed to an increase in the respondent's

perception of information security risk in their organization. This is essentially a "gut feeling" measure of risk among personnel responsible for supply chain and security functions within an organization.

When asked how collaborative activities with supply chain partners affect their firm's risk of information security incidents, nearly three-quarters of respondents felt risk was increased. These results are depicted in greater detail in Figure 1. Interestingly, non-technical managers in the study provided lower risk ratings on average than did their IT colleagues; however, statistical tests revealed no significant difference among the roles. Though we expected IT and security professionals to have a much higher perception of risk, these results imply a fairly consistent sentiment of concern at all organizational levels over securing information resources within the supply chain. However, as discussed in the section of Managerial Implications, there was strong disagreement among respondents on how management should respond to these risks.

We then desired to test whether high levels of collaboration heightened risk perceptions. Participants were asked a series of questions about the scope and maturity of relationships, the amount of information exchanged and the level of IT integration with supply chain partners. Tests were then conducted to assess the statistical relationship between each of these variables. Not surprisingly, firms supplying higher ratings for these collaborative activities also demonstrated a significantly elevated estimation of information security risk. This trend was further amplified among firms requiring constant IT connectivity with partners or sharing information they deemed to be highly sensitive. When asked for the three most worrisome security risks stemming from supply chain partners, respondents most often cited network intrusions (68%), data theft (64%), virus infections (49%) and fraud/misuse (43%).

Figure 1. Perceived effect of supply chain collaboration on information security risk.



Collaboration and Incident Probability

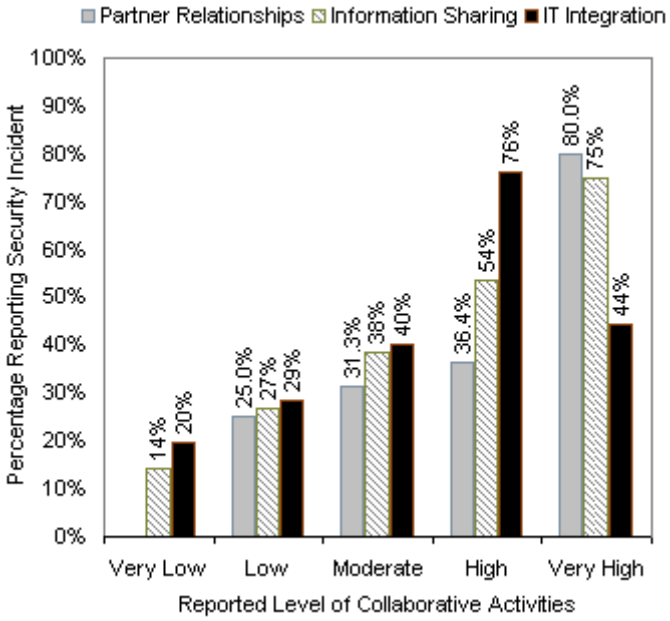
Though perceptions of risk provide valuable insight, they obviously cannot reveal factors that actually increase information security risk in collaborating firms. To assess whether perceptions of risk were founded, we asked respondents if their firm had suffered an information security incident directly involving their supply chain partners within the previous year. We were quite surprised to find that 37% of firms reported at least one incident. Again, we note that the survey question specifically referred to incidents directly involving partners rather than general security incidents from outside the supply chain. We believe this finding offers compelling evidence that information security is a real and critical problem for supply chain management.

Analysis was then conducted to determine how collaborative activities among supply chain partners affected the probability of security incidents. Using the information supplied by respondents pertaining to their partner relationships, information sharing and IT integration, we calculated the percentage of firms reporting an incident at successive levels of each activity. The result, shown in Figure 2, is a steady increase in incident probability as collaborative activities increase.

The notable exception to this trend is the over 30% drop in incident likelihood as IT integration moves from high to very high levels. Our first hypothesis was that this peculiarity was related to sampling problems (only 9 firms reported being highly integrated with their supply chain partners). A deeper analysis, however, revealed that these firms had significantly more advanced security practices in place to mitigate risks. This was not the case with either partner relationships or information sharing. As will be discussed in the following section,

improved security practices were shown to be strongly linked with a reduced probability of security incidents. Therefore, it is logical that the few very highly integrated firms in the study necessarily maintained higher levels of IT security in order to support their aggressive integration goals.

Figure 2. Effect of collaborative activities on incident probability



Though Figure 2 appears to depict a definite relationship between collaborative activities and information security incidents, it does not reveal if the relationship is statistically significant. Therefore, we ran several significance tests to measure the association between these activities and reported incidents. The results are included in the top section of Table I.

The Chi-square and ordinal statistics reveal highly significant relationships among the variables. Therefore, it is extremely unlikely that the trends shown in Figure 2 are simply random. While such tests cannot prove causality, they offer compelling evidence that partner relationships, information sharing and IT integration each increase supply chain information security risk.

Table I. Significance tests[2] for variable relationship to incident probability

	Chi-square	Gamma	Sommer's d	Kendall's Tau-c	Spearman	Pearson's R
	Sig.	Sig.	Sig.	Sig.	Sig.	Sig.
Collaborative Activities						
Partner Relationships	.000	.001	.001	.001	.001	.001
Information Sharing	.011	.000	.000	.000	.001	.000
IT Integration	.000	.000	.000	.000	.000	.000
Mitigating Factors						
Security Practices	.008	.001	.001	.001	.001	.000
Time of Assessment*	.282	-	-	-	-	-
Type of Assessment*	.042	-	-	-	-	-
Mgt Consideration	.107	.053	.053	.053	.059	.086
Consideration Disparity	.100	.024	.024	.024	.030	.033

Mitigating Factors on Incident Probability

Clearly, an appropriate response to these findings does not involve cessation of supply chain collaboration. In fact, it is entirely possible that the relationship depicted in Figure 2 argues for collaboration in order to improve coordination of IT security among partners. Regardless, the close tie between collaboration and information security makes it imperative that those responsible for supply chain operations be aware of measures that can be taken to reduce potential risks. A few such measures are discussed in this section.

We chose to examine four factors suggested by a group of information security professionals to mitigate risk within the context of interconnected IT systems: 1) Practices adopted to improve the firm's IT security posture, 2) If/When assessments of a potential partner's information systems security are conducted, 3) How this assessment is conducted, and 4) management's consideration of security risks in decisions regarding supply chain partnerships. To be sure, the list is not exhaustive but it provides ample opportunity to test whether incident probability can be controlled among collaborating firms.

Survey respondents were asked to rate their firm's level of adherence to each of these factors. Our subsequent analysis revealed mixed results, which are shown in the latter half of Table I. The level of security practices was, by far, the most significant mitigating factor in

[2] Note: Variables 'Time' and 'Type' of Assessment are categorical. Ordinal statistics do not apply.

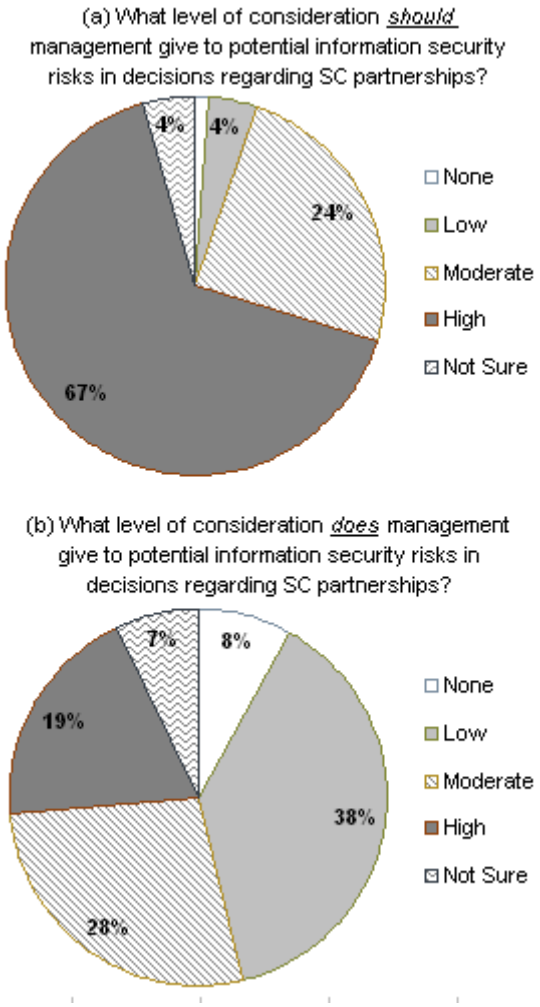
reducing incident probability. 83% of firms with reporting very poor security practices suffered incidents while the 9 firms having the highest level of security reported none. We expected firms conducting security assessments of a potential partner's IT systems prior to and at intervals during a collaborative relationship to reduce the likelihood of adverse incidents. Although this was true in general, the difference was not statistically significant. On the other hand, the method of assessment was significantly related to incident probability. On-site or virtual audits of information systems and 3rd party assessments proved to be far more effective than no assessments or those based on mere attestation. Not surprisingly, there was also significant correlation between such firms and a tendency to avoid supply chain partnerships over security concerns. This fact likely introduced complementary improvements to the security record.

Of particular interest to us was obtaining a better understanding of how managerial involvement related to the issues discussed within this paper. From Table I it can be determined that an association exists between management consideration and incident probability at higher levels of significance (.053 - .107). This result, however, is somewhat dissatisfying and insufficient to adequately address this important topic. Consequently, we further explore the role of management in supply chain information security in the next section.

Managerial Implications

As a starting point, we felt it beneficial to gather respondents' opinions pertaining to the level of consideration that management should give to potential information security risks during decisions regarding supply chain partnerships. A breakdown of responses is shown in Figure 3a. Two-thirds of participants felt management consideration should be high while only 5% answered none or low. Thus, our sample consisting of managers and non-managers techies and non-techies widely views managerial involvement to be essential.

Figure 3. Opinions concerning the amount of consideration management should give information security in supply chain management and the amount actually given.



Next, participants were queried about the level of consideration actually given by management to these issues at their firm. The results, found in Figure 3b, display an obvious contrast between "should" and "does". Almost half of respondents believe management gives little to no consideration to information security in supply chain management. Moreover, the amount of disparity between ratings of "should" and "does" was significantly linked to the firm's likelihood of suffering a security incident (See Table I). Possible reasons behind this are numerous and may include problems arising from inadequate funding of security initiatives, communication breakdown within the firm, poor leadership, managerial disregard of recommendations from IT staff, etc.

In addition to a direct association between management and security incidents, our investigation revealed strong indirect effects as well. In fact, the strongest statistical relationship in our study existed between management consideration and improved security practices. As previously discussed, the strongest mitigator of security incidents was security practices. One of the crucial roles of management, therefore, appears to be one of leadership, support, and promotion of a culture of security in the context of supply chain relationships.

Conclusions and Future Research

As IT increasingly becomes the medium of business functionality, a reliance upon its secure and continued operation has redefined corporate risk (Loch and Carr, 1992). In the supply chain, collaboration is designed to drive down supply chain risk (Christopher and Peck, 2004) through seamless integration and coordination among partners. Alternatively, our study finds a wide consensus of opinion that activities essential to this goal may actually increase risk. More importantly, it provides empirical evidence favoring this position by establishing a highly significant relationship between collaboration and security incidents. With collaboration hailed as the supply chain's most pressing need (Ashayeri and Kampstra, 2005), these results are disconcerting to say the least.

Far from assuming the role of doomsday prophets, we believe this study offers positive findings as well. It appears that measures taken to improve organizational security have some ability to combat the risk of security incidents exacerbated by higher levels of collaboration. Robust IT assessments of potential partners also seem helpful in mitigating information risk. Furthermore, although our survey shows management involvement to be widely underdeveloped, those managers exhibiting high consideration of these issues garnered significant benefits to their firms.

It is our intention that this brief empirical assessment of information security in supply chain management stoke the interest of the research community while serving as a springboard for future study in the area. To be sure, collaboration introduces great benefits but at what cost? Is the more than five-fold increase in incident likelihood between information sharing extremes (Figure 2) worth the benefits incurred? Is it possible for a firm to determine optimal levels of collaborative activities that optimize benefits while minimizing information security risks? The answer to these important questions at this time is, quite simply, more research is needed. The

importance of finding answers to these and other related questions to firms operating within today's highly interconnected, information-intensive supply chains cannot be overemphasized.

References

1. (1992) Risk: Analysis, Perception and Management. London, UK, Royal Society.
2. Ashayeri, J. & Kampstra, R. P. (2005) Realities of Supply Chain Collaboration. EurOMA International Conference Proceedings. Budapest, Hungary, European Operations Management Association.
3. Christopher, M. & Peck, H. (2004) Building the Resilient Supply Chain. International Journal of Logistics Management, 15, 1.
4. Corbett, C. J. & Blackburn, J. D. (1999) Partnerships to Improve Supply Chains. (Cover story). Sloan Management Review, 40, 71.
5. Frohlich, M. T. & Westbrook, R. (2001) Arcs of integration: an international study of supply chain strategies. Journal of Operations Management, 19, 185.
6. Gunasekaran, A. & Ngai, E. W. T. (2004) Information systems in supply chain integration and management. European Journal of Operational Research, 159, 269.
7. Kang, T. S. (1973) Ordinal Measures of Association and Forms of Hypotheses. The Sociological Quarterly, 14, 235-248.
8. Kolluru, R. & Meredith, P. H. (2001) Security and Trust Management in Supply Chains. Information Management & Computer Security, 9, 233-236.
9. Kotulic, A. G. & Clack, J. G. (2004) Why Aren't There More Information Security Research Studies. Information & Management, 41, 597-607.
10. Lee, H. L., Padmanabhan, V. & Whang, S. (1997) Information Distortion in a Supply Chain: The Bullwhip Effect. Management Science, 43, 546.
11. Lee, H. L. & Whang, S. (2000) Information sharing in a supply chain. International Journal of Technology Management, 20, 373.
12. Li, L. (2002) Information Sharing in a Supply Chain with Horizontal Competition. Management Science, 48, 1196.
13. Loch, K. D. & Carr, H. H. (1992) Threats to information systems: Today's reality, yesterday's understanding. MIS Quarterly, 16, 173.
14. Mclaren, T., Head, M. & Yuan, Y. (2002) Supply Chain Collaboration Alternatives. Internet Research: Electronic Network Applications and Policy, 12, 348-364.
15. Mentzer, J. T. (2002) Managing Supply Chain Collaboration. Supply Chain Management Review, 83.
16. Metters, R. (1997) Quantifying the bullwhip effect in supply chains. Journal of Operations Management, 15, 89.
17. Narus, J. A. & Anderson, J. C. (1996) Rethinking Distribution: Adaptive Channels. Harvard Business Review, 74, 112.
18. Sahay, B. S. (2003) Supply Chain Collaboration: The Key to Value Creation. Work Study, 52, 76-83.
19. Simatupang, T. M. & Sridharan, R. (2005) The collaboration index: a measure for supply chain collaboration. International Journal of Physical Distribution & Logistics Management, 35, 44.
20. Smith, G. E., Watson, K. J., Baker, W. H. & Pokorski, J. (2007) A Critical Balance: Collaboration and Security in the IT-Enabled Supply Chain. International Journal of Production Research, Forthcoming.

Chapter 5: Describing and Analyzing Data Breaches in Supply Chains

Abstract

Chapter 3 discussed the lack of useful data to drive cyber risk models and proposed an approach by which threats and impacts can be better categorized and measured. Chapter 4 expanded the discussion beyond single organizations by surveying perceptions and reports of IT risk factors related to 3rd parties. This chapter builds on these concepts through an in-depth investigation of nearly 1000 real-world data breaches occurring over a ten-year period. It further validates the perceptions and exploratory findings of chapter 4, but more importantly, provides a robust data model and rich database required by a DSS for cyber risk in the extended enterprise. To our knowledge, it is the most comprehensive field study ever conducted on the subject.

1. Introduction

One of the most critical and persistent challenges plaguing efforts to manage cyber risk is a lack of data. Many nations, organizations, or individuals do not have data of sufficient quality or quantity to consistently make informed decisions or take justified action to protect information assets. This state of being is well described using the definition of uncertainty; "the difference between the amount of information required to perform the task and the amount of information already possessed by the organization" (Galbraith, 1977). Removing uncertainty, therefore, involves shrinking the gap between what is known and what needs to be known.

The question, therefore, is what do we need to know and what do we measure in order to know it? Chapter 3 proposed an approach by which threats and impacts can be better measured, but we still need a reliable source of real security incidents that allows us to apply and refine this framework. Over the years, there have been many initiatives to amass and share security incident data, but widespread participation and success have been elusive for many reasons.

Surveys, sensors, and other sources can inform risk management; what better source of data exists than first-hand examination of actual security incidents? While organizations are not apt to expose the nitty-gritty details of their security failures to academic researchers, they do often turn to 3rd party forensic firms to investigate and contain them. Thus, we found it necessary to partner with (actually—gain employment with) a leading global incident response (IR) provider to create an incident database to support the needs and goals of this research.

This study is unique in that it offers an objective, first-hand view of nearly 1000 breaches taken directly from the casebooks of forensic investigators. Tens of thousands of data points weave together the stories and statistics from compromise victims around the world, and form the basis of a high-quality database needed to drive a DSS for cyber risk management.

2. Data Collection

As one might imagine, forensic investigations of security breaches are a potential goldmine of data and insight. This is especially true when one considers that the security industry has long suffered from a dearth of quality data. The Verizon IR team has a wealth of experience, handling roughly 2000 paid external forensic investigations from 2005 through 2014. This includes a majority of the largest publicly reported breaches during that timeframe. During such engagements, the team regularly interacts with client staff, third-party stakeholders, and law enforcement personnel from around the world. This level of rigor and oversight produce a high confidence and high fidelity data source that forms the basis of this research.

The analysis of data breach trends has been an important function of the Verizon IR practice for years. Anecdotes and simple statistics were collected and used to fuel further inquiries into various topics of interest. The authors, however, believed a more extensive and systematic process was needed to tap the full potential of IR investigations as an unparalleled source for quality security incident data. At considerable investment in time and resources, an initiative was begun in 2007 to identify a comprehensive set of metrics to record during each data compromise investigation.

2.1 Initial data collection and calibration

This data collection initiative spanned two phases over the ten-year timeframe of this study. The first, a retrospective analysis of cases worked from 2005 to 2006, was conducted in 2007. The purpose of this initial phase was twofold: 1) vet the risk metrics framework proposed in chapter 3, and 2) validate the exploratory findings of chapter 4 with hard evidence on how partners contribute to security breaches.

To accomplish this, we identified all cases involving a confirmed security breach during the period (approximately 150) and reviewed the official case reports[3] as well as investigator logbooks when available. Interviews with case investigators provided a wealth of supplemental data and insight.

The retrospective analysis showed the data framework introduced in chapter 3 was suitable for the areas it addressed, but it also revealed that it failed to capture many valuable risk-relevant data points that could be gleaned from the forensic case reports. Thus, the framework was expanded dramatically to take advantage of the rich data available from this source and thereby maximize utility for a DSS. This was an important step because it allowed us to develop an evidence-based approach to IT risk management that would become the foundation of this research. The final data model comprising dozens of elements is presented later in this chapter.

2.2 Ongoing data collection process

From 2007 through 2014, data collection occurred at the close of each case as part of standard operating procedure. An internal application was created to capture all data points defined by the model. Either the principal investigator or a trained security analyst input data from first-hand experience and/or directly from the official case documents. All client identifiers were removed during the process.

2.3 The incident database

The result of these efforts is the creation of an information repository unlike any other in the world. It includes 982 confirmed security incidents[4] from 2005 to 2014, with 822 of those incidents resulting in the disclosure[5] of over 457 million compromised records[6].

---

[3] These are the final deliverables provided to IR clients and other relevant 3rd parties such as law enforcement agencies, payment card processors, merchants, service providers, and legal firms.
[4] We define a security incident broadly as any event that compromises the confidentiality, integrity, or availability of an information asset.
[5] We define a data disclosure as an incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party. We use this term interchangeably with "data compromise" and "data breach" throughout this document.
[6] A "record" refers to the unit of data disclosed in an incident. For instance, a payment card or social security number.

While we believe this database to be unique in terms of quantity and quality, it is by no means perfect. For various reasons[7], not every possible element in the data model was collected for every incident. Though challenges such as sampling techniques, response rates, and self-selection are not relevant to the research method used in this study, it cannot be concluded that the findings are therefore unbiased. Perhaps most obvious is that the database is dependent upon cases which Verizon was engaged to investigate. Those familiar with publicly available statistics on data loss will quickly recognize differences between these sources and the results presented in this report. This has much to do with caseload. For instance, it is simply more likely that an organization will desire a forensic examination following a network intrusion than a lost laptop. Similarly, the evolution of disclosure and notification laws influences an organization's decision to pursue investigation.

That said, there is a wealth of information here and no shortage of practical lessons that form a strong database for a DSS.

3. Data Model

As discussed earlier, the model described in this section began as a general classification system proposed in chapter 3, but was expanded and refined through field research to arrive at its current form. That current form is the A4 Threat Model, which provides a robust schema for describing security incidents in a structured and repeatable manner.

The A4 model is a response to one of the most critical and persistent challenges in security management—a lack of reliable information on the types and frequency of incidents. It targets this problem by helping organizations track useful incident metrics and then share that data (anonymously, responsibly, and meaningfully) with others. The overall goal is to lay a foundation from which we can constructively and cooperatively learn from our experiences to better measure and manage risk, which is especially important in tightly integrated and highly collaborative supply networks. In short, The A4 model aims to provide a database for an information security DSS.

[7] For instance, computer forensic investigations are dependent upon the availability of logs from the victim's network and host devices. Many victims fail to record or retain suitable logs, which hampers the investigations and limits findings.

The model comprises 3 major sections—Victim, Event (represented as the "4A's" Actor, Action, Asset, Attribute), and Impact—along with some miscellaneous context about the incident itself. There are certainly other things one might want to record about an incident and its effects, but the model attempts to strike a balance between exhaustiveness and usefulness. In keeping with the goals stated above, everything in the A4 model must directly support decisions and practice.

The full A4 data schema (in JSON) is included in Appendix A. Data elements defined by that schema are listed and described in the remainder of this section.

3.1 Incident context

This portion of the schema captures general information about the incident. Its purpose is to enable organizations to identify, store, and retrieve incidents over time.

- *incident_id* (string): Uniquely identify incidents for storage and tracking over time.
- *source_id* (string): Associate an incident with an entity that is handling or reporting it. Should be a non-attributable pseudonym if anonymity is desired.
- *security_incident** (string; enumeration; *required): Designates confirmed incidents from those that are suspected or non-incident events.
- *summary* (string): Capture a short free-form narrative of the incident as a supplement to the A4 classification.
- *related_incidents* (string): Provides a simple and explicit way to associate different incidents.
- *confidence* (string; enumeration): Provides a level of confidence associated with the information submitted for this incident.
- *notes* (string): Captures any additional information, observations, etc., about the incident that are not captured elsewhere.

3.2 Victim Description

The Victim section describes (but does not identify) the organization affected by the incident. The primary purpose is to aid comparisons between different organizational demographics (across industries, sizes, regions, etc.). While any number of characteristics could be tracked, those listed below provide an adequate basis for interesting and useful comparisons.

- *victim.victim_id* (string): To associate incidents with the entity that was affected by them (without identifying the entity itself). Even in anonymous incident sharing scenarios, this can be useful for many purposes. For instance, it is necessary to study things like the average number of incidents per organization, why certain organizations suffer more incidents, whether certain corrective actions lead to reduced incidents/losses, etc.
- *victim.industry* (string): Allows industry-specific analysis, trending, and comparisons.

- *victim.country* (string): Allows geographic analysis, trending, and comparisons.
- *victim.state* (string): Allows more specific in-country geographic analysis, trending, and comparisons if desired.
- *victim.employee_count* (string): Allows analysis, trending, and comparisons based on organizational size.
- *victim.revenue* (comprised of the amount (integer) and *iso_currency_code* (string): Allows analysis, trending, and comparisons based on organizational revenue (another indicator of size).
- *victim.locations_affected* (integer): Gives a sense of scale for the incident with respect to the organization affected.
- *victim.notes* (string): Captures any additional victim information.

3.3 Event Description

The event section translates the narrative of "who did what to what (or whom) with what result?" into a form suitable for sharing and analysis. Thus, classifying a security incident essentially means identifying all the actors, actions, assets, and attributes (the 4 A's) involved. It is our position that the four A's represent the minimum information necessary to adequately describe any threat event or incident. Furthermore, this structure provides an optimal framework within which to measure frequency, associate controls, link impact, and many other concepts required for risk management.

Actors: Whose actions affected the asset

Actions: What actions affected the asset

Assets: Which assets were affected

Attributes: How the asset was affected

3.3.1 Actors

There can be more than one actor involved in any particular incident, and their actions can be malicious or non-malicious, intentional or unintentional, causal or contributory. The A4 model recognizes three primary categories of threat actors - External, Internal, and Partner.

> *Classification note: If the actor's role in the breach is limited to a contributory error, the actor would not be included here. For example, if an insider's unintentional misconfiguration of an application left it vulnerable to attack, the insider would not be considered a threat actor if the application were successfully breached by another actor. An insider who deliberately steals data or whose inappropriate behavior (e.g., policy violations) facilitated the breach would be considered a threat actor in the breach.*

External threats originate from sources outside of the organization and its network of partners. Examples include criminal groups, lone hackers, former employees, and government entities; also included are God (as in "acts of"), "Mother Nature," and random chance. Typically, no trust or privilege is implied for external entities.

- *actor.external.motive* (string): Motive is a key component of understanding and defending against intelligent threat actors.
- *actor.external.variety* (string): Identifying the specific variety helps assess the resources, capabilities, and tendencies of the actor.
- *actor.external.country* (string): Identifies the geographic origin of the actor, which is useful on multiple investigatory, operational, and strategic levels.
- *actor.external.notes* (string): Captures any additional external actor information.

Internal threats are those originating from within the organization. This encompasses company full-time employees, independent contractors, interns, and other staff. Insiders are trusted and privileged (some more than others).

- *actor.internal.motive* (string): Motive is a key component of understanding and defending against intelligent threat actors.
- *actor.internal.variety* (string): Identifying the specific variety helps assess the resources, capabilities, and tendencies of the actor.
- *actor.internal.notes* (string): Captures any additional internal actor information.

Partners include any third party sharing a business relationship with the organization. This includes suppliers, vendors, hosting providers, outsourced IT support; some level of trust and privilege is usually implied between business partners.

- *actor.partner.motive* (string): Motive is a key component of understanding and defending against intelligent threat actors.
- *actor.partner.industry* (string): Identifying the partner's industry (or the services provided) helps to assess and manage risk in dealing with 3rd parties.
- *actor.partner.country* (string): Identifies the geographic origin of the actor, which is useful on multiple investigatory, operational, and strategic levels.
- *actor.partner.notes* (string): Captures any additional partner actor information.

3.3.2 Actions

Threat actions describe what the threat actor(s) did to cause or contribute to the incident. Every incident has at least one, but most will comprise multiple actions (and often across multiple categories). The A4 model uses 7 primary categories of threat actions: Malware, Hacking, Social, Misuse, Physical, Error, and Environmental.

Malware is any malicious software or computer code that alters a device's state or function without the owner's informed consent. Examples include viruses, worms, spyware, keyloggers, backdoors, etc.

- *action.malware.variety* (string): In the short term, variety is necessary to adequately describe the incident and its ramifications. In the long term, it gives insight into the evolving nature of malware and how criminals use it.
- *action.malware.vector* (string): Understanding how malware was introduced into the network or system is essential to assessing control weaknesses/vulnerabilities and identifying mitigation strategies.
- *action.malware.cve* (string): Identifying the specific vulnerability exploited is useful on many levels. It enables one to determine the percentage of malware that exploit vulnerabilities and which ones are exploited. The vulnerability ID also allows for useful secondary metrics like how long the vulnerability was publicly known, whether a patch existed (and for how long), etc.
- *action.malware.name* (string): Collecting (and hopefully sharing) attributes like these can aid more effective detection and response.
- *action.malware.notes* (string): Captures any additional malware action information.

Hacking is defined as all attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms. Includes brute force, SQL injection, cryptanalysis, denial of service attacks, etc.

- *action.hacking.variety* (string): The specific variety involved is essential to adequately describing the incident, assessing control weaknesses/vulnerabilities, and identifying mitigation strategies.
- *action.hacking.vector* (string): The vector of attack supplements information regarding the type selected above. In some cases, the same type of action conducted through different vectors requires very different defenses.
- *action.hacking.cve* (string): Identifying the specific vulnerability exploited is useful on many levels. It enables one to determine the percentage of attacks that exploit vulnerabilities and which ones are exploited. The CVE also allows for useful secondary metrics like how long the vulnerability was publicly known, whether a patch existed (and for how long), etc.
- *action.hacking.notes* (string): Captures any additional hacking action information.

Social tactics employ deception, manipulation, intimidation, etc., to exploit the human element, or users, of information assets. Includes pretexting, phishing, blackmail, threats, scams, etc.

- *action.social.variety* (string): The specific variety involved is essential to adequately describing the incident, assessing control weaknesses/vulnerabilities, and identifying mitigation strategies.
- *action.social.vector* (string): Because the social tactics can be conducted through different vectors (e.g., pretexting over the phone or in-person), this helps to further establish policies and procedures and educate employees to recognize and resist social tactics.
- *action.social.target* (string): Knowing who is targeted helps to focus policies and procedures and better educate appropriate employees to recognize and resist social attacks.
- *action.social.notes* (string): Captures any additional social action information.

Misuse is defined as the use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended. Includes administrative abuse, use policy violations, use of non-approved assets, etc. These actions can be malicious or non-malicious in nature. Misuse is exclusive to parties that enjoy a degree of trust from the organization, such as insiders and partners.

- *action.misuse.variety* (string): The specific variety involved is essential to adequately describing the incident, assessing control weaknesses/vulnerabilities, and identifying mitigation strategies.
- *action.misuse.vector* (string): Identifying the vector helps to further establish policies and procedures to deter, prevent, and detect misuse.
- *action.misuse.notes* (string): Captures any additional misuse action information.

Physical actions encompass deliberate threats that involve proximity, possession, or force. Includes theft, tampering, snooping, sabotage, local device access, assault, etc.

- *action.physical.variety* (string): The specific variety involved is essential to adequately describing the incident, assessing control weaknesses/vulnerabilities, and identifying mitigation strategies.
- *action.physical.vector* (string): Further informs mitigation strategies. Depending on the location whole groups of controls may not apply (i.e., biometric access to corporate facilities does not protect a laptop left in a car).
- *action.physical.notes* (string): Captures any additional physical action information.

Error broadly encompasses anything done (or left undone) incorrectly or inadvertently. Includes omissions, misconfigurations, programming errors, trips and spills, malfunctions, etc. It does NOT include something done (or left undone) intentionally or by default that later proves to be unwise or inadequate.

