A Systematic Approach for Cybersecurity Risk Management

by

Kristin YiJie Chen

B.S., National Chengchi University, 2016

Submitted to the System Design and Management Program
and the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degrees of
Master of Science in Engineering and Management
and
Master of Science in Electrical Engineering and Computer Science
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
September 2021

Author . . . .
System Design and Management Program
Department of Electrical Engineering and Computer Science
August 6, 2021

Certified by . . . .
Michael D. Siegel
Principal Research Scientist
Thesis Supervisor

Accepted by . . . .
Joan Rubin
Executive Director
System Design and Management Program

Accepted by . . . .
Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students

A Systematic Approach for Cybersecurity Risk Management

by

Kristin YiJie Chen

Submitted to the System Design and Management Program
and the Department of Electrical Engineering and Computer Science on August 6, 2021, in partial fulfillment of the
requirements for the degrees of
Master of Science in Engineering and Management
and
Master of Science in Electrical Engineering and Computer Science

Abstract

In the last few years, the concern over cybersecurity has grown dramatically. With all the existing, and sometimes competing, guidelines and frameworks intended to inform cyber risk strategies, organizations face the problem of deciding which is right for them. To resolve the confusion, this research proposes a practical and effective model that can be used by organizations of any size or in any industry for cyber risk management. We propose a Cyber Risk Cube (CRC) tool designed to be practical for all parts of an organization, which examines three fundamental pairings for looking at cyber risk: Internal/External, Measurement/Management, and Qualitative/Quantitative. The CRC tool can be used as a common language for sharing ideas and solutions to cyber risk management. Ultimately, the CRC provides details for implementing solutions to managing cyber risks in a concise and standardized manner.

Thesis Supervisor: Michael D. Siegel
Title: Principal Research Scientist

Acknowledgments

There are many people that I would like to thank for supporting me as I pursued my dual degree and worked on this research at MIT during the COVID-19 pandemic.

First and foremost, I want to express my gratitude to the MIT community, especially my thesis advisor. I want to thank my thesis advisor, Dr. Michael Siegel, for his insights, support, and encouragement throughout this journey. I benefited and learned a lot from him because of his erudition and extensive experience and his constant willingness to help students despite his busy schedule. I am blessed to have him as my advisor, providing valuable, timely, and sincere feedback as I developed my research. Also, I want to thank Dr. Howard Shrobe for being my thesis reader, and an inspiration in many ways.

I'd also like to express my gratitude to the Cybersecurity at MIT Sloan (CAMS) for providing me with a way to discuss my research and helpful feedback. Without Daniel Goldsmith's valuable input and feedback, this project would not have been possible.

Also, I want to thank the SDM program and the EECS program, especially Joan Rubin, and the 2020 and 2021 SDM & EECS cohorts. I have formed many connections and learned a lot from professors and peers that I would not discover in other places. I'm grateful for this once-in-a-lifetime learning experience provided by the SDM and EECS community.

Lastly, and most importantly, I want to express my gratitude to my family and friends, especially Celestine and David. Without their support, I would not be where I am now. Without their unwavering help and inspiration, this work would not have been possible.

Contents

List of Figures

Chapter 1

Introduction

This chapter provides an introduction to the topic of cybersecurity risk management. It describes the motivation behind this thesis and explains why this topic is of such great interest. Primary research questions are shown below and will guide the remainder of the thesis.

1.1 Background

In recent years, there has been a dramatic increase in data breaches and other cyberattacks. Moreover, the global spread of the COVID-19 epidemic has increased the number of internet users [1]. Increased internet activity and bandwidth have resulted in a greater risk to digital data security [2]. A study shows that 90% of companies faced increased cyberattacks during COVID-19 [3]. In 2020 alone, there are 3,950 confirmed data breaches such as SolarWinds, Twitter, MGM Resorts, Microsoft Breach, etc [4, 5, 6, 7, 8]. Because these events result in customer information loss, trade secrets, and other confidential assets, this increase has seriously threatened corporate credibility, competitive advantage, and financial stability. In response, organizations have made cybersecurity risk management as their top priorities nowadays. During a typical meeting with the Board of Directors and C-level executives, here are several common cybersecurity risk management questions:

- Where should we start?

- What are the major components for cybersecurity risk management and are we prepared for it?
- What approaches are our peers adopting?
- Comparing to peers, how do we rank when it comes to cyber risk preparedness?
- What cyber risk management framework, tools and techniques are we using? Is it the right one for our organization?

When asked these questions, executives often lack concrete, and actionable answers. Organizations understand that as threats become more diverse and sophisticated, they have to respond to cybersecurity's dynamic nature. However, they are often unsure of exactly where to start or what to do when it comes to cyber risk. Security solutions are growing at about the same rate as cyber threats. There are hundreds, if not thousands, of cyber risk publications, white papers, standards, frameworks, guidelines, tools, and academic articles. With the vast selection of frameworks, regulations, tools, and resources, it is challenging for organizations to know, choose, and implement the right ones. CSO Magazine stated that there were over 30,000 attendees interfaced with over 400 security vendors, each of which was promoting their security widget as a critical lynchpin in any security architecture on a 2019 RSA conference [9].

The process may involve a wide range of consultants and approaches for larger firms, while hard choices must be made to direct security spending for small and medium enterprises. There is a need for a high-level strategy that allows organizations to build a holistic road map and compare themselves to their peers. Hence, our first research objective is to help organizations create a basic and appropriate cyber risk management strategy. During our research, we noticed that a lot of organizations, even many reputable ones, fell into several common traps that subvert well-intended organizational security efforts although they had spent a lot of time and effort establishing security framework, and resources. Some manifestations of these traps include: the wrong choice of cyber risk frameworks, poor requirements definition, unnecessary work and rework, and the waste of scarce resources, all of which can create significant security gaps that eventually lead to a cyber-attack. Therefore, our second research objective is to help organizations identify these common pitfalls after they build their basic cyber risk management strategy.

1.2 Objectives and Research Questions

First of all, to provide companies with a guide to build a basic cybersecurity risk management strategy, this work aims to build an information-sharing tool for cybersecurity risk management. Second, to help organizations avoid the common pitfalls after establishing their basic cybersecurity risk management strategy, this thesis aims to apply the System Dynamics methodology to enable business leaders to develop a holistic understanding of different tradeoffs and dynamics in the environment. Specifically, the questions this thesis aims to address are:

- What risk management practices are others conducting? How are others doing it? How effective is the approach?
- How can this tool help to build a basic and appropriate cybersecurity risk management strategy?
- Can a simulation model explain the common pitfalls in cybersecurity risk management strategy and execution?
- Can organizations use the model to identify main success and failure modes?
- Can companies test various strategies or combination of strategies in a simulation environment prior to making mistakes in the real world?

1.3 Research Methodology and Thesis Overview

To achieve the first object, a new information-sharing tool is developed to provide companies with a guide to build their basic cybersecurity risk management strategy, the Cyber Risk Cube (CRC). This tool seeks to guide organizations to a common understanding of cyber risk management. Using case studies and literature reviews, the CRC tool consolidates data on current cybersecurity practices and their relative effectiveness. The CRC tool evaluates which approaches are most favorably reviewed and most commonly undertaken and filter these by size, industry, goal, budget, compliance, and other characteristics to create a database of these approaches. Thus, the CRC tool can effectively make personalized recommendations to organizations. Another system dynamics model is built to achieve the second objective - to help organizations avoid the common pitfalls. This model aims to identify common traps that actually subvert well intended organizational security efforts and enable business leaders to develop a holistic understanding of different tradeoffs and dynamics in the environment.

This thesis consists of six following sections:

- **Chapter Two - Literature Review** Chapter Two is the literature review section. This chapter contains an overview of past and present cyber crime, cybersecurity risk management studies, and a review of the prior cybersecurity works using system dynamics approach.

- **Chapter Three - Cyber Risk Cube** Chapter Three introduces an information-sharing tool called the Cyber Risk Cube (CRC). It also explores the six major components in cybersecurity risk management, and the overall research methodology used in the CRC tool.

- **Chapter Four - A System Dynamics Model for Cybersecurity Risk Management Strategy** Chapter Four focuses on the exploration of cybersecurity risk management strategy to identify common pitfalls. This chapter includes the development of the cybersecurity risk management strategy causal loop diagrams.

- **Chapter Five - Conclusions** Chapter Five includes a summary of the Cyber Risk Cube, concludes the key findings from the system dynamics model for cybersecurity risk management, a discussion on the accomplished research aims, and possible areas of further research.

Chapter 2

Literature Review

This chapter introduces a variety of approaches currently used in cybersecurity risk management as well as found in academic literature for managing cybersecurity risk. It also explores the history of cybercrime to provide a better understanding of the damages caused by cybersecurity attacks.

2.1 Cybersecurity

One of the most essential and fast-moving fields in technology is cybersecurity. According to research conducted by Cybersecurity Ventures, cybersecurity experts have forecasted that cybercrime will cost the global economy $6.1 trillion per year by 2021. Cybercrime is likely to become the world's third-largest economy shortly due to the pandemic as a driver. Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015 [10]. Hence, it is no surprise that banks, tech businesses, healthcare, government organizations, and nearly every other industry are investing in cybersecurity infrastructure to secure their corporate practices and the millions of customers who trust them with their personal information.

In this section, the historical cases of cybersecurity incidents are discussed [11]. The creation and evolution of important cybersecurity frameworks and standards are explored to provide a better understanding of existing cybersecurity approaches.

2.1.1 History of Cybercrime

The history of cybercrime goes back to 1971 when the first computer worm was created by Bob Thomas, displaying the words, “I am the Creeper: catch me if you can.” [12] Due to the creation of the computer worm, the first cybercrime occurred even before the Internet exists. In 1981, Ian Murphy was the first person convicted of a cybercrime. He hacked into the AT&T network and changed the internal clock to charge off-hours rates at peak times. [13] Cyber threats started to develop rapidly in the 80s, attempting to steal intellectual property, customer lists, new product development. The increased nation-state cyber attacks lead to the Computer Fraud and Abuse Act expanded the Comprehensive Crime and Control Act passed in 1984 to cover hacking [14]. Breaking into computer systems became illegal under this law. In 1988, the “Morris worm” that impacted approximately 6,000 computers after 24 hours of being released was the first of many Denial of Service (DOS) attacks of the era [15]. Morris became the first person to be successfully charged under the Computer Fraud and Abuse Act. The Morris worm also led to the formation of the Computer Emergency Response Team (CERT) at the direction of the Defense Advanced Research Projects Agency (DARPA) [16].

Later on, the first ransomware attack called the AIDS Trojan occurred in 1989. A Trojan Horse Program was mailed to a UK electronic journal to 20,000 AIDS researchers and subscribers [17]. Terrified users deleted their hard drives, resulting in the loss of years of work for certain research and medical organizations. Furthermore, the AIDS Trojan emphasized the idea of utilizing malware as a form of leverage. Traditionally, viruses like Creeper would annoy people by clogging up their hard drives or deleting their files. The AIDS Trojan, on the other hand, went a step further by forcing users to pay a sum of money, taking advantage of the world’s growing reliance on computers to store and modify data, as well as the victims’ ignorance [18]. Ransomware attacks has risen exponentially since the AIDS Trojan Attack. It also led to the result of United Kingdom passing the Computer Misuse Act, which criminalised unauthorised attempts to access IT systems in 1990 [19].

In the 1990s, viruses such as “Melissa” and “ILOVEYOU” were widespread. The Melissa Virus infected Microsoft Word records, transmitting itself via email as an attachment automatically [20]. It mailed out to the first 50 names mentioned in the Outlook email address box of an infected device. The ILOVEYOU virus affected more than 500,000 systems and led to $15 billion worth of damage [21]. These threats stimulated the improvement of antivirus software that can detect a virus signature and prevent it from execution. It also raised user awareness of the risks of opening e-mail attachments from unknown or untrustworthy senders.

When social media first became popular in the early 2000s, cybercrime exploded. The inflow of people placing all the information they could into a profile database resulted in a flood of personal data and an increase in ID theft. Hackers exploited the information to gain access to bank accounts, create credit cards, and commit other types of financial crimes. Cybersecurity attacks became more complex and targeted in the 2000s. In 2001, the Council of Europe drafted a Cybercrime Treaty to define cyber crimes committed by using the internet as a response to the challenge of cyber crime in the age of the internet [22]. In 2002, a distributed denial-of-service (DDoS) attack targeted the entire Internet for an hour by attacking the 13 root servers of the Domain Name System (DNS) [23].This first DDOS attack did not sustain much damage and there was little to no impact on Internet users. To defend against cyber attacks, the Department of Homeland Security was created a month later and assigned in part with IT infrastructure [24]. Later on, they created a cybersecurity division. However, this does not stop the increasing numbers of cybercrime. Not only did cyber attack strategies and motivations develop, but new kinds of perpetrators emerged: state-sponsored hackers supporting foreign governments’ political goals and criminal gangs with enormous technical and financial resources. Between 2005 and 2007, TJ Maxx had their first massive data breach, when credit card information for more than 94 million consumers was compromised [25]. The TJ Maxx Breach acted as a wake-up call for the management level to be aware of the security risks involved in operations but also make a committed and focused effort to ensure the information they possess is protected and secure. Cyber-attacks acquired a new degree of severity at this moment, affecting regulated data and requiring firms to inform authorities as well as set up funds to compensate victims.

To help selection an appropriate defense mechanism, the US Department of Homeland Security released a taxonomy of attack patterns in 2008. However, in 2009, Heartland Payment Systems announced that it had suffered a devastating breach: 134 million credit cards were exposed through SQL Injection attacks used to install spyware on Heartland's data systems [26].

By the 2010s, cyber-attacks became significantly more sophisticated. In 2010, the first software bomb called the Stuxnet Worm was released [27]. It was a destructive computer virus that could attack control systems used for controlling manufacturing facilities. Stuxnet targeted supervisory control and data acquisition (SCADA) systems and was believed to be responsible for causing substantial damage to the nuclear program of Iran [28]. Epsilon, an e-mail marketing firm, stated in April 2011 that one of its databases had been compromised, exposing customer names and e-mail addresses for organizations that use Epsilon to handle their marketing communications. After Epsilon announced the data breach, e-mails from companies like Citibank, Chase, Capital One, Walgreens, Target, Best Buy, TiVo, TD Ameritrade, Verizon, and Ritz Carlton were sent out. The hack affected about 2% of Epsilon's estimated 2,500 clients, resulting in millions of documents being exposed [29]. Afterwards, the US retailer Target suffered a massive data breach, exposing the personal data of 40 million credit and debit card customers in 2012 [30]. The Target breach was significantly more complicated in terms of technological sophistication than the TJ Maxx incident, which included a direct intrusion of the local wireless network. The criminals realized that they needed to take an indirect approach to access the data they wanted, which entailed a third-party heating and ventilation vendor to Target and a series of complex methodical processes [31, 32]. An investigative journalist found the breach after noticing credit card data for sale on the dark web, all of which had one thing in common: they had been used at Target. Target's data breach was so high-profile that its CEO resigned as a result. Following high-profile attacks, such as those at Sony, OPM, and Home Depot, boards of directors have been obliged to better understand the threats of cyber-attacks. The management level started diverting more resources to prevent breaches before they happened, detecting them when they did, and responding effectively after a breach.