- *action.error.variety* (string): The specific variety involved is essential to adequately describing the incident, assessing control weaknesses/vulnerabilities, and identifying mitigation strategies.
- *action.error.vector* (string): Helps establish policies and procedures and educate employees on how errors can be avoided.
- *action.error.notes* (string): Captures any additional error action information.

Environmental not only includes natural events such as earthquakes and floods, but also hazards associated with the immediate environment or infrastructure in which assets are located. The latter encompasses power failures, electrical interference, pipe leaks, and atmospheric conditions.

- *action.environmental.variety* (string): Helps establish strategies to avoid or recover from environmental events.
- *action.environmental.notes* (string): Captures any additional environmental action information.

3.3.3 Assets

This section describes the information assets that were compromised during the incident. "Compromised" refers to any loss of confidentiality/possession, integrity/authenticity, availability/utility (primary security attributes). Naturally, an incident can involve multiple assets and affect multiple attributes of those assets.

- *asset.variety* (comprised of the *name* (string) and *amount*(integer) variables): The specific variety involved is essential to adequately describing the incident, assessing control weaknesses/vulnerabilities, determining impact, and identifying mitigation strategies.
- *asset.governance* (string): Identifies potential risk factors related to 3rd party or personal ownership, management, etc. Trends over time can help inform risk, governance, and sourcing decisions.
- *asset.country* (string): Tracks assets that might be hosted in a facility that is not in the same country as the victim organization.
- *asset.cloud* (string): Trends over time can inform risk, governance, and deployment decisions.
- *asset.notes* (string): Captures any additional asset information.

3.3.4 Attributes

This section describes which security attributes (of the previously-identified assets) were compromised during the incident. To accomplish this, the A4 model uses a paired version of the six primary security attributes of confidentiality/possession, integrity/authenticity, availability/utility. An extension of the "C-I-A Triad," they are commonly called the "Parkerian

Hexad," after their originator, Parker (1998). Multiple attributes can be affected for any one asset and each attribute contains different metrics.

Confidentiality refers to limited observation and disclosure of an asset (or data). Possession refers to the owner retaining possession and control of an asset (or data). A compromise of these security attributes involves unauthorized access, disclosure, exposure, or loss of control.

- *attribute.confidentiality.data_disclosure* (string): Distinguishes between data compromise and exposure (at-risk) events.
- *attribute.confidentiality.data* (comprised of the *variety*(string) and *amount* (integer): The variety and amount of data affected is central to assessing impact, proper response and reporting, etc.
- *attribute.confidentiality.state* (string): Controls for data at-rest and data in-motion are often different.
- *attribute.confidentiality.notes* (string): Captures any additional confidentiality/possession attribute information.

Integrity refers to an asset (or data) being complete and unchanged from the original or authorized state, content, and function. Authenticity refers to the validity, conformance, correspondence to intent, and genuineness of the asset (or data). A compromise of these attributes involves unauthorized change, non-conformance or invalidity.

- *attribute.integrity.variety* (string): Provides some additional context and structure around how integrity/authenticity was affected.
- *attribute.integrity.notes* (string): Captures any additional integrity/authenticity attribute information.

Availability refers to an asset (or data) being present, accessible, and ready for use when needed. Utility refers to the usefulness or fitness of the asset (or data) for a purpose. A compromise of these security attributes involves assets being inaccessible or unusable as needed when needed.

- *attribute.availability.variety* (string): Provides some additional context and structure around how availability/utility was affected.
- *attribute.availability.duration* (comprised of the *unit*(string) and *value* (number): The duration of availability/utility loss provides useful context and helps assess impact.
- *attribute.availability.notes* (string): Captures any additional availability/utility attribute information.

3.4 Impact Assessment

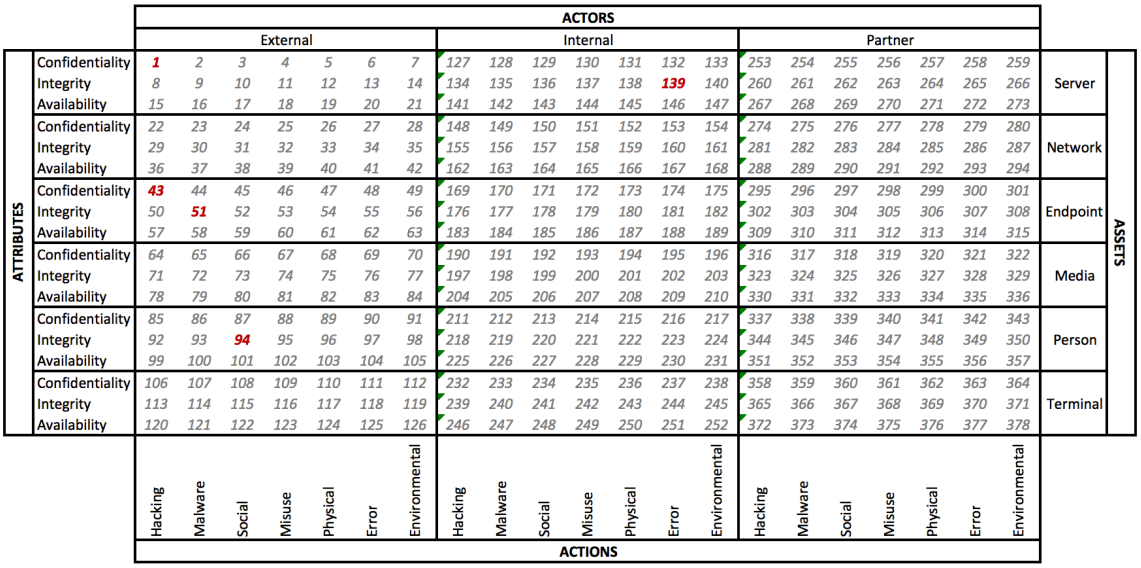
One of the more important pieces of information about an incident is the impact it has on the organization. Unfortunately, the true scope and extent of consequences can be difficult to measure since a wide array of tangible and intangible costs can be involved. With this in mind, we assess impact from three perspectives in order to provide an understanding and measure of consequence associated with the incident. Together they seek to 1) categorize the varieties of losses experienced, 2) estimate their magnitude, and 3) capture a qualitative assessment of the overall effect on the organization.

- *impact.overall_rating*(string): Provides a sense for the relative impact of the incident to the organization. The scale is constructed around the notion of an injury to help answer the simple (but important) question of "How bad did it hurt?"
- *impact.overall_amount*(number), *impact.overall_min_amount*(number), *impact.overall_max_amount*(number): Quantifying the impact of an incident (even using broad estimations) is a useful exercise for many reasons. It allows for direct comparison with other incidents and helps to put security-related losses in context with other types of risk. Furthermore, since impact is an essential component of risk, tracking losses is important to fueling risk assessment and treatment efforts. It also provides fodder for some very interesting metrics around spending and losses within the security program.
- *impact.loss* (comprised of the *variety* (string),*rating* (string), and *amount, min_amount, max_amount* (number) variables): Identify the types of impact experienced after an incident, and indicate how overall losses are distributed among them.
- *impact.iso_currency_code* (string): Allows for normalization across estimates using different currencies.
- *impact.notes* (string): Captures any additional impact information.

4. Describing Incidents with the A4 Model

If we calculate all the combinations of the A4 model's highest-level elements, (3 actors, 7 actions, 6 assets, and 3 attributes), 378 distinct threat events emerge. Figure 1 graphically represents these threat events as numbered intersections in a grid format. Threat Event #1, for instance, coincides with an external actor using hacking actions to compromise the confidentiality of a server. Theoretically, the grid captures all possible threats to information assets, but not all 378 A4 combinations are directly feasible. For instance, malware cannot infect people, whereas social actions only affect people.

Figure 1. A4 grid depicting all 378 high-level threat events.



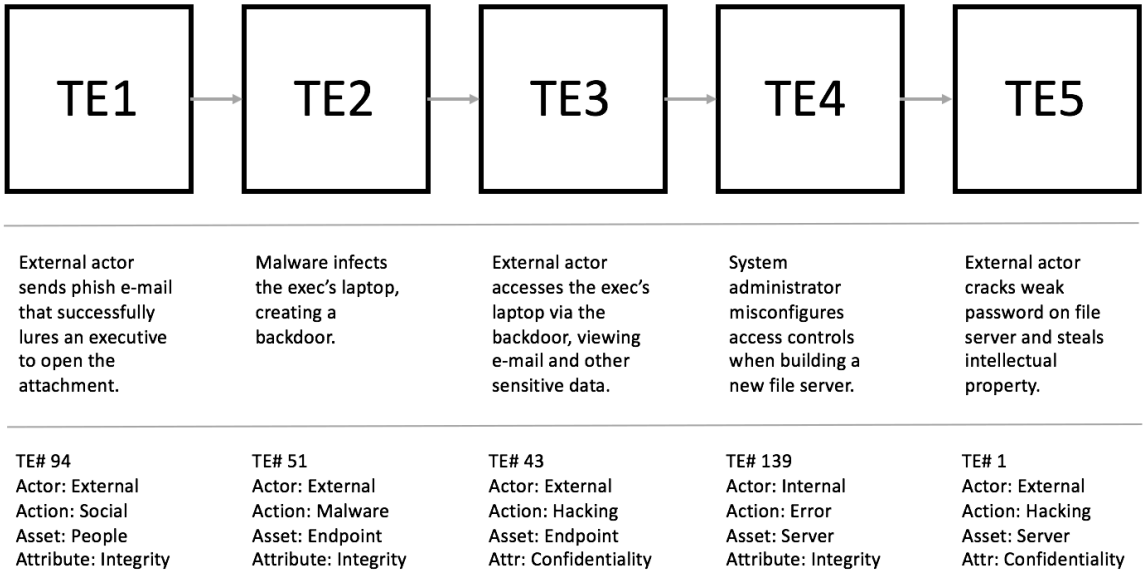
Incidents often involve multiple threat events, and so will span multiple intersections in the grid. Reconstructing that chain of events using the A4 ontology is how we model incidents to generate the statistics that follow in the next section. Figure 2 demonstrates this concept for a incident where a "spear phishing" attack eventually leads to the exfiltration of intellectual property (IP) from an organization.

The incident includes five threat events, which are described in both narrative and A4 form. The Threat Event (TE) numbers correspond to the numbered grid intersections from Figure 1. Once the main event chain is complete, additional classification can add more specificity around the elements comprising each event (i.e., the particular type of external actor or exact hacking methods used, etc.).

One final note before we conclude this sub-section. The process described above has value beyond just describing the incident itself; it also helps identify what might have been done (or not done) to prevent it. The goal is straightforward: break the chain of events and you stop the incident from proceeding. For instance, security awareness training and e-mail filtering could help keep TE1 from occurring. If not, anti-virus and a least-privilege implementation on the laptop might prevent TE2. Impeding progression from TE2 to TE3 may be accomplished through egress filtering or network traffic analysis to detect and prevent backdoor access. Security policy automation and change control procedures could help avoid the administrator's misconfiguration described in the conditional event and preclude the compromise of intellectual property in TE4.

These are just a few examples of potential controls for each event, but the ability to visualize a layered approach to deterring, preventing, and detecting the incident should be apparent.

Figure 2. Example A4 model event chain consisting of 5 threat events (TE).



4.1 A4 Model Terminology

A^4 Threat Model: A framework that contains all theoretical threats against information assets. The "4A's" are Agent, Action, Asset, and Attribute.

Event: Any threat action against an information asset, whether deliberate or unintentional. This action may or may not compromise a security attribute (confidentiality, integrity, or availability) of an asset. If it does, the event constitutes an incident.

Incident: Any event (or series of events) that compromises a security attribute (confidentiality, integrity, availability) of an information asset.

Data disclosure: An incident resulting in the disclosure of data to unauthorized parties.

Campaign: A set of two or more related incidents, usually conducted by a common threat actor(s) and a common purpose.

Threat scenario: A threat event (or series of events) that *could theoretically* occur rather than something that actually occurred. Generally used for threat assessment and modeling purposes.

4.2 The A4 data format

When it comes to formats for storing data, there is no shortage of options. The incident data described above *could* be stored in a relational database, a "NoSQL" database, Extensible Markup Language (XML) documents, JavaScript Object Notation (JSON), or a number of other options. The question is what format is most suitable to the nature of the data and what we want to do with the data once it is stored.

The primary drivers for our incident database are simple storage, analysis, and sharing. Based on these criteria, we chose to represent all incidents in the A4 model as JSON objects. JSON is simpler to work with (by people, software, and machines) than XML and relational databases and it imports directly into many modern programming languages like Python. It also can be easily loaded into a NoSQL database like Mongo and accessed using JavaScript to query the data. Another advantage of JSON is that, unlike XML, one doesn't need to define new tags and attributes as data fields evolve over time. This is very important for incident data because experience over the last decade shows that the desire to expand our understanding of risk factors necessitates that we expand the data we collect. Perhaps the single biggest benefit of JSON, however, is that it provides an optimal data exchange format to facilitate sharing of incident information within a community of peers.

The full JSON object for the incident depicted in Figure 2 is included in Appendix A. It should be noted that not all A4 threat model elements listed in the previous section are included. This is not an omission; JSON objects include whatever data elements were recorded and no more (i.e., if there were no physical actions, physical.vector and physical.variety will not be part of the object).

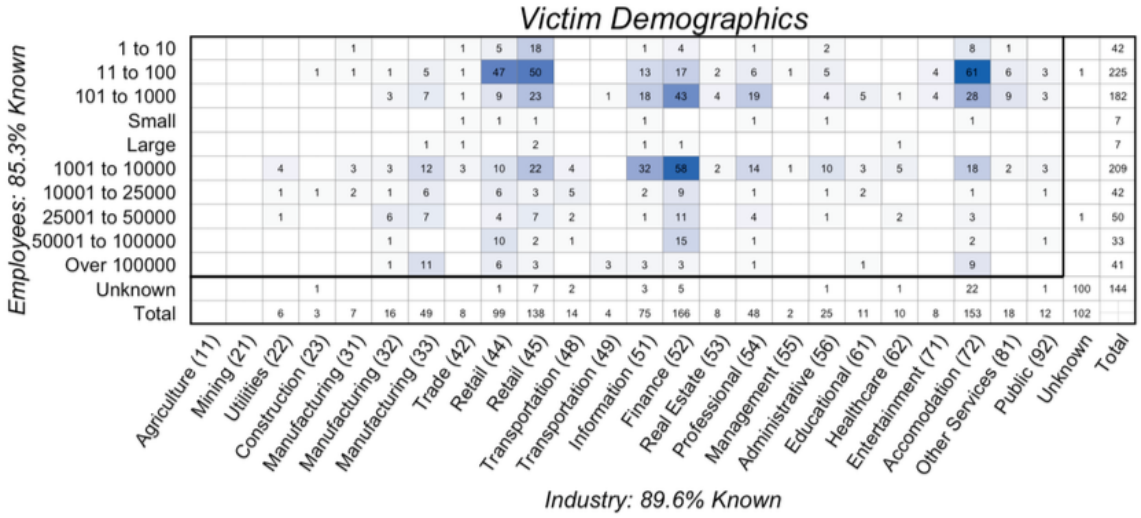
5 Data Analysis

In this section, we present the findings from the data collection efforts described earlier in this chapter. We seek to better understand and measure the "who, what, when, where, how, and why" behind security breaches so that we can better manage risk. We pay particular attention to how supply chain partners cause and contribute to breaches. Our goal here is descriptive only; we dig deeper into research questions, supply chain risk factors, and modeling in the next chapter.

5.1 Victim Demographics

It's tempting to skip directly to describing the details of the incident itself rather than the organization affected by the incident. But demographic information is critically important to modeling and decision support because it helps answer questions like "how is my risk different from that of other organizations?" and "who should I share information with to better understand the risks to my organization?" This is even more important from a supply chain perspective, since risk is aggregated and shared across collaborating partners.

Figure 3. Breach count by victim industry (x axis) and size (y axis).



The major takeaway from Figure 3 is that breaches affect organizations of all types and sizes. This suggests that any partner, regardless of their industry or size, adds cyber risk to the supply chain. Figure 4 provides a simplified categorical view of victim demographics according to basic supply chain roles. While not a perfect measure of incident frequency across the supply chain, this view does hint that certain roles may be comparatively riskier than others. For instance, a "more is better" approach may not be the best strategy for partnering with various types of support organizations like IT service providers and professional consultancies. As with interpersonal relationships, each organization brings its own set of problems and each connection brings a chance of getting hurt. This finding appears to support those of Chapter 4, which showed incident likelihood increasing with the number of partners and level of integration.

Figure 4. Simplified breach count by victim's role in supply chain.

SC Role	***Related industries***	***# breaches***
Upstream	Manufacturing	72
Midstream	Transportation	18
Downstream	Retail, Trade	245
Support	Finance, Information, Professional, Management, Administrative	316

It is not clear from these data exactly why certain industries recorded a higher number of incidents than others. This may be due to criminal motives (i.e., they often follow the money trail to banks and retailers) or victim vulnerabilities (i.e., criminals also follow the path of least resistance) or something else entirely. It is most likely a combination of many factors. Something else we cannot determine from Figures 3 and 4 is whether different demographics exhibit different risk profiles (i.e., varying actors, actions, assets), but this critical question will be addressed later in this chapter.

5.2 Incident Description

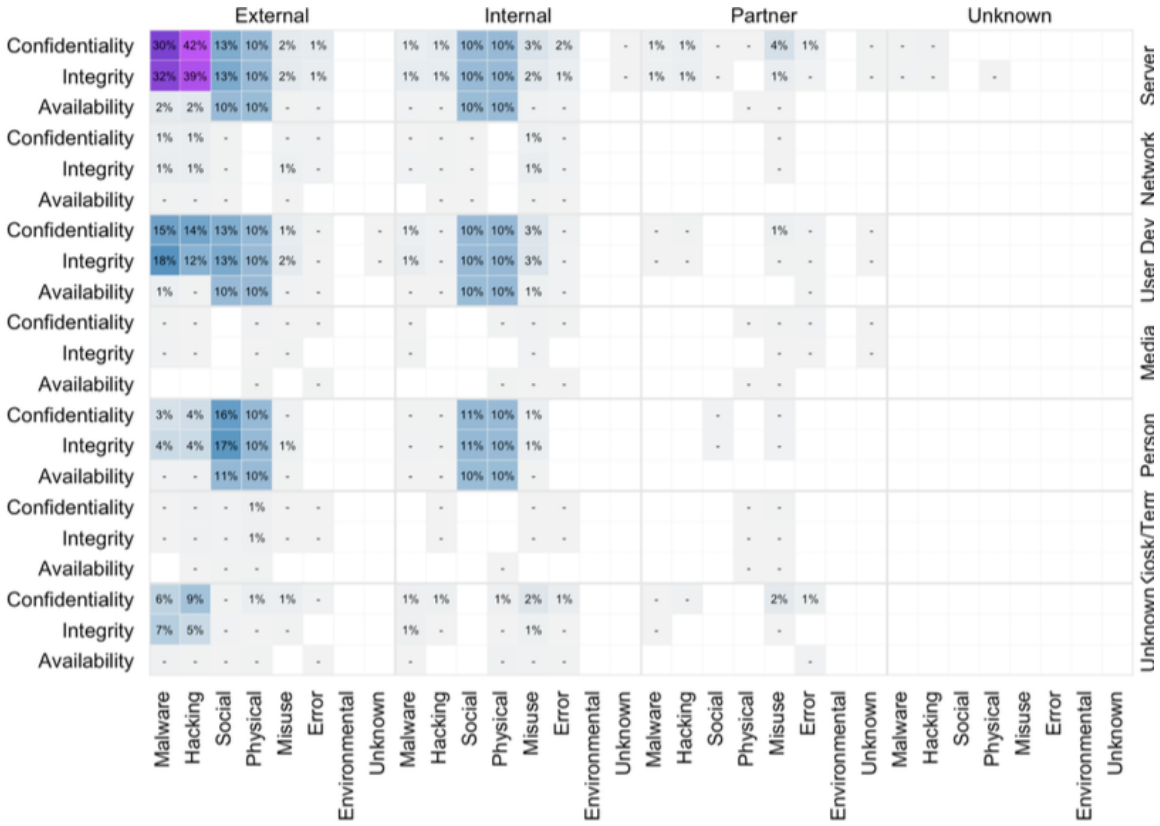
The next few sub-sections provide analyses of the actors, actions, assets, and attributes (the 4 A's), but first we present a big-picture view that ties them all together. Figure 5 shows *associations* between the four A's within incidents, and is our most consolidated view of the 982 incidents analyzed in this study. The proper way to interpret Figure 5 is "30% of all incidents involved an external actor AND a malware action AND a server asset AND the confidentiality attribute" (upper left intersection). It does NOT necessarily mean that an external actor installed malware that compromised the confidentiality of a server.

The first observation is that much of the grid is blank or almost blank, meaning the intersecting A's never (or rarely) appeared together within a single incident (the "." represent values greater than 0 but less than 1%). On the other end of the spectrum, a relatively few hot spots jump out. As we dive deeper into these results, reasons for this will become apparent, but for now we note that the intensity is confined to a relatively few associations.

Also apparent from Figure 5 is that we observed all high-level categories under each of the 4 A's (with the one exception of environmental actions). In other words, all types of threat actors (external, internal, and partner), assets (servers, network devices, user devices, media, people, and kiosks), etc., were involved in incidents. The frequency differed dramatically among

them, but this offers evidence that our framework isn't bloated with unrealistic, theoretical possibilities; these things really happen.

Figure 5. Grid depicting associations between actors, actions, assets, and attributes.



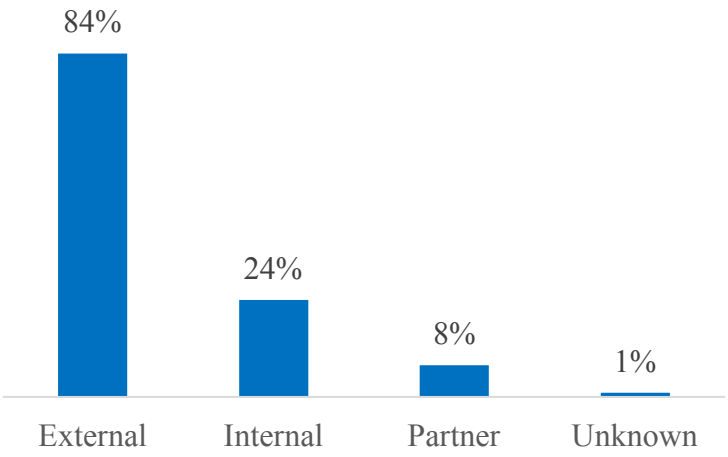
What may be less obvious from Figure 6, is that we did NOT see things that fall outside of the scope of our A4 designations, at least at a high level. This is due largely to the two-phased data collection approach described above. During the first pass, we found many incidents that could not be described within the original scope, but using several hundred incidents to refine the model achieved the completeness characteristic needed in a taxonomy.

We could elaborate on high-frequency associations such as External > Hacking > Server > Confidentiality, but this is more meaningful at a lower level of analysis. We provide this in the A4 subsections that follow. The important thing is that this provides security management with a quick overview of high risk scenarios to focus further investigation and remediation efforts.

5.2.1 Actors

Identifying "whodunit" is a primary goal of any criminal investigation, and it is no different for cybercrime. This piece of information is critical to incident response, longer-term defensive strategies, and, quite possibly, military, political, legislative, and legal actions. Figure 6 shows the percentage of incidents tied to external, internal, and partner threat actors. These sum to over 100% because incidents sometimes involve more than one category of actor (~16% of the time). An outsider colluding with an insider or partner to steal corporate secrets is an example of this.

Figure 6. Number (and Percent) of incidents per threat actor category.



These results strongly challenge classic information security doctrine that insiders are responsible for 80% of incidents (Bejtlich, 2009). That our findings suggest the exact opposite may surprise many, and are thus worthy of additional explanation. First, remember that this database does not represent all incidents; it is a subset biased in various ways as described above. If one were to arrange all incidents on a spectrum from minor to critical, these would skew heavily to the critical end. Minor to moderate incidents occur regularly, often involve employee mistakes and misconduct, and are routinely handled by internal staff. Conversely, this study encompasses some of the worst breaches on record over the last decade. These results, then, suggest that 80%+ of major security breaches stem from external threat actors.

Figure 6 should not, however, be interpreted to advise that insiders and partners can be safely ignored. They still contribute to 24% and 8% of incidents, respectively. Both offer a reminder of risk inherent to supply chain partnerships. Partners compromise other organizations

and people inside those organizations steal data from their employer (which may include data shared by other partners). What's more, we often observed external actors exploit partner infrastructure and accounts as step on the path toward compromising the target victim. These indirect "partner-as-a-vector" attacks nearly tripled direct "partner-as-an-actor" attacks (202 vs 76). This offers strong evidence that the survey results from chapter 4 reveal more than mere perception.

5.2.1.1 External Actors

Figure 7 and Figure 8 present more detailed information on the varieties of external threat actors involved in these incidents. Over three-quarters of all external breaches were tied to organized criminal groups, which is a good indicator of the highly professional nature of crime in the Internet Age. Although unaffiliated individuals with no known ties rank a distant second in Figure 7, it is clear our data tell a story that cybercriminals prefer to hunt in packs rather than as lone wolves.

Figure 7. Varieties of external threat actors (unknown=58%).

Variety	Breach %	Breach #
Organized crime	76%	264
Unaffiliated	13%	45
Activist	4%	12
Former employee	3%	10
State-affiliated	3%	9
Force majeure	1%	4
Nation-state	1%	3
Competitor	1%	3
Other	0.3%	1

While actor varieties and motives drop off quickly after the money-hungry pros are accounted for, Figure 7 and Figure 8 still reveal some important trends below the surface. Attacks launched by activist groups "just for fun" or as a means of protest are not uncommon. Nor is cyber espionage from competitors, nation states, or state-affiliated groups. Even grudges lead some to offensive action. Overall, these findings seem to suggest that crime in the online world imitates crime in the physical world.

One additional item deserves further brief explanation regarding external threat actors. It is often difficult to ascertain details about externally-sourced attacks. The Internet affords ample opportunity to hide one's identity and intentions, and many cybercriminals are quite good at hiding their tracks. Attribution also requires that the victim log and retain information about activity in their networks so that investigators have access to the evidence they need. Unfortunately, such evidence often does not exist. The combination of these circumstances is why the number of unknowns is so high in Figure 7 and Figure 8.

Figure 8. Motives of external threat actors (unknown=16%).

Motive	Breach %	Breach #
Financial	94%	646
Espionage	2%	15
Fun	2%	12
Ideology	1%	9
N/A	1%	7
Grudge	2%	4
Secondary	0.1%	1

5.2.1.2 Internal Actors

We find the statistics on the types of insiders behind breaches in Figure 9 a bit counterintuitive. Lesser-privileged end-users outnumber highly-privileged system administrators by a ratio of almost 3 to 1. Apparently, one does not need high levels of access to information systems in order to conduct or contribute to security incidents. This is another lesson for managing risk in the supply chain—sharing data with partners puts it in reach of many more employees than one might initially suspect.

Breaches tied to executives, financial staff, and HR make the list, but altogether sum to less than 5%. It should also be noted that former employees are considered external actors, and so appear in Figure 7 (10 breaches).

Figure 9. Varieties of internal threat actors (unknown=7%).

Variety	Breach %	Breach #
End user	68%	144
System admin	25%	53
Developer	4%	9
Executive	3%	7
Finance	1%	2
Human resources	1%	1
Helpdesk	1%	1
Call center	1%	1
Auditor	1%	1

When it comes to the motives behind internal breaches, two broad categories stand out. They usually either did it for the money (financial gain) or they did not mean to do it at all (NA). Every now and then, they did it for other things too, which can be seen in Figure 10.

Figure 10. Motives of internal threat actors (unknown=14%).

Motive	Breach %	Breach #
Financial	66%	130
N/A	26%	51
Fun	5%	9
Convenience	3%	6
Grudge	2%	3
Ideology	1%	1
Espionage	1%	1

5.2.1.3 Partner Actors

It must be stated up front that the following statistics refer to cases where the actions of a business partner played a **direct causal role** in the breach. There are other ways partners indirectly contributed to incidents, and these will be discussed within the appropriate section. Per Figure 6 above, about 8% of incidents were directly caused by partner actions during the timeframe of our study.

The obvious question is "what types of partners cause the most incidents?" Answering this is the purpose of Figure 11, which shows the distribution of industries (organized by NAICS

code) for partner threat actors[8]. Note that the list excludes industries responsible for fewer than 1% of incidents.

Figure 11. Industry distribution of partner threat actors

NAICS #	NAICS Description	Breach %
518	Data Processing, Hosting, and Related Services	24%
541	Professional, Scientific, and Technical Services	19%
0	Unknown	17%
561	Administrative and Support Services	9%
562	Waste Management and Remediation Services	3%
622	General Medical and Surgical Hospitals	3%
492	Couriers and Messengers	3%
491	Postal Service	2%
423	Merchant Wholesalers, Durable Goods	2%
519	Other Information Services	2%
511	Publishing Industries (except Internet)	2%
56	Administrative and Support and Waste Management and Remediation Services	2%
62	Health Care and Social Assistance	1%
524	Insurance Carriers and Related Activities	1%
238	Specialty Trade Contractors	1%
522	Credit Intermediation and Related Activities	1%
334	Computer and Electronic Product Manufacturing	1%

A review of Figure 11 reveals just under half of offending partners fall into some type of IT service provider. Roughly one-quarter are data processing and hosting providers, which is a meaningful result in light of findings from Chapter 4. There we proposed the level of data sharing and IT interconnectivity were highly significant factors in supply chain risk. Arguably,

[8] Figure 6 shows 76 incidents tied to partner actors. Figure 11 supplements these with another 162 incidents from an open incident repository, called VCDB (https://github.com/vz-risk/VCDB/tree/master/data). We did this to give the most complete view of industries possible for partner threat actors.

relationships with 3rd party data processors and hosting providers represent the highest echelon of these criteria. Because NAICS code 541 (Professional, Scientific, and Technical Services) is a bit ambiguous, we submit Figure 12. From that, it becomes more apparent that this category is IT-focused as well, which gives further credence to our findings.

Figure 12. Distribution of partner threat actors within NAICS sector 541 (Professional, Scientific, and Technical Services) and 561 (Administrative and Support Services).

NAICS #	NAICS Description	Breach %
541 (Professional, Scientific, and Technical Services)		
541513	Computer Facilities Management Services	11
541512	Computer Systems Design Services	7
541511	Custom Computer Programming Services	6
541219	Other Accounting Services	4
541611	Administrative Management and General Management Consulting Services	3
541519	Other Computer Related Services	2
541990	All Other Professional, Scientific, and Technical Services	2
561 (Administrative and Support Services)		
561720	Janitorial Services	4
561110	Office Administrative Services	3
561499	All Other Business Support Services	3
561320	Temporary Help Services	2
561330	Professional Employer Organizations	2
561990	All Other Support Services	2

While Figure 11 and Figure 12 do indeed suggest data sharing and interconnectivity lead to riskier relationships, they also demonstrate that low-tech partners shouldn't be ignored. For instance, the most frequent offender in the 561 industry code (Administrative and Support Services) is Janitorial Services. Parcel and postal services, accountants, office administrators, and management consultants also fell in the top 20 3rd party industries. None of these necessitate high degrees of IT integration, but they do often involve a high degree of access to information. Consider a janitor in a typical enterprise workplace; they have the literal keys to the kingdom after everyone else has gone home. Combine that with a motive (a bribe from a competitor or identity thief should suffice) and the amount of sensitive information scattered across desks,

filing cabinets, and wastebaskets, and you have all the essential ingredients for low-tech—yet effective—data theft. This serves as an excellent reminder that both physical and digital threats must be considered to properly manage risk in modern supply chains.

Figure 13. Motives of partner threat actors (unknown=12%).

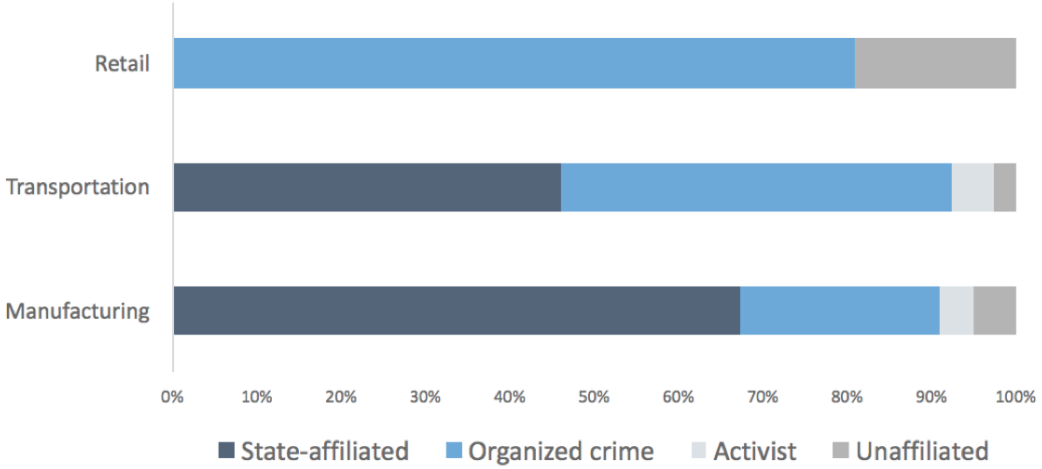
Motive	Breach %	Breach #
Financial	76%	51
N/A	19%	13
Convenience	3%	2
Other	2%	1

When it comes to motives, partners follow the same basic pattern of internal actors. Figure 13 reveals over three-quarters acted with financial gain in mind, while "un-motivated" (unintentional) incidents fell a distant second (20%). This makes sense given that partners are essentially insiders within another organization and thus would share similar inclinations.

5.2.1.4 Threat Actors by Industry

One might suspect that threat actor trends vary across different types of organizations. To test this, Figure 14 shows the percentage of breaches attributed to several common varieties of threat actors for three industries representing common supply chain roles. The disparities between them are readily apparent. Retail is plagued by organized criminal groups, while state-affiliated actors hammer Manufacturing. Transportation suffers fairly equally from both. Clearly, different industries are targeted by very different actors with very different motives.

Figure 14. Threat actor profiles by industry.



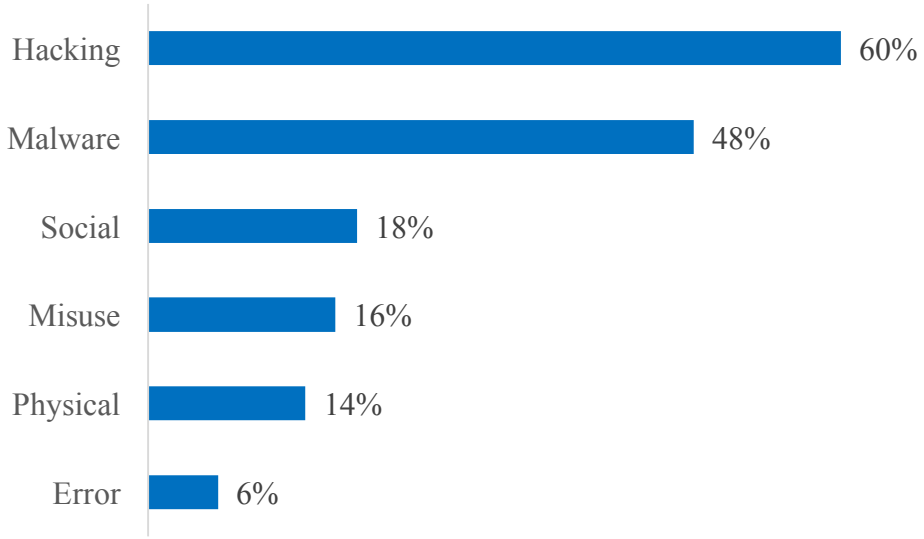
5.2.2 Actions

Arguably, determining the actions that led to a security incident is the single-most useful step toward preventing similar incidents in the future. While it's definitely helpful to know who was behind those actions, "how" typically has a more immediate bearing on corrective actions than "who." This is probably why most incident reporting efforts focus mainly on actions (e.g., see Federal Agency Incident Categories[9]).

The A4 model recognizes 7 high-level threat categories, each of which specify additional varieties and vectors. While these classifications are mutually exclusive from a singular event perspective, incidents often involve actions across multiple categories (because often incidents span multiple events). The incident depicted earlier in Figure 2, for instance, spans actions within the Social, Malware, Hacking, and Error categories. While more complicated from a classification perspective, the ability to capture all these details is one of the primary advantages of the A4 model. Incident taxonomies using a single "incident type" field would force a choice (i.e., either phishing or malware, or intrusion) that would lose critical information for remediation and decision support.

[9] https://www.us-cert.gov/government-users/reporting-requirements#tax

Figure15. Number (and percent) of breaches per threat action category.



Together, Figures 15 and 16 paint a very telling picture of modern cybercrime and reinforce what we saw from Figure 6 (threat actors). As business in the Internet age becomes interdependent on networks of information systems, the potential pool of threats that can access them illegitimately multiply exponentially. Hacking in malware is often the tool by which such access is gained because such actions circumvent physical distances and boundaries that have limited criminal actions for millennia. A relatively unskilled adversary can use commodity tools and techniques to exploit hundreds of victims across the world very quickly with little effort, while enjoying the high degree of anonymity the Internet affords.

Of course, Figure 15 serves as a reminder that breaches aren't limited to just network intrusions. Social tactics that target human vulnerabilities rather than those found in computer systems were not uncommon (18%), nor were physical attacks and various forms of privilege misuse. The low percentage attributed to error in Figure 15 deserves explanation. Security incidents almost always involve some poor decision, oversight, or mistake. Here we chose to include only those cases where errors were the proximate, or direct, cause of the incidents. An employee losing a laptop or accidentally posting non-public information to a website are common examples of such errors.

Figure 16. Top 20 varieties of threat actions across all breaches.

Category	Action Variety	Breach #	Breach %
Malware	Backdoor	182	19%
Hacking	Use of stolen creds	182	19%
Hacking	Brute force	149	15%
Hacking	Use of backdoor or C2	133	14%
Malware	Export data	131	13%
Physical	Theft	115	12%
Social	Pretexting	114	12%
Hacking	SQL injection	103	10%
Physical	Tampering	102	10%
Malware	Spyware/Keylogger	96	10%
Malware	Command/control (C2)	89	9%
Malware	Downloader	58	6%
Malware	Adminware	58	6%
Misuse	Privilege abuse	57	6%
Malware	Capture stored data	45	5%
Malware	RAM scraper	44	4%
Malware	Capture app data	40	4%
Social	Phishing	37	4%
Misuse	Net misuse	28	3%
Malware	Scan network	25	3%

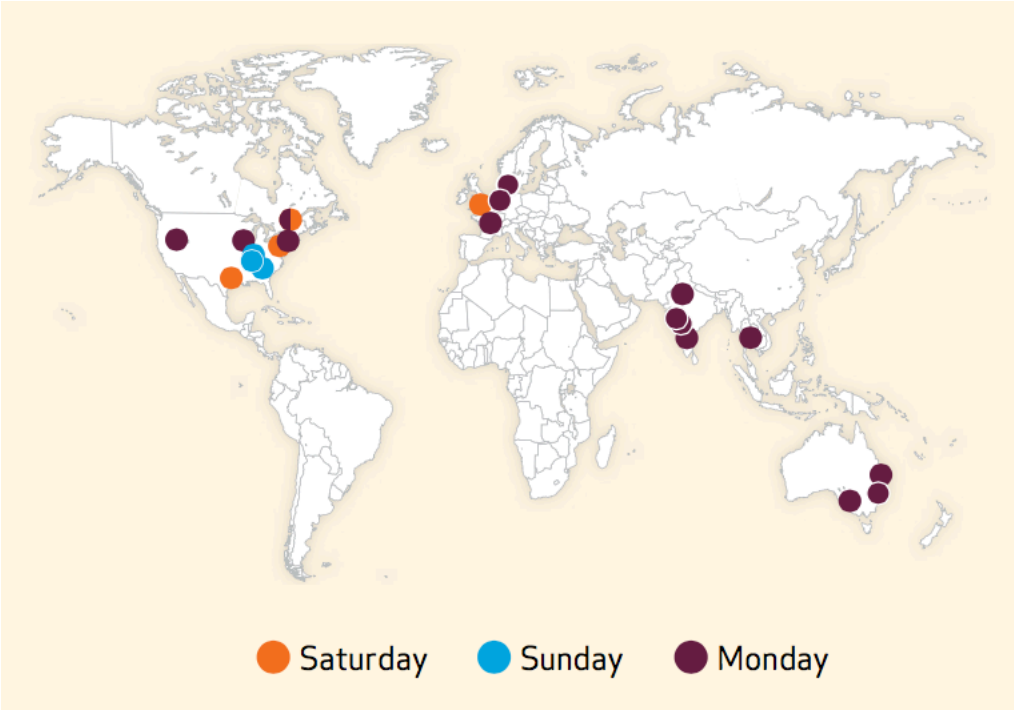
Figure 16 presents a more detailed view of threat actions observed across incidents, and highlights many findings useful for decision support. The A4 model defines over 150 varieties of threat actions, yet those outside the top 20 account for less than 3% of all incidents. This hints that threat actors do not act randomly; they actively use and reuse techniques that meet with success. If this holds true, then it further emphasizes the importance of data-driven risk management. Most security regulations and compliance standards weight all controls equally, yet these results suggest a more effective approach to risk reduction by prioritizing those that solve the biggest problems first. Per Figure 16, that may be a relatively short list, which would greatly help stressed security budgets and staff.

Those familiar with some of the hacking and malware techniques in Figure 16 will note that, for the most part, they are not terribly sophisticated. For instance, the most common methods of infiltrating corporate networks don't involve exploiting obscure zero-day software vulnerabilities or cracking military-grade encryption algorithms. Real cybercriminals prefer

plucking the low-hanging fruit of weak passwords, reusing stolen passwords, and leveraging malware backdoors (often planted through one of the first two methods). Such techniques are highly scalable, automatable, and unfortunately, available to many attackers via easy-to-use tools.

These concepts come to life in Figure 17 in a way that charts and stats simply cannot convey. While conducting one of the forensic investigations supplying this dataset, a law enforcement agency supplied us with a list of network intrusions tied to a small eastern European organized criminal group. These attackers managed to successfully compromise 22 organizations across nine countries in just three days using fairly simple—and completely automated—techniques. They hit hundreds more over a period of six months before finally being apprehended.

Figure 17. Location of successful network intrusions by a group of cybercriminals over a three-day period.



5.2.2.1 Partner Threat Actions and Vectors.

Given that external attacks greatly outnumber those attributed to partners in our dataset, it's difficult to discern Figure 16's relevance to 3rd party risk. Figure 18 makes this easier and

shows a similar list comprised of actions associated with partner-related breaches. While some similarities exist between the two lists (e.g., "Use of stolen creds" ranks #2 in both), overall they tell a very different story about how incidents occur. Instead of heavily skewed toward malware and hacking techniques, incidents caused by partner actors tilt strongly toward misuse and error. In terms of prioritization, it seems that policies and training are equally (if not more) important to technical countermeasures in terms of controlling cyber risk in the supply chain.

Figure 18. Top 20 varieties of threat actions across partner-related breaches.

Category	Action Variety	Breach #	Breach #
Misuse	Privilege abuse	15	20%
Hacking	Use of stolen creds	8	11%
Error	Misconfiguration	6	8%
Misuse	Data mishandling	5	7%
Error	Loss	4	5%
Error	Omission	4	5%
Error	Publishing error	3	4%
Malware	Export data	3	4%
Hacking	Brute force	2	3%
Hacking	Use of backdoor or C2	2	3%
Malware	Backdoor	2	3%
Malware	Capture app data	2	3%
Misuse	Knowledge abuse	2	3%
Misuse	Net misuse	2	3%
Misuse	Possession abuse	2	3%
Misuse	Unapproved hardware	2	3%
Misuse	Unapproved workaround	2	3%
Physical	Theft	2	3%
Social	Pretexting	2	3%
Error	Disposal error	1	1%

It is also interesting to examine how partner-facing accounts or infrastructure serve as the vector through which threat actions are conducted. Such incidents may be directly caused by external actors, but they exploit partner IT and trust relationships in order to be successful. Across the 982 incidents in this study, 202 (~21%) exploited a partner-related vector. Thus, the overall "partner problem" (defined as incidents directly caused or indirectly enabled by 3rd parties) represents over one-quarter of all incidents. As will be discussed in the next section, this

problem gets even bigger if this definition is further expanded to include all incidents affecting assets hosted or managed by partner organizations. We can't help but wonder if a similar ratio of the typical security budget and effort is allocated on managing 3rd party risk.

5.2.2.2 Threat Actions by Industry

We observed in the previous section that threat actors differed across industries. Following up on that line of analysis, we now examine whether this trend holds true for threat actions as well. Figure 19 compares the top five varieties of threat actions leading to data breaches within manufacturing, transportation, and retail firms.

Figure 19. Top threat action varieties by industry.

Category	Action Variety	Breach %
	Manufacturing	
Malware	Backdoor	23%
Hacking	Use of stolen creds	18%
Hacking	Use of backdoor or C2	18%
Malware	Command/control (C2)	17%
Malware	Export data	14%
	Transportation	
Malware	Command/control (C2)	36%
Malware	Spyware/Keylogger	29%
Hacking	Use of backdoor or C2	21%
Malware	Backdoor	21%
Malware	Destroy data	14%
	Retail	
Hacking	Use of stolen creds	22%
Hacking	Brute force	17%
Hacking	SQL injection	16%
Malware	Backdoor	15%
Malware	Export data	12%

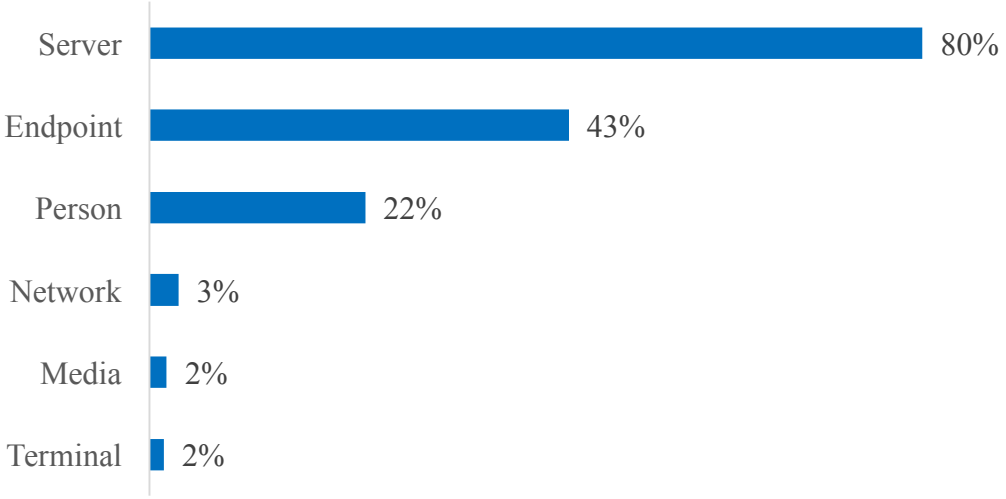
Only one threat action – backdoor malware - makes the cut for all three industries. While several appear in two of the three lists, several others are unique to only one industry. For industries that share common actions the proportions diverge substantially. The ratio of

command and control (C2) malware in the transportation sector, for instance, was twice that of manufacturing. This is an important finding because if the methods by which breaches occur differ across industries, so too must the methods for defending against them.

5.2.3 Assets

This section details the types of information assets compromised by the actors and actions heretofore examined. This is an important piece of the A4 model because it turns the conversation from an outward-looking "Who are they and what are they doing?" to a more personal "What do we have that needs protecting and what harm might arise if we fail?"

Figure 20. Categories of compromised assets.



As one might expect given the diversity of the modern IT environment, the list of all compromised assets is quite lengthy. Figure 20 presents statistics for high-level asset categories, while Figure 21 focuses on the 10 most oft-affected varieties (all the rest fall below the 3% mark).

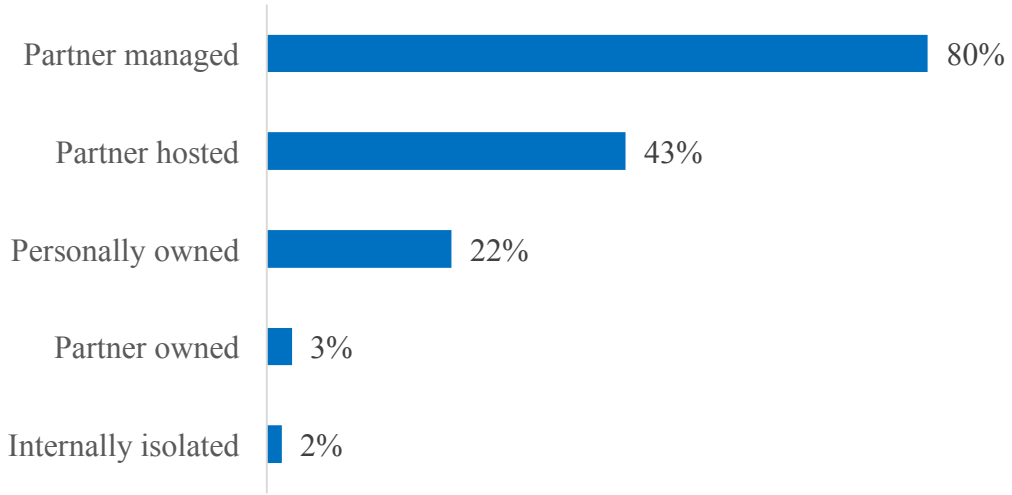
From Figure 20, it's apparent that the large majority (80%) of incidents compromise servers. This finding has much to do with the role and placement of servers within organizations. Some, like those running web services, occupy the "front lines" and are a company's digital representation to the outside world. Others, such as databases, usually sit deep within the network but are a high-value target for cybercriminals.

Figure 21. Varieties of compromised assets.

Category	Asset Variety	Breach #	Breach %
Server	Web server	260	33.2%
Server	Database server	246	31.5%
Terminal	POS terminal	184	23.5%
Terminal	POS controller	137	17.5%
Person	End-user	130	16.6%
Endpoint	Desktop	124	15.9%
Endpoint	Laptop	60	7.7%
Server	File server	42	5.4%
Server	Mail server	29	3.7%
Server	Remote access server	26	3.3%

User devices are not typically external-facing, but they do have one glaring feature that entangles them in many security incidents—users. They're used to browse the wilds of the web, open evil email attachments, download dubious software, and all manner of other activities that put them in harm's way. Users themselves are also targeted through various forms of social engineering, which is why the asset category of "Person" places third on the list at 22% of all incidents.

Figure 22. Governance of compromised assets (unknown=17%).

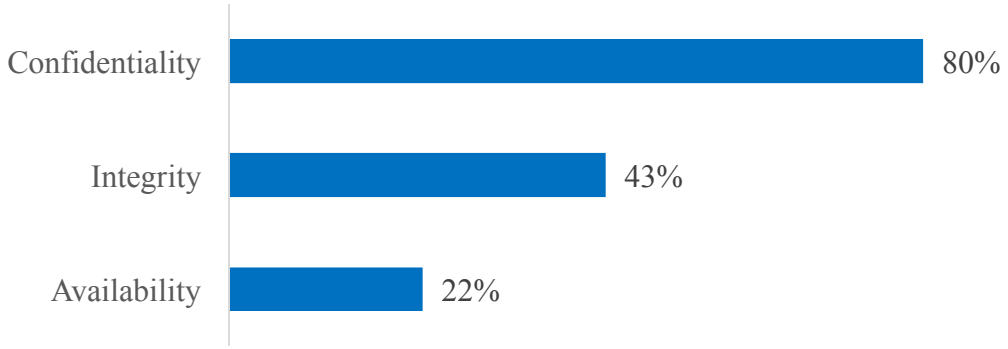


Due to the findings of chapter 4 linking IT interconnectedness between partners to incident likelihood, we wanted to study relevant trends among these compromised assets. Specifically, we tried to identify whether the asset was owned, hosted, or managed by 3rd parties. Figure 22 clearly shows a strong trend of 3rd party management and/or hosting of assets, but we must be careful drawing conclusions. Correlation does not necessarily mean causation. While it is certainly true that many partners directly caused or otherwise contributed to incidents, there were many cases where management or hosting of the asset (whether internal or partner) was believed to be irrelevant. However, these findings do seem to align with those of chapter 4 and offer further evidence that partners represent a risk factor that must be considered and controlled.

5.2.4 Attributes

We now turn attention to the last (but not least) "A" of the A4 Threat Model. When an information asset is compromised through the actions of a threat actor, one or more of the three primary security attributes will be affected. Those attributes are confidentiality, integrity, and availability and each will be analyzed in this section.

Figure 23. Primary security attributes compromised in security incidents.



5.2.4.1 Confidentiality

Compromises of confidentiality can be reasonably viewed on a sliding scale from unauthorized system access to potential data disclosure (or exposure) to confirmed data disclosure. Naturally, since information systems by definition contain information, most system-level compromises inevitably disclose or expose information. Of the 887 incidents that

compromised the confidentiality attribute, only 21 (2%) did not result in potential or confirmed data disclosure; most (93%) led to disclosure.

Figure 24. State of data at time of disclosure (unknown=73%).

State of data	Breach %	Breach #
Stored	62%	147
Processed	25%	59
Stored unencrypted	15%	36
Stored encrypted	2%	4
Transmitted unencrypted	1%	3
Transmitted	1%	3

For confirmed data disclosures, an attempt was made to determine the state of the data at the time of compromise. Per Figure 24, the majority was accessed while in storage, about one-quarter was actively being processed, and less than 3% was in transmission.

One of the critical lines of inquiry following a disclosure concerns the type and amount of records compromised. Not only is this essential for understanding the scope of the problem for proper containment and response, but many regulatory and legal issues are tied to these aspects. For example, Virginia mandates that entities must report disclosures of personal information on Virginia residents to the Office of the Attorney General and the affected resident. If over 1000 individuals are affected, then the various consumer reporting agencies must also be notified[10].

Regarding the type or variety of data compromised, payment card information was by far the most common among the incidents we studied. This corresponds to the threat actor motives discussed earlier, which strongly tilted toward financial and gain. Stolen payment cards can easily be converted to cash through fraudulent charges in both digital and physical markets. For this reason, they are the primary currency of the cybercrime economy. Personal and bank account information also have black market value, but requires a bit more work to monetize through various fraud schemes.

[10] SB 307.2; Virginia Code § 18.2-186.6

Figure 25. Variety and amount of compromised data.

Data Variety	# of Records	% of Records	Breach #	Breach %
Payment	273,203,708	60%	444	50%
Personal	172,047,662	38%	75	8%
Bank	12,344,102	3%	23	3%
Credentials	161,582	<1%	182	21%
Medical	2,022	<1%	2	<1%
Internal	414	<1%	58	7%
Unknown	239	<1%	266	30%
Secrets	22	<1%	25	3%
Classified	14	<1%	2	<1%
Copyrighted	14	<1%	2	<1%
System	13	<1%	32	4%

Theft of internal information (e.g., emails, corporate reports) and trade secrets represents another side of the data breach story. They are usually sought by a different type of threat actor and often involve more targeted and persistent attacks. Furthermore, they aren't as readily converted to money, so tend to be tied more to industrial and corporate espionage as well as ideological motives.

Access credentials and system information are not typically the primary objective of an attack, but rather enable deeper and/or prolonged access to the target environment. Thus, they are typically compromised en route to the true target.

Figure 26. Number of data records compromised per breach

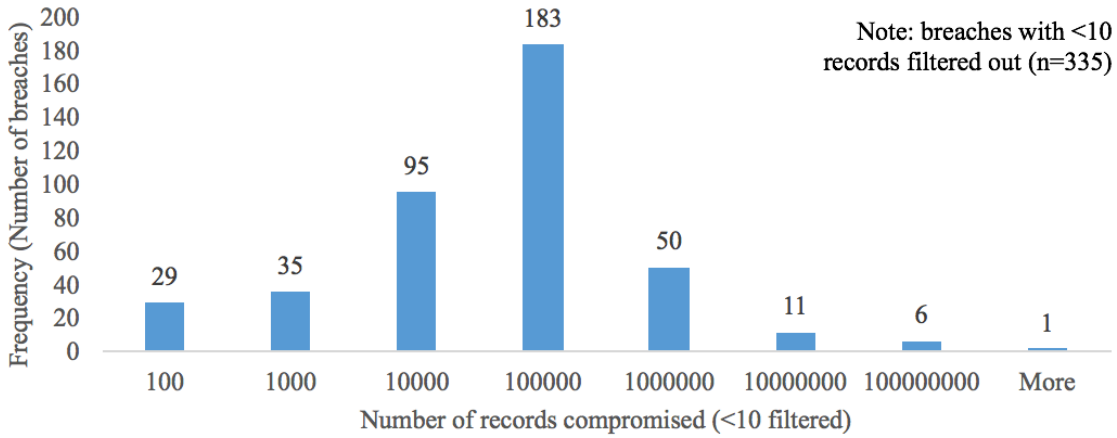


Figure 26 displays a histogram of records lost per incident, and gives insight into the relative frequency of smaller vs larger breaches. We filtered breaches with less than 10 records because they more often reflect an inability to forensically determine a proper count than the actual size of the breach. An example would be a situation where it was clear than an account credential was compromised and then used to access, encrypt, and exfiltrate additional data from the system. Because the stolen data was encrypted, there may be no way to get a precise record count, and thus this breach would show only 1 compromised record (the credential).

Aside from such cases, Figure 26 shows a distribution with a long tail to the right. Most breaches involve fewer than 100,000 records (the median is 25,000), but a few mega breaches skew the mean to just over 1,000,000 records.

5.2.4.2 Integrity

Broadly defined, every incident will encompass a loss of integrity in some form or fashion. Simply trying to access a system, for instance, alters log files and technically constitutes unauthorized modification. Thus, we set bounds around recording the integrity attribute such that its inclusion helps inform decisions or practice. Figure 27 depicts the varieties of integrity losses observed for the incidents examined in this study.

Figure 27. Variety of integrity losses.

Variety	Breach %	Breach #
Software installation	66%	470
Alter behavior	25%	175
Repurpose	19%	134
Hardware tampering	16%	111
Modify data	9%	65
Modify configuration	9%	64
Log tampering	4%	31
Fraudulent transaction	4%	29
Account creation	3%	21
Other	2%	14

Unauthorized software installation was the most common form of integrity compromise, driven largely by malware infections and, to a much lesser extent, insider misuse. Alter behavior

is an attempt to capture the outcome of social actions directed against people, which are considered an asset category by the A4 model. It seems a bit odd, but if you think about a person as a system whose state or actions can be modified (constituting an integrity loss), it begins to make a bit more sense from a modeling perspective. Repurposing an asset for unauthorized activities rounds out the top 3 types of integrity losses. Common examples of this include directing an infecting system to spam other victims or conduct DDoS attacks as part of a botnet. The remaining varieties of integrity compromises are fairly self-explanatory.

5.2.4.3 Availability

This research focuses on breaches and data loss events, which do not normally involve compromises availability losses unless they are a byproduct of the incident. A study on system crashes, network outages, disk failures, environmental hazards, etc., would certainly show very different findings. Nevertheless, we did observe breaches that affected availability in various ways and these are summarized in Figure 28.

Figure 28. Variety of availability losses.

Variety	Breach %	Breach #
Loss	74.1%	120
Interruption	14.8%	24
Destruction	9.9%	16
Degradation	4.3%	7
Obscuration	2.5%	4

The most prevalent by far is “loss” and this ties back to incidents involving physical theft. Interruption and degradation relate more to performance or quality of service that can be impacted during certain types of attacks. While destruction could refer to the physical asset itself, those we observed here involved the destruction of critical data within the asset. In a handful of incidents the attackers did not delete data outright, but encrypted it to prevent the owner from gaining access (obscuration).

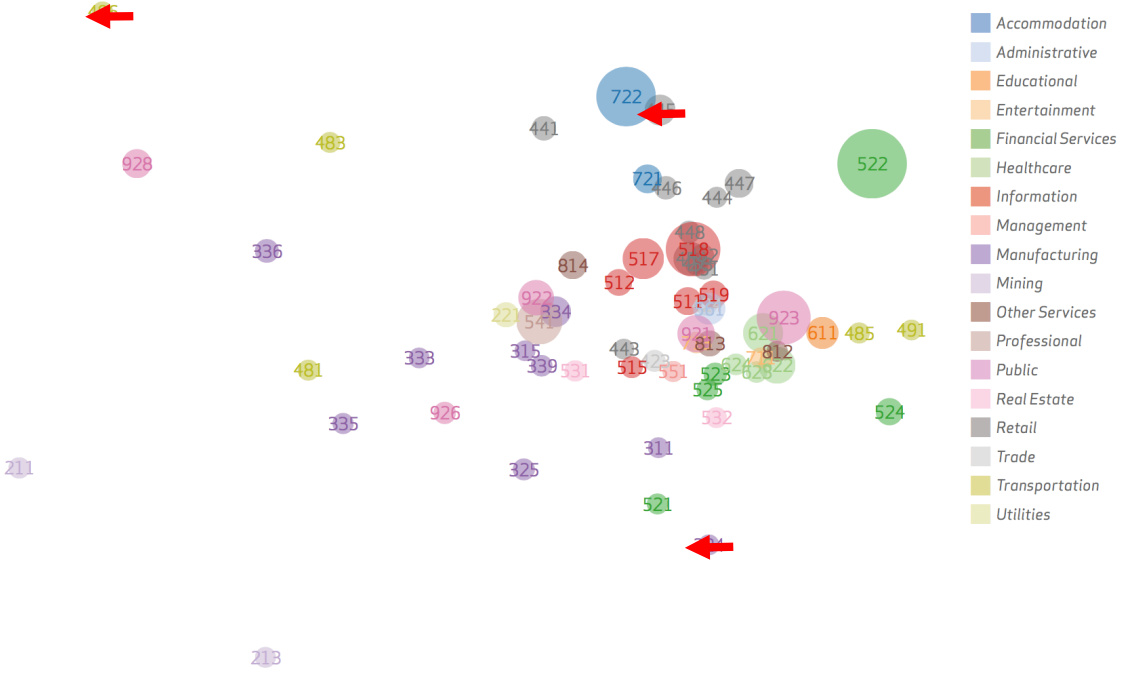
5.3 Industry Breach Profiles

It seems obvious that patterns of cyber threats experienced by an organization would differ dramatically based on a myriad of external and internal risk factors. Such factors include the determination and sophistication of threat actors, the IT systems and data supporting business processes, and the strength of security controls deployed to protect those assets.