Although companies and individuals were aware of cybercrime, many more cyber-attacks occurred later on. Since late 2013, an unidentified group of hackers has been suspected of stealing $300 million and above (as much as triple that amount) from banks worldwide, with Russia accounting for the majority of the victims [33]. In 2016, Yahoo announced a 2013 breach, in which hackers stole personal details from one billion user accounts [34]. The EU adopted its first EU-wide cybersecurity legislation — the Network and Information Security (NIS) Directive in the same year [35]. Even though there were more security regulations released, the numbers of cyber-attacks continued to increase. In 2017, ransomware exploits almost doubled from 82,000 to 160,000 within a year. For example, the WannaCry ransomware attack infected an estimated 300,000 computer systems in four days [36]. Even Uber was hacked by ransomware in 2016 and it paid hackers $100,000 to delete stolen data on 57 million people [37]. Another significant cybercrime was the Equifax breach. A breach against credit reporting agency Equifax affected 145 million US consumers, 45 percent of the US population [38]. The Equifax breach made national and international headlines and caused its shares to drop 13 percent in the immediate aftermath.

Besides stealing personal information from companies, hackers also utilized sophisticated and malicious strategies to destabilize critical infrastructure, steal intellectual property and innovation, conduct espionage, and threaten democratic institutions. In 2018, Russian hackers have won remote access to the control rooms of many US power suppliers [39]. The access could have let them shut down networks and cause blackouts. In May 2018, the European General Data Protection Act (GDPR) came into force across EU countries [40]. The GDPR allows the EU's Data Protection Authorities to issue fines of up to €20 million ($24.1 million) or 4% of annual global turnover (whichever is higher). In 2019, the UK Information Commissioner fined British Airways $230 million and Marriott Hotels $123 million for GDPR breaches [41]. An interesting thing to note was that the hype around cryptocurrency grew becasue of the massive rise of bitcoin in the 2000s, which hackers took advantage of [42]. Bitcoin is a digital currency that can be transferred from one person to another without the use of a bank. Hence, hackers like to use bitcoin because of its anonymity. In 2019, hackers demanded $76,000 in Bitcoin after a ransomware attack froze systems in Baltimore [43].

In 2020, the US state of California introduced a Consumer Privacy Act to enhance citizens' data privacy rights [44]. However, the threat of the COVID-19 virus forced companies into a abrupt shift worldwide to remote working and increased the risk of cybersecurity attacks [45]. Zoom went from a little-known boutique service to one of the most well-known and frequently used video and audio conferencing systems almost overnight, because to the rapid growth in individuals working from home as a result of COVID-19. With such massive growth, Zoom had multiple security incidents, the most notable of which was the sale of over 500,000 user accounts on a dark web forum [46]. Besides the Zoom hack, one of the well-known cybersecurity attacks in 2020 was the SolarWinds hack. This attack was first discovered by the cybersecurity firm FireEye in December 2020. This hack impacted companies and high-level organisations like Microsoft and the US Department of Defense, while investigations into the scale of the attack are still ongoing. However, because of the large number of high-level parties targeted, this attack could be the most severe of 2020 [47]. Another severe attack was the Marriott hack. Marriott revealed that personal details of approximately 5.2 million hotel guests were fraudulently accessed in 2020. This data included passport and credit card numbers, and was found to have been attacked as early as 2014, prior to Marriott acquiring the Starwood brand properties [48]. In another travel-related incident, personal data on more than 10.6 million guests of MGM Resorts properties was shared on a hacking forum [49]. This is not the largest leak of hotel guest information since the Marriott hack exposed 500 million guests' data in 2017. However, hackers can use all sorts of information, even data that is less sensitive, to target an individual online.

According to a survey from cybersecurity firm Check Point Software, ransomware attacks have increased by 102 percent in the first half of 2021 compared to the same period last year [50]. The survey also stated that healthcare is the industry sector currently experiencing the most ransomware attack attempts globally, with an average of 109 attacks per company per week as shown in Figure 2-1. It is because that the ability of an attack to shut down operations at a medical facility has life-or-death consequences, motivating victims to pay the ransom. Take the Irish health service as an example, which shut down its computer systems after being hit with a "sophisticated" ransomware attack in May 2021 [51]. It can also be observed that the utilities sector experiences an average of 59 attacks per company per week from Figure 2-1. In May 2021, one of the nation's largest pipelines in the US, which carries 45% of the east coast's fuel supplies has been shut down after an apparent cyber-attack [52]. This shutdown raised concerns about cybersecurity risks and threatened to affect pricing far beyond the pump. Specifically, the attack on the Colonial Pipeline is the latest incident to raise concerns about the need to modernize and reinforce cybersecurity in America's critical infrastructure.

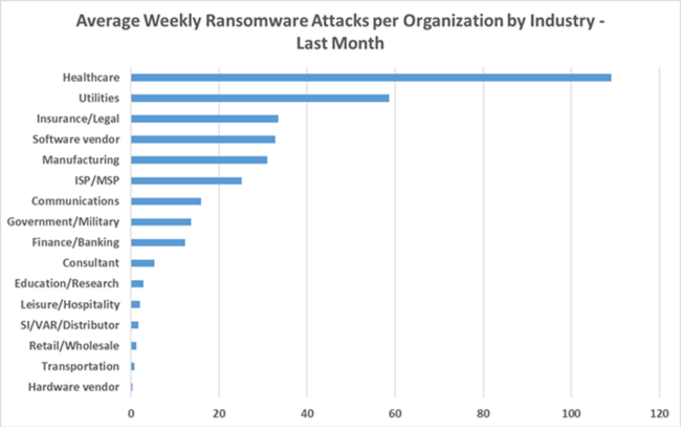


Figure 2-1: Average number of ransomware attacks per organization per week by industry – April 2021

In conclusion, cybersecurity attacks overgrew during the 1980s and 1990s, when computer processing and the nature of cyberwar were still constantly evolving. The creation of an annual worldwide crime organization worth over half a trillion dollars is how the status quo. These criminals operate in groups, using well-established strategies, and target anything and everyone with a web presence. Moreover, with breakthroughs in computer processing, quantum computing, and Artificial Intelligence, it is reasonable to believe we will be in for more speed-of-light shocks in the ongoing cyberwar.

2.1.2 Creation and Evolution of Cybersecurity Framework and standards

Users and service providers have collaborated in various local and international forums to affect the essential capabilities, policies, and practices across several decades, with the majority of these arising from work at the Stanford Consortium for Research on Information Security and Policy in the 1990s [53]. This section introduces the creation and evolution of selected cybersecurity framework and standards to get a basic understanding of the many frameworks available.

The Trusted Computer System Evaluation Criteria (TCSEC), often known as the Orange Book, was established by the US government in the early 1980s [54]. Although this standard was only required for government software and systems, the goal was that the private and public sectors would take notice and follow the government's lead in implementing TCSEC. However, this did not happen. TCSEC was rigorous and practical, but it took a long time to execute and was expensive. The fact was that by the time a computer was constructed and considered secure, it could not run many of the software programs that businesses had come to rely on, such as Microsoft Office, which was especially problematic [55]. Simultaneously, in Europe, an identical standard had been approved, with one key difference: the separation of security functionality and security assurance. Functionality and assurance were intertwined under US cybersecurity requirements, meaning that the more functionality a system had, the more assurance it was expected to have. The cybersecurity regulations in Europe, on the other hand, allowed for a system with high functionality but low assurance. The decoupling of functionality and assurance was a significant departure from American standards, but it allowed Europe to bring systems to market faster and save years of security assessment. In 2002, the TCSEC standard was canceled because it was too time-consuming and expensive [56].

The United States and Europe partnered to develop the Common Criteria to replace the TCSEC standard [57]. Each country would accept evaluation assurance levels up to level 4 under this new standard, after which governments would have to do their own security due diligence. The Common Criteria assurance levels, on the other hand, ranged from EAL1 to EAL7, with EAL7 being the highest and EAL1 being the lowest. As a result of the agreement to accept systems up to EAL4, a market emerged in which the majority of systems did not exceed EAL4 [58]. The Common Criteria is now essentially following in the footsteps of the TCSEC standards. While not entirely extinct, it is being phased out, as many businesses increasingly rely on a checklist of best practices.Systems are assessed against a compliance checklist and considered secure if they can check all of the boxes.

In February 2013, President Barack Obama requested Institute of Standards and Technology (NIST) to develop a "Cybersecurity Framework." The framework is a completely optional basis. This approach can be used by organizations or the private sector to secure their own critical infrastructure [59]. According to a 2016 US security framework adoption research, the NIST Cybersecurity Framework (CSF) is the most common best practice for Information Technology (IT) computer security [60]. However, many firms observe that it demands a significant investment. Hence, 64 percent of respondents from organizations currently using the NIST CSF reported implementing some of the NIST recommended controls, but not all of them. The other frameworks most widely used by respondents include: Payment Card Industry Data Security Standard (PCI-DSS), Center for Internet Security Critical Security Controls (CIS), and ISO/IEC 27001/27002 (ISO 27001) in 2016. The PCI-DSS sets guidelines for payment data security [61]. There are six primary groups of requirements (goals) for proper compliance with the PCI-DSS framework. Among these groups are distributed 12 separate requirements that need to be met individually. The CIS has outlined best practices for internet security and cyber threats in a collection of 18 essential security controls. The basic, foundational, and organizational categories are used to classify the 18 critical security controls [62]. A study of the previous release indicated that by adopting just the first five controls of CIS, 85 percent of attacks may be prevented, according to a TripWire report [63]. As for ISO 27001, it is the leading international standard focused on information security, published by the International Organization for Standardization (ISO) [64]. Not only does the ISO 27001 standard offer organizations with the required know-how for safeguarding their most sensitive data, but it also allows them to become ISO 27001 certified and prove to their clients and partners that their data is safe. The ISO 27001 framework consists of 11 clauses and an Annex that provides guidelines to controls that can be implemented. Like some of the other vastly used frameworks mentioned above, it can be integrated with other frameworks [65]. Overall, being compliant with these cybersecurity framework and standards can be a positive change-driver in an organization; it creates a sense of urgency towards improving an organization's cybersecurity posture. Sometimes, regulations force executives to understand the importance of cybersecurity and represent an important first step from which to build on.

However, compliance does not make organizations secure [66]. While the increase in organizations being compliant with certain framework, there has been a rise in the numbers of data breaches. This is because when regulations are extremely specific, one of the issues with compliance emerges. A high level of specificity is not necessarily the best method to regulate the rapidly changing cybersecurity landscape. Compliance is an overreaching task if it does not give firms with possibilities to acquire greater levels of maturity. In addition, to be compliant with certain regulations or standards, companies often spend most of their budgets and efforts focused on preparing for the external audits. This can lead to major issues since the remaining budget may not be sufficient for the maintenance process of security controls required to meet compliance requirements. In order to minimize expenses and address budget constraints, companies may choose to maintain the compliance requirements with minimum effort until the arrival of the next external audit. In this situation, companies may actually become more vulnerable after being compliant, and can encounter serious security incidents even though they have passed the compliance audit. Take one of the most vastly used frameworks - PCI-DSS as an example. Target was certified PCI-DSS compliant in 2013, just weeks before hackers infiltrated the retailer's network. While others, such as Heartland Payment Systems, experienced a severe breach despite assessors considering them compliant for six years in a row [26]. Hence, it can be observed that compliance may provide some legal protection, but it does not eliminate the risk of data breaches.

2.1.3 Information-Sharing

Information sharing to strengthen national security and public safety has been at the heart of a government reform movement aimed at making the public sector more efficient and effective through data utilization. The New York Police Department (NYPD) launched community policing reforms based on sophisticated crime mapping in the 1990s, which resulted in a significant crime reduction [67]. Many other police departments have used similar strategies since then.

On October 7, 2011, Executive Order 13587, titled "Structural Reforms to Improve Sharing and Safeguarding of Classified Information on Computer Networks," was signed by President Obama [68]. EO 13587 established a Senior Information Sharing and Safeguarding Steering Committee, an Insider Threat Task Force, and an Executive Agent for Safeguarding comprised of the National Security Agency and the Department of Defense to coordinate efforts to improve security on classified networks. EO 13587 also established a Classified Information Sharing and Safeguarding Office (CISSO) under the Program Manager for the Information Sharing Environment (PM-ISE) to ensure adequate safeguarding efforts support those information-sharing initiatives. The PM-ISE's role in responsible information sharing was significantly expanded with the creation of CISSO and the consolidation of its operation with the more considerable information sharing and safeguarding mission. International attempts to increase information exchange are still ongoing. Canada and Mexico have strengthened their information-sharing programs and established sharing of best practices with the PM-ISE. It is worth noting that Canada has its own PM-ISE, modeled after the one in the United States.

In 2014 and 2015, a host of cyberattacks have been perpetrated on many high-profile American companies (discussed in 2.1.1). The high-profile cyberattacks of 2014 and early 2015 appear to reflect a broader trend: cyberattacks are becoming more frequent and ferocious, posing significant threats to US national interests. While there is much debate about the best strategies and methods for protecting America's various cyber-systems, one point of "general agreement" among cyber-analysts is the need for better and timely cyber-threat intelligence sharing both within the private sector and between the private sector and the government [69]. The argument for real-time cyber-intelligence sharing—which could include vulnerability, threat, and countermeasure data—is based on the idea that effective cybersecurity requires a thorough understanding of potential threats and widespread dissemination of the best practices and strategies for dealing with them [70]. Despite general agreement on the importance of better cyber-information sharing, cyber-experts also concur that present public and private sector information sharing efforts are insufficient [71]. While there are various reasons why corporations may choose not to engage in a cyber-information sharing scheme, one of the most common reasons is the risk of liability associated with sharing internal cyber-threat information with other private organizations or the government.

To gain insight into cybersecurity threats and vulnerabilities, private-sector information security specialists have relied heavily on information from other private entities. And the most helpful cyber-intelligence typically comes from peers in other organizations, especially direct competitors who may be victims of identical cybercrime. Informal arrangements, such as peer talks over the phone, email, or in-person, formal sharing arrangements, such as cyber-intelligence sharing through an Information Sharing and Analysis Center (ISAC), are examples of private cyber-information sharing. ISAC is a private nonprofit corporation intended to facilitate sharing cyber threats, incidents, and vulnerabilities among members of a specific industry [72]. According to Choucri, Madnick, and Koepke, there are 24 operating ISACs, including the Financial Services ISAC (FS-ISAC) and Information Technology ISAC (IT-ISAC) [73]. Due to variances in size and formality between sectors, each ISAC operates differently, regardless of the model under which it was established. They also differ significantly in terms of the amount of data collected, analyzed, and distilled.