What is not so obvious is whether organizational threat factors "roll up" to the industry level, resulting in distinct and discernable profiles across a supply chain spanning multiple industries or roles. Our analysis thus far offers evidence of this; the top threat actions leading to data breaches differed across retailers, manufacturers, and distributors. But threat actions are only one component of a data breach, and so we now expand that line of analysis to include a broader array of factors in order to develop and compare industry-based breach profiles.

To accomplish this, we used a multi-dimensional scaling technique incorporating 65 fields from the data model described in this chapter to group industries according to breach profiles they tend to exhibit. The algorithm, which leverages a Manhattan distance function, computed millions of comparisons between breach patterns across industries and the measure of similarity/dissimilarity among them was projected on a two-dimensional plane in Figure 29.

Figure 29. Cluster analysis comparing incident patterns across industry sub-sectors.



Each dot in Figure 29 represents an industry subsector identified by a three-digit North American Industry Classification System (NAICS) code[11]. Subsectors within the same higher-level sector are grouped by color (i.e., several retail (44x) subsectors in the upper right are all grey). The size of the dot corresponds to the number of breaches recorded for that subsector (larger = more). The distance between the dots shows how breaches in one subsector compare to that of another. If dots are close together, it means breaches in those subsectors share similar A4 Threat Model characteristics such as actors, actions, assets, and attributes. If far away, it means the opposite. In other words, subsectors with similar breach profiles appear closer together.

One major observation is that subsectors exhibit a fairly strong sector-level grouping tendency, indicating that "industry breach profiles" do in fact exist. While other sectors like Public (926) and Financial Services (521) intermingle somewhat with Manufacturing (31x-33x), the clustering algorithm perceives definite similarities among breaches affecting manufacturers. The Transportation sector (48x-49x) may seem to defy this norm, but closer examination reveals it to be more an outcome of NAICS coding than an outlier. The 486 dot in the upper left corner is the pipeline transportation subsector. On the other side of Figure 29, the 491 dot represents the postal service. Though in the same NAICS sector, intuition suggests (and evidence substantiates) that oil pipelines and mail trucks would have fundamentally different breach profiles because they represent very different types of firms.

We added red arrows to three subsectors o highlight what happens when different types of organizations collaborate within a supply chain. A very basic supply chain will have a manufacturer, a distributor, and a retailer. Notice in the figure how the Manufacturing subsector 324, Transportation subsector 486, and Retail subsector 445 form a triangle of points on opposite ends of the spectrum of industries. That means their breach profiles are very, very different. When those organizations connect systems and processes to form a supply chain, they expose each other to threats the other party has never seen before. This insight may help to explain the large proportion of breaches investigated in this chapter tying back to partner actors and vectors.

[11] https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012

5.4 Impact

Assessing the impact of security incidents is considered by many to be the "Holy Grail" of the industry. A huge amount of security spending is driven by a perception of consequences (be that small or large), yet relatively little actual data exists detailing and quantifying financial losses. This is understandable; if organizations are reluctant to even admit they had a breach, they certainly do not want to show everyone the bill. We set out with the goal of collecting impact information from every incident investigation, but we did not succeed. However, merely the attempt at doing so was a fruitful learning experience.

While forensic investigations are an excellent means of collecting details about the incident itself, they are not well suited to assessing impact. The simple reason for this is that impact isn't something that can be objectively analyzed in network or system logs. It is not a merely technical characteristic of the incident. This is a primary reason the approach described in chapter 3 separates technical impact (how an information system was affected) from outcomes (how the business was affected).

Another reason forensics is not an ideal source for impact information is because the investigation is over long before the losses are fully tallied. Furthermore, such investigations are typically conducted during the high-stress, high-sensitivity period that follows soon after the victim learns of a breach. Customers simply are not in the right frame of mind for an objective, analytical analysis of impact.

Finally - and this may be the most important reason - we found that organizations were not all that interested in counting their losses. Most just wanted to clean up the mess and get back to business as usual. This is certainly understandable, but it is also unfortunate and does not bode well for attempts to study this critical factor of the risk equation.

Thus, we determine that impact data for a DSS cannot be collected within the scope of this research. The size (number of records) and nature (type of data stolen) of the breach may be useful and measurable proxies, but we cannot test that hypothesis using the current database. Future efforts to objectively study financial losses should consider analyzing public records (e.g., stock value performance and annual financial reports) or insurance claims/payouts.

6 Conclusions for Supply Chains

We live and work in a highly interconnected world where the malicious intentions of distant criminals and the innocuous intentions of companies and consumers come crashing together with harmful and unforeseen consequences. The breaches studied in this chapter demonstrate this phenomenon very clearly and offer many lessons for organizations seeking to understand, evaluate, and mitigate cyber risk.

Though neither the data model nor the dataset presented herein are specific to breaches in supply chains, the analysis reveals many important implications for that domain. These were discussed throughout the commentary above, but are worth summarizing and emphasizing in one place.

1. Breaches affect organizations of all types, be they small retailers or giant manufacturers. No corner or member of the supply chain is exempt.
2. The frequency of breaches differs across organizations and industries. While we weren't able to study losses stemming from these breaches, there is sufficient evidence to conclude that impact differs by industry as well. Thus, cyber risk is not evenly distributed among members of the supply chain.
3. 3rd parties (including supply chain partners) cause or contribute to breaches in 3 primary ways:
    1. A partner can directly cause a breach through deliberate or unintentional actions.
    2. When an organization suffers a breach, the actor(s) (whether outsiders, insiders, or partners) may exploit trusted IT connections to compromise its partners.
    3. When an organization suffers a breach, the actor(s) (whether outsiders, insiders, or partners) may also compromise locally stored or hosted data shared by its partners.
4. The motives and methods behind breaches differ across industries. Thus, members in a supply chain expose each other to novel threats and may benefit from sharing what they know about those threats and sharing the burden of defending against them.
5. External management and hosting of assets may be a contributing factor in data breaches in some circumstances. This warrants closer evaluation of 3rd party IT systems that support collaboration among supply chain members.

Overall, these findings reinforce the fact that breaches have causes and effects that extend well beyond the boundaries of a particular organization. Because of this, cyber risk is fraught with externalities stemming from and spilling over to partners in a value chain. As chapter 4 stresses, the very same collaborative activities that reduce supply chain risk also conspire to increase and redistribute cyber risk across members of a supply network. Further research should explore how different models and levels of supply chain collaboration affect this transference of risk and how members can collectively mitigate its effects.

References

1. Bejtlich, R. (2009). Insider Threat Myth Documentation. Retrieved July 5, 2015, from https://taosecurity.blogspot.com/2009/05/insider-threat-myth-documentation.html
2. Galbraith, J. (1977). Organization Design. Reading, MA: Addison-Wesley.
3. Parker, D. B. (1998). Fighting Computer Crime. New York, NY: John Wiley & Sons.

Chapter 6: Building a Theory and Model of the Impact of Collaboration on Cybersecurity Risk in Supply Chains

1.0 Introduction

Firms have invested heavily to gain the many advantages promised by the IT-enabled supply chain. But similar to the double-edged sword of information sharing, the benefits of interconnectivity are not attained without risk. Cybersecurity is inherently a risk management issue, whereby risk can be mitigated through the implementation of effective controls. In the literature we find no approaches that incorporate real-world data to resolve risk in financial terms such as Annualized Loss Expectancy (ALE) so that it can be directly and reliably compared to other categories of risk. This dissertation chapter maintains that information sharing in a supply chain breeds cybersecurity risk, and this risk to date is poorly understood and often inadequately considered when supply chain formation is considered or implemented.

Secondly, the literature, as suggested, has advanced no real theory of cybersecurity risk in a supply chain. We tackle the specification of such a theory as our first order of business. We do so based on analysis of approximately one thousand case studies we conducted in industry, often at the behest of the U.S. Secret Service, over a ten-year period.

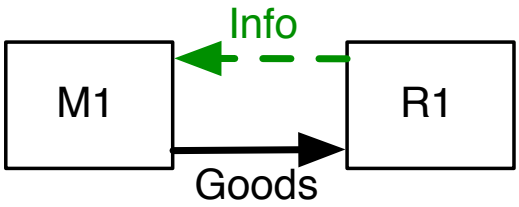
Third, we formulate a mathematical model of a general organization, specifying major factors influencing risk and its control noted in the literature and verified through our forensic investigations. We then use our case studies as a data source to specify parameters in our model. We illustrate with a scenario using a simple sequential supply chain consisting of a supplier, a manufacturer, a distributor, a retailer, and an IT service provider. The reader should be cautioned at this point that this model with its data is *not* generalizable to all firms in the world as the data collected was generally gathered within the context of breach incidents that occurred and were then investigated. Hence, the data model is almost certainly biased to represent larger firms that have or are likely to incur breaches due to their interactions with other firms.

Finally, we pose some research questions to our model when utilized on a small supply chain. Our primary motivation is to begin to build upon the theory we have developed and show how the model may be used by managers. Ultimately, we want to be able to offer quantifiable advice to managers about the degree of risk incurred when joining a supply chain, how to reduce such risk, bad ways of configuring the chain, etc.

2.0 Literature Review

A supply chain is a network of organizations engaging in collaborative relationships to exchange material goods, services, and information. Figure 1 shows a simple supply chain consisting of two organizations, a manufacturer (M1) and a retailer (R1). Material goods flow downstream from the manufacturer while the retailer sends orders, inventory levels, and other information upstream. In a perfect world, everything is coordinated so the right materials make it to the right place at just the right time. In the real world, however, these flows are vulnerable to various sources and types of risk that must be adequately managed for the supply chain to function optimally (Christopher & Peck, 2004; Juttner, Peck, & Christopher, 2003; Spekman & Davis, 2004).

Figure 1. A simple supply chain with goods flowing downstream and information upstream.



Disruptions to material flows by natural hazards, accidents, and intentional acts is a recognized category of risk in supply chain management, and maintaining resiliency is a common topic within the literature (Christopher & Peck, 2004; Hohenstein, Feisel, Hartmann, & Giunipero, 2015; Kungwalsong, 2005). Distortion of information flows is also considered a major risk category because it impairs the coordination of these material flows through a phenomenon commonly referred to as the Bullwhip Effect (H L Lee, Padmanabhan, & Whang, 1997). This has, in turn, spawned a great deal of focus on information sharing within supply chains to combat these problems and thereby reduce risk for all members (Kembro, Selviaridis, & Näslund, 2014; Sahin & Robinson, 2002).

The notion that information sharing might itself become a source of risk to collaborating firms was suggested early in the progression of literature on that topic (Hau L Lee & Whang, 2000). Information shared confidentially with one partner might be leaked to or otherwise inferred by third parties who may benefit from that knowledge to the detriment of the original sharer (Hau L Lee, 2002; Li, 2002). Some considered this serious enough to declare preserving confidentiality in information sharing models as one of the most important problems that must be addressed by

OR/MS researchers (Sarathy & Muralidhar, 2006). Acknowledging that many agree with this assessment, a wealth of articles over the last 15 years has explored various methods, effects, and frameworks of information and knowledge leakage in supply chains (Tan, Wong, & Chung, 2016).

As the use and importance of information sharing has grown, so too has the dependence on information technology (IT) to empower this growth. This reliance has prompted some to argue that efficient, competitive, and collaborative modern supply chains are impossible without IT (Gunasekaran & Ngai, 2004). Recognizing this, firms have invested heavily to gain the many advantages promised by the IT-enabled supply chain. But as is the case with information sharing, the benefits of interconnectivity are not attained without risk. Though essential, IT integration has eroded traditional layers of separation that acted as protective barriers between firms. The result is increased exposure to a host of IT-centric risks that necessitate a need to balance the opposing goals of collaboration and security (Smith et al. 2007).

Although security has emerged as a recognized topic within the supply chain management (SCM) literature, it has focused mostly on physical rather than cyber security (Gould, Macharis, & Haasis, 2010; Williams, Lueg, & LeMay, 2008). Mounting evidence of real-world failures stemming from insecurely interconnected IT systems, however, has begun to draw more research attention in recent years. Kolluru & Meredith (2001) assert that firms can no longer afford to ignore the impact of their cybersecurity policies on the larger supply chain, but must consider them in light of their close supply chain partners. Echoing this sentiment, Shih & Wen (2005) note that highly-collaborative business partnerships change the nature of the challenge from securing a network to protecting the virtual supply network as a whole, and they develop a security management life cycle with this goal in mind.

Though often viewed through a computer science or engineering lens, cybersecurity is inherently a risk management issue, whereby risk can be mitigated through the implementation of effective controls (Straub & Welke, 1998). SCM researchers have understood this, but differed for some time on where IT-related risk fits within the broader context of supply chain risk. Recognizing this, Smith et al. (2007) proposed a conceptual framework for information security risk in the supply chain and called for future work to quantify risk for improved decision-making. Whether in direct answer or by coincidence, a handful of articles followed sharing the goal of quantifying information risk in supply chains.

Faisal et al. (2007) employed interpretive structural modeling and graph theory to understand and quantify the relative importance of variables that contribute to information risk. Smith et al. (2008) established a positive correlation between the likelihood of security incidents caused by partner firms and higher levels of information sharing and interconnectivity. Deane et al. (2009) developed a mathematical model for quantifying IT security risk in supply chains and demonstrated optimal solutions for minimizing upstream risk, downstream risk, and global (chain-wide) risk. Bandyopadhyay et al. (2010) quantified the impact of network vulnerability and degree of integration on investment levels, breach probability, and expected costs to each firm. Sharma et al. (2016) created a Bayesian belief network for analyzing information risk in supply chains that incorporates objective and subjective data.

Beyond these efforts, we find very little research other than our own efforts to quantify information risk within supply chains. Furthermore, we find no approaches that incorporate real-world data to resolve risk in financial terms such as Annualized Loss Expectancy (ALE) so that it can be directly and reliably compared to other categories of risk.

Our own research over the past ten years has been focused on developing the theory of cybersecurity risk and ultimately providing insights for managers in dealing with such risk. Chapter 4 of this dissertation, developed ten years ago, presented exploratory research into perceptions and experiences surrounding cybersecurity incidents within supply chains. One of the more important findings was establishing a positive correlation between higher levels of information sharing activities among partners and an increased likelihood of incidents involving those partners.

To corroborate findings from Chapter 4 with real-world data, Chapter 5 proposed a rich data model for describing security incidents in a structured manner and presented an analysis of nearly 1,000 breaches over a ten-year period. The chapter held two major implications for managing cybersecurity risk in a supply chain:

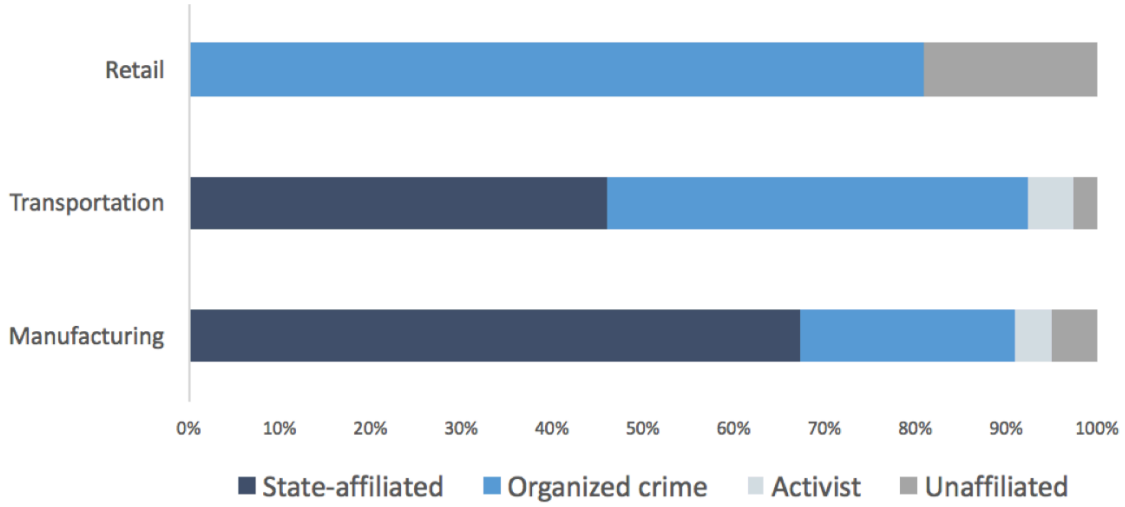
1. Partner firms directly cause or contribute to a large proportion of breaches
2. The types of breaches differ significantly across traditional supply chain roles.

Moreover, particular findings from Chapters 4 and 5 that we will use in constructing a theory of an organization's cybersecurity risk include the following insights:

- Figure 2 shows various threat actor profiles by industry, i.e., the "actors" responsible for causing these breaches for different industries. The disparities between the bar charts is

readily apparent. Retail is plagued by organized criminal groups, while state-affiliated actors hammer Manufacturing. Transportation suffers fairly equally from both. Clearly, different industries are targeted by very different actors with very different motives.

Figure 2. Threat actor profiles by industry.



- Breach types vary in their rate of occurrence from each other (see Table 1) and by industry.

Table 1. Breach types vary by industry

		INT	MAL	ABU	PHY	ERR	SUM
General		**52%**	**9%**	**13%**	**15%**	**11%**	**100%**
Mining		29%	3%	54%	11%	3%	100%
Manufacturing		62%	14%	19%	3%	2%	100%
Transportation		32%	10%	15%	14%	30%	100%
Retail		67%	7%	8%	13%	6%	100%
IT Services		52%	17%	14%	3%	15%	100%

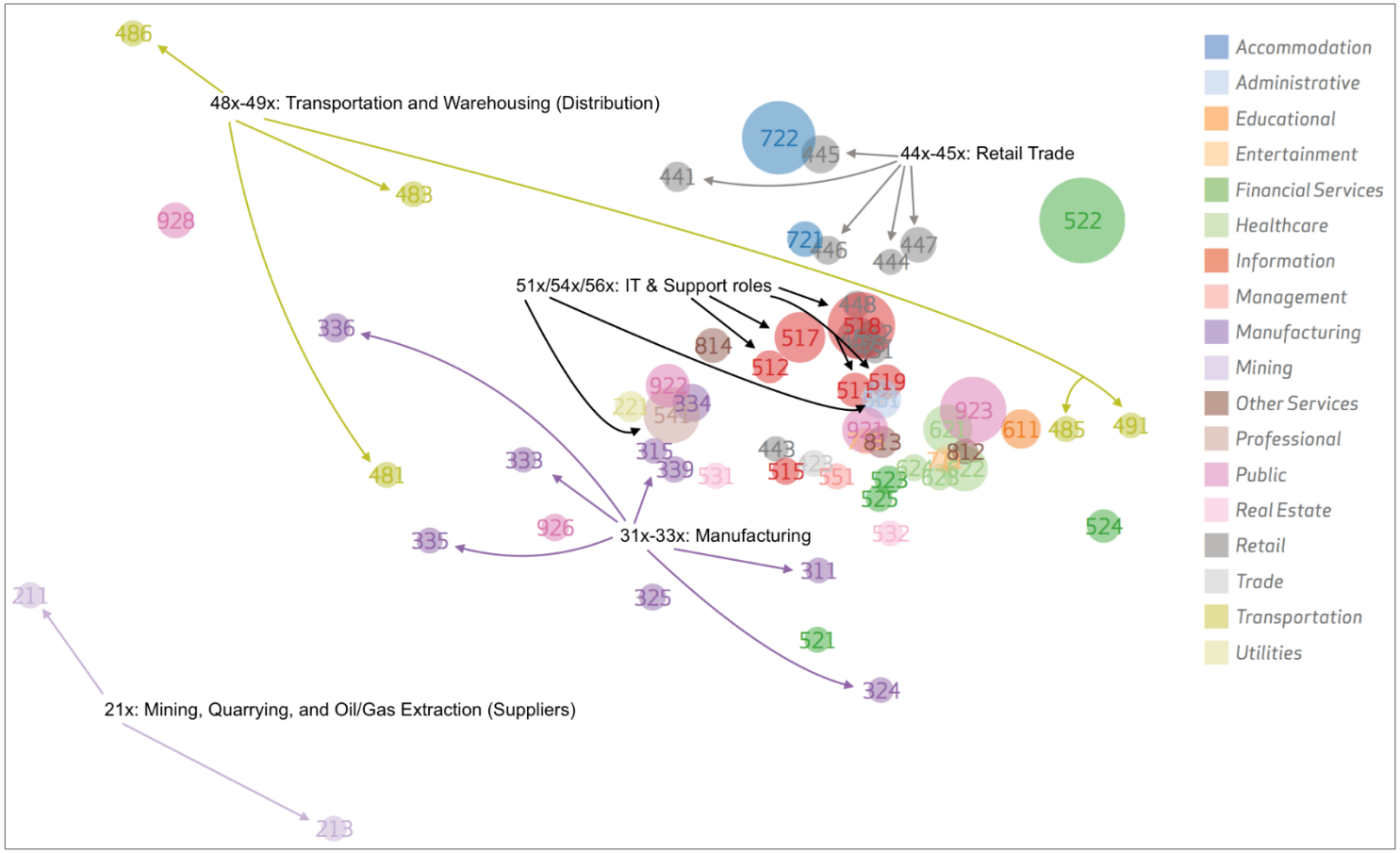
- Incident patterns vary across industry subsectors (Note Figure 3).

Chapter 5 also introduced the notion of industry-based threat profiles and used a multi-dimensional scaling technique to group industries according to incident patterns they tend to exhibit. Figure 3 first appeared in that chapter and we now add annotations to highlight industry groups relevant to the supply chain context. Each dot represents an industry subsector identified by a three-digit North American Industry Classification System (NAICS) code. Subsectors

within the same higher-level sector are grouped by color (i.e., several retail (44x) subsectors in the upper right are all grey). The size of the dot corresponds to the number of breaches recorded for that subsector (larger = more). If dots are close together, it means breaches in those subsectors share similar characteristics such as actors, actions, assets, and attributes. If far away, it means the opposite. In other words, subsectors with similar breach profiles appear closer together.

Interesting observations from Figure 3 abound, but the major takeaway for our current focus is that the annotated sectors exhibit vastly dissimilar breach profiles. It's a powerful visual explanation of cybersecurity risk exposure in a supply chain. Consider, for example, a simple gas supply chain consisting of subsectors 211 (Oil and Gas Extraction), 486 (Pipeline Transportation), 324 (Petroleum Products Manufacturing) and 447 (Gasoline Stations), which literally spans the four corners of the chart. The exposure widens from a relatively small pocket of threats for the subsector to the whole gamut for the supply chain. Furthermore, one assumes cybersecurity defenses are tuned against known threats and would be far less effective against broader and different threat profiles. Thus, there is strong empirical evidence to believe that organizations participating in a highly interconnected and collaborative supply chain will expose each other to different types and levels of cyber threats, potentially impacting the balance of cyber risk across the supply chain.

Figure 3. Cluster analysis showing that threat profiles vary by industry subsector.



- There is "Targeting." If an organization has a lot of valuable data, it will inevitably attract unwanted attention from those who wish to obtain it illicitly. Advanced, persistent adversaries like nation states and organized criminal groups are especially adept at exploiting trust relationships in supply chains.
- The connectivity and sharing between organizations affects risk. We model two primary aspects:
    - Level of IT interconnectivity between organizations (L, M, H)
    - Degree of information sharing (None, Partial, Full), regardless of interconnectivity
    - Scope of information shared (Transactional, Operational, Strategic), regardless of interconnectivity or sharing degree
- Controls matter; security posture and partner-facing controls also affect the degree of cyber risk incurred. See the two surveys we did on this topic (Baker & Wallace, 2007; Gregory E Smith et al., 2008).

In this research we leverage data we collected via forensic investigations of over 900 security incidents as well as thousands of publicly-reported breaches to build a theory and then a mathematical model of an organization for analyzing and quantifying cyber risk in supply chains. We incorporate key factors identified by prior SCM research such as scope of information sharing and degree of integration between firms to study their effect on risk levels. We believe such a model that is entirely derived and driven by actual data to be both unique within the literature and useful within practice.

3.0 Toward a Theory of Cybersecurity Risk

Based on (first) the (roughly) 2,000 paid, external forensic investigations and (second) the 982 confirmed security case studies, with 822 of those incidents resulting in the disclosure of over 457 million compromised records we performed over the past ten years, plus (third) the research cited above—both by others and ourselves, we now proceed to develop a theory of cybersecurity risk for an organization. As stated, our primary motivation is to be able to offer quantifiable advice to managers about the degree of risk incurred when joining a supply chain, how to reduce such risk, bad ways to configure your chain, etc. This research is the first step in this direction.

3.1 Four Types of Supply Chain Cyber Risks.

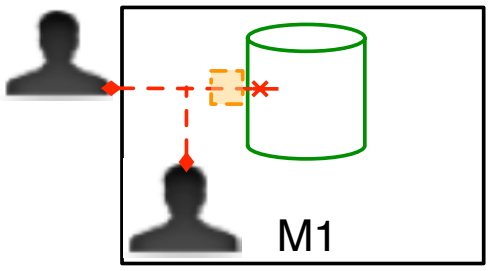
We now stipulate what we believe to be the fundamental tenets necessary to analyze cybersecurity risk in a supply chain. We drive the theory with the concept of a breach:

- A data breach is any event involving the disclosure of information to an unauthorized party.
- There are many sources and motives and methods of breaches observed via our case studies, but five broad types stood out: network and system intrusions (INT), malicious software infections (MAL), abuse of system access by trusted parties (ABU), physical theft and sabotage (PHY), and errors or omissions of various forms (ERR). Table 1 above showed from our database the percentage of each type breach for five types of breaches and for six different industries.
- For organizations in a supply chain, we have identified four primary *ways* in which they may be breached. We will describe each and the main factors influencing each.
- We will then postulate a mechanism to measure the financial magnitude of the risk incurred per year. We will do this by saying the risk is the product of two factors:
    - *breach rate per year* and approximate *loss per breach*.
    - We will derive our measures for loss per breach including the criterion of data availability. That is, certain measures may be ideal for estimating loss per breach, but if the data are not available and there is no reasonable expectation that companies will be willing to divulge such information, there is no point or hope for developing a theory based on such a measure.

The four ways an organization participating in a supply chain may be breached are now discussed. The first breach type occurs for organizations whether they are in a supply chain or not. The last three occur only because the organization has supply chain partners.

3.1.1 Direct Breach. Irrespective of any supply chain, as is illustrated in Figure 4, individual organizations are vulnerable to *breaches from external and internal threats*. Security controls (orange lines/shading) can be deployed to reduce the likelihood of breaches and mitigate the impact should they occur.

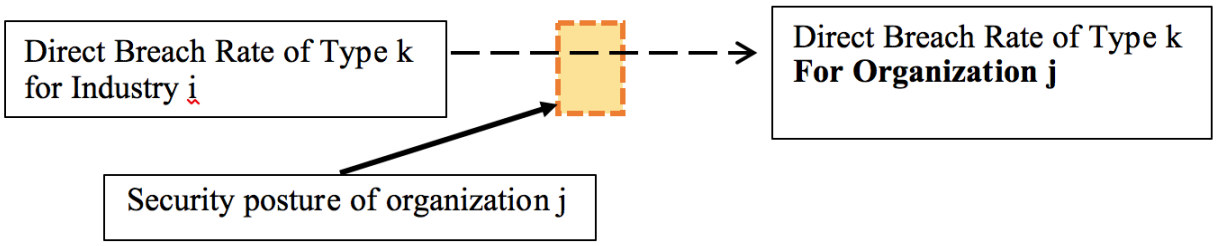
Figure 4. External and internal threats to a manufacturing firm's internal data.



Based on ten years of observation and investigation of breaches, we specify that each organization has an annual rate of *direct* breaches from external and internal actors. Furthermore, as shown in Figure 5:

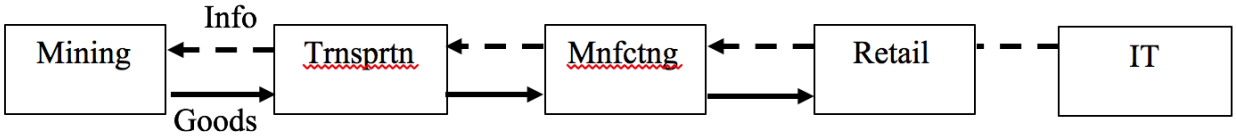
- The base rate is a function of the partner's industry, as was shown in Figure 3.
- The base rate is modified if the organization has an abnormally strong or poor security posture.
- The type of breach is probabilistically assigned based on predetermined industry threat profiles.

Figure 5. Factors determining probability of a direct breach from external and internal actors (a direct breach)



Additional factors also influence the breach base rate to a lesser degree, but these are still poorly understood at the present time. However, it is our experience that (1) obtaining the bulleted data mentioned above *is* possible, and in fact we have done so, while (2) obtaining real-world data about factors such as litigation from firms can be next to impossible; we therefore classify these additional factors as "second-order" influences, and leave these for refinement of our theory and models in future research.

Figure 6. A simple, linear five-organization, sequential supply chain.



Although perhaps obvious, let us first define by way of example a partner. Consider Figure 6, which shows five organizations arranged linearly in a supply chain. First note the obvious that the number of partners an organization has depends upon the configuration in which they are arranged, as well as the total number of partners in the chain. For the arrangement shown in Figure 6, partners are as shown in Table 2:

Table 2. Partner assignments and relationships for the supply chain of Figure 6.

Member industry assignments

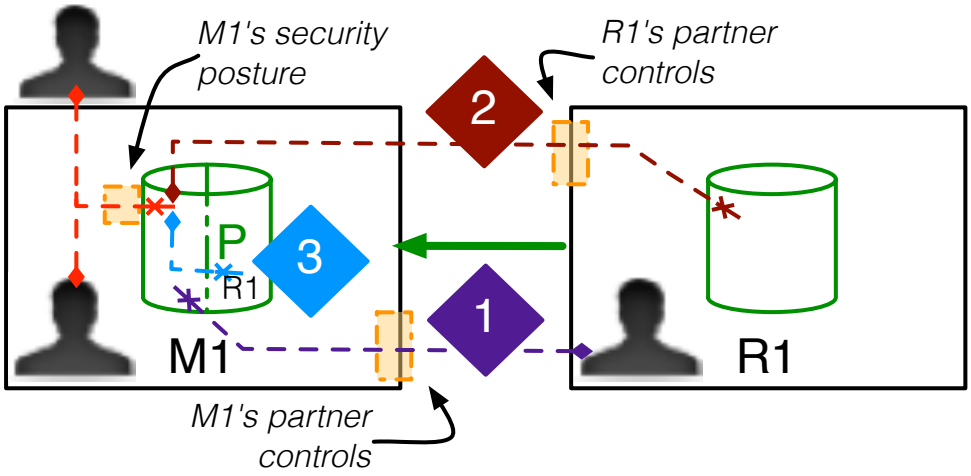
	Name	Role	# of Partners
Org1	S1	Mining	1
Org2	T1	Transportation	2
Org3	M1	Manufacturing	2
Org4	R1	Retail	1
Org5	I1	IT Services	1

Partner Relationships

	S1	T1	M1	R1	I1
S1	**0**	1	0	0	0
T1	1	**0**	1	0	0
M1	0	1	**0**	1	0
R1	0	0	1	**0**	1
I1	0	0	0	1	**0**

Beyond direct breaches, organizations that are part of a supply network are also be affected by breaches from—and occurring to—other partners in the network. Our analysis of thousands of breaches finds there are three main ways this can occur, which are labeled in Figure 7.

Figure 7. Three scenarios of partner-related breaches in a supply chain.



1. ***A partner can directly cause a breach through deliberate or unintentional actions***. We say that Retailer1 (R1) is the "**actor**" that breaches Manufacturer1 (M1) in this scenario.
2. When an organization suffers a breach, ***partners may also indirectly suffer because of the breach***. That is, the actor(s) (whether outsiders, insiders, or partners) may deliberately exploit or innocently use trusted IT connections or credentials to compromise the victim's partners. In this example, Manufacturer1 is compromised and then becomes the "**vector**" by which the attacker breaches Retailer1.
3. When an organization suffers a breach, the actor(s) (whether outsiders, insiders, or partners) may also ***compromise locally stored or hosted data shared by its partners***. Manufacturer1 is the "**custodian**" of Retailer1's data in this scenario (note "R1's data in the "P" (partner) side of M1's data store).

We now elaborate upon these three cases.

3.1.2 Partner-Actor Breach. The first type of partner breach we specify is called a partner-actor breach. Beyond direct breaches a firm incurs, each organization also has an annual rate of direct breaches from EACH partner it is connected to in the network. Based on our observation and analysis of years of breaches, we furthermore note the following (see Figure 8):

- The base rate of this kind of breach is a function of the partner's industry.
- The base rate is modified if partner security controls are abnormally strong or poor.

- The base rate is also modified if the partner organization is a highly-desirable target in the network. The degree of targeting is based upon the degree and nature of information sharing that the partner has.

3.1.3 Partner-Vector Breach. The second type of partner breach we specify is called a partner-vector breach. If an organization has a breach of any type or source, there is a probability that the breach will "propagate" to all partners in the network connected to the original victim. Thus by connecting in a supply chain, a firm may incur the "side-effects" of any of its partners being breached. We also note the following characteristics (shown in Figure 9) of a partner-vector breach:

- The base probability of the breach is modified for each relationship if the level of IT integration between partners is abnormally high or low.
- The base probability is modified if the organization has abnormally strong or poor partner-facing security controls.
- The base probability is also modified if the organization is a highly-desirable target for other partners in the network.

In more complicated supply chains than illustrated in Figure 6, it is possible that a breach will propagate not only to one other connected partner, but from that affected partner on to another and to another. In developing this theory, we believe that not only first-order partner-vector breaches, but at least second and third order partner-vector breaches must be included as well if realism in understanding actual chains is to be attained.

Figure 8. Factors determining probability of a direct breach from partner actors (the "partner actor" scenario)

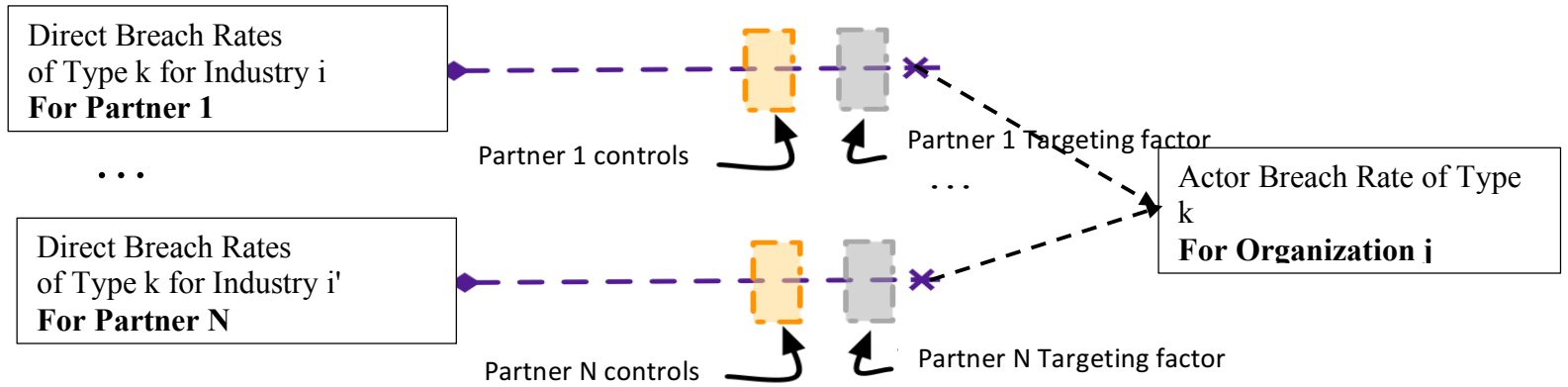
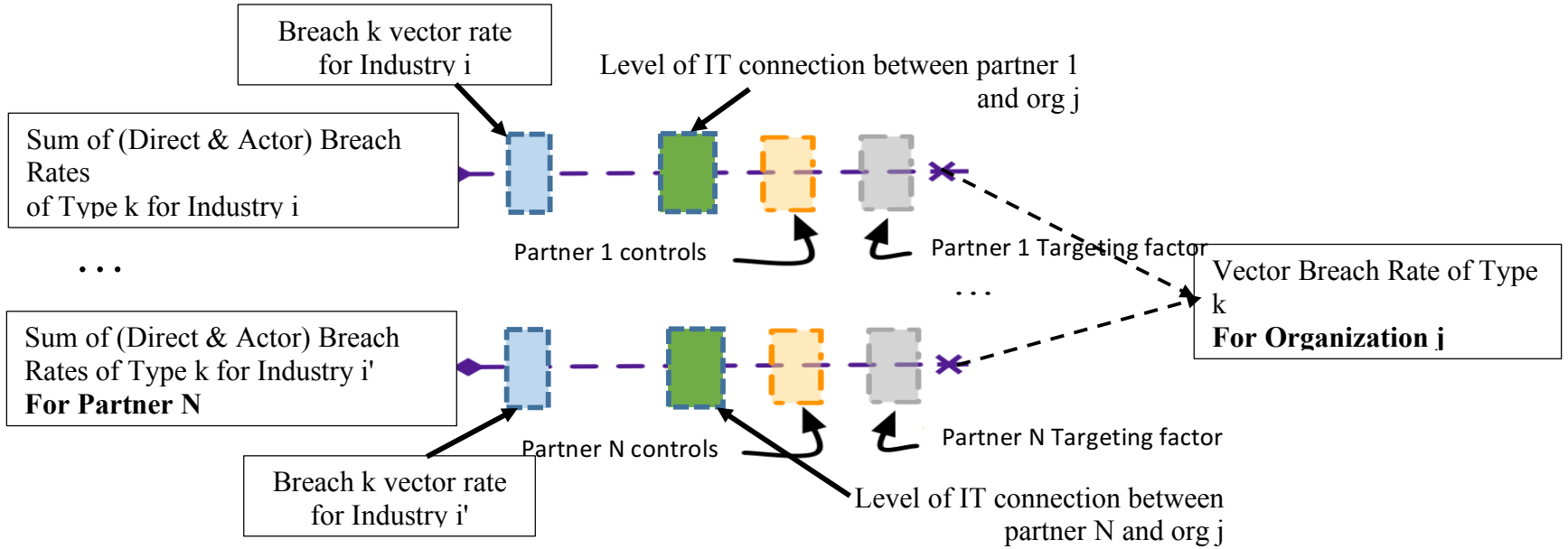


Figure 9. Factors determining probability of a breach spreading to other partners in the supply chain (the "partner vector" scenario).



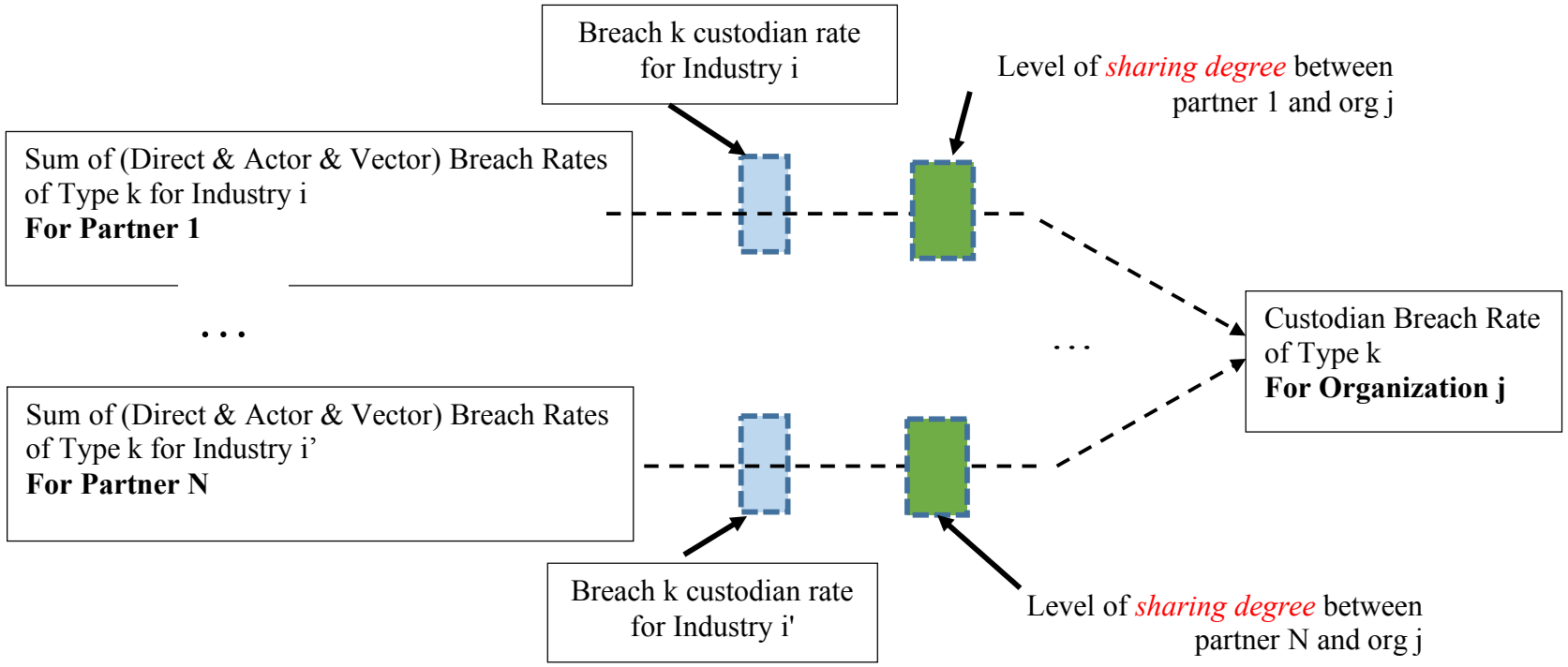
3.1.4 Partner-Custodian Breach. Organizations can reduce the probability of partner "actor" (#1) and "vector" (#2) partner scenarios by implementing partner-facing controls. However, these controls do not reduce the probability of the "custodian" scenario (#3) because the data are outside the influence of that organization's security controls. To protect data shared with—and thus under the control of—partners, there must be additional incentives or requirements in place that cause the partner to strengthen its own security posture.

We again note that the probability of partner "actor" and "vector" scenarios increases with the level of IT interconnectivity between organizations. We now state that the probability of partner "custodian" breaches increases with the number of partners the organization shares data with and also with the **degree (amount) of sharing** (Figure 10). Furthermore, if an organization has a breach of any type or source, there is a probability that any partner data stored by the victim will also be compromised (a "partner custodian" breach).

- The base probability is modified for each relationship if the *degree*/amount of *information sharing* between partners is abnormally high or low.

Finally, as a point of clarification, we note that in order to determine the rate of custodian breaches an organization experiences, we should form the sum of all possible breach sources for each partner in the chain. The probability of a custodian breach will be some fraction of that sum.

Figure 10. Factors determining probability of a breach compromising locally stored partner data (the "partner custodian" scenario).



4.0 Building a Cybersecurity Risk Model from the Theory

Given the key elements of the new cybersecurity risk theory developed in the previous section, we now formulate a mathematical model quantifying the relationships established. The goal is to describe the cyber-risk from all key sources for an organization mathematically, and then to be able to connect organizations into a supply chain of any desired configuration.

4.1 *Breaches*

The four types of breaches developed above that an organization connected within a supply chain may incur are now examined. A mathematical representation of each type is developed.

4.1.1 ***Direct Breaches***. Define $B_{S1,ALL}^{Dir}$ to be the ***direct*** annual breach rate for organization *S1* (which belongs to the mining industry) across ALL breach types. Then

$B_{S1,ALL}^{Dir} = B_{Mine,ALL}^{Dir}$ * SecPost_{S1}, (1)

where

$B_{Mine,ALL}^{Dir}$ is the direct annual breach rate for the mining industry across ALL breach types, and

$SecPost_{S1}$ is the security posture modifier of organization *S1*.

4.1.2 ***Partner-Actor Breaches***. Define $B_{S1,ALL}^{PA}$ to be the ***Partner-Actor*** annual breach rate for organization S1 across ALL breach types. In order to determine this, we must first determine the breach rate from each partner *i* of organization S1, and then sum these. Referring to Figure 8, the breach rate contributed by each partner is

$B_{Industry\ i,ALL}^{Dir}$ * TFac_i * PrtSec_i, (2)

where

i is the i^{th} partner of org S1;

Industry i is the industry subsector to which partner *i* belongs;

$TFac_i$ is the Targeting Factor based on degree and amount of information sharing; and

$PrtSec_i$ represents the level of partner *i*'s partner-facing controls.

Then

$B_{S1,ALL}^{PA} = \sum_{i=1}^{N_p}(B_{Industry\ i,ALL}^{Dir}$ * TFac_i * $\text{PrtSec}_i)$, (3)

where N_p is the number of partners of organization *S1*.

4.1.3 ***Partner-Vector Breaches***. Define $B^{PV}_{S1,ALL}$ to be the ***Partner-Vector*** annual breach rate for organization S1 across ALL breach types; this breach rate is due to both direct *and* actor breach rates incurred across all partners, with each partner contributing breaches according to the industry to which that partner belongs. Again to determine this, we first determine the breach rate from each partner *i* of organization S1, and then sum across all partners. Thus, drawing on the bullet points in section 3.1.3 and on Figure 9,

$B^{PV}_{Industry\ i,ALL}$ * ConnLev_i * TFac_i * PrtSec_i, (4)

where

i, Industry i, $TFac_i$, and $PrtSec_i$ are as defined above, and

$ConnLev_i$ is the Level of Connection between partner *i* and organization *j*;

Then

$B^{PV}_{S1,ALL} = \sum_{i=1}^{N_p}(B^{PV}_{Industry\ i,ALL} * \text{ConnLev}_i * \text{TFac}_i * \text{PrtSec}_i)$, (5)

where N_p is the number of partners of organization S1 (as above).

4.1.4 ***Partner-Custodian Breaches***. Define $B^{PC}_{S1,ALL}$ to be the ***Partner-Custodian*** annual breach rate for organization S1 across ALL breach types. According to section 3.1.4 (and Figure 10), this breach rate is a function of the level of sharing degree between each partner *i* taken alone and organization *S1*. Thus the breach rate contributed by each partner *i* is

$B^{PC}_{Industry\ i,ALL}$ * ShareDeg_i, (6)

and

$B^{PC}_{S1,ALL} = \sum_{i=1}^{N_p}(B^{PC}_{Industry\ i,ALL} * \text{ShareDeg}_i)$, (7)

where $ShareDeg_i$ is the Level of Sharing Degree between partner *i* and organization *S1*.

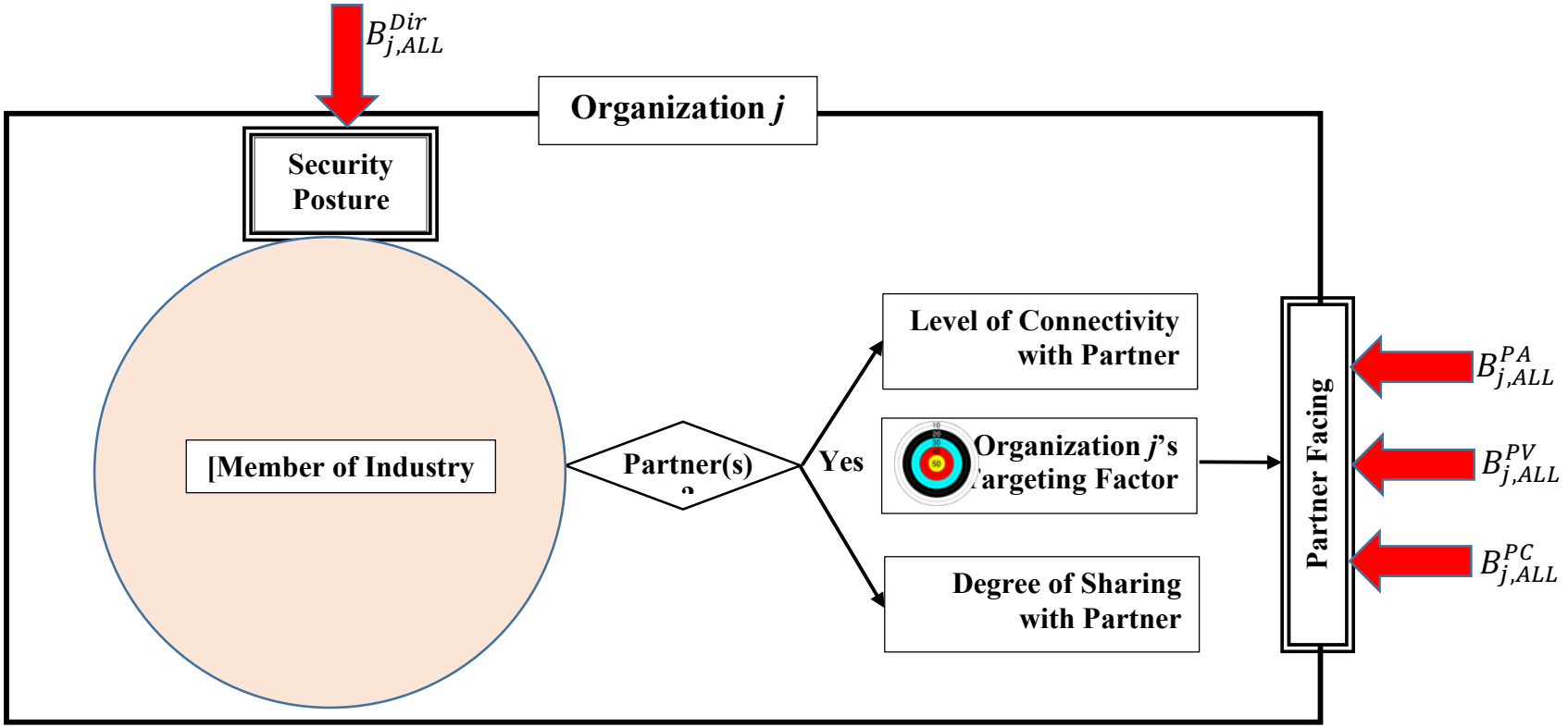
4.2 Modeling a Supply Chain

In this section a model for a single organization that can connect to other organizations is developed first. Then we show how to connect the model of an organization into a supply chain. Next we use real-world data to develop estimates of breach data, etc. Finally, we convert successful breaches against an organization into various financial measures including *Annual Loss Expectancy* and *Loss Exceedance Probabilities*.

4.2.1 A Single Organization. A single general organization that does not belong to a supply chain may be breached in a *direct* manner as explained above, while a firm in a supply chain exposes itself to three additional (*partner*) varieties of attack. Thus to model a general organization ***j***, we construct a firm (see Figure 11) that may be attacked in up to four ways and include the factors that accentuate or diminish that organization's being impacted by each breach type. Note first that we specify the industry to which the firm belongs, and secondly, that in this figure we are only showing how ***j*** may be attacked by outside entities, not how organization ***j*** itself may breach other firms.

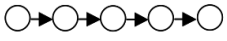
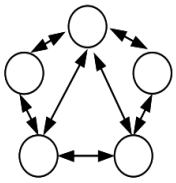
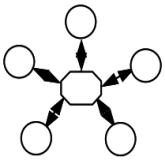
Included in Figure 11 are the firm's *security posture*, which can ameliorate *direct* breaches, and three other factors that affect an organization belonging to a supply chain. The three partner related elements are organization ***j***'s targeting factor; the level of connectivity with partners; and the degree of sharing between organization ***j*** and each of its partners. And finally, a fifth factor, the firm's partner-facing controls (if any), are also critical. As mentioned, although other factors influence a firm's annual losses due to breaches, specifying these five plus the firm's industry gives us a good handle on a firm's behavior.

Figure 11. Model of an organization j that may connect to a supply chain. Also (not shown), organization j may breach other organizations.



4.2.2 The Entire Supply Chain. A model of an entire supply chain may now be configured merely by using the model of Figure 11 for each organization, and then specifying its industry, its security posture and targeting factor, and then – for each partner it has – the level of connectivity and degree of sharing. Basically, any configuration of organizations may be modeled. Three common arrangements from the Supply Chain Management literature are shown in Table 3. In that table, only five organizations are placed in each chain, but many more organizations may be included.

Table 3. Three basic information sharing structures commonly recognized in the Supply Chain Management literature. Taken from Liu and Kumar (2003) and inspired by Hong (2002) and Kumar and van Dissel (1996).

Information Sharing	Sequential	Reciprocal	Hub-and-Spoke
Structure			

4.2.3 Gathering Data to Use this Model to Assess Risk Quantitatively. In order to use the model of Figure 11 to determine financials such as risk or annual expected loss for organizations connected in a supply chain, data representing the four types of breaches and the five other factors of Figure 11 must be obtained. Recall that the five factors are the security posture and partner-facing controls; the targeting factor, the level of connectivity with partners; and the degree of sharing between organization ***j*** and each of its partners.

With respect to breach data, it must be recognized that even basic statistics on data breach frequencies and losses are difficult to obtain, especially on a per-firm basis. There are a number of reasons for this. First, it has been estimated that as much as 89% of data breaches go unreported and are thus never known or tallied outside the victim organization (Claburn, 2008). While many of these unreported breaches are never detected in the first place, organizations may not be required or incentivized to report these statistics. Secondly, no entity exists that is officially charged with centralizing breach information or making it available to the public. It is true that certain breach events must be disclosed by law and

certain entities share or report on those disclosures, but such regulations typically pertain only to specific data types and certain amounts (e.g., see HHS Breach Notification Rule[12]). Furthermore, when a breach must be reported by law, there is no requirement to disclose key information like root causes or financial losses. Thus, visibility into data breach statistics tends to be summaries of those incidents that trigger mandatory reporting requirements or become public via some other means (e.g., see KrebsOnSecurity[13]).

Fortunately, reporting/visibility is increasing over time. Entities such as Privacy Rights Clearinghouse[14] (PRC), Identity Theft Resource Center[15] (ITRC), and the VERIS Community Database[16] (VCDB) track over 5100, 6500, and 6700 data breaches respectively in their free public repositories (with overlap, naturally). Though not free to the public, Advisen maintains a proprietary database of over 32,000 cyber incidents available for purchase[17]. Risk Based Security provides access to another proprietary collection of 20,000 plus breaches[18].

Additionally, a growing body of research papers leverages these public and proprietary datasets to share useful statistics and insights with the community (Edwards et al. 2015; Romanosky, 2016). Vendor technical reports like Verizon's annual Data Breach Investigations Report series[19] offer detailed analysis into thousands of breaches, many of which never end up in public or proprietary databases for various reasons. Finally, numerous ongoing survey-based studies seek estimates on breach rates and losses from respondents. While none of these individual sources is sufficient in itself, taken together they help paint an increasingly reliable portrait of firms that do incur cyber loss.

We have accessed all the above data sources and in fact have composed over the last ten years what we believe to be the largest collection of data breach data anywhere in the world. Nonetheless, the reader must be aware that these data are biased in the sense that they are largely forensically determined. That is, the data we have are real and accurate,

[12] https://www.hhs.gov/hipaa/for-professionals/breach-notification/
[13] http://krebsonsecurity.com/2016/01/wendys-probes-reports-of-credit-card-breach/
[14] https://www.privacyrights.org/data-breaches
[15] http://www.idtheftcenter.org/Data-Breaches/data-breaches.html
[16] http://vcdb.org/
[17] http://www.advisenltd.com/analytics/advisens-cyber-dataset/
[18] https://www.riskbasedsecurity.com/cyber-risk-analytics/
[19] http://www.verizonenterprise.com/dbir

but largely represent firms that have actually been breached. Thus the data are not hypothetical, yet they do not necessarily represent firms that have never reported breaches or been studied by outside cyber teams. In this sense, they actually constitute one or two-thousand case studies we have done. Yet they were not conducted on a random sample of all firms world-wide. We therefore do not postulate that our data model represents all firms—in particular, smaller, less innocuous firms. Nonetheless, given this *a priori* understanding, we believe it is impossible to get better data at this time or in the foreseeable future, and we hold that this data model is the best available and in fact is very accurate given a careful interpretation of results.

In this supply chain model, the notion of a base rate of breaches per year is first developed. This is an overall rate for all firms on average; this rate is then adjusted in two different manners to provide more realism and detail. One way the rate is adjusted is by industry; i.e., we produce base rates for each major industry (e.g., mining, transportation, manufacturing, retail, etc.). A second adjustment is to modify the rate for all breaches to reflect five major, different types of breaches. That is, we develop rates based on historical data for breach types such as insider abuse, network intrusion, malware infection, etc.

Our base rate breach estimation procedure was initially to fit breach data incidents to a triangular (most common; worst; best) distribution using minimum, maximum, and most likely values based on our case studies and the references above. This did not give us the detail of breach behavior we wanted in the tails, however. We noted that Edwards et al. (2015) found a lognormal distribution to be the best fit in modeling certain data breach factors because of the refinement possible in the tails (for example, fitting both the 95^{th}-percentile value and the maximum value), and we followed their recommendation for that reason. Given those lognormal distributions for base breach rates, we incorporated modifiers for each industry sector and further refined these rates across the five breach types (network intrusions, etc.) in our model. Modifier values were based on relative observed frequencies from our case studies and public data sources.

Data driving the five factors of Figure 11 were obtained either via prior survey research (Baker & Wallace, 2007; Gregory E Smith et al., 2008) or the 900+ forensic investigations we preformed from 2006-2015. Our standard approach was to construct a simple triangular distribution around each parameter based on the data available. For

instance, the survey results showed weak partner-facing security controls increased the likelihood of a data breach by a factor of 1.44 to 1.68, with a mean of 1.57.

We estimated the loss magnitude or "cost" of each breach by utilizing the number of data records compromised as a predictor. Although not as desirable as direct dollar loss information, the latter is simply not generally available; firms are unwilling, naturally, to make public their losses. Furthermore, our forensic investigations into breaches logically focused on causal factors and direct technical impacts rather than overall financial impacts to the victim organizations, which often aren't fully known until long after the incident.

Forensic investigations are well-suited to determining the number of records compromised and these data are also almost always included in public breach disclosures. We sample data loss values directly from our breach investigations and public databases. Our model for predicting financial loss from the number of records compromised is based on research conducted by Verizon (2015), which is itself modeled on insurance claims data shared by NetDiligence. Verizon reports a modest R^2 of 54% for the model, but confirms that it is the strongest predictor variable amongst the data made available to them and that adding additional data points did little to improve the model. Thus, we have constructed wide distributions around this base loss model to encapsulate the high degree of uncertainty. We assess the reasonableness of this approaching using public loss information in a later section.

In summary, in support of our contention that there is also a down-side to supply chain formation that must be protected against, in particular, increased cyber risk, we have formulated a theory of supply chain cyber risk; have built a mathematical model to assess risk quantitatively in a chain; and have collected what we believe to be more data than anyone else in the world and then fit these data to our model of Figure 11. The reader should be cautious in generalizing from our results to all firms as our breach data tend to be representative of firms that have been, or are likely to be, breached.

5.0 An Initial Quantitative Investigation of Supply Chain Cyber Risk

Having built a model and collected actual data, we now investigate quantitatively several basic questions such as, does connecting in a supply chain actually increase an organization's cyber risk? If so, does the risk increase uniformly for all members of the

chain? How much risk is involved, approximately? Et cetera. As we have distributions of data, a closed form solution is not possible in answering these questions; we thus turn to simulation as our basic methodology.

5.1 Methodology

As mentioned in section 4.2.2, a model of an entire supply chain may be configured by using the model of Figure 11 for each organization, and then specifying each firm's industry, its security posture and targeting factor, and then – for each partner it has – the level of connectivity and degree of sharing. We specify these five factors for each organization in such a way as to address the research questions posed in the next section. As breach and other data are probabilistic and are not amenable to closed-form solutions, we turn to simulation. In particular, we utilize Frontline Solver's *Risk Solver* software.[20] Procedurally, we built one supply chain to address each research question by connecting organizations modeled after Figure 11 in the requisite chain, and then we simulated each chain for one year with 10,000 statistically independent replications.

We addressed the research questions of the next section with very small chains, not because the model developed cannot handle large chains, but because we believed that if we could show effects even in small chains, then larger chains would most likely exacerbate the situation. Moreover, smaller chains might provide more understanding to us due to the lack of complexity. But this itself is a further research question.

5.2 Research Questions

RQ1: Does information sharing affect a firm's overall level of cyber risk?

This may at first appear rather obvious as all firms have a greater-than-zero chance of suffering a security incident and all incidents have a greater-than-zero cost. But the real question here is whether the net increase in risk due to partner collaboration is significant when compared to a firm's individual or independent risk level. If not, then the rest of our research questions are moot and firms can safely pursue aggressive information sharing

[20] http://www.solver.com/risk-solver-platform

agendas without regard to security concerns. As mentioned, however, our previous survey findings suggest this is not the case.