Although information sharing is universally acknowledged to be beneficial, the most challenging part that is in the way of cyber-intelligence sharing is the problematic legal questions posed by the regulation of cyber-intelligence sharing, such as how cyber-intelligence can be collected and shared within the private and public sectors.

2.1.4 Cyber Risk Management

Given the plethora of existing frameworks, standards and guides for managing cyber risk, choosing the best approach can be challenging. Although there exist some blog posts and journal-published papers, which compare well-known and commonly used frameworks by listing the merits and shortcomings of each, these are targeted for a point in decision making rather than the beginning of the process and do not appear to follow a standardized model. For example, blog posts on TechRepublic [74], Security Boulevard [75], Edureka [76], and CIO [77] explain the basics of the common frameworks and considerations when starting to think about cybersecurity. However, there is an apparent lack of simplified models for starting the process and comparing across and inside organizations with a holistic view, leaving a gap to be filled both in research and practical tools. Therefore, we propose an information-sharing tool for best cybersecurity practices with the aim of filling this gap.

There is a significant amount of literature in cybersecurity that studies information-sharing tools. Choucri, Madnick, and Koepke categorize and summarize institutions propelling data-sharing initiatives [73]. They report over sixty CERTs, ISACs, International Entities, US national entities, Non-US national entities, Non-profits, and private sector companies and the types of information they share. It is evident that a large institutional landscape is dedicated to information sharing of cyber threats and vulnerabilities.

In a technical report for Microsoft, Goodwin *et al.* present a guide for the development of information sharing tools related to cyber threats [78]. Their framework identifies methods and mechanisms of exchange, including person-to-person and machine-to-machine sharing, and models of exchange, which includes voluntary exchange models and mandatory disclosure models. The CRC tool fits nicely into the authors' identified framework as a voluntary exchange model of information from machine-to-machine.

In addition, the CRC tool employs many of the suggestions to reduce barriers to information sharing outlined in Lewis *et al.* which focuses on the supply-chain level [79]. They suggest anonymizing data in order to prevent misuse of sensitive information and other organizations gaining competitive advantages. Our tool provides the option for organizations to be anonymous.

Crucially, none of the above-mentioned models focus on information-sharing related to frameworks and related decision making. Choucri, Madnick, and Koepke, target threats and vulnerabilities. Goodwin *et al.* target cyber threat information sharing and Lewis *et al.* targets supply chain information sharing. We contribute to the literature by reviewing and selecting the foundations of information sharing for other types of information and applying them to decision making regarding frameworks.

We reviewed articles and papers that address approaches to the six components of the cyber risk cube – Internal, External, Qualitative, Quantitative, Measurement and Management. Some reports and papers have addressed approaches to gain internal and external views of cyber risk such as conducting periodic internal audits, self-assessments, and assessments by third parties. For example, Deloitte [80], Crowe Horwath [81], Debra Cope [82] and Jacob Olcott [83] stated the importance and potential of managing cyber risk and gaining an internal view of it by performing internal audits and self-assessments periodically. However, these approaches only present the organization with a partial view of their cyber risk. Bozkus Kahyaoglu, S. and Caliyurt, K determined key issues and weaknesses within the internal audit and the risk management perspective which further proved that these previous approaches do not consider other aspects of cyber risk management [84].

In the Gartner Security and Risk Management Summit of 2019, a session addressed quantitative versus qualitative cyber risk assessments and covered the pros and cons of each [85]. They discussed the state of risk assessments and whether the industry was ready for reporting cyber risk analytics quantitatively. In the end, participants agreed that while there is still a place for qualitative assessments as a communication tool, the quantitative approach to cyber risk is the rising trend.

Other papers and several blog posts attempt to compare across qualitative and quantitative approaches. A few attempts to compare across frameworks. Roldán-Molina *et al.* contribute to the literature on aiding cyber risk related decision making [86]. They propose a model "addressing the perception, comprehension, projection and decision/action layers" allowing one to identify which framework/approach is most suitable to support each of the layers. Another useful resource are the websites of companies that have created these frameworks and guides, both quantitative and qualitative. They often compare various frameworks on a number of characteristics declaring one as most effective. A RiskLens blog compares the qualitative and quantitative approach and describes the strengths and weaknesses of each, based on a Gartner debate [85]. The article focuses on the FAIR model that powers RiskLens. In a post, UpGuard compares BitSight, SecurityScorecard and UpGuard [87]. However, these blog posts, although insightful, are often biased towards the hoster's framework.

As for the measurement and management component of the CRC, Filippo Curti contributed to the literature on Cyber Risk Definition and Classification for Financial Risk Management [88]. In their Appendix A, they proposed to conduct a "aggregated monthly level" schedule that would track both the cyberattacks that resulted in financial losses (incidents), and the ones that did not result in financial losses. According to the Guide for Conducting Risk Assessments published by NIST [89], the frequency of cyber risk assessment and risk factor monitoring should be determined by the organization. Organizations that follow this guidance can use the CRC to understand cyber risk management and measurement approaches taken by peers.

Gartner PeerInsights examines what frameworks competitors and peers are using and their relative effectiveness [90, 91]. Here, reviewers can rate various kinds of software and tools, comment on their experiences with it, and compare them to other competing software and tools. Reviewers were identified by company size, industry and region. This is an extremely useful tool but one that lends itself to considerable selection bias. The subset of people and organizations that write reviews are likely not representative of all users and customers are likely to post reviews if they are either extremely satisfied or dissatisfied with the particular risk management tool. In addition, although Gartner PeerInsights focuses on various categories including Blockchain Platforms, Data Intergration, and IT Risk Management, there is no broader category dedicated to cybersecurity risk management tools outside of a SIEM tools category. The CRC tool specifically focuses on this aspect along with cyber risk strategies. It utilizes the same principle of collecting and presenting peer reviews but on a more focused category, allowing for more detail and relevance for users.

In brief, these prior systems are helpful but have some drawbacks that the CRC tool address. First, these only focus on the most well-known, largely quantitative frameworks so they do not allow for a combination of quantitative and qualitative approaches which are often the best way forward. Moreover, these guides are general and not tailored to an organization's size, industry, budget, or other defining characteristics all of which impact the optimal cyber security strategy an organization should seek to implement. These papers and blogposts also do not lend any insight into what competitors may be doing or how to compare an organization's level of cybersecurity with its peers. Moreover, these papers and articles only consider and present a partial view of the organization's cyber risk. In the following section, a review of system dynamics approach and related cybersecurity research will be explored to achieve the second research objective.

2.2 System Dynamics

A system dynamics approach is a simulation method for describing interactions among variables in complex systems in real-world challenges [92]. System dynamics modeling has proven useful in a variety of fields for assisting decision-makers in analyzing and explaining the dynamic behavior of complex systems [93]. In this section, to reach the ultimate goal of applying capability traps in cybersecurity, previous work in capability traps and cybersecurity using the system dynamics approach is discussed.

2.2.1 Capability Traps

Repenning and Sterman suggest that the critical determinants of success in efforts to learn and improve are the interactions between managers' attributions about the cause of poor organizational performance and the physical structure of the workplace, particularly delays between investing in improvement and recognizing the rewards [94]. They developed the theory of the capability trap to explain the failure of many process improvement programs. Three key conclusions can be drawn from the capability trap theory. First, turning the vicious cycle into a virtuous cycle of enhanced performance, lower costs, increased capability investment, and even better performance is required. Second, because of the gap between capability investment and outcomes, this leads to Worse-Before-Better behavior. Third, because capabilities are stocks, the system reveals a tipping point. To break free from the trap, sufficient resources must be invested in capabilities to ensure that they are built faster than they are degraded. Despite the short-term costs, managers may be willing to increase resources for improvement, but unless such expenditures are significant enough and sustained long enough to build capabilities faster than they degrade, performance will deteriorate over time [95]. For this thesis, the capability trap theory and the causal loop diagram are particularly useful to capture and explore the dynamics and tradeoffs between cybersecurity capability and efforts.

2.2.2 Cybersecurity Research using System Dynamics Approach

Several researchers have attempted to utilize system dynamics approach in cybersecurity. Andersen and twenty-four other researchers from eight institutions explores the preliminary system dynamic maps of the insider cyber-threat [96]. Later on, Fagade *et al.* utilizes system dynamics modeling to better understand the interrelationships between three different indicators of a malicious insider, in order to predict the likelihood of a security breach based on emerging trends and patterns [97]. In 2013, Polatin-Reuben *et al.,* create a system dynamics model of cyber conflict which may facilitate the identification of a culpable state or states in a cyber attack through publicly available information [98]. The system dynamics model simulates diplomatic tension between two countries to evaluate the probability of a cyber conflict. The model is tested using nine case studies in which the likely cyber combatant has been recognized. Although system dynamics modeling bring much value to research and business, it is sometimes referred to as theory-rich data-poor modeling. Pruyt *et al.,* disagrees with this point of view and claims that this does not imply that SD modeling is data-poor by definition [99]. He discusses three ways in which big data and data science may play a role in system dynamics and points out that many application domains in which the combination of system dynamics and big data would be beneficial. The latest cybersecurity research using system dynamics approach is done by Dolezal *et al.,*. Their work introduces systems thinking and system dynamics as ways to solving complex problems, as well as its possible applications in cybersecurity, with an emphasis on the Czech Republic's current status of cybersecurity [100]. In conclusion, there is no current research exploring the capability traps in cybersecurity and the second research objective of this thesis is to fill in this gap.

Chapter 3

Cyber Risk Cube

This chapter provides an introduction to the Cyber Risk Cube (CRC) Tool. It describes the six components in pairs. For purposes of illustration, this chapter will consider Acme Corporation a fictitious medium-sized technology company.

3.1 Six Components

Senior management at Acme Corporation has examined a lot of articles and online information about cybersecurity. They have determined that cyber risk management would be their priority this year and plan to implement a strategy to reduce cybersecurity risk. The executives learned about the Cyber Risk Cube (CRC) Tool and wanted to know more about how it works. They begin by understanding the six components that form the CRC Tool in Figure 3-1.

The CRC Tool with the six components (Internal, External, Quantitative, Qualitative, Measurement, and Management) impacts understanding, communicating, and building a risk management approach. The six components are in pairs: Internal and External, Quantitative and Qualitative, and Measurement and Management:

- Internal/External has to do with what is being assessed and by whom
- Measurement/Management is the frequency and oversight of that risk assessment output

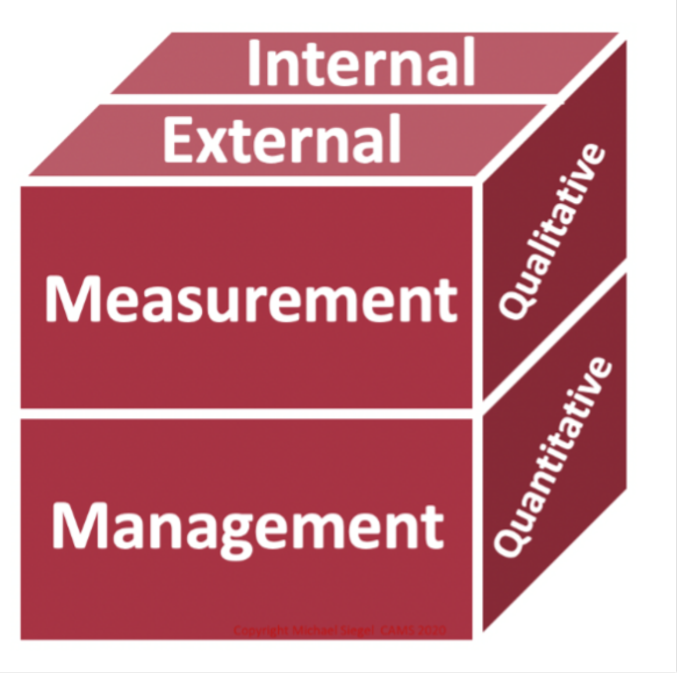


Figure 3-1: Cyber Risk Cube Tool

- Qualitative/Quantitative has to do with how risk is being measured during the assessment

The CRC Tool synthesizes the common tools, frameworks, methodology, and literature on cyber risk management from these six aspects. Acme Corporation thinks this is a reasonable approach to dealing with cyber risk management based on their previous research. They decide to learn more about each pair's definitions and examples on the faces of the CRC Tool.

3.1.1 Internal and External

This face of the cube makes the critical distinction between the organization's cybersecurity risk's internal and external views. An internal view comprises all risk factors that the organization itself can monitor and manage along with the security controls applied to mitigate the organization's internal cyber risk. An external view describes the facets of the risk that are detected externally about an organization, for example, the cyber risk associated with a third-party supplier. This includes assessing the organization's risk level, as seen by third parties, and the organization's assessment of third-party risks.

An organization needs to measure its security to determine whether they are taking the right steps to protect the business from cyber threat. Examples of approaches to internal or external cyber risk views will be included in the Tools and Techniques Database (see Appendix B). For instance, yearly internal security audits, self-assessments, and managing security control for external assessment are effective ways to gain an internal view of the organization's risk level. Management for the external evaluation refers to security controls that the organizations can adopt to reduce the organization's risk level, as seen by external parties.

As for gaining an external view of third-party risk level, due diligence must be conducted before selecting and entering contracts or relationships with third parties. Organizations should not rely solely on experience with or prior knowledge of the third party as a proxy for cyber risk assessment. Approaches to the external component could be onsite or offsite vendor audits and specific third-party risk management guidelines such as OCC's third-party relationships - a risk management guideline mostly for banking industries. Onsite visits may be useful to examine the third party's operations and capabilities. Finally, technical assessments are possible by incorporating technical measures (e.g., BitSight, Security Scorecard) of cyber risk.

3.1.2 Measurement and Management

This face of the cube represents a choice between static and dynamic management of cyber risk. For the most part, the choice will depend on the periodicity of managing and measuring their cyber risk. The Measurement component assumes that measuring cyber risk is always associated with some level of management. Therefore, the Measurement component means cyber risk measurement with infrequent management (e.g., set intervals such as monthly, yearly). The Management component is associated with cyber risk measurement and management that is more frequent (e.g., set intervals with shorter duration – daily, weekly and, in some cases approaching real-time). For the Management component, it refers to the dynamic management of cyber risk. Examples include organizations that perform audits to measure and manage cyber risk daily or weekly. The infrequent management of cyber risk the Measurement component is an example of organizations conducting annual or monthly security goal evaluations.