The second research question progresses logically from the first:

RQ2: Does information sharing affect cyber risk uniformly for all firms in a supply chain?

The SCM literature suggests the *benefits* of collaboration are not equal for all involved. For instance, in modeling a simple two-level supply chain, Lee and Whang (2000) found information sharing can provide significant cost reduction to manufacturers, but does not offer much direct value to the retailer. This research question asks whether cybersecurity risk similarly exhibits uneven and perhaps even unfair behaviors. If so, this fact would strengthen claims that information sharing and security policies should take on a supply chain-wide perspective rather than stopping at the network perimeter of individual firms.

Since information sharing and security policies can have upstream and downstream effects, it is conceivable that cyber threats to one firm may affect others as well. Furthermore, if the types, frequencies, and severity of those threats vary enough across the supply chain, it may fundamentally change the nature, or profile, of cyber risk for each member firm. This notion drives our third research question:

RQ3: Does information sharing alter a firm's cyber risk profile?

If so, this discovery has fascinating and critically important implications to managing inter-organizational risk. It would also create pressure to better understand risk factors so that justified decisions can be made to minimize cyber risk for all members while maximizing the benefits of collaboration. Ostensibly, each supply chain would exhibit unique conditions and configurations that might make a perfect solution in one context a disaster in another. Hence, we posit our fourth and final research question in this initial quantitative investigation:

RQ4: How do various information sharing factors affect cyber risk in a supply chain?

Specifically, we wish to examine different supply chain *structures*, varying *intensities of information sharing*, and the effect of *internal and partner-facing cybersecurity practices*.

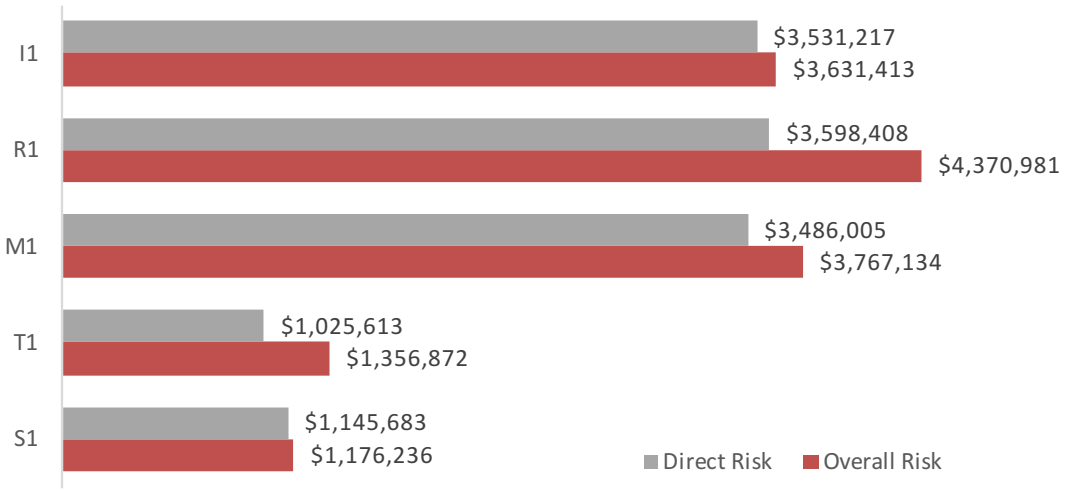
5.3 Research Findings

We now address the four questions by examining them on a small (five organization) supply chain. In particular, we examine the supply chain of Figure 6 using our simulation model of each organization given in Figure 11. We answer each research question using *Risk Solver* to make ten thousand statistically independent replications of each one-year study. Our overall purpose is to qualify and quantify the impact of collaborative activities on cyber risk for individual members as well as the supply chain as a whole.

5.3.1 Does supply chain collaboration change a firm's overall level of cyber risk?

As described in Section 4.0, all organizations are exposed to cyber threats from external and internal sources. Those that do business with other organizations are also subject to threats inherent to those partner relationships. Thus, this question essentially asks a comparison of expected losses from external and internal breaches (direct risk) to overall expected losses, including breaches tied to supply chain partners. Figure 12 illustrates this comparison.

Figure 12. Comparison of annual expected losses from external and internal breaches (Direct Risk) vs. breaches from all sources, including partners (Overall Risk), for firms in the simple sequential supply chain scenario.



Several observations can be made from the figure. It is evident that expected losses from external and internal breaches represent a much higher proportion of overall risk than do breaches involving supply chain partners. The increase from partner breaches, however,

appears greater for some (e.g., the retailer) than for others (the supplier). On average, risk to each firm rose 12%. Whether this increase represents "a lot" or "a little" is subjective and not pertinent to our current line of inquiry; we seek to determine if the increase is statistically significant.

Table 4 summarizes results of significance tests comparing mean differences between direct and overall risk for each firm. A 95% confidence interval is constructed around the mean and a determination is made as to whether that interval includes zero. If so, we conclude there is no meaningful difference between direct and overall expected losses for that firm. If not, we have sufficient evidence to conclude that risk to the firm is significantly changed by participating in the supply chain.

Table 4. Statistical significance test comparing mean differences between direct and overall (direct + partner) cyber risk for firms in the sequential supply chain scenario.

Org	Mean Difference	Half-Width of 95% CI	Lower Bound CI	Upper Bound CI	CI incl 0?	Significant?
S1	$30,553	$1,486	$29,066	$32,039	No	Yes
T1	$331,259	$13,997	$317,262	$345,256	No	Yes
M1	$281,130	$11,490	$269,639	$292,620	No	Yes
R1	$772,573	$44,046	$728,528	$816,619	No	Yes
I1	$100,196	$5,436	$94,760	$105,632	No	Yes

The results in Table 4 are clear – integration and information sharing with partners leads to a significant increase in cyber risk for all firms in our simple sequential supply chain scenario. This is an important finding because it confirms that a trade-off between risk and reward does indeed exist and may erode or perhaps even erase the benefits achieved through collaboration. At the very least, it warrants further investigation into these effects and the factors that heighten or dampen them. We continue this with our next research question.

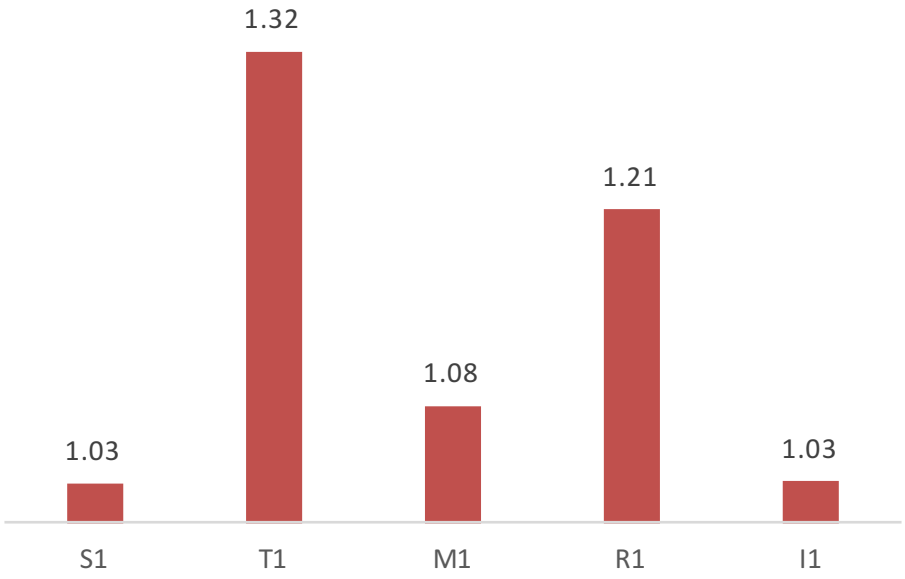
5.3.2 Does collaboration change cyber risk uniformly across the supply chain?

Figure 12 above hints that the increase in cyber risk we established in RQ1 may not be equal among all members of the supply chain. If true, it would imply that some firms take an unfair share of the disadvantages, while others receive more than their fair share of

the advantages. To visualize this more plainly, we present Figure 13, which shows the mean growth factor in risk for each firm caused by partner-related breaches.

As previously stated, the mean growth factor across all organizations was 1.12 (+12%). Firm T1, however, suffered an average increase of 32% while S1 and T1 edged up by a mere fraction of that amount. These findings revealing growth in risk for one member of the supply chain is 10X that of another feel incongruent with the promise of information sharing to reduce risk for all. This is especially true since our current scenario sets all variables to "normal." In other words, T1's surge in risk is not due to a poor security posture or high interconnectivity compared to its peers.

Figure 13. Mean growth factor in risk for each firm caused by partner-related breaches in the simple sequential supply chain scenario.



Given the extent of this disparity, it seems a foregone conclusion that these results are meaningful, but we will test this statistically nonetheless. Constructing a 95% confidence interval around the mean growth in risk for all firms yields a lower bound of 1.11 and an upper bound of 1.13. This is indicated in the top portion of Table 5. We then simply check whether the mean growth factor for each firm falls within the 95% confidence interval across all firms. If so, we would concede that the mean growth in cyber risk to that firm did not differ meaningfully from the global average. That turns out not to be the case

for any firm in our scenario, and therefore we conclude that collaboration does NOT change risk uniformly across all members of the supply chain.

Table 5. Statistical significance test comparing mean risk growth factor by organization for firms in the simple sequential supply chain scenario.

	Mean Factor	Upper Bound	Lower Bound
All	1.12	1.11	1.13

Org	Mean Factor	Within 95% CI for All?	Significant?
S1	1.03	No	Yes
T1	1.32	No	Yes
M1	1.08	No	Yes
R1	1.21	No	Yes
I1	1.03	No	Yes

Having increased our confidence that firms' cyber risk postures actually are affected disproportionately by information sharing, we ask why this is. There is no test that provides definitive answers to that question, but we can offer some informed explanations. As presented in chapter 5, our forensic investigations of data breaches often identified partner connections and/or credentials as the vector of attack. This was especially common among retailers (second only to the hospitality industry), and so we are not surprised to see this reflected in elevated risk levels for that industry.

We find the impact of collaboration on the transportation firm's expected losses, however, to be somewhat curious. The transportation industry did exhibit a higher proportion of partner-actor breaches (8%) than other industries, but partner-vector and partner-custodian percentages fell among the others. Neither seem to fully account for the 32% increase in expected losses for that industry. Another explanation is that this effect may simply be a matter of scale. We are reminded in Figure 12 that firm T1 exhibited the lowest individual risk, making a moderate increase a relatively profound factor. It is also possible that the position in the supply chain is a factor and the distributor is in a sense accumulating and amplifying risk from upstream and downstream partners. RQ4 holds additional clues about this possibility.

5.3.3 Does supply chain collaboration change a firm's cyber risk profile?

Recall that a firm's cyber threat profile consists of the types and relative frequencies of threats it experiences. A cyber *risk* profile is a similar concept, except it describes expected losses from threats rather than just frequency. Thus, malicious software infections may rank high on a firm's threat profile (occurs often), but be relatively low when it comes to risk (minor losses).

Figure 2 demonstrated that different industries can exhibit drastically different threat profiles. Because of this and the shared nature of threats/risk in a supply chain, we foresee the possibility of a sort of blending effect of profiles as member firms integrate and collaborate. This question seeks to know if such an effect exists and whether it can significantly alter the expected losses for each type. For extra clarity and insight, we approach this question in three iterative phases or sub-questions.

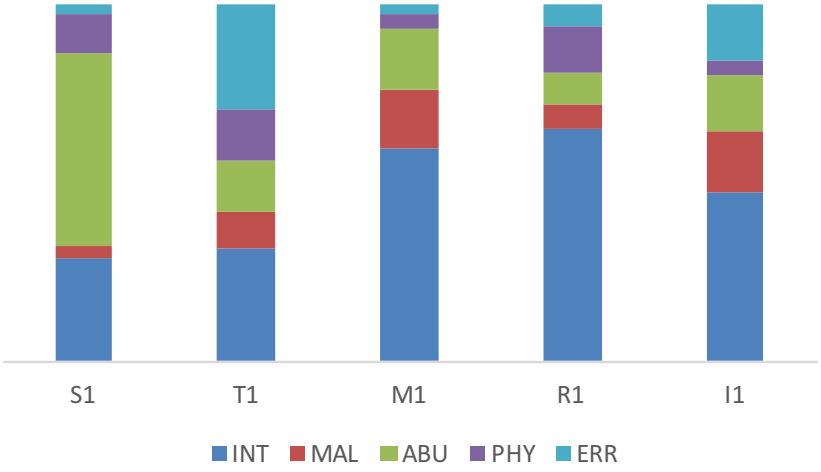
5.3.3.1 Establishing threat profiles.

We first seek to establish a threat profile for each firm. Granted, this largely reflects the industry-base rates and modifiers that drive our model, but those input variables cannot foresee dynamic outcomes of the simulation like breaches caused by and propagated between partners. Figure 14 displays proportionality among breach types for each firm.

It is readily apparent from Figure 14 that there is indeed variation among firms when it comes to the types of breaches experienced. Network intrusions (INT) are a big problem for everyone, but range from 29% of breaches for S1 to 66% for R1. Privilege abuse (ABU) is a major issue for S1 but much less so for others. T1 and I1 suffer comparatively high amounts of errors and omissions (ERR), which hardly register for the other firms.

Given these differences, it's easy to see how security controls tailored to defend against threats experienced by S1 might differ greatly from those implemented by R1. Furthermore, one may postulate that integrating T1 and M1 may leave the former overly prone to intrusions and the latter susceptible to errors.

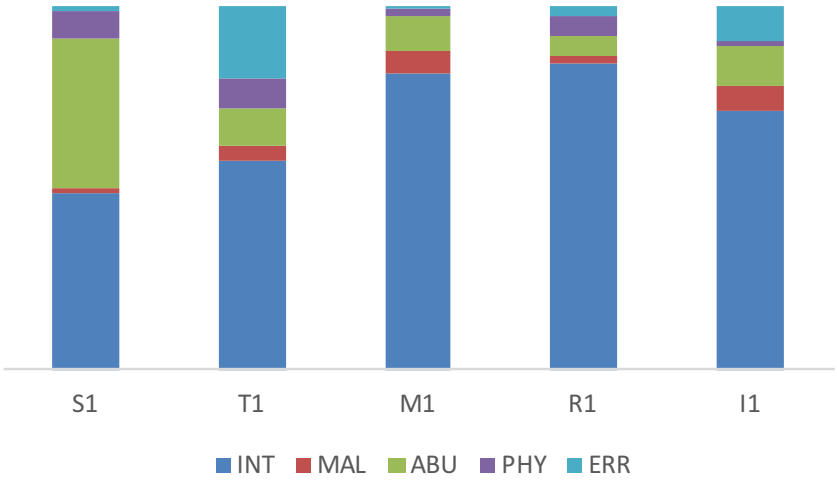
Figure 14. Threat profile for each firm depicted by the percentage of breaches for each breach type in the simple sequential supply chain scenario.



5.3.3.2 Establishing risk profiles.

Threat profiles are useful in many ways, but what most organizations really care about is the amount of risk associated with the threats arrayed against them. To that end, Figure 15 displays the ratio of expected losses across the five breach types for each firm in the supply chain. This effectively creates the risk-based corollary of Figure 14 above.

Figure 15. Risk profile for each firm depicted by the ***percentage of losses*** for each breach type in the simple sequential supply chain scenario.



Note this represents the individual risk for each firm from external and internal data breaches, and so does not incorporate any risk-altering effects introduced by supply chain

partners. We isolate and evaluate those changes in the next sub-section. For now, we are simply interested in discernable differences in profiles.

The distribution of expected losses across breach types in Figure 15 appears somewhat similar to Figure 14's frequency-based ratios, with the most discernable difference being a greater predominance for network intrusions (INT), in line with the fact that most of the largest losses on record fall in that category. Overall, it's clear from Figure 15 that these firms do indeed possess distinctive risk profiles, and this makes our original question posed in RQ3 much more interesting and important.

5.3.3.3 Establishing risk profiles.

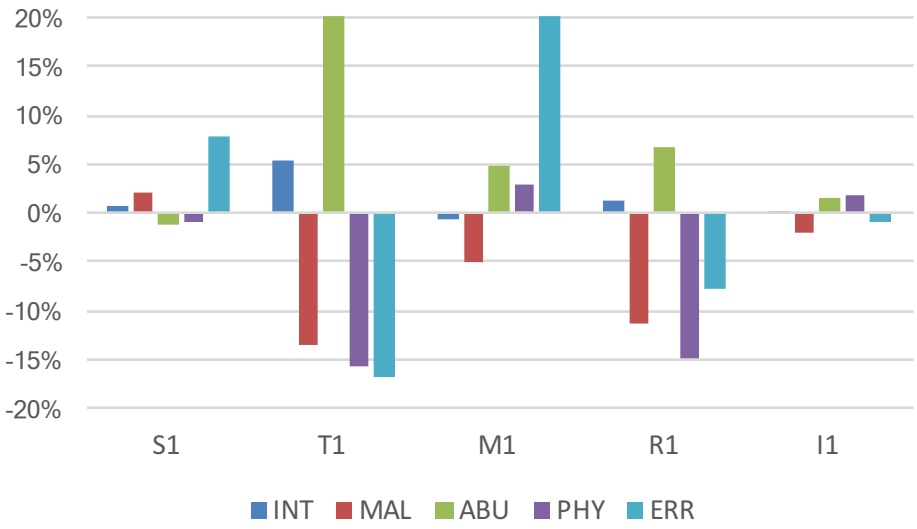
We now seek to evaluate the impact of partner breaches on each firm's risk profile. There are many different angles from which to approach this line of inquiry, but we have chosen one that captures the essence of what we wish to know. Figure 16 depicts the relative percentage change between individual risk (no collaboration) and overall risk (including collaboration) for each breach type for each organization. Several observations emerge from the figure.

First, all firms are affected differently and at varying degrees. Firm I1's risk profile seems barely moved, while T1 underwent substantial changes for every category. Beyond that, we note that the most upstream and most downstream firms in the supply chain show the least impact on their risk profiles. It is difficult to determine whether this is a product of their position, role, or something else, but we will explore this further in RQ4.

We find it somewhat surprising that no firms register large changes in the percentage of network intrusions (INT). This likely stems from the expected losses for that category being so high to begin with (see Figure 14 and Figure 15). It would take a huge increase or decrease in expected losses to move the needle.

The degree of change is also worth noting: ±20% appears to be the range of movement within each breach type. Considering this measure in light of managing risk within a firm, it is not hard to imagine that swings in four categories of 10% or more might tilt what was once a well-balanced security posture. This, in turn, may necessitate changes in strategy, spending, and practice (i.e., T1 might need deploy and/or strengthen controls against privileged system abuse).

Figure 16. Change in risk profile for each firm depicted by the percentage change in losses for each breach type in the simple sequential supply chain scenario.



The import of these findings grows even more when one considers the profile changes seen in Figure 16 have nothing to do with security efforts – good or bad – of any individual firm. These effects are solely a byproduct of integrating and collaborating with supply chain partners. Obviously, firms will want to minimize these adverse effects while at the same time retaining the benefits of information sharing to reduce their overall risk. We examine the mechanics of this in the next section.

5.3.4 How do various collaboration factors affect cyber risk in a supply chain?

All examples and analysis to this point have focused on a simple sequential supply chain where collaboration levels, security postures, and other factors are set to their "normal" levels. While useful pedagogically, this does not reflect reality where all of this varies considerably. We saw in Chapter 4 that such variables can significantly alter incident likelihood, and we now extend that analysis using our simulation model to study the effect these different conditions and factors have on cyber risk.

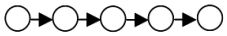
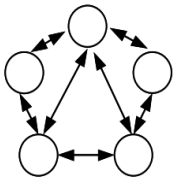
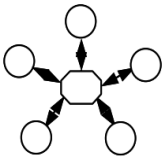
5.3.4.1 Effect of Information Sharing Structure.

The concept that information sharing relationships utilize different structures or typologies was introduced early and remained a steady topic of research in the years that

followed (Hong, 2002; Kumar & van Dissel, 1996; Hau L Lee & Whang, 1998; Samaddar, Nargundkar, & Daley, 2006). Much of this research examined the comparative benefits of these structures under different collaboration requirements, technologies, and strategies. While the terminology differs, the literature generally recognizes three basic information sharing structures: sequential, hub-and-spoke, and reciprocal (many-to-many). This is illustrated in Table 6, which is adapted from Liu and Kumar (2003).

Our focus to this point has been on a scenario linking five firms in a sequential information sharing structure. This is a very common approach in the literature for general model building and exploratory analysis, but not representative of the many different types of inter-organizational systems that exist to support collaboration. In pursuit of more robust managerial implications, we now seek to understand how these different structures impact cyber risk.

Table 6. Three basic information sharing structures commonly recognized in the Supply Chain Management literature. Taken from Liu and Kumar (2003) and inspired by Hong (2002) and Kumar and van Dissel (1996).

Information Sharing	Sequential	Reciprocal	Hub-and-Spoke
Structure			

To accomplish this, we altered information sharing variables to create the Reciprocal and Hub-and-Spoke structures pictured above. Both new structures use the same five types of firms as our sequential scenario described above (a supplier, a distributor, a manufacturer, a retailer, and IT services).

Two model variables were changed for the Hub-and-Spoke structure. Firms S1, T1, M1, and R1 engage in direct two-way information sharing with firm I1 but are not connected to each other. In this arrangement, I1 could represent some kind of cloud-based data exchange or service provider. These same two variables were altered to achieve the

Reciprocal structure, except all firms are interconnected and engage in direct two-way collaboration with each other. There is no "middleman."

All other model variables remain static (at their "normal" levels) for the three structures. Just like the sequential scenario analyzed before, we ran 10,000 trials of the simulation with each of the new configurations. Table 7 shows the output of these trials in the form of annual expected losses (ALE) for each firm under each information sharing structure.

Table 7. Expected losses by firm for each information sharing structure.

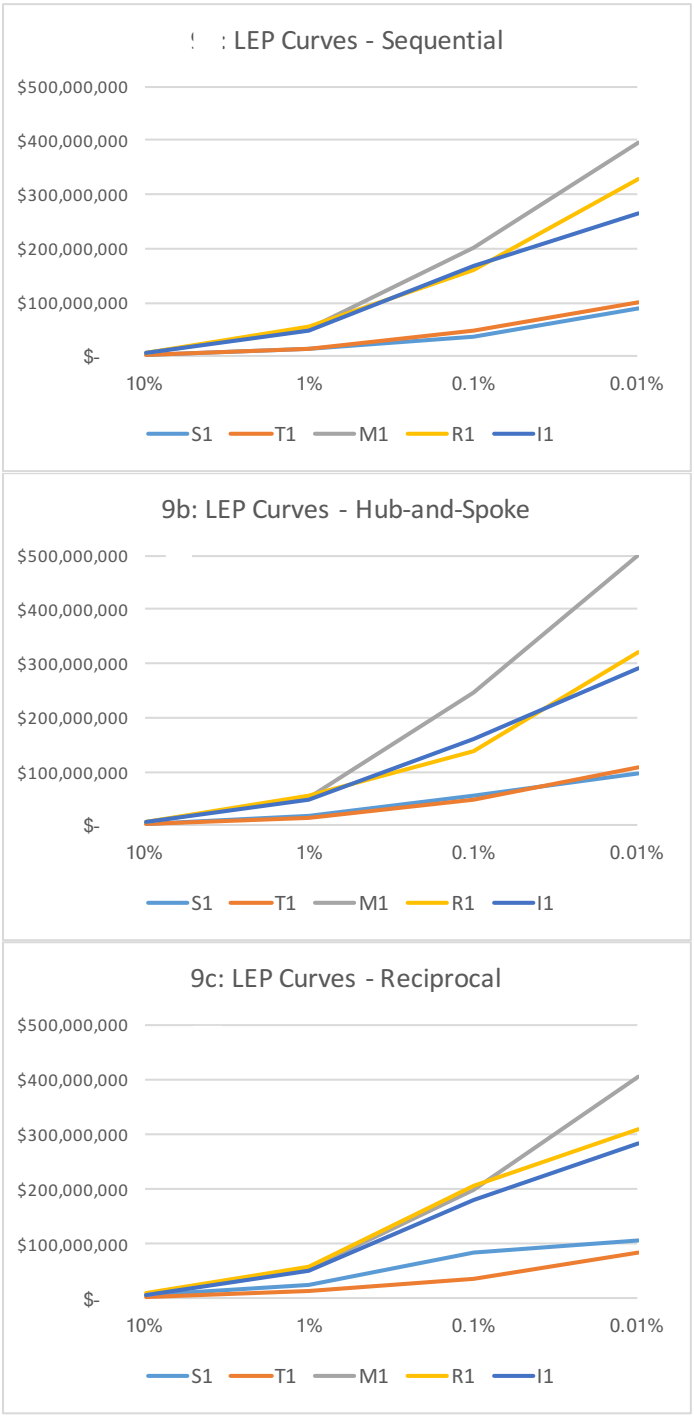
Firm	Mean	10%	1%	0.1%	0.01%
SEQUENTIAL STRUCTURE					
S1	$ 1,176,236	$ 2,341,090	$ 15,673,155	$ 38,213,167	$ 88,215,024
T1	$ 1,356,872	$ 2,714,679	$ 12,569,782	$ 47,949,039	$ 100,878,504
M1	$ 3,767,134	$ 6,711,835	$ 51,698,559	$ 199,425,302	$ 397,026,959
R1	$ 4,370,981	$ 8,298,117	$ 56,113,502	$ 159,848,785	$ 327,773,669
I1	$ 3,631,413	$ 7,146,853	$ 46,107,538	$ 166,295,179	$ 264,317,360
HUB-AND-SPOKE STRUCTURE					
S1	$ 1,478,425	$ 2,969,514	$ 17,392,951	$ 56,700,113	$ 96,748,645
T1	$ 1,337,841	$ 2,631,774	$ 13,108,696	$ 48,544,577	$ 107,037,727
M1	$ 4,004,093	$ 6,809,068	$ 52,946,683	$ 245,385,916	$ 500,512,747
R1	$ 3,900,258	$ 7,148,984	$ 56,471,870	$ 136,874,767	$ 322,148,776
I1	$ 3,881,349	$ 7,643,150	$ 46,751,088	$ 161,074,390	$ 290,890,245
RECIPROCAL STRUCTURE					
S1	$ 2,266,870	$ 4,884,039	$ 23,736,002	$ 85,331,997	$ 107,451,605
T1	$ 1,653,919	$ 3,558,562	$ 15,261,323	$ 35,068,987	$ 84,211,248
M1	$ 4,039,509	$ 7,425,529	$ 52,747,209	$ 197,498,023	$ 402,891,730
R1	$ 4,935,120	$ 9,512,771	$ 57,982,479	$ 206,156,953	$ 307,869,588
I1	$ 4,070,916	$ 7,644,783	$ 50,915,153	$ 179,501,166	$ 281,512,624

The most fundamental question answered by Table 7 is "Which structure represents the most cyber risk to the entire supply chain?" The answer does, however, depend on what one means by "most." According to the results, the absolute maximum annual expected loss value occurs in the Hub-and-Spoke scenario. But that represents an exceedingly rare set of events, as will become clearer in Figure 17. The Reciprocal structure exhibits the most chain-wide risk when considering the mean and 95th percentile values. In most cases, Reciprocal is also the highest loss value for the individual firms. To better examine expected losses for individual firms, we create a more helpful visualization.

Figure 17 shows loss exceedance probability curves for each firm for the three information sharing structures. There's little discernable difference among the structures 99% of the time. Within the 1% territory, however, the structures begin to exhibit some deviation. Perhaps most notable is that expected losses for the manufacturer rise more sharply than the others in the Hub-and-Spoke structure. It is the only scenario in which a firm crosses the $500 million threshold at a 1/10,000 probability. Granted, this represents an extremely rare event, but is noteworthy nonetheless.

We find the effect on M1 participating in a Hub-and-Spoke sharing structure somewhat of an enigma. Logic would dictate that I1 – the hub – would be affected the most in this scenario since it is the only firm directly connected to all the others. Conversely, I1 is also an aggregation point for everyone else's data, which means a breach there could impact the whole chain.

Figure 17. Loss exceedance probability curves for each information sharing structure.

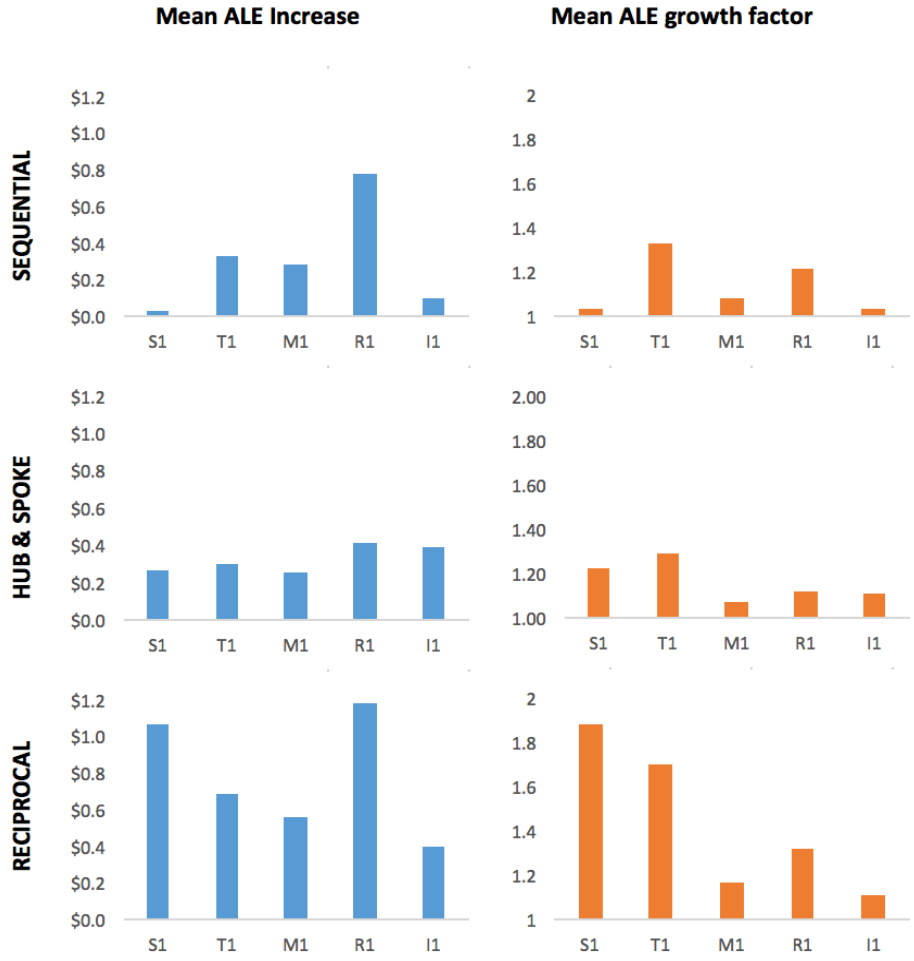


Probability curves are an excellent tool for viewing and comparing overall expected losses, but they do not make it easy to discern the net change in risk to each firm. To help with that, we present Figure 18.