An interesting example of practicing either a Measurement or Management using the same measure is demonstrated by Key Performance Indicators (KPIs). KPIs are used to track the performance of the organization's implemented controls periodically because using KPIs is an effective way to measure the success of a cybersecurity program and aid in decision-making. It provides a snapshot of how the security team functions over time and helps the organization understand better what is working and what is not and improve decision-making about future projects. KPIs can assess cyber risk at varying frequencies. Therefore, KPIs are a quantitative approach that can be used in either the Measurement component or the Management component based on the frequency that the organization is assessing. If the organization is tracking cyber risk through KPIs and manage cyber risk daily, for example, that is a relatively high frequency and it would be categorized in the Management component. Otherwise, it would fall into the Measurement component.

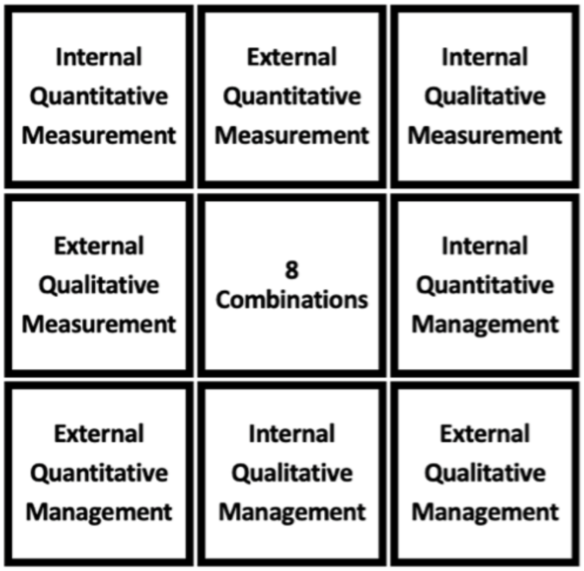
3.1.3 Qualitative and Quantitative

Qualitative risk assessments use ordinal rating scales to plot risk based on likelihood of occurrence and impact of loss. For instance, the FFIEC cybersecurity assessment tool [101] or NIST Cybersecurity Framework [102] which measures the use of cybersecurity controls is classified as a qualitative approach. Quantitative risk assessments use dollars, cents or scalar values such as Value-at-Risk (VaR) rather than an ordinal measure. Other examples of quantitative approaches include Factor Analysis of Information Risk (FAIR) [103], BCG Cyber Doppler [104], Security Assessment Framework for Enterprise (SAFE) [105], Cyber Security Evaluation Tool (CSET) [106], BitSight [107], SecurityScoreCard [108], and Cyber Resilience Assessment Framework Tool [109].

Acme Corporation is now even more convinced that they want to go ahead with using the CRC Tool. After understanding the three pairs of components, they will select at least one component from each of the pairs on each cube's face. This means they choose either internal or external, measurement or management, and qualitative or quantitative.

3.2 Methodology of the Cyber Risk Cube Tool

Organizations will choose one or more faces of the Cube as shown in Figure 3-2. The selection will be based on their rationales, budget constraints, workforce, or organization posture.

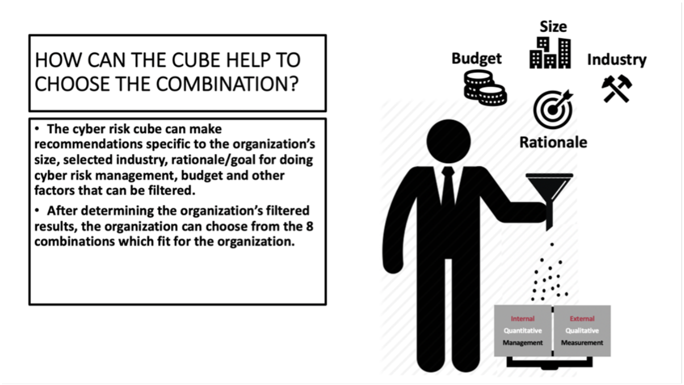


Internal Quantitative Measurement	External Quantitative Measurement	Internal Qualitative Measurement
External Qualitative Measurement	8 Combinations	Internal Quantitative Management
External Quantitative Management	Internal Qualitative Management	External Qualitative Management

Figure 3-2: Combinations of the Cyber Risk Cube Tool

3.2.1 Filters

Not all organizations are going to handle cyber risk management in the same way. Organizations will vary their approach based on size, selected industry, rationale for doing cyber risk management, budget, compliance and other factors. We have included a filter function for organizations to more easily get appropriate combinations based on factors in Figure 3-3. The CRC Tool applies to organizations of all sizes and industries.



HOW CAN THE CUBE HELP TO CHOOSE THE COMBINATION?

- The cyber risk cube can make recommendations specific to the organization's size, selected industry, rationale/goal for doing cyber risk management, budget and other factors that can be filtered.
- After determining the organization's filtered results, the organization can choose from the 8 combinations which fit for the organization.

Figure 3-3: Filtering feature of the Cyber Risk Cube

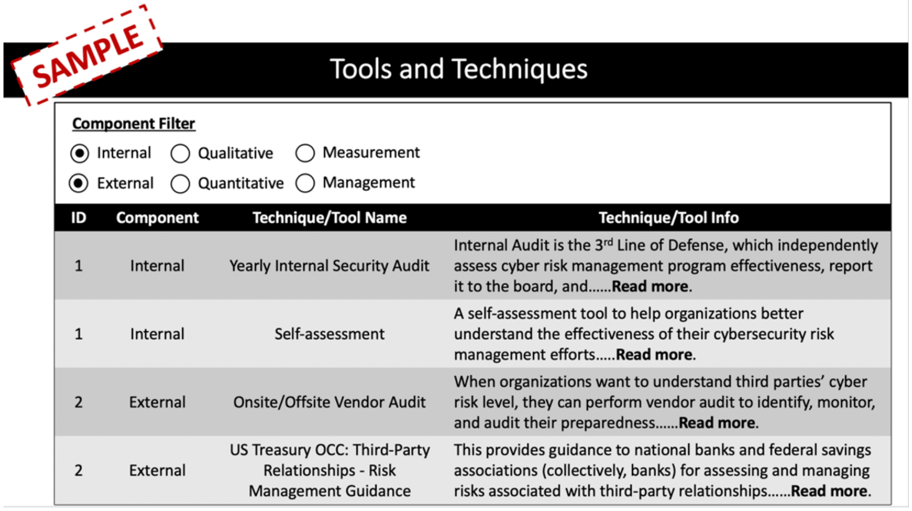
The management team at Acme Corporation examined these components and they feel that they will analyze the cyber risk to gain an internal view of their cyber risk level. This year, as cyber risk management is their priority, they have selected the management approach to frequently measure and manage their cyber risk. They decide to use a qualitative approach due to their time and budget constraints. These are their initial choices of components, but they will confirm the combination after looking at more detail provided in the CRC Tool. Acme management has decided to use this combination as its first cyber risk project; it may consider other combinations later.

The Acme Corporation looked at this closely and classified themselves as a medium-size technology company. Their rationale for implementing cyber risk management is to comply with regulations and requirements requested from their customers. Acme Corporation has chosen the Internal – Qualitative – Management combination after going through the definitions and examples of the six components. They plan to use the Tools and Techniques and Cases databases described below to look at examples of how others have approached cyber risk management.

3.2.2 Cases Database, and Tools and Techniques Database

After filtering, the CRC Tool will help organizations make practical decisions by displaying two databases: Tools and Techniques and Cases. Possible tools and techniques used for each of the six components available in the Tools and Techniques Database, while collecting organizational implementations of the eight combinations of components will be included in the Cases Database. We have developed an initial set of records in both databases using existing case studies, literature, and online information sources.

A sample of possible tools and techniques is shown in Figure 3-4. The initial schema of the Tools and Techniques database is shown in Figure 3-5. Organizations can browse options for tools and techniques for each of the six components. Additional examples of tools and techniques can be found in Appendix B that includes a limited set of examples which are used in the paper.



Tools and Techniques

Component Filter

● Internal ○ Qualitative ○ Measurement
● External ○ Quantitative ○ Management

ID	Component	Technique/Tool Name	Technique/Tool Info
1	Internal	Yearly Internal Security Audit	Internal Audit is the 3rd Line of Defense, which independently assess cyber risk management program effectiveness, report it to the board, and……**Read more.**
1	Internal	Self-assessment	A self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts…..**Read more.**
2	External	Onsite/Offsite Vendor Audit	When organizations want to understand third parties' cyber risk level, they can perform vendor audit to identify, monitor, and audit their preparedness……**Read more.**
2	External	US Treasury OCC: Third-Party Relationships - Risk Management Guidance	This provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships……**Read more.**

Figure 3-4: Sample of the Tools and Techniques Database

A sample of the Cases that a user can access is shown in Figure 3-6 and the initial database schema in Figure 3-7. The sample case study is a Large Healthcare Organization with approximately 3,600 employees [110]. Cyber risk management is performed by the University of Kansas Medical Center (KUMC)'s Office of Information Security (OIS) which is a relatively new department that formerly existed as a

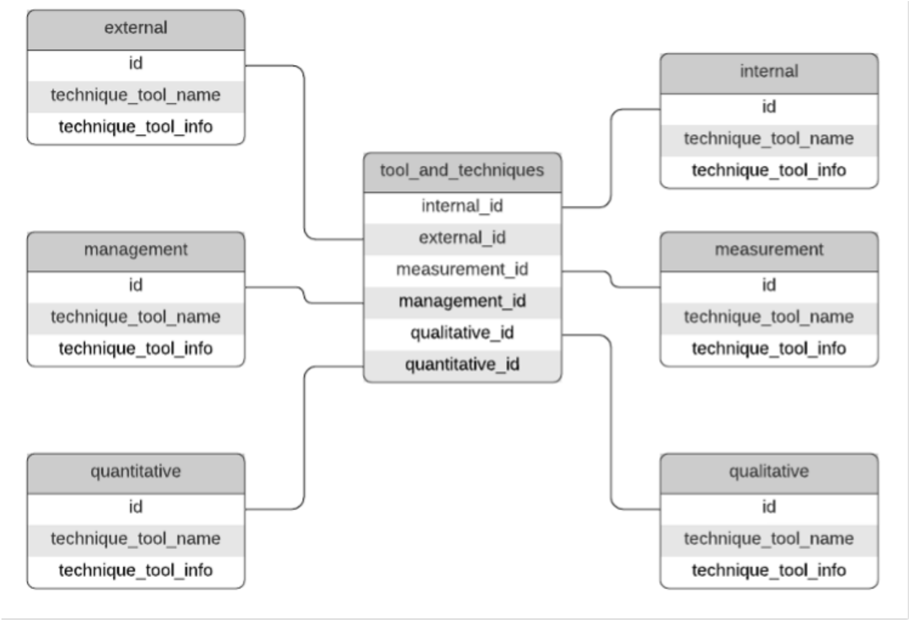
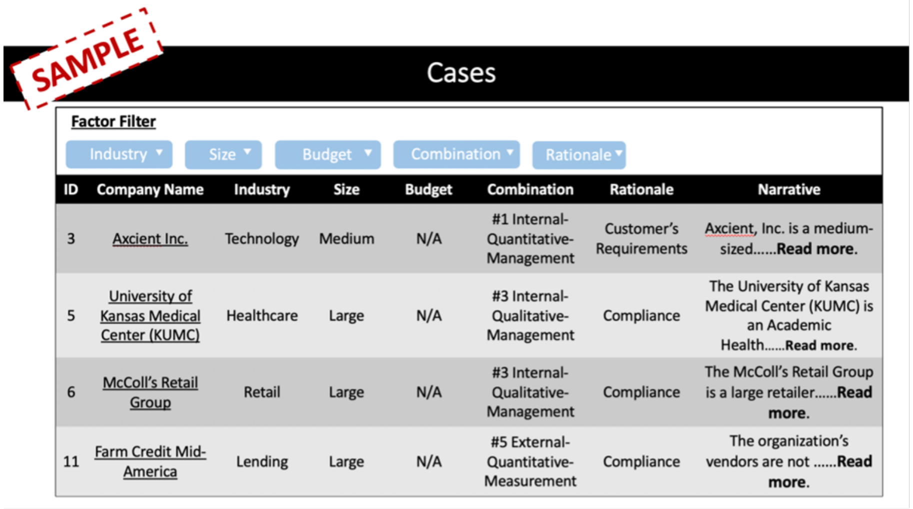


Figure 3-5: Schema of the Tools and Techniques Database

subunit of the IT Department.



ID	Company Name	Industry	Size	Budget	Combination	Rationale	Narrative
3	Axcient Inc.	Technology	Medium	N/A	#1 Internal-Quantitative-Management	Customer's Requirements	Axcient, Inc. is a medium-sized......**Read more.**
5	University of Kansas Medical Center (KUMC)	Healthcare	Large	N/A	#3 Internal-Qualitative-Management	Compliance	The University of Kansas Medical Center (KUMC) is an Academic Health......**Read more.**
6	McColl's Retail Group	Retail	Large	N/A	#3 Internal-Qualitative-Management	Compliance	The McColl's Retail Group is a large retailer......**Read more.**
11	Farm Credit Mid-America	Lending	Large	N/A	#5 External-Quantitative-Measurement	Compliance	The organization's vendors are not ......**Read more.**

Figure 3-6: Sample of the Cases Database

KUMC performs a self-assessment, which is identified as an Internal approach in the previous Tools and Techniques Database. As for the Qualitative component, the organization uses the Baldrige Cybersecurity Excellence Builder in conjunction with the NIST Cybersecurity Framework for self-assessment and program development. For the Management component, it implements management controls from the NIST

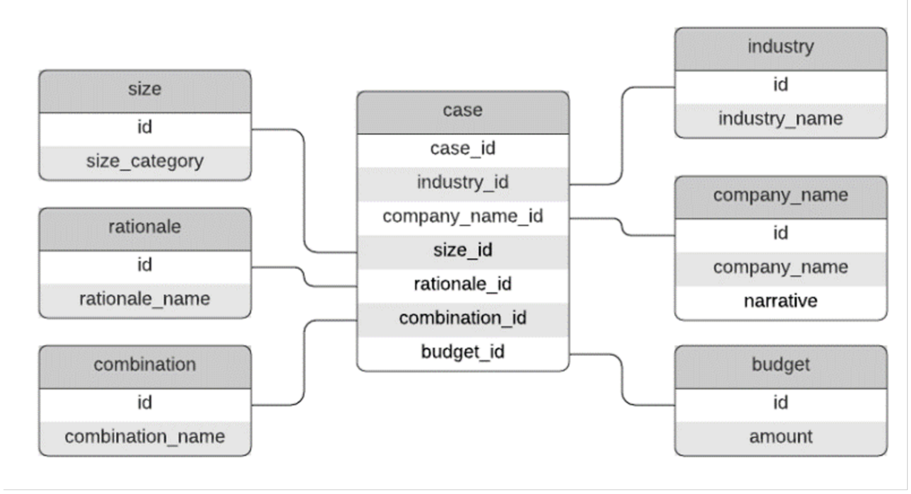


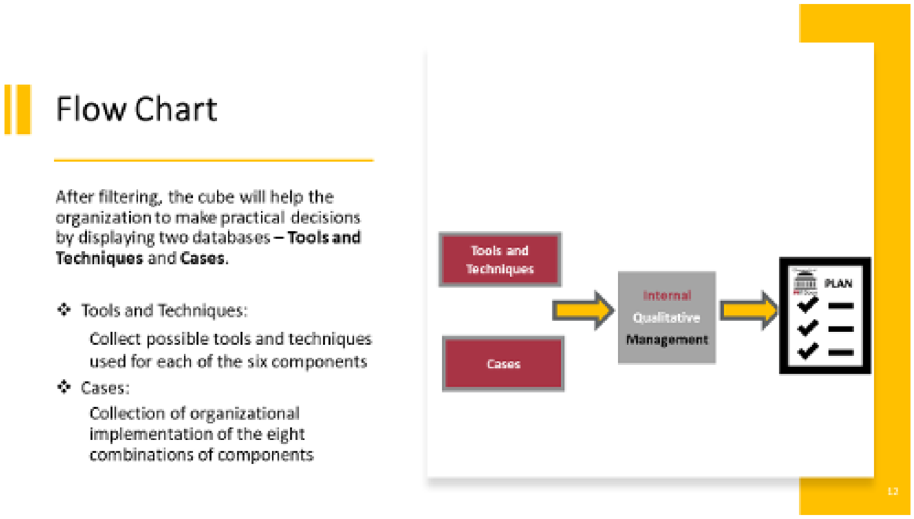
Figure 3-7: Schema of the Cases Database

Cybersecurity Framework and actively manages cyber risk by daily monitoring of risk. The narrative describes how this process helped the KUMC OIS team understand their roles and engage their customers in protecting the organization. Moreover, it helps them establish a better approach to intake, response, and follow- up, improving stakeholder relationships and getting the right solutions to their customers.

After going through these two databases, organizations will decide what tools and techniques they would like to adopt in their organization. Organizations can finalize their decision of on which combination(s) to apply and develop an implementation plan for the organization. Additional examples of cases can be found in Appendix A.

After deciding the combination that they want to adopt, the Acme Corporation uses the CRC tool's filtering feature to help them make practical decisions by displaying two databases – Tools and Techniques, and Cases as shown in Figure 3-8. The factors that they use to filter in the Cases database are Industry – Technology, Size – Medium, and Combination – #3 Internal/Qualitative/Management. For the Tools and Techniques database, the Acme Corporation filter the component – Internal, Qualitative, and Management. These two databases display the possible tools and techniques and case studies according to the filtering results.

The Acme Corporation has decided to take an Internal view of cyber risk using a Qualitative method for the Management of cyber risk after going through these



Flow Chart

After filtering, the cube will help the organization to make practical decisions by displaying two databases – **Tools and Techniques** and **Cases.**

- Tools and Techniques:
  Collect possible tools and techniques used for each of the six components
- Cases:
  Collection of organizational implementation of the eight combinations of components

Figure 3-8: Flow Chart of the Cyber Risk cube

two databases in the cyber risk cube as shown in Figure 3-9. To obtain an internal view of their cyber risk, they decide to conduct a self-assessment just like what the other medium-sized organization is doing to understand the internal view of its cyber risk level. The Acme Corporation chooses to adopt the Qualitative component with the NIST cybersecurity risk assessment. For the Management component, they will be reviewing cyber risk results bi-weekly and making changes based on the reviews. SIEM tools and KPIs are also adopted to measure and mange cyber risk. Examples of these tools and techniques are described in Appendix B.

Tools and Techniques
Cases
Internal
Qualitative
Management

With the help of the two databases in the Cyber Risk Cube, a large tech organization decides to take an Internal view of cyber risk using a Qualitative method for the Management of cyber risk.

Internal

The organization decides to conduct a self-assessment to understand the internal view of its cyber risk level.

Qualitative

The organization decides to adopt the NIST cybersecurity risk qualitative assessment.

Management

The organization decides to review cyber risk results bi-weekly to actively manage it. SIEM tools and KPIs are also adopted.

Figure 3-9: Decision made with the help of Cyber Risk Cube Tool

Acme also believes that this language and approach to cyber risk management will help deal with governance and compliance issues.

3.2.3 Data Collection System

A data collection system supports the Tools and Techniques and Cases databases. A schematic of the systems is shown in Figure 3-10.

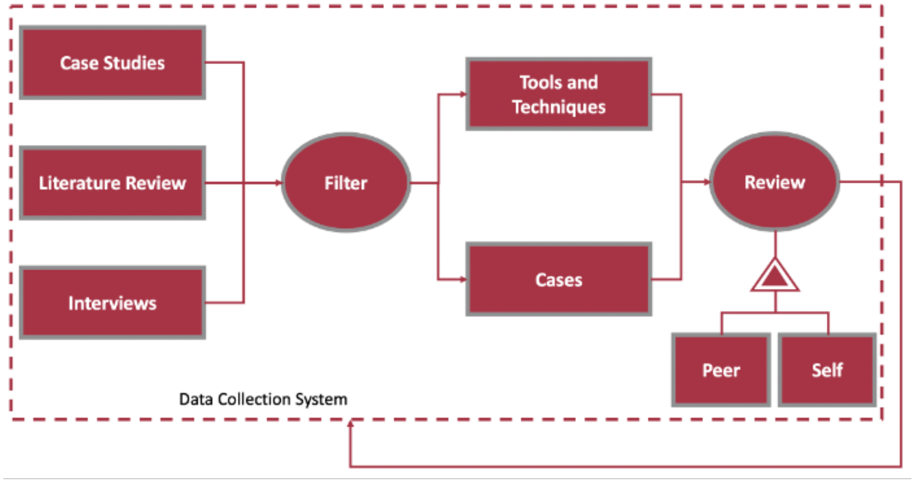


Figure 3-10: Flow Chart of the Data Collection System

We start by conducting case studies, literature reviews, and collecting feedback from organizations to build database instances. We then apply filter variables to the cases. Filter variables include but are not limited to size (small, medium, large) or industry (banking, energy, industrial, technology, etc.). Organizations will use the same filter variables to find practices that may fit their needs. These same filter variables will allow them to compare with industry peers' cyber risk practice (or other groups inside a single organization).

The review process will contain both a peer review and self-review process to provide feedback on individual instances in the database. This is where reviewers can suggest how well a tool worked for their practice or how well a case worked as an implementation. This cycle ensures the CRC Tool's information can continue to be improved and be more effective and reliable for companies to use.

Information in the databases will be enhanced by the continuous review of the literature and available case studies. Additionally, we will collect data from individual companies, industry groups, government and non-governmental organizations to create a rich set of tools, techniques, and cases for the CRC Tool. An option for adding anonymous data will be available.

3.2.4 Continuous Improvement of the Database

We are planning to improve the Cyber Risk Cube Tool by adding features such as a scoring system. Cases will be graded in the selection process, making it easier for organizations to select possible implementations. Organizations can also study others' improvement in the industry by keeping up with new and changing tools and techniques, and cases. We do not advocate for the organization blindly copying security solutions without reflecting on how they fit their own organization. A lot can be learned from studying how other organizations (or other parts of your organization) have solved similar cyber risk management problems.

3.3 Cyber Risk Cube: Options for Implementation

We envision the CRC and associated toolset to be useful for all organizations with varying models for data collection and sharing. For example, a large company may have a private option where the Cube is used for internal knowledge collection and sharing. It may also take advantage of a semi-private implementation provided by an industry specific Information Sharing and Analysis Centers (ISACs). Alternatively, the company may look for a larger private platform for additional information on tools, techniques and applications of specific cases. On the other hand, a small to medium-size enterprise may turn to a sponsoring industry consortium to use the CRC Tool in providing advice on cyber risk management approaches through data collected anonymously from consortium members.

Below are some examples of how different types of organizations may use the CRC Tool to support development of cyber risk management approaches:

1. **Large Organizations** Large organizations can develop an internal database for the cyber risk cube and use it in your organization to share knowledge across departments.

2. **Industry Organizations (ISACs, Foundations, Academic Organizations, etc.)** Industry organizations can develop data collection strategies and provide a version of the Cyber Risk Cube for members. The CRC databases will continue to collect information allowing for continuous learning and improvement, and new approaches and past experiences are evaluated by members.

3. **Consulting Firms** Consulting firms can collect this information based on experience with clients and provide services that analyze approaches to new and developing cyber risk management implementations. An internal evaluation process will allow the firm to rate various tools and techniques, and cases. The Cube will help the firm provide advice to clients on their cyber risk maturity level and its practices compared to peers in the industry.

4. **Governments and Non-Governmental Organization** Government and NGOs can use the Cube internally, similar to large organizations, and also provide services to its constituency that includes developing better approaches to cyber risk management. Governments and NGOs can analyze tools and techniques their stakeholders and vendors are using. They can also compare their vendors' cyber risk maturity level to vendors' peers when doing vendor risk assessments. Information from vendors and stakeholders can be collected to build the database to support the use of the Cube.

5. **Small and Medium Enterprises (SMEs)** Small and medium-sized enterprises can leverage Government, NGO and Industry Organizations offering implementation of the Cyber Risk Cube to develop current and targeted approaches to cyber risk management. This can be extremely helpful as these organizations may have limited budgets for developing and implementing strategies. Simplifying the analysis phases and selecting a range of implementations

can be a beneficial head start to SMEs, wanting to reduce their cyber risk exposure.

These are just a few of the many possible development approaches and uses of the CRC Tool. Cyber risk has become a significant challenge due to the growth of cybersecurity threats. All organizations must make advances in managing cyber risk. The Cyber Risk Cube tool presented in this paper decomposes cyber risk management into six components and provides companies with a guide to manage cyber risk. The tool also provides a platform for communicating about approaches to managing cyber risk. Moreover, it allows organizations to map to practical solutions in industry, including selecting tools and techniques and their implementation. It also allows for continuous improvement to keep up with the changes in the industry and regulations.

In order to facilitate its use, we provide a structure for the data needed to instantiate this tool. To demonstrate the applicability of the Cyber Risk Cube tool, we used existing case studies to contextualize this tool. Finally, we made suggestions about how different organizations may have varying approaches to developing and using the Cyber Risk Cube.

More research and systematic collection and evaluation of data can be valuable for identifying other factors that should be considered during the filtering process. At this stage, the factors we placed are the size and industry of an organization, rationale for performing cyber risk management, and budget constraints. A review system (scoring) is suggested to better select and evaluate approaches to cyber risk management. As we work with more organizations in developing implementations of the Cyber Risk Cube, we expect to gain additional insights and provide continuous improvement in cyber risk management.

Chapter 4

System Dynamics Model

This chapter presents a System Dynamics Model for Cybersecurity Risk Management Strategy. It focuses on the exploration of cybersecurity risk management strategy to identify common pitfalls for organizations. The development of the cybersecurity risk management strategy causal loop diagrams will also be introduced. For purposes of illustration, this chapter will consider Acme Corporation a fictitious medium-sized technology company.

4.1 Causal Loop Diagram

An approach for identifying the dynamics and tradeoffs in cybersecurity is the causal loop diagram. The causal loop diagram is a frequently-used methodology in the system dynamics field [111]. It is a useful tool to find out the structure of cybersecurity systems in order to achieve a better understanding of a cybersecurity risk management strategy model. The causal loop diagram's main goal is to illustrate causal hypotheses and present a more aggregated view of both cause and result. The causal loop diagram enables the users to communicate the feedback structure and underlying assumptions rapidly [112].

A causal diagram is made up of variables connected by arrows that indicate the causal relationships between them. The diagram also shows essential feedback loops. Arrows depict Cause-and-effect relationships between variables [113]. The causal relationship displays one factor affecting another. This causal relationship was modeled using a causal loop diagram. A positive relationship is defined as "a state in which a causal element, A, has a positive influence on B, where a rise in A value corresponds to a positive increase in B value." A negative relationship is defined as "a state in which a causal element, A, has a negative influence on B, with a rise in A value corresponds to a decrease in B value." [111] Link polarities describe the system's structure. They do not illustrate how the variables behave. In other words, they describe what may happen if anything changed, but they do not depict what happens in real life. The causal diagram does not indicate what will occur. Instead, it informs users what would happen if users changed the variable [113].

Figure 4-1 is an example adapted from the Book Business Dynamics: Systems thinking and modeling for a complex world: Tools for Systems Thinking [113]. This causal loop diagram depicts that the birth rate is determined by both the population and the fractional birth rate. Each causal link is assigned a polarity, either positive (+) or negative (-) indicate how the dependent variable changes when the independent variable changes. The important loops are highlighted by a loop identifier which shows whether the loop is a positive (reinforcing) or negative (balancing) feedback. It can be easily observed that the positive feedback relating births and population is clockwise and so is its loop identifier; the negative death rate loop is counterclockwise along with its identifier. An increase in the fractional birth rate means the birth rate (in people per year) will increase above what it would have been, and a decrease in the fractional birth rate means the birth rate will fall below what it would have been. That is, if average fertility rises, the birth rate, given the population, will rise; if fertility falls, the number of births will fall. When the cause is a rate of flow that accumulates into a stock then it is also true that the cause adds to the stock. In the example, births add to the population. An increase in the average lifetime of the population means the death rate (in people per year) will fall below what it would have been, and a decrease in the average lifetime means the death rate will rise above what it would have been. That is, if life expectancy increases, the number of deaths will fall; and if life expectancy falls, the death rate will rise [113].

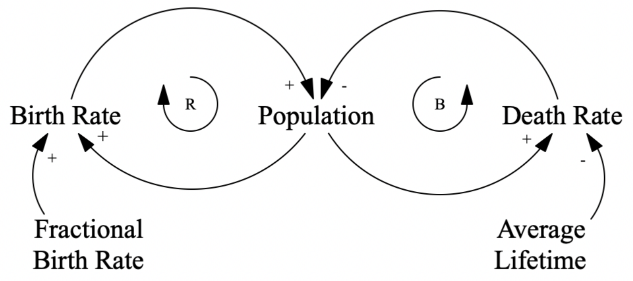


Figure 4-1: An Example of Causal Loop Diagram, Adapted from the Book Business Dynamics: Systems thinking and modeling for a complex world: Tools for Systems Thinking

A causal loop diagram will be created to illustrate the logic and structure of the introduced cybersecurity risk management strategy model in the following sections and then show how that causal loop diagram is validated.