Figure 18 displays two perspectives for the effect of information sharing structures on cyber risk. The leftmost column compares each structure according to the mean increase in expected losses brought about by supply partner relationships. That same value is expressed as a growth factor (total/individual) in the column on the right.

The charts for the Sequential structure are reproductions of the data found in Figure 12 and Figure 13, so we do not offer further comment on those other than to calibrate interpretation of the others. In that structure, R1 exhibits the highest absolute increase in expected losses (~$800K), while T1 shows the largest relative gain (+32%).

Figure 18. The effect of information sharing structure on expected losses for each firm.



Comparatively, the risky effects of collaboration in a Hub-and-Spoke supply chain appear much more balanced across all firms. R1 and T1 are still hit hardest in their respective views, but not nearly to the degree we see in the Sequential structure. We surmise this has something to do with risk being pooled or shared to a certain extent in this model. Everyone connecting to and sharing via one point means that nobody is left holding a disproportionately large share of the risk. The potential downside of this, however, is that the hub becomes a single point of failure in the system. One wonders what happens if the hub is insecure and/or becomes a target of choice for cyber criminals. We shall pick this up in a later section.

The charts for the Reciprocal structure are equally intriguing, but the distribution of risk is far from equal. R1 once again takes on the most risk from collaborating with partners, but it the supplier and distributor that are hurt the most in this configuration. Expected losses nearly double for S1 and soar 70% for T1. We confess no small amount of surprise at this outcome, since intuition suggests the "everyone connected to everyone" approach would more evenly distribute risk across the supply chain. Instead, cyber risk is concentrated and amplified for upstream firms.

We want to reiterate that the main purpose of this analysis is to isolate and understand the effects of information sharing structure on cyber risk. In a real supply chain, variables such as interconnectivity, security posture, and information sharing would differ for every firm-to-firm relationship in all of these structures. We do, however, consider these experimental results important in their own right. For example, we mentioned previous research that found information sharing offered little value to retailers but brought substantial cost reduction to manufacturers (Hau L. Lee, So, & Tang, 2000). If that is indeed the case, then our findings imply the imbalance of benefits may be even worse since the retailer consistently incurs the most cyber risk from information sharing and the manufacturer is among the least affected.

5.3.4.2 Effect of Cybersecurity Practices.

We have consistently maintained that uncovering managerial implications is a primary driver for this research. After reviewing results in the previous section, perhaps the main question on any manager's mind is "Can we lower our risk exposure to supply

partners?" That is the question we take up now as we assess the impact of security practices on cyber risk in supply chains.

While there is an almost endless number of aspects one could consider when examining security practices, we focus on two broadly comprehensive categories: *security posture* and *3rd party security*. By security posture, we refer to all people, processes, and technologies dedicated to defending the firm against external and internal threats. 3rd party security, as the name implies, includes controls specifically focused on threats related to a firm's partners, service providers, and other such business-to-business relationships. Our model allows both to be rated for each firm as an overall measure of strength.

Our main interest at present lies in reducing cyber risk by strengthening security practices. We could certainly study the effect of weakening security, but it is unlikely any manager would consciously decide to do this. On the other hand, they are faced with decisions every day about how best to improve their cybersecurity programs. To support our enquiry on this matter, we refer to the data contained in Table 8.

Table 8. Expected losses by firm under "Strong" security practices.

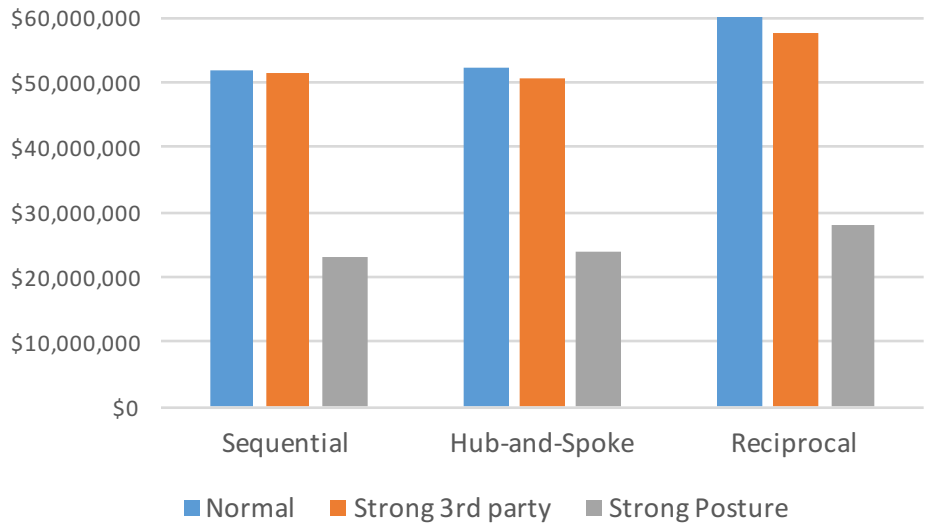
Firm	Mean	10%	1%	0.1%	0.01%
SEQUENTIAL STRUCTURE					
S1	$ 603,287	$ 1,262,550	$ 8,100,330	$ 13,493,972	$ 46,857,806
T1	$ 731,246	$ 1,404,690	$ 6,606,751	$ 29,532,937	$ 68,195,296
M1	$ 2,005,325	$ 3,566,743	$ 30,183,686	$ 113,929,209	$ 243,437,900
R1	$ 2,478,359	$ 4,687,859	$ 32,214,445	$ 92,366,507	$ 162,027,303
I1	$ 1,958,407	$ 4,019,741	$ 24,224,620	$ 97,646,887	$ 122,949,642
HUB-AND-SPOKE STRUCTURE					
S1	$ 812,548	$ 1,586,611	$ 9,683,486	$ 32,471,200	$ 43,300,389
T1	$ 716,629	$ 1,304,980	$ 7,132,084	$ 30,429,384	$ 76,997,167
M1	$ 2,236,700	$ 3,647,025	$ 27,911,926	$ 167,183,316	$ 368,430,215
R1	$ 2,073,459	$ 3,883,681	$ 31,290,170	$ 59,995,860	$ 181,423,489
I1	$ 2,065,838	$ 4,248,933	$ 24,876,515	$ 80,190,396	$ 157,984,542
RECIPROCAL STRUCTURE					
S1	$ 1,224,563	$ 2,759,241	$ 12,576,341	$ 52,610,649	$ 14,291,695
T1	$ 890,119	$ 1,989,804	$ 8,902,664	$ 14,547,353	$ 16,026,902
M1	$ 2,118,653	$ 3,871,916	$ 28,712,548	$ 118,072,518	$ 209,306,168
R1	$ 2,923,548	$ 5,590,494	$ 36,306,272	$ 125,432,984	$ 148,370,903
I1	$ 2,274,720	$ 4,037,640	$ 29,524,378	$ 106,263,499	$ 146,041,621

Table 8 mirrors Table 7 from the previous section, except that it shows predicted reductions in expected losses when both security posture and third party security variables

are set to strong for each firm. No other variables were changed for these trials. The difference between the two tables is essentially the value of good security within moderately collaborative supply chains. That value nets out to an average 55% drop in cyber risk for each structure (there is little difference between them).

Per results to the right side of Table 8, robust security practices pay even more dividends when it comes to catastrophic events, translating to reductions of hundreds of millions of dollars in "long-tail risk." Given that these extreme but rare events are the ones that most executives and boards of directors fear the most, this makes a compelling case for firms seeking to justify investments to improve cybersecurity practices.

Figure 19. The effect of security practices in mitigating cyber risk.



An interesting follow-up question at this point concerns which category of security practices has the most power to mitigate risk. Figure 19 gives the relevant model output as well as a surprisingly definitive answer. Strengthening partner-facing controls without also improving security posture does relatively little to lower expected losses across the supply chain. Per-firm savings from better 3rd party security averaged only 1% for Sequential and Hub-and-Spoke structures and 6% for Reciprocal chains.

The direct implications of this finding are obvious – given the choice, all firms should improve their own security posture before focusing on 3rd party controls. The indirect implications are not so plain. Does this contradict earlier references that firms must

begin considering cybersecurity policies in light of their supply chain partners rather than merely their own agenda (Kolluru & Meredith, 2001)? Absolutely not! Far from being a call for firms to pursue independent, isolationist security programs, these results actually urge quite the opposite behavior. Our interpretation – and hearty recommendation – is that the best way to improve overall cybersecurity in a supply chain is for individual firms to strengthen their security postures for the greater good. This reasoning is not unlike hygienic practices in everyday life such as washing your hands and covering your mouth when you cough. Taking care of your own health does, in a very real way, take care of the community. It appears this concept applies to cybersecurity as well.

5.3.4.3 Effect of Information Sharing Intensity.

Another question may arise at this point concerning the effect varying levels of collaboration have on cyber risk. The SCM literature commonly refers to three aspects that define information sharing intensity:

1. Degree or amount of information sharing. These are commonly parameterized as "None," "Partial," and "Full."
2. Scope or nature of shared information. These are parameterized as "None," "Transactional," "Operational," and "Strategic."
3. Level of IT integration or interconnectivity. Parameters are "None," "Low," "Moderate," and "High."

While it is a rather unrealistic scenario, we begin by turning all information sharing variables to their highest setting and all security variables to their weakest setting. This effectively creates a highly-collaborative, poorly-secured supply chain. Not surprisingly, this configuration turns out to be a recipe for disaster.

Table 9 displays the results under Scenario 2 (HC;PS) in the form of mean ALE and the corresponding change factor compared to the base scenario of normal collaboration and normal security. On average, this nearly triples expected losses for each firm in the supply chain. The combination of high intensity sharing and weak security wreak havoc on firms in a Reciprocal arrangement, likely due to the amplification effects of the many-to-many relationships in that sharing structure.

Table 9. Expected losses by firm under maximal sharing and poor security practices.

	Mean ALE			Change Factor	
Firm	1 (NC;NS)	2 (HC;PS)	2 (HC;SS)	2 (HC;PS)	2 (HC;SS)
SEQUENTIAL STRUCTURE					
S1	$ 1,176,236	$ 2,585,049	$ 599,686	2.20	0.51
T1	$ 1,356,872	$ 4,339,555	$ 877,023	3.20	0.65
M1	$ 3,767,134	$ 8,850,899	$ 1,967,435	2.35	0.52
R1	$ 4,370,981	$ 10,708,570	$ 2,127,916	2.45	0.49
I1	$ 3,631,413	$ 7,747,877	$ 1,761,961	2.13	0.49
HUB-AND-SPOKE STRUCTURE					
S1	$ 1,478,425	$ 3,587,637	$ 823,194	2.43	0.56
T1	$ 1,337,841	$ 3,649,257	$ 838,487	2.73	0.63
M1	$ 4,004,093	$ 8,119,560	$ 1,914,320	2.03	0.48
R1	$ 3,900,258	$ 10,248,984	$ 2,125,418	2.63	0.54
I1	$ 3,881,349	$ 9,310,095	$ 1,972,412	2.40	0.51
RECIPROCAL STRUCTURE					
S1	$ 2,266,870	$ 9,025,802	$ 1,723,937	3.98	0.76
T1	$ 1,653,919	$ 8,732,567	$ 1,292,473	5.28	0.78
M1	$ 4,039,509	$ 10,739,143	$ 2,276,060	2.66	0.56
R1	$ 4,935,120	$ 19,116,925	$ 3,013,061	3.87	0.61
I1	$ 4,070,916	$ 9,238,037	$ 2,081,458	2.27	0.51

We now take a short detour from Table 9 to revisit a more realistic scenario combining intense collaboration with poor security. During the discussion on Figure 18 regarding the Hub-and-Spoke scenario, we speculated about the potential of the hub (I1) becoming a single point of failure and/or attack. Figure 20 shows the outcome of simulating such a scenario by setting I1's security posture to poor, 3rd party controls for all firms to poor, and information sharing intensity to high. When compared to Figure 18, the effect is quite dramatic, and highlights the wisdom in the old adage "a chain is only as strong as its weakest link." The risk to each firm in the supply chain increases by an average of 150%. This finding suggests cybersecurity should be a very important decision criterion for evaluating and selecting cloud-based 3rd-party service providers.

Returning now to Table 9, we address the third and final scenario of high collaboration with high security. While it is unlikely that one would find a supply chain in which these variables are uniformly high for all members, this configuration does allow us to answer what is perhaps the most important and practical question within the scope of this research – can strong cybersecurity practices enable firms to enjoy the benefits of intense information sharing without incurring intolerable risk? Based on results in Table

9, we must conclude that they can indeed. Expected losses in Scenario 3 (high collaboration; high security) are roughly half to two-thirds that of our base scenario where all variables are normal.

Figure 20. Expected losses by firm in a Hub-and-Spoke structure based on a Hub with poor security practices and weak 3rd party controls between partners.

The bottom line in all of this is that collaboration and security in a supply chain is not so much a binary tradeoff as it is a delicate but doable balance. And that is something that can be built upon to achieve a more prosperous future for all in our highly competitive and connected world.

5.4 Caveats and Reasonableness

As mentioned multiple times, although we believe these results to be informative and valid, there was necessary bias introduced with using 1,000 security incidents (most of which were forensic) as part of our data collection: results obtained here tend to describe firms that either have been breached or will be breached. That is, firms such as *Joe's Cash-Only Local Sandwich Shop* may not experience the behavior described above. Nonetheless, we can and do provide below some evidence of the *reasonableness* of the data we have generated.

5.4.1 Assessing the Reasonableness of Breach Rates

We first examine our data output from the standpoint of *annual rates of occurrence of breaches on a per firm basis.* As noted, the literature does not provide such direct empirical data on annual rates of occurrence on a per-firm basis. We can, however, derive some useful approximations for comparison to our model output. Statistics on breach rates for the five organizations in our basic sequential supply chain are found in the table below.

Table 10. Annual breach rate statistics for firms in the simple sequential supply chain scenario.

Firm	Median	Mean	95th Perc.	Max
Mining1	0.14	0.28	0.82	5.20
Transportation1	0.15	0.29	0.75	4.22
Manufacturing1	0.34	0.67	1.89	11.46
Retail1	0.35	0.73	1.95	10.25
IT Services1	0.38	0.72	2.10	14.79

The maximum breach rate is the most directly comparable to available data. According to analysis by Risk Based Security, Shell Oil Company experienced 14 (known/reported) breaches in 2015, while 7-Eleven, Bank of America, and Circle K Convenience Stores each reported ten or more (Risk Based Security, 2016). The same report states another 138 organizations suffered multiple breaches that year. A study examining the entire Advisen dataset of cyber incidents (not exclusively data breaches) found that 4800 firms (38%) were "repeat offenders," logging multiple incidents over a ten-year span and 8% of all firms experienced 10 or more (Romanosky, 2016). Our own analysis of the public PRC, ITRC, and VCDB databases also confirms that it is not rare for organizations to suffer multiple incidents in a given year. Given those data, we deem the 95th percentile and maximum rates shown in Table 4 to be reasonable.

Deriving a mean or median rate of occurrence of breaches from public listings is also not realistic given the current nature of those datasets. While such statistics have been presented in aggregate, they are not available in the per-firm, annual rates produced by our model. For such comparisons, we must rely on surveys and studies that specifically seek these data points from participating firms.

The 2016 Cost of a Data Breach Study from the Ponemon Institute claims the typical firm has about a 26% chance of suffering a data breach of 10,000 records over a two-year period (Ponemon Institute, 2016). This translates to a rate of 0.13 per year (per every 10K records), which is just under our lowest modeled median breach rate and half that of the mean. Yet two-thirds of the breaches in our dataset had fewer than 10,000 records, and adjusting for this places the Ponemon rate well within our range.

Another report found that 37% of the companies represented suffered a material or significantly disruptive security exploit or data breach one or more times over the last two years (Ponemon Institute, 2015). This suggests our modeled rates are on the high side, but the qualifier of "material" is difficult to interpret. We have no such distinction and include breaches of all types and severity. As mentioned previously, smaller/minor breaches outnumber larger/major ones by a substantial margin. Thus, we believe that this data point does not provide information contradictory to our results.

A 2015 Price Waterhouse Coopers survey provides an overall breach rate of 0.9 for large enterprises and 0.74 for smaller businesses (PWC, 2015). This exceeds our median and mean rates, but PWC's definition of "breach" is unclear. Other findings in the report suggest the term refers to a broader scope of security incidents beyond data breaches. The same study later offers rates of 0.66 and 0.25 for "serious" breaches within large and small firms respectively. This better approximates our concept of data breaches and fits our output quite well.

One important factor to consider when assessing the frequency of incidents is the security posture of the firm in question. Earlier research found poor security programs reported data breaches at a rate 3 to 4 times that of strong programs. It also must be recalled that studies have indicated that as much as 89% of security incidents go unreported (Claburn, 2008). Thus, actual rates are likely higher than what survey respondents like those above report and will in fact vary substantially from firm to firm. All in all, we find no compelling evidence among multiple independent sources to invalidate our model output for annual breach rates in Table 10 or to conclude that the findings are not *reasonable*.

5.4.2 Assessing the Reasonableness of Loss Magnitude

Loss magnitude refers to the total cost of a single breach event. This includes direct costs such as incident response fees and business disruptions but also indirect or secondary impacts like regulatory penalties, class action lawsuits, brand damage, etc. Losses predicted by our model are based largely on the amount of data records compromised, which is itself based on historical data collected for each breach type. Thus, losses for any single event are more a function of the type and size of breach than the type of firm involved. Table 11 provides output from our model pertaining to loss magnitude for each of the 5 breach types.

Table 11. Single-event loss magnitude statistics for breach types in the simple sequential supply chain scenario.

Breach Type	Median	Mean	95th Perc	Max
INT	$1,557,000	$7,579,000	$32,456,000	$351,101,000
MAL	$843,000	$2,013,000	$6,768,000	$90,450,000
ABU	$489,000	$3,331,000	$11,275,000	$363,129,000
PHY	$981,000	$2,655,000	$9,935,000	$213,125,000
ERR	$830,000	$3,066,000	$ 9,374,000	$378,691,000

As with breach rates, comparable data are more readily available for extreme cases. Large breaches generate attention-garnering headlines and prompt greater inquiry into the financial impact on the victim organization. Consider Table 12, which lists reported losses associated with some of the more well-publicized data breaches. As large as these values are, they amount to less than 1% of annual revenues of the likes of Target, Home Depot and Sony (Dean, 2015).

Though the number of records is the best known predictor of breach cost, it only explains half the variation observed in reported financial losses (Verizon, 2015). This can be seen in Table 12, where, for example, Heartland's breach of 130 million records cost $140M, while the fallout from the 28 million records stolen from OPM purportedly stands at $350M and counting.

Table 12. Example losses reported for some of the largest known data breaches. Adapted from Widmer (2015).

Victim organization	Year of breach	No. records breached	Estimated loss magnitude
TJ Maxx	2007	94M	$162M to $256M
Heartland Payment Systems	2008	130M	$140M
Sony Playstation	2011	77M	$171M
Target Corporation	2013	70M	$262M
Home Depot	2014	56M	$232M; $1B potential
Sony Pictures	2014	10M	$35M to $100M
Anthem	2015	80M	$100M+
Office of Personnel Management (OPM)	2015	28M	$350M to date

Moving on from the extreme cases, a consensus on the cost of more typical data breaches proves difficult to find. The most well-known practitioner reference on this topic is the annual Cost of a Data Breach Study from the Ponemon Institute. The study surveys participants to derive a flat cost of $158 per record and claims average losses from a data breach to be $4 million (Ponemon Institute, 2016).

More recently, research efforts have emerged that leverage actual reported losses to study loss magnitude. One such example from NetDiligence analyzed 183 cyber insurance claims and exposed the folly of using a flat rate per record to predict cost (NetDiligence, 2015). Their results place the minimum cost per record at $0.03 and the maximum at $1.6M. Overall, their analysis found the average loss magnitude for a breach to be $665,000, while the median drops to $60,000. Another effort analyzed a proprietary breach dataset from Advisen and assessed a mean cost of $6M per breach event with the median at $170,000 (Romanosky, 2016). Though these figures are well below our corresponding estimates in Table 11, this may be explained by the nature of our case studies, which are biased toward more severe incidents requiring external investigation.

As with our assessment of breach rates, we find the loss magnitude data available for validation rather messy, but overall more supportive than contradictory. Since breach rates and loss magnitude are the two base components of ALE, we find no compelling argument against the reasonableness of our basic loss predictions or our analysis pertaining to the stated research questions.

6.0 Conclusions and Managerial Implications

The management of 3rd party cybersecurity risk, whether in the context of traditional supply chains or otherwise, represents a major source of concern and expense for many organizations. Ensuring the protection of sensitive data is difficult enough when it is in your control; protecting it while in the possession of others is another matter entirely and fraught with uncertainty. As a result, the modus operandi is to subject partners to lengthy questionnaires (of dubious value) in an attempt to ascertain security posture and create some measure of accountability in the event something goes wrong. As this paper has made abundantly clear, things often do go wrong.

Obviously, managers desire greater control over their cybersecurity destiny when it comes to dealing with supply chain partners. Simply hoping that partners will uphold their end of the bargain is not a winning data protection strategy. This paper has sought to improve understanding of how data breaches occur in supply chains, measure the risk of these events, and explore how various supply chain collaboration and configuration factors affect that risk. In summary, 5 key conclusions emerged from this research:

1. *Information sharing affects a firm's overall level of cyber risk.* While intuitive, validating this assumption using empirical data and simulation modeling is an important step toward properly assessing and mitigating this risk.
2. *Information sharing does not affect cyber risk uniformly for all firms in a supply chain.* As with the benefits of collaboration, we found that the risks therein are not evenly distributed. This is very important because it means that conflict will likely arise among partner firms regarding how much collaboration and security is "enough."
3. *Information sharing alters a firm's cyber risk profile.* Not only is a firm's overall level of risk affected by its partners, but the nature and types of risk changes as well. A firm that has successfully adapted its security posture to deal with known threats may, through collaboration with partners, find itself vulnerable to previously unknown or less critical *threats.*
4. *Information sharing structure affects cyber risk in a supply chain.* The way in which collaborating firms are logically connected to one another appears to matter a great deal when it comes to risk transfer across the chain. Certain structures

cause risk to aggregate upstream, while others downstream. The impact individual firms have on risk across the chain can also be greatly impacted, for instance, in a "cloud-like" structure where one firm acts as the centralized data aggregator.

5. *Cybersecurity practices can effectively mitigate cyber risk in a supply chain.* It is not surprising that poor cybersecurity practices were found to greatly exacerbate risk for individual firms and the entire chain. We were pleasantly surprised to discover that strong security posture and 3rd party controls could offset the additional risk incurred through higher levels of collaboration among members.

Given the findings of this research summarized above, we infer several high-level managerial implications for consideration:

1. *Security and collaboration are a balance rather than a trade-off.* Our findings show that strong security practices can go a long way toward mitigating cyber risk incurred through collaboration. Yet our findings made it clear that effectiveness is severely restricted when security levels vary widely across the chain. Thus, there must be a coordinated balance of security and collaboration.
2. *3rd party risk should not be handled separately or differently from cyber risk management.* As we have shown, direct breaches and partner-related breaches are intrinsically connected. Too many firms separate these in their security programs—some to the point where entirely different teams manage them. Not only does this waste precious resources, but considering these findings one cannot help but assume that such an approach is much less effective at reducing overall risk.
3. *Firms participating in highly co-dependent supply chains should assess – and perhaps treat – information risk corporately rather than individually.* While it is understandable that security decisions and policies are usually handled by individual firms, this research clearly shows the actions of one can affect the whole. It may be that, just as cyber security governance has adapted to vanishing network perimeters to protect data wherever it exists, it must also adapt to vanishing organizational boundaries.

4. *Firms should consider how to optimize supply chain collaboration factors based on risks and benefits for each partner.* Since all firms exhibit a unique risk profile, it follows that all firms possess an optimal security posture that best minimizes risk. Furthermore, it also makes sense that partner-facing security controls cannot be a "one size fits all" approach if they are to be maximally efficient. Tailoring 3rd party controls based on collaboration factors with each partner should be a goal.
5. *It is more effective overall for partners improve their own security posture than for a firm to improve its own partner-facing security controls.* This seems counterintuitive, but our findings strongly suggest that it is true. If some firms in the supply chain have poor security postures, this will likely negate the benefit of great 3rd party security efforts.
6. *Security leaders should consider incentivizing, mandating, and/or paying for Security laggards.* If the prior point is true, then it may be necessary to collectively "raise the bar" across the supply chain when it comes to security posture. Such a concept is not without precedent in the world of supply chain management; firms like Walmart took a very active role in maturing the IT systems of its partners because the benefits of doing so outweighed the costs. This same principle may well apply to securing those IT systems.
7. *Threat intelligence operations should be centralized – or at least aggregated – for the supply chain.* A wealth of evidence from real-world data breaches shows that threat actors routinely target weakest links in the supply chain. Knowledge of those adversaries and methods for thwarting them is disproportionately held across partners. Therefore, all firms within the supply chain are better served pooling their knowledge to better protect themselves and each other from today's adaptive and determined threats.

7.0 Conclusions and Future Work

The research provides foundational thinking and exploratory analysis around cyber risk and collaboration in modern supply chains. While the conclusions and implications outlined above represent important contributions to the field, ample opportunities for extending and improving this research exist. These include:

- *Expand scenarios beyond five firms.* Do the effects identified in this paper diminish or amplify in larger, more complex supply chains? How so? In a world where supply chains involve hundreds (or more) of collaboration firms, these questions will be critical for efforts to study.
- *Explore a broader range of conditions.* We restricted our analysis to a handful of security and collaboration variables commonly observed in the literature, which is appropriate for this initial investigation. Future research should consider additional factors and a greater range of levels for each factor (i.e., beyond "high, medium, low"). This admittedly represents a formidable challenge since there are essentially a limitless number of variables that could be incorporated, but identifying those that are essential to improved models for support greater understanding is one of many next steps.
- *Perform a case study using data and settings specific to a real supply chain.* This model was developed and run using an amalgamation of real-world data to generate results. Such an approach is suitable for gaining broad-level insights, but is perhaps less reflective of particular supply chains comprised of particular firms. Thus, a case study in which the data used for this research are gathered from actual firms/chains would be immensely beneficial.

References

1. Baker, W. H., & Wallace, L. (2007). Is information security under control? IEEE Security & Privacy, 5(1), 36–44. https://doi.org/10.1109/MSP.2007.11
2. Bandyopadhyay, T., Jacob, V., & Raghunathan, S. (2010). Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. Information Technology and Management, 11(1), 7–23. https://doi.org/10.1007/s10799-010-0066-1
3. Christopher, M., & Peck, H. (2004). Building the Resilient Supply Chain. The International Journal of Logistics Management, 15(2), 1–14. https://doi.org/10.1108/09574090410700275
4. Claburn, T. (2008). Most Security Breaches Go Unreported. Retrieved from http://www.darkreading.com/attacks-and-breaches/most-security-breaches-go-unreported/d/d-id/1070576?
5. Dean, B. (2015). Why companies have little incentive to invest in cybersecurity. Retrieved April 11, 2016, from https://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570
6. Deane, J. K., Ragsdale, C. T., Rakes, T. R., & Rees, L. P. (2009). Managing supply chain risk and disruption from IT security incidents. Operations Management Research, 2(1–4), 4–12. https://doi.org/10.1007/s12063-009-0018-2
7. Edwards, B., Hofmeyr, S., & Forrest, S. (2015). Hype and Heavy Tails : A Closer Look at Data Breaches. In Workshop on the Economics of Information Security.
8. Gould, J. E., Macharis, C., & Haasis, H.-D. (2010). Emergence of security in supply chain management literature. Journal of Transportation Security, 3(4), 287–302. https://doi.org/10.1007/s12198-010-0054-z
9. Gunasekaran, a, & Ngai, E. W. . (2004). Information systems in supply chain integration and management. European Journal of Operational Research, 159(2), 269–295. https://doi.org/10.1016/j.ejor.2003.08.016
10. Hohenstein, N.-O., Feisel, E., Hartmann, E., & Giunipero, L. C. (2015). Research on the phenomenon of supply chain resilience: A systematic review and paths for further investigation. International Journal of Physical Distribution & Logistics Management, 45(1/2), 90–117. https://doi.org/10.1108/IJPDLM-05-2013-0128
11. Hong, I. B. (2002). A new framework for interorganizational systems based on the linkage of participants' roles. Information & Management, 39(4), 261–270. https://doi.org/10.1016/S0378-7206(01)00095-7
12. Juttner, U., Peck, H., & Christopher, M. (2003). Supply Chain Risk Management: Outlining an Agenda for Future Research. International Journal of Logistics: Research and Applications, 6(4), 197–210.
13. Kembro, J., Selviaridis, K., & Näslund, D. (2014). Theoretical perspectives on information sharing in supply chains: a systematic literature review and conceptual framework. Supply Chain Management: An International Journal, 19(5/6), 609–625. https://doi.org/10.1108/SCM-12-2013-0460
14. Kolluru, R., & Meredith, P. H. (2001). Security and trust management in supply chains. Information Management & Computer Security, 9(5), 233–236. https://doi.org/10.1108/09685220110408031
15. Kumar, K., & van Dissel, H. G. (1996). Sustainable Collaboration: Managing

Conflict and Cooperation in Interorganizational Systems. MIS Quarterly, 20(3), 279–300.
16. Kungwalsong, K. (2005). Managing Disruption Risks in Global Supply Chains. Production & Operations Management, 14(1), 53–68. https://doi.org/10.1017/CBO9781107415324.004
17. Lee, H. L. (2002). Aligning Supply Chain Strategies with Product Uncertainties. California Management Review, 44(3), 105–119.
18. Lee, H. L., Padmanabhan, V., & Whang, S. (1997). Information Distortion in a Supply Chain: The Bullwhip Effect. Management Science, 43(4), 546–558. https://doi.org/10.1287/mnsc.43.4.546
19. Lee, H. L., So, K. C., & Tang, C. S. (2000). The Value of Information Sharing in a Two-Level Supply Chain. Management Science, 46(5), 626–643.
20. Lee, H. L., & Whang, S. (1998). Information Sharing in a Supply Chain (No. 1549).
21. Lee, H. L., & Whang, S. (2000). Information sharing in a supply chain. International Journal of Technology Management, 20(3,4), 373.
22. Li, L. (2002). Information Sharing in a Supply Chain with Horizontal Competition. Management Science, 48(9), 1196–1212. https://doi.org/10.1287/mnsc.48.9.1196.177
23. Liu, E. R., & Kumar, A. (2003). Leveraging Information Sharing To Increase Supply Chain Configurability. In Twenty-Fourth International Conference on Information Systems (pp. 523–537).
24. NetDiligence. (2015). 2015 Cyber Claims Study. Retrieved from https://netdiligence.com/wp-content/uploads/2016/05/NetDiligence_2015_Cyber_Claims_Study_093015.pdf
25. Nishat Faisal, M., Banwet, D. K., & Shankar, R. (2007). Information risks management in supply chains: an assessment and mitigation framework. Journal of Enterprise Information Management, 20(6), 677–699. https://doi.org/10.1108/17410390710830727
26. Ponemon Institute. (2015). 2015 Global Cyber Impact Report. Retrieved from http://www.aon.com/risk-services/thought-leadership/2015-global-cyber-impact-report.jsp
27. Ponemon Institute. (2016). 2016 Cost of Data Breach Study. Retrieved from https://www-03.ibm.com/security/data-breach/
28. PWC. (2015). 2015 Information Security Breaches Survey. Retrieved from http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html
29. Risk Based Security. (2016). 2015 Data Breach Trends.
30. Risk Solver. (n.d.). Frontline Systems. Retrieved from http://www.solver.com/risk-solver-platform
31. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 0(0), 1–15. https://doi.org/10.1093/cybsec/tyw001
32. Sahin, F., & Robinson, E. P. (2002). Flow coordination and information sharing in supply chains: Review, implications, and directions for future research. Decision Sciences, 33(4), 505–536.
33. Samaddar, S., Nargundkar, S., & Daley, M. (2006). Inter-organizational information sharing: The role of supply network configuration and partner goal congruence. European Journal of Operational Research, 174(2), 744–765.

https://doi.org/10.1016/j.ejor.2005.01.059
34. Sarathy, R., & Muralidhar, K. (2006). Secure and useful data sharing. Decision Support Systems, 42(1), 204–220. https://doi.org/10.1016/j.dss.2004.10.013
35. Sharma, S., Routroy, S., Irani, Z., & Irani, Z. (2016). Modeling information risk in supply chain using Bayesian networks. Journal of Enterprise Information Management, 29(2), 238–254. https://doi.org/10.1108/JEIM-03-2014-0031
36. Shih, S. C., & Wen, H. J. (2005). E-enterprise security management life cycle. Information Management & Computer Security, 13(2), 121–134. https://doi.org/10.1108/09685220510589307
37. Smith, G. E., Watson, K. J., & Baker, W. H. (2008). PERCEPTION AND REALITY : AN INTROSPECTIVE STUDY ON SUPPLY CHAIN INFORMATION SECURITY RISK. Issues in Information Systems, IX(2), 272–278.
38. Smith, G. E., Watson, K. J., Baker, W. H., & Pokorski II, J. a. (2007). A critical balance: collaboration and security in the IT-enabled supply chain. International Journal of Production Research, 45(11), 2595–2613. https://doi.org/10.1080/00207540601020544
39. Spekman, R. E., & Davis, E. W. (2004). Risky business: expanding the discussion on risk and the extended enterprise. International Journal of Physical Distribution & Logistics Management, 34(5), 414–433. https://doi.org/10.1108/09600030410545454
40. Straub, D. W., & Welke, R. J. (1998). Coping with systems Risk: Security Planning Models for Management Decision Making. MIS Quaterly, December(4), 441–469. https://doi.org/10.2307/249551
41. Tan, K. H., Wong, W. P., & Chung, L. (2016). Information and Knowledge Leakage in Supply Chain. Information Systems Frontiers, 18(3), 621–638. https://doi.org/10.1007/s10796-015-9553-6
42. Verizon. (2015). 2015 Data Breach Investigations Report. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf
43. Widmer, L. (2015). The 10 most expensive data breaches. Retrieved April 11, 2016, from http://www.lifehealthpro.com/2015/06/18/the-10-most-expensive-data-breaches
44. Williams, Z., Lueg, J. E., & LeMay, S. a. (2008). Supply chain security: an overview and research agenda. The International Journal of Logistics Management, 19(2), 254–281. https://doi.org/10.1108/09574090810895988

Chapter 7: Conclusions and Future Work

When I began my doctoral studies in the fall of 2003, the state and practice of cybersecurity was very different than it is now. Back then, the predominant concerns were embarrassing website defacements and mass-spreading worms that would zip around the Internet in milliseconds infecting tens of thousands of hosts. These were legitimate risks to be sure, but few, I think, envisioned the cybersecurity world in its modern-day form where large-scale cybercrime and espionage campaigns have become commonplace. Between the time I wrote the introduction of this dissertation to these lines that I now compose, the discussion of cybersecurity migrated from the backroom of IT teams into family living rooms, company boardrooms, and even national war rooms.