4.2 Cybersecurity Risk Management Strategy Model Structure

In this section, the Causal Loop Diagram is used to provide a better understanding of cybersecurity risk management strategy model. It explains the logic of model and shows the interaction of each model building blocks; it also facilitates the understanding of the model and consequently facilitates the applying of it. While a well-defined Causal Loop Diagram that is consistent with the aims of this thesis is available in Appendix C, Figure 4-2 that illustrates a simple Causal Loop Diagram which only shows the main loops and main interactions for ease of explanation. Although Acme Corporation has established an essential strategy for its cybersecurity risk management using the CRC Tool in Chapter 3, Acme Corporation still suffers from several cybersecurity incidents observed in other reputable companies. Acme Corporation decides to explore the cybersecurity risk management strategy model structure and get a better understanding of the dynamics and tradeoffs. There are three main loops shown partially in the Figure 4-2:

- Working Harder Loop (Balancing Loop)
- Working Smarter Loop (Balancing Loop)
- Perception Trap Loop (Balancing Loop)

Whether it is production, project management, maintenance, human resources, or environmental quality, managers of any process are accountable for the process's performance versus its goals [95]. In cybersecurity, managers are also responsible for the performance. Cybersecurity performance can be managed, but only if measured. Cybersecurity performance management is the process of measuring the maturity of a company cybersecurity program based on top-level risks and the level of investment (people, procedures, and technology) required to achieve legal requirements and business objectives [114]. Hence, an increase in the cybersecurity maturity level will enhance the overall cybersecurity performance in organizations. Managers have two fundamental options to close the gap: work harder or work smarter if their cybersecurity maturity level falls short of the target.

4.2.1 Working Harder Loop

Figure 4-3 shows the structure of the balancing *Working Harder* feedback. Adding resources (hiring, capacity expansion), enhancing resource utilization (overtime, shorter breaks, speeding up), and improving production per person-hour by cutting corners (skipping steps, cutting testing, deferring maintenance, failing to follow security procedures) will alll influence the working harder loop [95]. These activities form the negative *Working Harder* feedback. In short, a cybersecurity maturity level shortfall leads to longer hours, corner-cutting, deferring maintenance, and other shortcuts that improve its cybersecurity maturity level.

For example, the cybersecurity manager of Acme Corporation wants to fill the cybersecurity maturity level gap and achieve the required cybersecurity maturity level. The cybersecurity manager chooses to spend more time on fixing as many vulnerabilities as possible they can find in their systems. The time spent working will increase, and it will, of course, improve the security maturity level to some degree.

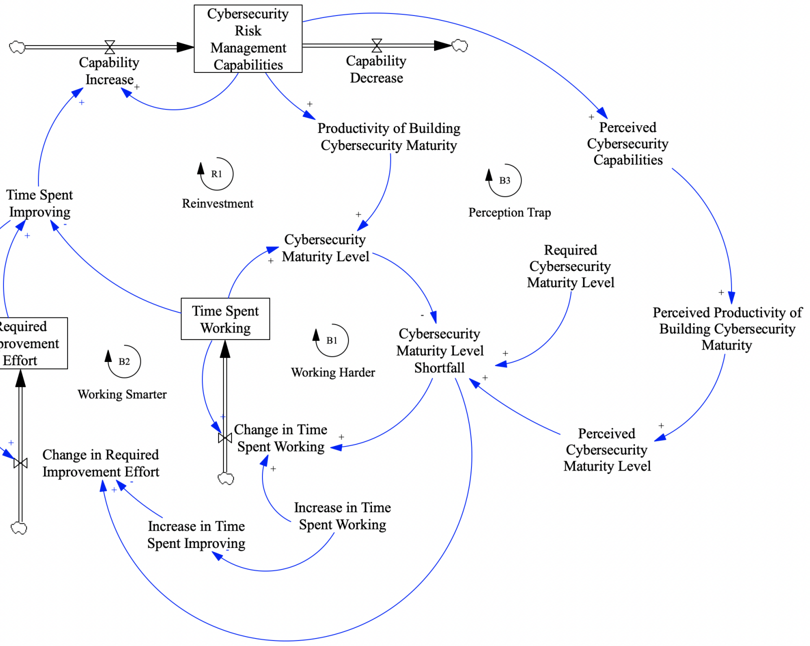

Cybersecurity Risk Management Capabilities
Capability Increase
Capability Decrease
Productivity of Building Cybersecurity Maturity
Perceived Cybersecurity Capabilities
R1
Reinvestment
B3
Perception Trap
Time Spent Improving
Cybersecurity Maturity Level
Required Cybersecurity Maturity Level
Perceived Productivity of Building Cybersecurity Maturity
Required Improvement Effort
Time Spent Working
B2
Working Smarter
B1
Working Harder
Cybersecurity Maturity Level Shortfall
Change in Time Spent Working
Change in Required Improvement Effort
Perceived Cybersecurity Maturity Level
Increase in Time Spent Working
Increase in Time Spent Improving

Figure 4-2: The causal loop diagram of cybersecurity risk management strategy model

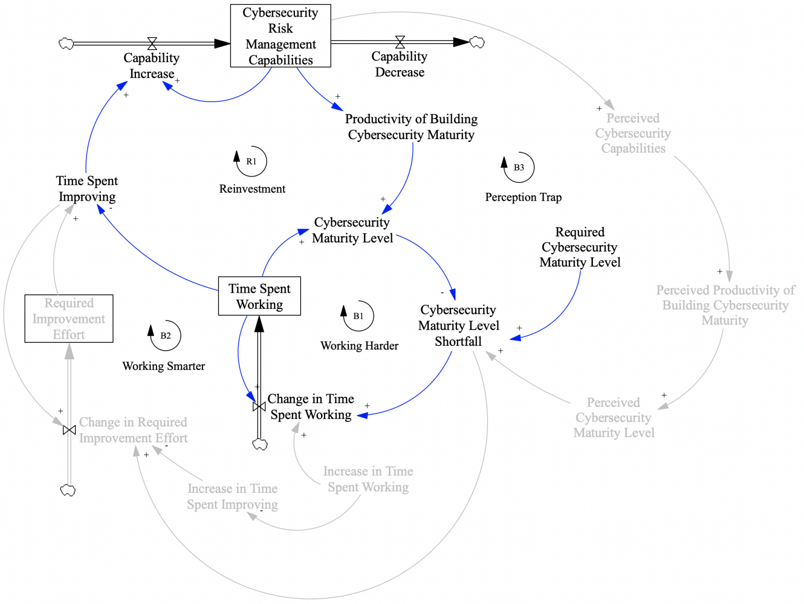

Cybersecurity Risk Management Capabilities
Capability Increase
Capability Decrease
Productivity of Building Cybersecurity Maturity
Perceived Cybersecurity Capabilities
R1
Reinvestment
B3
Perception Trap
Time Spent Improving
Cybersecurity Maturity Level
Required Cybersecurity Maturity Level
Perceived Productivity of Building Cybersecurity Maturity
Required Improvement Effort
Time Spent Working
B2
Working Smarter
B1
Working Harder
Cybersecurity Maturity Level Shortfall
Change in Time Spent Working
Change in Required Improvement Effort
Perceived Cybersecurity Maturity Level
Increase in Time Spent Working
Increase in Time Spent Improving

Figure 4-3: The partial causal loop diagram of cybersecurity risk management strategy model: Working Harder Loop (Balancing Loop)

4.2.2 Working Smarter Loop

Instead of working harder to close the cybersecurity maturity level gap, managers can also perceive the cybersecurity maturity level gap as an indication that the organization's cybersecurity risk management capabilities are insufficient. They can boost improvement activities aimed at addressing the root causes of poor cybersecurity maturity level and invest in the capabilities that make improvement efforts more effective, such as investments that improve people's skills, knowledge of best practices, and enhance cooperation and trust across organizational boundaries. Overall, investing in cybersecurity capability improvement forms the Work Smarter feedback as shown in Figure 4-4.

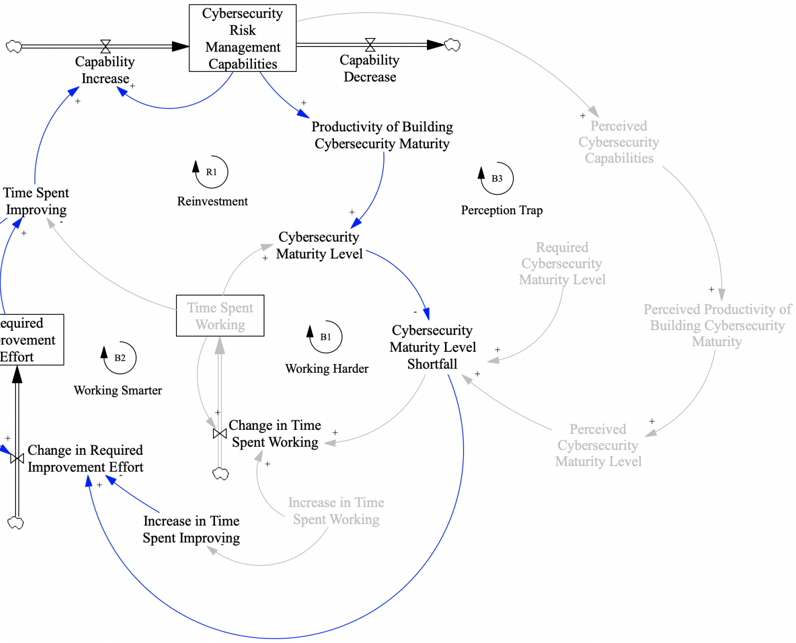

Cybersecurity Risk Management Capabilities
Capability Increase
Capability Decrease
Productivity of Building Cybersecurity Maturity
Perceived Cybersecurity Capabilities
R1
Reinvestment
B3
Perception Trap
Time Spent Improving
Cybersecurity Maturity Level
Required Cybersecurity Maturity Level
Perceived Productivity of Building Cybersecurity Maturity
Time Spent Working
Required Improvement Effort
B2
Working Smarter
B1
Working Harder
Cybersecurity Maturity Level Shortfall
Change in Time Spent Working
Change in Required Improvement Effort
Perceived Cybersecurity Maturity Level
Increase in Time Spent Working
Increase in Time Spent Improving
+
-

Figure 4-4: The partial causal loop diagram of cybersecurity risk management strategy model: Working Smarter Loop (Balancing Loop)

Organization often fall into the trap of choosing to work harder instead of work smarter because that working harder — including overtime, corner cutting and deferring maintenance — will quickly boost the cybersecurity maturity level. In terms of time and space, effort and outcome are closely intertwined, measurable, and predictable: a 10% increase in work hours rapidly produces a 10% increase in output.

On the other hand, working smarter takes time, and both the length of the delay and the result are unknown: Security mechanisms for improvement require time and tend to fail; additionally, it takes time to train employees in advance, establish procedures and norms that prevent corner-cutting. These features bias many businesses to work harder even though the benefit of working smarter is more significant.

After understanding more about the Working Smarter loop, the cybersecurity manager of Acme Corporation decided to interpret the cybersecurity maturity level gap as a sign that Acme Corporation's cybersecurity risk management capabilities are inadequate. He decided to increase improvement activity designed to eliminate the root causes of poor cybersecurity maturity level and invest in the capabilities that make improvement effort effective. For instance, he invested in employee training to enhance people's skills, and knowledge of best practices. He also invested heavily in getting a more advanced and sophisticated systems and technologies instead of fixing hundreds of vulnerabilities in the old system.

4.2.3 Perception Trap Loop

A common mistake made by organizations is to think of cybersecurity maturity level as something that can be evaluated by the number of layers of defense in place by the IT department. Unfortunately, when organizations look at cybersecurity through this perspective, they can not tell the difference between self-perception and reality. A proper assessment of security maturity can only be acquired by evaluating several critical components holistically, such as people, organizational culture, technology, tools and controls, and security operations — merely collecting a long list of security tools would not suffice. A recent study looked at the security maturity level of hundreds of organizations in the United Kingdom and 52% of large UK firms fall into the "Underprepared" group [115]. Of those Underprepared UK businesses, 44% claim to offer a higher level of security. This study reveals that many organizations can not tell the difference between cybersecurity perception versus the reality and fall into the balancing *Perception Trap* feedback shown in Figure 4-5.

This happens frequently when cybersecurity managers feel like their systems are

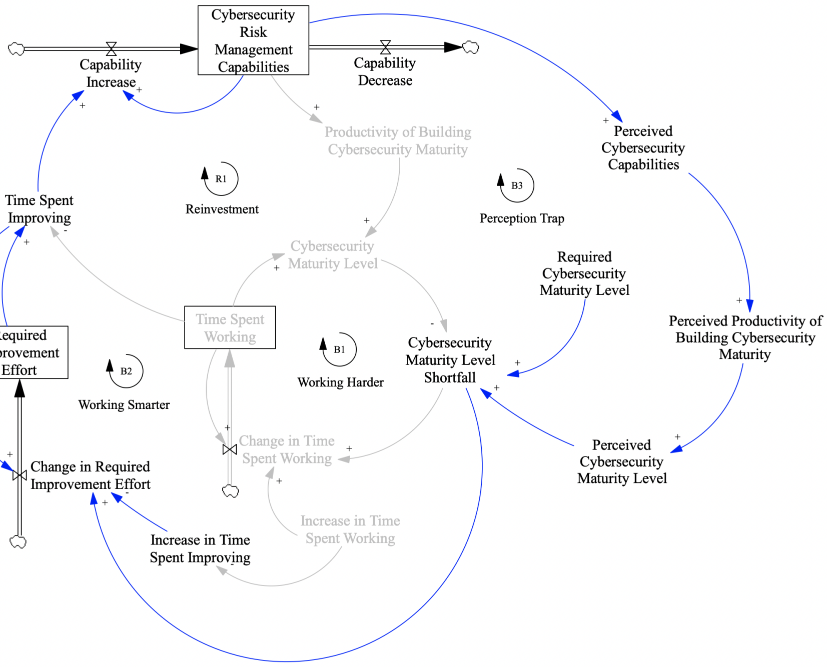

Cybersecurity Risk Management Capabilities
Capability Increase
Capability Decrease
Productivity of Building Cybersecurity Maturity
Perceived Cybersecurity Capabilities
R1
Reinvestment
B3
Perception Trap
Time Spent Improving
Cybersecurity Maturity Level
Required Cybersecurity Maturity Level
Perceived Productivity of Building Cybersecurity Maturity
Required Improvement Effort
Time Spent Working
B1
Working Harder
Cybersecurity Maturity Level Shortfall
B2
Working Smarter
Change in Time Spent Working
Change in Required Improvement Effort
Perceived Cybersecurity Maturity Level
Increase in Time Spent Working
Increase in Time Spent Improving
+
-

Figure 4-5: The partial causal loop diagram of cybersecurity risk management strategy model: Perception Trap Loop (Balancing Loop)

secured and overrate their cybersecurity maturity level. For example, the cybersecurity manager of Acme Corporation may think he has closed the security maturity level gap and achieved the next maturity level by fixing hundreds of vulnerabilities. However, they are still at the same maturity level, so the maturity level gap is still there. If the perceived cybersecurity maturity level increases, the cybersecurity maturity level shortfall will increase, which means the gap is more significant than what the managers expected.

4.3 Utilize the System Dynamics Model for resource allocation in the CRC Tool

The System Dynamics Model is designed for organizations to optimize resource allocation when they decide to implement multiple approaches/tools/techniques in one or more components of the CRC Tool. The flow chart is shown in Figure 4-6.

In Chapter 3, the Acme Corporation has chosen the Internal – Qualitative – Management combination using the CRC Tool. They decided to conduct a self-assessment to understand the internal view of its cyber risk level. The Acme Corporation chooses to adopt the Qualitative component with the NIST cybersecurity risk assessment. For the Management component, they will be reviewing cyber risk results bi-weekly and making changes based on the reviews. SIEM tools and KPIs are also adopted to measure and manage cyber risk. This corresponds to the phase of 'Decide What To Do' in Figure 4-6.

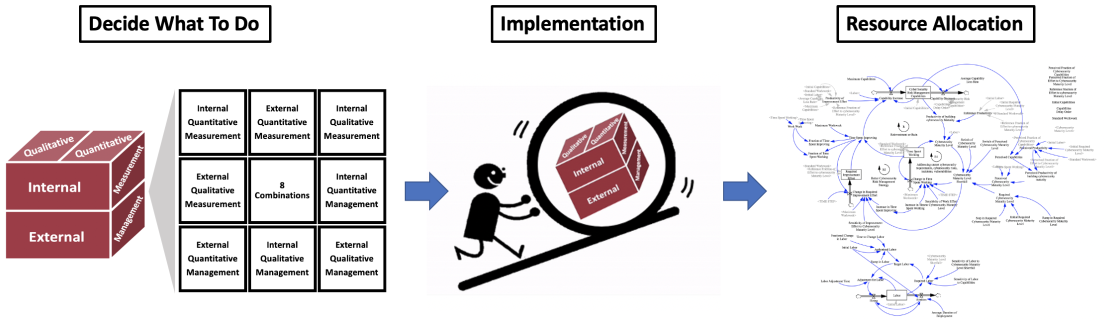

Decide What To Do
Implementation
Resource Allocation
Qualitative
Quantitative
Internal
External
Measurement
Management
Internal Quantitative Measurement
External Quantitative Measurement
Internal Qualitative Measurement
External Qualitative Measurement
8 Combinations
Internal Quantitative Management
External Quantitative Management
Internal Qualitative Management
External Qualitative Management

Figure 4-6: The flow chart of the CRC Tool and the System Dynamics Model

After successfully implementing their primary strategy, the Acme management plans to implement multiple approaches in the Internal component. For example, Acme management intends to conduct an additional internal audit and review cyber risk results weekly instead of bi-weekly to have a more holistic and deeper understanding of its cyber risk level.

The Acme management utilizes the System Dynamics Model to optimize its resource allocation in the Internal and Management components, which corresponds to the 'Resource Allocation' phase in Figure 4-6. For example, Acme management can add up to 10 employees to work on the internal audit or the weekly cyber risk results review. They are not sure how many staff should be assigned to do the internal audit to reach the highest efficiency and they decided to use the System Dynamics model to resolve this issue. In Plan A, they assign more staff to review cyber risk results on a

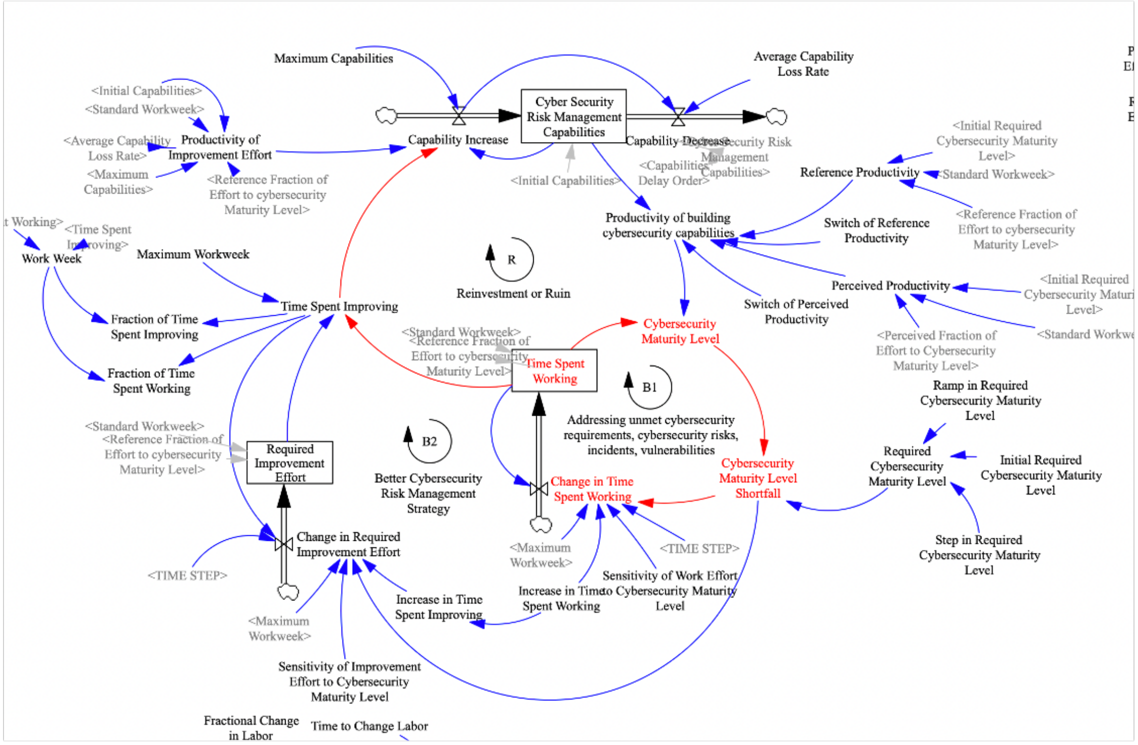

Maximum Capabilities
<Initial Capabilities>
<Standard Workweek>
<Average Capability Loss Rate>
Productivity of Improvement Effort
<Maximum Capabilities>
<Reference Fraction of Effort to cybersecurity Maturity Level>
Capability Increase
Cyber Security Risk Management Capabilities
<Initial Capabilities>
Capability Decrease
<Cyber Security Risk Management Capabilities>
<Capabilities Delay Order>
Average Capability Loss Rate
<Initial Required Cybersecurity Maturity Level>
Reference Productivity
<Standard Workweek>
<Reference Fraction of Effort to cybersecurity Maturity Level>
Productivity of building cybersecurity capabilities
Switch of Reference Productivity
Perceived Productivity
<Initial Required Cybersecurity Maturi Level>
Switch of Perceived Productivity
<Perceived Fraction of Effort to Cybersecurity Maturity Level>
<Standard Workwe
t Working>
<Time Spent Improving>
Work Week
Maximum Workweek
R
Reinvestment or Ruin
Time Spent Improving
Fraction of Time Spent Improving
Fraction of Time Spent Working
<Standard Workweek>
<Reference Fraction of Effort to cybersecurity Maturity Level>
Time Spent Working
Cybersecurity Maturity Level
B1
Addressing unmet cybersecurity requirements, cybersecurity risks, incidents, vulnerabilities
Ramp in Required Cybersecurity Maturity Level
<Standard Workweek>
<Reference Fraction of Effort to cybersecurity Maturity Level>
Required Improvement Effort
B2
Better Cybersecurity Risk Management Strategy
Change in Time Spent Working
Cybersecurity Maturity Level Shortfall
Required Cybersecurity Maturity Level
Initial Required Cybersecurity Maturity Level
<TIME STEP>
Change in Required Improvement Effort
<Maximum Workweek>
<TIME STEP>
Sensitivity of Work Effort to Cybersecurity Maturity Level
Increase in Time Spent Working
Increase in Time Spent Improving
Step in Required Cybersecurity Maturity Level
<Maximum Workweek>
Sensitivity of Improvement Effort to Cybersecurity Maturity Level
Fractional Change in Labor
Time to Change Labor

Figure 4-7: A Close-up View of System Dynamics model optimizing resource allocation: Working Harder

weekly instead of bi-weekly basis, leaving the remaining staff to conduct the internal audit. The action of adding more staff to review cyber risk results will lead to the 'Working Harder Loop' shown in Figure 4-3 as they try to reduce more vulnerabilities to improve cyber resilience. The Time Spent Working will increase, which leads to an immediate rise in cyber resilience and reduces their cyber risk immediately, as shown in red on Figure 4-7. This scenario will also have an indirect contribution to the cybersecurity maturity level. However, Plan A does not have any long-term value and the Acme Corporation may eventually exhaust its resources to resolve its shortfall in cybersecurity maturity.

In Plan B, the Acme management may add fewer employees to review cyber risk results weekly instead of bi-weekly and instead assign more employees to conduct the internal audit. This triggers the 'Working Smarter Loop' shown in Figure 4-4. The Required Improvement Effort will increase, resulting in a rise in the Time Spent Improving as shown in red on Figure 4-8. However, they will encounter a delay in the growth of Cybersecurity Risk Management Capabilities, often called Worse Before Better. The Acme Corporation will suffer worse performance for a while and then have a rapid growth in the Cybersecurity Risk Management Capabilities afterward, which leads to a massive increase in both cyber resilience and the cybersecurity maturity level in the long term.

The Acme Corporation may simulate different frequencies of reviewing cyber risk results and various resource allocation plans for self-assessment and internal audit using the System Dynamics model. After testing multiple resource allocation strategies in the simulation environment, the Acme Corporation can then decide to implement the plans leading to success modes and avoid the ones that may lead them to common pitfalls in cybersecurity and failure modes.

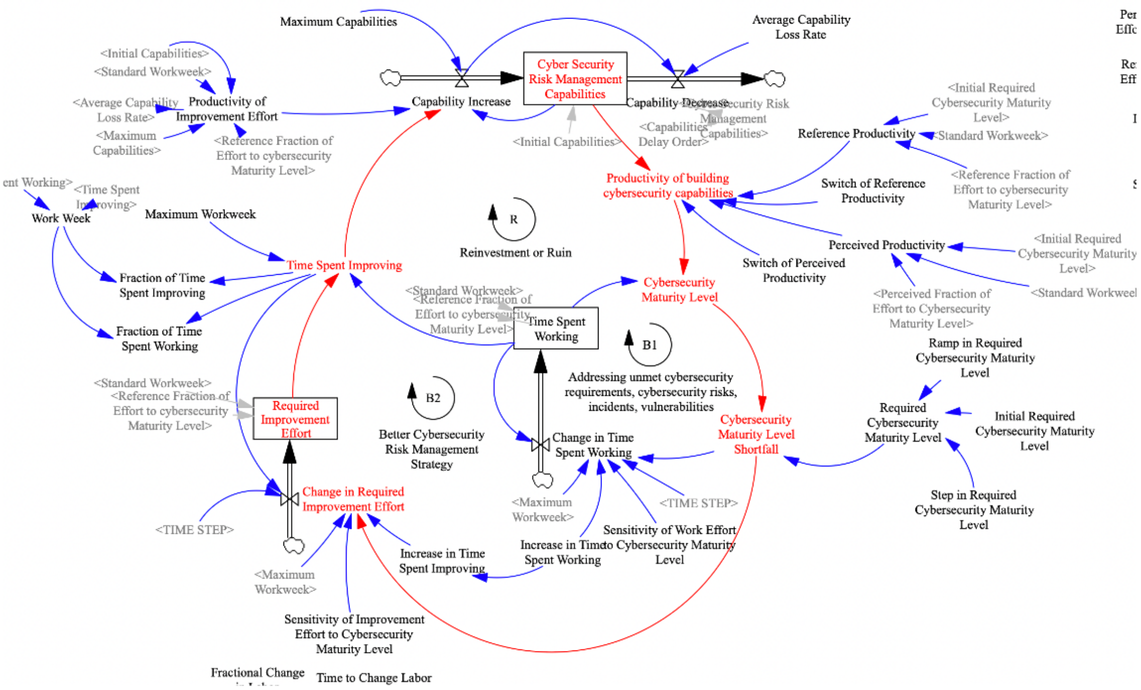

Maximum Capabilities
Average Capability Loss Rate
Per Effc
Re Eff
I
S
<Initial Capabilities>
<Standard Workweek>
<Average Capability Loss Rate>
Productivity of Improvement Effort
<Maximum Capabilities>
<Reference Fraction of Effort to cybersecurity Maturity Level>
Capability Increase
Cyber Security Risk Management Capabilities
Capability Decrease
ecurity Risk Management Capabilities>
<Initial Capabilities>
<Capabilities Delay Order>
<Initial Required Cybersecurity Maturity Level>
Reference Productivity
<Standard Workweek>
<Reference Fraction of Effort to cybersecurity Maturity Level>
Switch of Reference Productivity
Productivity of building cybersecurity capabilities
ent Working>
<Time Spent Improving>
Work Week
Maximum Workweek
R
Reinvestment or Ruin
Perceived Productivity
<Initial Required Cybersecurity Maturity Level>
Switch of Perceived Productivity
<Standard Workweel
<Perceived Fraction of Effort to Cybersecurity Maturity Level>
Time Spent Improving
Fraction of Time Spent Improving
Fraction of Time Spent Working
<Standard Workweek>
<Reference Fraction of Effort to cybersecurity Maturity Level>
Time Spent Working
Cybersecurity Maturity Level
B1
Addressing unmet cybersecurity requirements, cybersecurity risks, incidents, vulnerabilities
Ramp in Required Cybersecurity Maturity Level
Required Cybersecurity Maturity Level
Initial Required Cybersecurity Maturity Level
<Standard Workweek>
<Reference Fraction of Effort to cybersecurity Maturity Level>
Required Improvement Effort
B2
Better Cybersecurity Risk Management Strategy
Change in Time Spent Working
Cybersecurity Maturity Level Shortfall
Change in Required Improvement Effort
<TIME STEP>
<Maximum Workweek>
<TIME STEP>
Step in Required Cybersecurity Maturity Level
Sensitivity of Work Effort to Cybersecurity Maturity Level
Increase in Time Spent Working
Increase in Time Spent Improving
<Maximum Workweek>
Sensitivity of Improvement Effort to Cybersecurity Maturity Level
Fractional Change in Labor
Time to Change Labor

Figure 4-8: A Close-up View of System Dynamics model optimizing resource allocation: Working Smarter

Chapter 5

Conclusions

This thesis examines the primary cybersecurity risk management methodologies and the complex interaction, dynamics, and tradeoffs in the cybersecurity environment to propose a holistic, simplified and systematic Cybersecurity Risk Management strategy. The literature review was conducted to provide an overview of a variety of approaches currently used in cybersecurity risk management and found in academic literature for managing cybersecurity risk. The history of cybercrime was explored to better understand the damages caused by cybersecurity attacks faced by organizations. Understanding the cyber risks present contextualizes the need for a comprehensive cybersecurity risk management strategy and the optimization of resource allocation within organizations. A Cyber Risk Cube (CRC) Tool was designed and built to equip organizations with a roadmap for developing fundamental cybersecurity risk management strategies. A System Dynamics Model was created to provide a broad perspective of the organization's ecosystem, resource allocation and a better understanding of the potential interactions between cyber risk management components and common traps.