In studying those events of yesteryear, however, I found hints of that future reality. Consider the following comments I received from surveys sent to hundreds of organizations after several malware outbreaks from that era:

Table 1. Survey comments relating to the impact of global malware outbreaks.

SQL Slammer, January 2003
"The worm took down two of our data exchange partners." *"A large part of the impact for us was related to the loss of access to our external trade partners/customers."* *"Although we were not infected by Slammer, many of our partners were. This severely interfered with our work."* *"We were cut off from partner sites when they went down."*
Blaster, August 2003
"We were infected when a vendor hooked up his laptop to our network." *"We were infected by a 3rd party on our network."* *"Blaster got in through a trusted partner network."* *"We were infected because partners are not keeping their machines up to date with anti-virus and OS patches. This is a real problem – our IT department doesn't have control over what they do yet we suffer the consequences of their poor practices."* *"Our suppliers could not confirm orders."* *"We had numerous Infected partners. This interfered with our productivity."*
MyDoom, January 2004
"Our customers and suppliers sent it to us." *"It originally came in from a partner who we have a direct connection with."* *"The major problems have been with our trading partners who have stopped allowing any outside emails to enter their system in an attempt to stop the worm's spread. In addition, some are restricting anything with an attachment. For our business, 99% of all our email traffic includes attachments of one type or another and so our operations have basically been shut down."* *"Several of our partners were infected causing numerous operational difficulties."*
Sasser, May 2004
17% of participants infected reported a disruption of customer computing functions (order processing, sales, marketing, etc.). 16% of participants infected reported a disruption of key corporate computing functions (payroll, inventory, manufacturing, etc.). 14% of participants infected reported a disruption of Partner network connectivity.

Although the scope of these post-event surveys did not reference business partners in any way, numerous respondents volunteered details clearly pointing to their partners as the source of infection. Furthermore, several organizations used free-form fields to describe various impacts to their supply chain operations after partners were infected. In analyzing these surveys, I also found some very counterintuitive results regarding the effectiveness of countermeasures in thwarting these infections. For example, many organizations claiming they did NOT have anti-virus (AV) software installed showed lower infection rates than those reporting extensive AV deployments across their endpoint devices. Digging deeper, I discovered these non-AV organizations

had default-deny policies on Internet-facing routers and firewalls that effectively neutralized these worms before they ever made their way to endpoints (an apparently more effective compensating control).

These studies opened my eyes to several important insights that would shape my research over the next decade:

1. Cybersecurity incidents must be studied more closely and more broadly across large numbers of victim organizations to better understand root causes and consequences.
2. Cybersecurity risk is not primarily a technical issue. Events do occur via IT infrastructure and technology can be used to mitigate the risk, but cybersecurity issues manifest themselves at the business level and must be managed there as well.
3. Cybersecurity risk cannot be effectively measured or mitigated within the boundaries of a single organization. There are too many interconnections and interdependencies between firms that interweave their risk postures and policies.
4. Cybersecurity risk reduction is not a linear function; every unit increase in control strength does not result in a consistent unit decrease in risk. Control efficacy, efficiency, and interdependency are poorly measured yet critical to successful risk management.

Appropriately, these themes are woven throughout the sections of this dissertation as well as research I've conducted outside these pages. Though I'd like to be able to say that I've "closed the book" on these topics, honesty compels me to admit that I've merely cracked the cover and skimmed the first few pages. Hence the inclusion of "Toward" in the title of this dissertation.

A great many things have changed over the ensuing years, but many things remain unchanged. The points made in the introduction of this dissertation provide a case in point; though written over a decade ago, I believe they are still as fundamentally relevant today as they were then. The industry has yet to solve many of the issues identified regarding the measurement and modeling of cybersecurity risk, nor has it provided a DSS-like solution that bridges operational security data for strategic security decisions.

The question we must ask is "why is this so?" and "how can we improve?" Regarding the "why," I have been consistent in my position that one of the primary challenges to cyber risk management is a lack of information. We—whether nations, organizations, or individuals—do not have data of sufficient quality or quantity to create solid models, make informed decisions, and take justified action to manage cyber risk.

On the "how" side, the good news is that this may currently be changing for the better. Painful and public security failures combined with increasing executive, regulatory, and commercial pressures are forcing changes in behavior and accountability, both of which necessitate better data. Data-driven research and development is currently experiencing a heyday in the cybersecurity industry, a trend that I am proud to say I have contributed to in some small way. The cyber insurance industry is growing rapidly, and I expect this will serve to mature both knowledge and practice. At the very least, I think actuarial techniques will help move us along the path from "you must do all of these 200 things" to "do these 20 first" to "these are the 2 things that really matter most." Furthermore, academic and industry circles are levying a host of interdisciplinary perspectives and approaches at various cybersecurity problems. I very much welcome this "outside" attention; we desperately need it and I think we'll be much better for it.

In closing, I would like to make two broad recommendations for future (preferably imminent) research. First, I strongly believe some entity—whether public or private—needs to be charged with, funded for, and supported in collecting and investigating cybersecurity incidents and making that information available for public use. Various groups do parts of this on an ad-hoc or commercial basis now, but compare these to corollary efforts for reporting and studying airline incidents. Imagine if all that was publicly reported on plane crashes was "X Airlines crashed; 172 killed." No explanation of pilot error vs mechanical failure vs terrorist activity. No way for the Federal Aviation Administration to know if or which regulatory or procedural changes were needed. No way for manufacturers to address faulty components. Crash reporting on this level wouldn't serve to meaningfully improve airline safety because we'd have nothing on which to base those improvements. Naturally, such ignorance would not be tolerated, and that is why organizations like the National Transportation Safety Board exist.

But such is the current state of cyber incident reporting (actually, it is much worse since only a fraction of incidents become public knowledge and only a fraction of the details about those incidents are typically released). As long as information and intelligence about incidents and adversaries is held as a competitive differentiator among cybersecurity vendors rather than openly shared for public good, efforts to fix the root problems behind these incidents will continue to be partially blind and bumbling.

My second broad recommendation concerns changing the way in which cybersecurity risk is researched. Event-driven and point-in-time assessments, surveys, and investigations focused on single organizations have served to build knowledge, but can only go so far in understanding fundamental issues like those identified above. We need more "clinical" or longitudinal studies encompassing comparable security aspects from numerous organizations if substantial progress is to be made. As an example, I would very much welcome research that studied security expenditures, control quality, policies, incidents, losses, etc. from several hundred organizations over a multi-year period. This would help answer simple questions like "what is the expected rate of incidents of type *x* in organizations of size *y* in industry *z*?" It would also enable more complex and critical inquiries like "if said organization implements control *a*, what is the expected reduction in incident rate and losses?" or "given a security budget of $*b*, which controls and which levels of implementation would achieve maximum risk reduction?"

I am hopeful such questions will soon be answered. Until then, I will keep asking and doing what I can to offer bits and pieces of the answers.

Appendix A: Example incident from Chapter 5 in A4 JSON format


```
{
 "schema_version": "1.3.0",
 "incident_id": "BGAA50DB-62DE-4F34-9075-F84A4B94C83C",
 "security_incident": "Confirmed",
 "source_id": "Demo",
 "analyst": "wbaker",
 "summary": "A competitor hired a criminal group to steal corporate secrets. They sent a
well-crafted phishing email with a malicious attachment to an executive, who clicked it,
consequently infecting her computer with a backdoor. The intruders gained access,
explored the network, and found the targeted documents on a misconfigured file server.",
 "timeline": {
  "incident": {
   "month": 8,
   "year": 2003
  }
 },
 "victim": {
  "country": [
   "US"
  ],
  "employee_count": "Over 100000",
  "industry": "325110",
  "locations_affected": 1,
  "region": [
   "019021"
  ],
  "victim_id": "ABC Corp"
 },
 "actor": {
  "external": {
   "country": [
    "DJ"
   ],
   "motive": [
    "Espionage"
   ],
   "notes": "Collaboration with law enforcement found that XYZ Corp, one of the
victim's main competitors, hired a criminal group.",
   "region": [
    "002"
   ],
   "variety": [
    "Competitor",
    "Organized crime"
```

```
    ]
   },
   "internal": {
    "motive": [
     "NA"
    ],
    "notes": "sysadmin was new to job.",
    "variety": [
     "Sysadmin"
    ]
   }
  },
  "action": {
   "hacking": {
    "variety": [
     "Use of backdoor or C2",
     "Brute force"
    ],
    "notes": "basic dictionary attack. Password was PASSWORD1.",
    "vector": [
     "Backdoor or C2"
    ]
   },
   "malware": {
    "cve": "CVE-2015-9640",
    "name": "BadCodez",
    "variety": [
     "Backdoor"
    ],
    "vector": [
     "Email attachment"
    ]
   },
   "social": {
    "target": [
     "Executive"
    ],
    "variety": [
     "Phishing"
    ],
    "notes": "Email had references to a recent conference executive attended.",
    "vector": [
     "Email"
    ]
   }
  },
```

```
 "asset": {
  "assets": [
   {
    "variety": "Laptop"
   },
   {
    "variety": "Executive"
   },
   {
    "variety": "File server"
   }
  ]
 },
 "attribute": {
  "confidentiality": {
   "data": [
    {
     "variety": "Secrets"
    },
    {
     "variety": "Internal"
    }
   ],
   "data_disclosure": "Yes",
   "data_victim": [
    "Other"
   ],
   "notes": "not exactly sure about the classified info, but assuming so.",
   "state": [
    "Stored"
   ]
  },
  "integrity": {
   "variety": [
    "Software installation",
    "Alter behavior",
    "Modify configuration"
   ]
  }
 },
 "discovery_method": "Unknown",
 "impact": {
  "overall_rating": "Unknown"
 }
}
```

References

1. (1992) Risk: Analysis, Perception and Management. London, UK, Royal Society.

2. Aberdeen Group. Internet Business Disruptions Benchmark Report, 2004.

3. Abrams, M.D. and Moffett, J.D. (1995). A Higher Level of Computer Security Through Active Policies. Computers and Security, 14, 147-157.

4. Anderson, J. P., Computer Security Technology Planning Study, ESD-TR-73-51, ESD/AFSC, Hanscom AFB, Bedford, MA (Oct. 1972).

5. Alexander, M., The Underground Guide to Computer Security, Addison-Wesley Publishing Company, 1996.

6. Alter, S., "A Study of Computer Aided Decision Making in Organizations," Ph.D. dissertation, M.I.T., 1975.

7. Alter, S.L., "A Taxonomy of Decision Support Systems", Sloan Management Review, Vol.19, No.1, Fall 1977, pp. 39-56.

8. Alter, S.L., "Why Is Man-Computer Interaction Important for Decision Support Systems?", Interfaces, Vol.7, No.2, Feb. 1977, pp.109-115.

9. Alter, S.L., Decision Support Systems: Current Practice and Continuing Challenge. Reading, MA: Addison-Wesley, 1980.

10. Ashayeri, J. & Kampstra, R. P. (2005) Realities of Supply Chain Collaboration. EurOMA International Conference Proceedings. Budapest, Hungary, European Operations Management Association.

11. Belchner, T., et al. Riptech Internet Security Threat Report, Riptech, 2002.

12. Bhargava, H., and D. J. Power. Decision Support Systems and Web Technologies: A Status Report. Proceedings of the 2001 Americas Conference on Information Systems, Boston, MA, August 3 - 5, 2001.

13. Bishop, M. What is computer security. IEEE Security & Privacy, 1 (1). 67-69.

14. Bonczek, R. H., C. W. Holsapple, and A. Whinston. Foundations of Decision Support Systems. Academic Press, 1981.

15. Bosworth, S., & Kabay, M. E. (2002). Computer Security Handbook. John Wiley and Sons, Inc., 4th ed.

16. Christopher, M. & Peck, H. (2004) Building the Resilient Supply Chain. International Journal of Logistics Management, 15, 1.

17. Corbató, F. J., M. M. Daggett, and R. C. Daley, "An Experimental Time-Sharing System," SJCC paper, May 3, 1962 at URL larch-www.lcs.mit.edu:8001/~corbato/sjcc62/.

18. Corbett, C. J. & Blackburn, J. D. (1999) Partnerships to Improve Supply Chains. (Cover story). Sloan Management Review, 40, 71.

19. Davis, G., Management Information Systems: Conceptual Foundations, Structure, and Development, New York: McGraw-Hill, 1974.

20. DBMS interview, "The Doctor of DSS," DBMS magazine, July 1994.

21. Department of Defense Computer Security Evaluation Center; Trusted Computer System Evaluation Criteria (Orange Book); (1983, 1985).

22. Dhar, V. & Stein, R., Intelligent Decision Support Methods: The Science of Knowledge. Upper Saddle River, NJ: Prentice-Hall, 1997.

23. Dhillon, G. and Backhouse, J. Information Systems Security Management in the New Millennium. Communications of the ACM, 43 (7). 125-128.

24. Dickson, G. W., M. S. Poole, and G. DeSanctis. "An Overview of the GDSS Research Project and the SAMM System", in Bosttrom, R. P., R. T. Watson, and S. T. Kinney, Computer Augmented Teamwork: A Guided Tour, New York: Van Nostrand Reinhold, 1992, pps. 163-179.

25. W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory IT-22(6) 644-654 (Nov. 1976).

26. Feigenbaum, A.V. Total Quality Control. Harvard Business Review, 34 (6). 93.

27. Ferguson, R. L. and C. H. Jones, "A Computer Aided Decsion System", Management Science, June 1969, pp. B550-B561.

28. Finne, T., (1998). A Conceptual Framework for Information Security Management. Computers and Security, 17, 303-307.

29. FROHLICH, M. T. & WESTBROOK, R. (2001) Arcs of integration: an international study of supply chain strategies. Journal of Operations Management, 19, 185.

30. Gasser, M. Building a Secure Computer System. Van Nostrand Reinhold Company Inc., New York, 1988.

31. Gerrity, T. P., Jr. "The Design of Man-Machine Decision Systems", Sloan Management Review, vol. 12, no. 2, pp. 59-75, Winter 1971.

32. Gordon, L., Loeb, M., Lucyshyn, W. and Richardson, R. Ninth Annual CSI/FBI Computer Crime and Survey Report, Computer Security Institute, 2004.

33. Gordon, L.A. and Loeb, M.P. The Economics of Information Security Investment. ACM Transactions on Information and System Security, 5 (4). 438-457.

34. Grace, B. F. "Training Users of a Decision Support System", IBM Research Report RJ1790, IBM Thomas J. Watson Research Laboratory, May 31, 1976.

35. Gray, P., "The SMU decision room project", Transactions of the Ist International Conference on Decision Support Systems (Atlanta, Ga.), 1981, pp. 122-129.

36. Gray, P., Guide to IFPS (Interactive Financial Planning System), New York: McGraw-Hill Book Company, 1987.

37. Gunasekaran, A. & Ngai, E. W. T. (2004) Information systems in supply chain integration and management. European Journal of Operational Research, 159, 269.

38. Houdeshel, G. and H. Watson, "The Management Information and Decision Support (MIDS) System at Lockheed-Georgia", MIS Quarterly, Vol. 11, No. 1, March 1987.

39. Huber, G. P., "Group decision support systems as aids in the use of structured group management techniques", Transactions of the 2nd International Conference on Decision Support Systems, 1982, pp. 96-103.

40. Inmon, W. H., "EIS and the Data Warehouse", Data Base Programming/Design, November 1992.

41. Inmon, W. H., Using Oracle to Build Decision Support Systems. QED Press, 1990.

42. ISO/IEC 17799 (2000), Information Technology Code of Practice for Information Services, International Organization for Standardization, Geneva.

43. ISO/IEC 17799 (2005), Information Technology Code of Practice for Information Services, International Organization for Standardization, 2nd ed., Geneva.

44. Iverson, K. E., A Programming Language, 1962.

45. Jelen, G., Information Security: An Elusive Goal (1985).

46. Kahn, D. (1996). The Codebreakers: The Story of Secret Writing. Scribner, 1230 Avenue of the Americas, New York, New York 10020, second (first copyright 1967) edition, 1996.

47. Kang, T. S. (1973) Ordinal Measures of Association and Forms of Hypotheses. The Sociological Quarterly, 14, 235-248.

48. Keen, P. G. W. and M. S. Scott Morton, Decision Support Systems: An Organizational Perspective. Reading, MA: Addison-Wesley, Inc., 1978.

49. Kimball, R., W. Thornthwaite, L. Reeves, and M. Ross, The Data Warehouse Lifecycle Toolkit, New York, NY: John Wiley and Sons, 1998.

50. Klein, M. and L. B. Methlie, Knowledge-based Decision Support Systems with Applications in Business. Chichester, UK: John Wiley & Sons, 1995.

51. Kolluru, R. & Meredith, P. H. (2001) Security and Trust Management in supply Chains. Information Management & Computer Security, 9, 233-236.

52. Kotulic, A. G. (2001). The Security of the IT Resource and Management Support: Security Risk Management Program Effectiveness. PhD thesis, University of Texas at Arlington, April, 2001.

53. Kotulic, A. G. & Clack, J. G. (2004) Why Aren't There More Information Security Research Studies. Information & Management, 41, 597-607.

54. Krol, E., (1992). The Whole Internet, O'Reilly and Associates, Inc.

55. Lee, H. L. & Whang, S. (2000) Information sharing in a supply chain. International Journal of Technology Management, 20, 373.

56. Lee, H. L., Padmanabhan, V. & WHANG, S. (1997) Information Distortion in a Supply Chain: The Bullwhip Effect. Management Science, 43, 546.

57. LeRoux, Y., Information security – the CIA model. Director, August 1993, pg. 53

58. Levy, S., (1996). Wisecrackers. Wired, pages 128–134, 196–198, 200, 202, March 1996.

59. LI, L. (2002) Information Sharing in a Supply Chain with Horizontal Competition. Management Science, 48, 1196.

60. Little, J. D. C., "Models and Managers: The Concept of a Decision Calculus". Management Science, vol. 16, no. 8, pp. B466-485, April 1970.

61. Little, J. D. C., Brandaid, an On-Line Marketing Mix Model, Part 2: Implementation, Calibration and Case Study. Operations Research, vol. 23, no. 4, pp. 656-673, 1975.

62. Loch, K. D. & Carr, H. H. (1992) Threats to information systems: Today's reality, yesterday's understanding. MIS Quarterly, 16, 173.

63. Lough, Daniel L. A Taxonomy of Computer Attacks with Applications to Wireless Networks. PhD thesis, Virginia Tech, April 2001.

64. Lynch, D. and Rose, M., Eds., Internet System Handbook, Addison-Wesley, 1993.

65. McCarthy, John. Reminiscences On The History Of Time Sharing. Stanford University, 1983.

66. McCosh, A. M and Scott Morton, M. S., Management Decision Support Systems, London, Macmillan, 1978.

67. Mclaren, T., Head, M. & Yuan, Y. (2002) Supply Chain Collaboration Alternatives. Internet Research: Electronic Network Applications and Policy, 12, 348-364.

68. Meglio, F. D. A Hacker Break-In Scrambles Kellogg. Businessweek, April 12, 2005.

69. Mentzer, J. T. (2002) Managing Supply Chain Collaboration. Supply Chain Management Review, 83.

70. Mercuri, R.T. Computer Security: Quality Rather than Quantity. Communications of the ACM, 45 (10). 12-14.

71. Merten, A. G., & Severance, D. G. Data processing control: A state-of-the-art survey of attitudes and concerns of DP executives. MIS Quarterly, 5(2), 11-32.

72. Metters, R. (1997) Quantifying the bullwhip effect in supply chains. Journal of Operations Management, 15, 89.

73. Mockapetris, P., "Domain names - concepts and facilities," RFC 1034, November 1987.

74. Narus, J. A. & Anderson, J. C. (1996) Rethinking Distribution: Adaptive Channels. Harvard Business Review, 74, 112.

75. Peter G. Neumann, L. Robinson, Karl N. Levitt, R. S. Boyer, and A. R. Saxena, A Provably Secure Operating System, M79-225, Stanford Research Institute, Menlo Park, CA 94025 (June 1975).

76. Nunamaker, J. F., Jr., A. R. Dennis, J. F. George, W. B. Martz, Jr., J. S. Valacich, and D. R. Vogel, "GroupSystems" in Bosttrom, R. P., R. T. Watson, and S. T. Kinney, Computer Augmented Teamwork: A Guided Tour, New York: Van Nostrand Reinhold, 1992, pps. 143-162.

77. Nylund, A., "Tracing the BI Family Tree", Knowledge Management, July 1999.

78. Parker, D.. (1979). Crime by Computer. Chris Schribners Sons, New York.

79. Pendse, N., "Origins of today's OLAP products," The OLAP Report, URL www.olapreport.com, 1997. (read local copy dated 07/22/2002).

80. Harold E. Peterson and Rein Turn. "System Implications of Information Privacy," Proceedings of the 1967 Spring Joint Computer Conference, pp 305 seq, vol. 30, 1967.

81. Powell, R., "DM Review: A 10 Year Journey", DM Review, February 2001, URL www.dmreview.com.

82. Power, D. J. Web-Based and Model-Driven Decision Support Systems: Concepts and Issues. Proceedings of the 2000 Americas Conference on Information Systems, Long Beach, California, August 10th - 13th, 2000.

83. Power, D. J., "A Brief History of Spreadsheets", DSSResources.COM, World Wide Web, http://dssresources.com/history/sshistory.html, version 3.3, 03/11/2000.

84. Power, D.J. and G. L. Rose. Improving Decision-Making Behavior Using the Hewlett Packard 2000/Access System. Proceedings of the American Institute for Decision Sciences, Nov. 1976, 47-49.

85. Raymond, E. S., editor, (1996). The New Hacker’s Dictionary. The MIT Press, Cambridge, Massachusetts, London England, third edition.

86. Rockart, J. F. "Chief Executives Define Their Own Data Needs," Harvard Business Review, vol. 67, no. 2 (March-April 1979), pp 81-93.

87. Sahay, B. S. (2003) Supply Chain Collaboration: The Key to Value Creation. Work Study, 52, 76-83.

88. Salus, P., (1995). Casting the Net: from ARPANET to INTERNET and beyond. Addison-Wesley Publishers.

89. Saydjari, O.S. Multilevel Security: Reprise. IEEE Security & Privacy, 2 (5). 64-67, 2004.

90. Schaker, B. CMU says hacker broke into computers. Pittsburgh Post-Gazette, April 21, 2005.

91. Schell, R. R., Downey, P. J., and Popek, G. J., Preliminary Notes on the Design of Secure Military Computer Systems, MCI-73-1, ESD/AFSC, Hanscom AFB, Bedford, MA (Jan. 1973).

92. Schiller, W. L., The Design and Specification of a Security Kernel for the PDP-11/45 (1975).

93. Scott Morton, M. S. and A. M. McCosh, "Terminal Costing for Better Decisions," Harvard Business Review, Vol. 46, Number 3, May-June 1968.

94. Scott Morton, M. S. and J. A. Stephens, "The impact of interactive visual display systems on the management planning process," IFIP Congress (2) 1968: 1178-1184.

95. Scott Morton, M. S. Management Decision Systems; Computer-based support for decision making. Boston, Division of Research, Graduate School of Business Administration, Harvard University, 1971.

96. Scott Morton, M. S., "Computer-Driven Visual Display Devices -- Their Impact on the Management Decision-Making Process," Doctoral Dissertaion, Harvard Business School, 1967.

97. Sharda, R., S. Barr, and J. McDonnell, "Decision Support Systems Effectiveness: A Review and an Empirical Test, Management Science, vol. 34, no. 2, 1988, pp. 139-159.

98. Simatupang, T. M. & Sridharan, R. (2005) The collaboration index: a measure for supply chain collaboration. International Journal of Physical Distribution & Logistics Management, 35, 44.

99. Smith, G. E., Watson, K. J., Baker, W. H. & Pokorski, J. (2007) A Critical Balance: Collaboration and Security in the IT-Enabled Supply Chain. International Journal of Production Research, Forthcoming.

100. Smith, M., (1993). Commonsense Computer Security: Your practical guide to information security. McGraw-Hill Book Company, London.

101. Solarz, A., (1987). Computer-related embezzlement. Computer Security, 6,1, 49-53.

102. Soo Hoo, Kevin J. How Much Is Enough? A Risk-Management Approach to Computer Security. PhD thesis, Stanford University, June 2000.

103. Sprague, R, H., Jr., "A Framework for the Development of Decision Support Systems," Management Information Systems Quarterly, vol. 4, no. 4, Dec. 1980, pp. 1-26.

104. Sprague, R. H., Jr. and E. D. Carlson. Building Effective Decision Support Systems. Englewood Cliffs, N.J.: Prentice-Hall, Inc.: 1982.

105. Sprague, R. H., Jr. and H. J. Watson, "Bit by Bit: Toward Decision Support Systems", California Management Review, vol. XXII, no. 1, Fall 1979, pp. 60-68.

106. Stallings, William, “Internet Security Handbook, IDG Books Worldwide, Inc., 1995.

107. Stoneburner, G., Goguen, A. and Feringa, A. Risk Management Guide for Information Technology Systems. Commerce, U.S.D.o. ed., National Institute of Standards and Technology, 2002.

108. Straub, D.W. and Welke, R.J. (1998) Coping with Systems Risk: Security Planning Models for Management Decision-Making. MIS Quarterly, 22 (4). 441-470.

109. Swanson, E. B., and M. J. Culnan, "Document-Based Systems for Management Planning and Control: A Classification, Survey, and Assessment", MIS Quarterly, vol. 2, no. 4, December 1978, pp. 31-46.

110. Thieme, R., (1997). Zen and the Art of Hacking. Internet Underground, 2(4):26–33, April 1997.

111. Turoff, M., and S. R. Hiltz, "Computer support for group versus individual decisions", IEEE Trans. Communications, COM-30, vol. 1, 1982, pp. 82-90.

112. Jerold Whitmore, Andre Bensoussan, Paul Green, Douglas Hunt, Andrew Kobziar, and Jerry Stern, Design for MULTICS Security Enhancements, ESD-TR-74-176, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA 01731 (Dec. 1973).

113. U.S. Department of Commerce, (2004). Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information systems. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900.

114. Weissman, C., System Security Analysis/Certification (1973).

115. White, D. E., and Farrell, M.H. (1994). Reengineering Computer Security Administration. Computer Security Journal, 10(1), 23-37.

116. Whiteside, T., (1978). Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud. Fitzhenry and Whiteside, Toronto.

117. Whitman, M.E. Enemy at the Gate: Threats to Information Security. Communications of the ACM, 46 (8). 91-95.

118. Wilkes, M. V., Time-Sharing Computer Systems, American Elsevier, New York, 1968.

119. Willis H. Ware, Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security, The RAND Corporation, Santa Monica, CA (Feb. 1970).