Using the CRC Tool, the method begins by identifying the appropriate cyber risk strategies for organizations. The ideal combination for their culture and environment can then be applied, and resource allocation can be refined using the System Dynamics Model.

5.1 Lessons Learned

Identifying the six components of the CRC Tool presented several obstacles. It was difficult to break down cybersecurity into a few components and make it intuitively apparent for organizations new to the field because cybersecurity is complex and intangible. In a similar vein, it was challenging to pin down critical but straightforward cyber risk management components to guide organizations of all sizes and industries in developing their cyber risk strategy. The issue was resolved by collaborating with cybersecurity executives from various organizations and incorporating the expertise of cybersecurity professionals.

Establishing the tradeoffs and interactions between the System Dynamics Model variables was another challenge in this work. According to the literature review in Chapter 2, no current research on cybersecurity capability traps exists. As a result, there was little direction for developing a cybersecurity system dynamics model that identified all conceivable and crucial interactions, dynamics, and tradeoffs among all variables in the complex cybersecurity environment. Consulting system dynamics expert Daniel Goldsmith and following Lyneis, J., and Sterman, J. [95] handled this problem. Lyneis, J., and Sterman, J. proposed the failure of win-win investments in sustainability and social responsibility due to capability traps.

5.2 Future Work

The author identifies several promising directions for future research. First, researchers can conduct studies of breached companies and categorize their cyber risk management strategy into the eight combinations of the CRC tool. It would be interesting to observe the relationships and trends between the combinations and the breached cases. Secondly, researchers can increase the existing work scope by collecting more study samples for the System Dynamics Model, applying a numerical model of the generated causal loop diagram, and doing a propagation index analysis to understand the role of each auxiliary variable. This expanded scope seeks to identify more cybersecurity dynamics and tradeoffs. Lastly, researchers can work with leaders from different company sizes to employ the CRC tool and the System Dynamics model in pilot studies, validating the applicability of this work.

Appendix A

Cases Narrative

A.1 Internal - Quantitative – Management

Large Financial Organization

- **ID**: 1
- **Company Name**: LPL Financial
- **Filter Variables**

  Industry = Financial;

  Size = Large;

  Budget = N/A;

  Rationale = Compliance;

  Combination = #1 Internal-Quantitative-Management

- **Narrative**

  LPL Financial is a platform for independent financial analysts, with $615 billion in assets. Teams for enterprise and technology risk and audit had no consistent definitions, often interchanging terms for risk, threat, vulnerability and impact, so there was a need for consistent language.

LPL is using the RiskLens to make internal audits more effective and better communicate their results by merging the FAIR framework – Quanitative method – with Enterprise Risk Management. Every internal audit finding is run through RiskLens. FAIR prioritizes investments in risk management by measuring how much residual risk is reduced [116].

Large Bank

- **ID**: 2
- **Company Name**: Investors Bank
- **Filter Variables**

  Industry = Banking;

  Size = Large;

  Budget = N/A;

  Rationale = Compliance;

  Combination = #1 Internal-Quantitative-Management
- **Narrative**

  The Investors Bank is a publicly traded, full-service bank that operates over 150 branches across New Jersey and New York. The Investors Bank decided to take compliance one-step further. It focuses on creating a culture of not only compliance but also resilient security to protect their customers, employees and partners. Hence, managing cyber risk efficiently and effectively is one of their challenges.

  The bank uses Frontline VM, a vulnerability management software to perform the work of running scans, analyzing the results, generating reports, and providing direct remediation planning guidance. The bank also establishes Key Risk Indicators (KRIs) and metrics to measure and manage risk frequently [117].

Medium Technology Organization

- **ID**: 3
- **Company Name**: Axcient, Inc.
- **Filter Variables**

  Industry = Technology;

  Size = Medium;

  Budget = N/A;

  Rationale = Customer's requirements;

  Combination = #1 Internal-Quantitative-Management

- **Narrative**

  Axcient, Inc. is a medium-sized United States-based data service organization with around 300 employees. Managed Service Providers (MSPs) use data backup and recovery solutions, like Axcient, to provide their customers with continuous access to business-critical services and information. If the cloud service provider experiences a data breach or leakage, the MSP is responsible for any of their customers' information impacted. Axcient manages cyber risk in order to fulfill their customer's requirement.

  Axcient uses SecurityScorecard's security rating system to review performance and ensure that their continuous monitoring also leads to ongoing compliance for a strong security posture. To strengthen their cybersecurity culture, Axcient posts their daily security rating in the office, leading to staff taking greater care of cybersecurity [118].

A.2 Internal - Quantitative – Measurement

Large Technology Organization

- **ID**: 4

- **Company Name**: Anonymous
- **Filter Variables**

  Industry = Technology;

  Size = Large;

  Budget = N/A;

  Rationale = Compliance;

  Combination = #2 Internal-Quantitative-Measurement
- **Narrative**

  A large technology organization turned to the RiskLens platform to address cyber risk assessment. The tech organization is subject to reporting to the Securities and Exchange Commission (SEC). In 2018, the SEC announced a guide to assist public companies in preparing disclosures about cybersecurity risks and incidents. The tech organization was only using qualitative heat maps before turning to the RiskLens platform when they quickly noticed that the qualitative approach was not enough to meet the SEC's requirement [119].

A.3 Internal - Qualitative – Management

Large Medical Center

- **ID**: 5
- **Company Name**: University of Kansas Medical Center (KUMC)
- **Filter Variables**

  Industry = Healthcare;

  Size = Large;

  Budget = N/A;

  Rationale = Compliance;

Combination = #3 Internal-Qualitative-Management

- **Narrative**

  The University of Kansas Medical Center (KUMC) is an Academic Health Center in Kansas City, Kansas with approximately 3,600 employees and 3,500 students. KUMC's Office of Information Security (OIS) is a relatively new department that formerly existed as a sub-unit of the IT Department.

  The Information Security team at KUMC is using the Baldrige Cybersecurity Excellence Builder in conjunction with the NIST Cybersecurity Framework for self-assessment and program development. This process helped the team to better understand their own roles and to engage their customers in protecting the organization. This process has helped the Information Security Team establish a better approach to intake, response, and follow-up, improving stakeholder relationships and getting the right solutions to their customers [110].

Large Retail Organization

- **ID**: 6

- **Company Name**: McColl's Retail Group

- **Filter Variables**

  Industry = Retail;

  Size = Large;

  Budget = N/A;

  Rationale = Compliance;

  Combination = #3 Internal-Qualitative-Management

- **Narrative**

  The McColl's Retail Group is a large retailer with over 18,652 employees and 1500 convenience stores and news agents across England, Scotland and Wales.

Convenience retailer McColl needs to stay compliant with the Payment Cards Industry (PCI) regulations and thus, decided to find a suitable security solution to address cyber risk.

McColl's Retail Group chooses to use this combination of the cyber risk cube by implementing the LogRhythm NextGen SIEM Platform. To ensure they stay compliant, the SIEM Platform can create personalized security alerts, helping McColl keep its high volumes of transactions safe [120].

Large Technology Organization

- **ID**: 7
- **Company Name**: Alibaba Cloud
- **Filter Variables**

  Industry = Technology;

  Size = Large;

  Budget = N/A;

  Rationale = Compliance;

  Combination = #3 Internal-Qualitative-Management
- **Narrative**

  Alibaba Cloud is one of the world's leading cloud computing service providers, and the leading cloud computing service provider in China, providing services for innovative enterprises and organizations around the world.Alibaba Cloud is committed to providing reliable, secure, and compliant cloud computing products and services. They need to stay compliant with more than 30 regulations, standards, framework, etc.

  Alibaba Cloud has established a risk management framework to identify, analyze and manage risks within the organization and those related to services provided. The risk management framework involves management and various teams, and covers strategic and operational risks, such as security and availability. The comprehensive risk management system is created in accordance with the ISO27001:2013 Standard, which requires an information security risk assessment to be carried out annually [121].

The organization uses a qualitative risk assessment method that calculates risk rating for changes based on potential impact. Likelihood of occurrence is also computed to ensure more additional resources and control measures are dedicated to higher risks.

Large Bank

- **ID**: 8
- **Company Name**: Standard Chartered PLC
- **Filter Variables**

  Industry = Banking;

  Size = Large;

  Budget = N/A;

  Rationale = Compliance;

  Combination = #3 Internal-Qualitative-Management
- **Narrative**

  Standard Chartered PLC is a large banking and financial services organization headquartered in London with more than 1,200 branches and outlets (including subsidiaries, associates and joint ventures) across over 70 countries, employing around 87,000 people. It is a universal bank with operations in consumer, corporate and institutional banking, and treasury services.

  The Standard Chartered bank defines Information and Cyber Security (ICS) Risk as the potential for loss from a breach of confidentiality, integrity or availability of the bank's information systems and assets through cyber-attack, insider activity, error or control failure. Hence, they have been managing cyber risk [122].

In 2018, the bank approved a Risk Type Framework (RTF) to formally set out the Group-wide strategy for managing cyber risk. ICS Risk is managed through a structured ICS Policy Framework comprised of a risk assessment methodology and supporting policies, procedures and standards that are aligned to industry best practice models. The bank also monitors and reports on the risk appetite profile to ensure that performance which falls outside the approved risk appetite is highlighted and reviewed at the appropriate levels.

A.4 Internal - Qualitative – Measurement

Small Healthcare Clinic

- **ID**: 9
- **Company Name**: Anonymous
- **Filter Variables**

  Industry = Healthcare;

  Size = Small;

  Budget = N/A;

  Rationale = Compliance;

  Combination = #4 Internal-Qualitative-Measurement
- **Narrative**

  This small healthcare clinic employs five people and uses eight stationary computing devices. A cloud service provider (CSP) is used as the primary method to handle roughly 1,600 patient ePHI records. The clinic has no dedicated IT personnel and so the owner took on all IT and security-related responsibilities. Since that information security risk assessments in the healthcare industry are legally required and demand an ongoing investment of time and resources, the small dental clinic decided to use the assessment tool recommended by the federal government(the SRA tool) [123, 124].

The clinic chooses to use measurement due to limited staff number by implementing an internal security system that included motion alarms and locks. The system was periodically tested to confirm it was in working order.

The small dental clinic is using the Security Risk Assessment (SRA) Tool provided by HealthIT.gov to cover the main benchmarks required by law. This tool was chosen because it is recommended by the federal government for the healthcare industry.

A.5 External – Quantitative – Measurement

Large Financial Organization

- **ID**: 10
- **Company Name**: Anonymous
- **Filter Variables**

  Industry = Financial;

  Size = Large;

  Budget = N/A;

  Rationale = Compliance;

  Combination = #5 External-Quantitative-Measurement
- **Narrative**

  This global financial firm is a leader in commercial banking with thousands of business partners around the world.

  The firm shares sensitive data with thousands of partners around the world. They were assessing the security risk of their third-party business relationships with annual questionnaires and audits, but this was not enough to enable the level of risk-based decision making the organization made in other areas of their business.

Using BitSight Security Ratings for Third Party Risk Management, the firm receives timely, data-driven analysis of a partner's security effectiveness. New ratings are generated on a daily basis, giving organizations continuous visibility into the security of their assets so the firm doesn't have to rely on subjective responses in questionnaires [125].

Large Lending Cooperative

- **ID**: 11
- **Company Name**: Farm Credit Mid-America
- **Filter Variables**

  Industry = Lending;

  Size = Large;

  Budget = N/A;

  Rationale = Compliance;

  Combination = #5 External-Quantitative-Measurement
- **Narrative**

  Farm Credit Mid-America is one of the largest agricultural lending cooperatives in the U.S. Farm Credit System, employing more than 1,100 people and serving more than 100,000 customers across Indiana, Ohio, Kentucky, and Tennessee The organization's vendors are not required to adhere to the same regulatory oversight so may have lower security standards. Farm Credit was relying on point in time assessments and questionnaires to review vendor risk, but that lead to ineffective resource allocation, inaccurate security data and limited visibility into security risks.

Farm Credit now uses SecurityScorecard to monitor, and report on the cyber health of its own IT infrastructure via an outside-in view This enables Farm Credit to proactively assess all connected third-party vendor environments and gain visibility into the organization's ecosystem risk [126].

A.6 External – Quantitative – Management

Large Healthcare Non-profit Organization

- **ID**: 12

- **Company Name**: Children's Hospital of Minnesota

- **Filter Variables**

  Industry = Healthcare;

  Size = Large;

  Budget = N/A;

  Rationale = Compliance;

  Combination = #6 External-Quantitative-Management

- **Narrative**

  Children's Hospital of Minnesota is a largest healthcare non-profit in the United States, with two hospitals.

  The organization was looking into selecting a security benchmark and policy that is meaningful and then sourcing the information to measure against that benchmark. Using the SecurityScoreCard platform, the CISO could frequently pull information on hospital systems in Boston, Seattle, Texas, and Colorado and see how their scores compared to Children's Minnesota in one comprehensive view [127].

Large institutional investment network

- **ID**: 13
- **Company Name**: Liquidnet
- **Filter Variables**

  Industry = Financial;

  Size = Large;

  Budget = N/A;

  Rationale = Compliance;

  Combination = #6 External-Quantitative-Management
- **Narrative**

  Liquidnet is the global institutional trading network where the world's top asset managers, managing over 15 trillion dollars in assets, come to execute their large equity trades. Liquidnet was relying on self-reported information provided by the vendors but needed to insure they were complying with third-party review requirements of customers and regulators. With SecurityScorecard Liquidnet could quantify the security performance of their vendors and provide continuous monitoring. The alternative to using SecurityScorecard for Liquidnet would have been to hire more employees in an attempt to make vendor assessments more frequent and more accurate, an expensive investment that could not come close to the capabilities of using a continuous monitoring platform [128].

A.7 External – Qualitative – Management

Large Financial Organization

- **ID**: 14
- **Company Name**: Blackstone

- **Filter Variables**

  Industry = Financial;

  Size = Large;

  Budget = N/A;

  Rationale = Efficiency;

  Combination = #7 External-Qualitative-Management

- **Narrative**

  Blackstone is an alternative investment management and financial services firm. It specializes in private equity, credit, and hedge fund investment strategies. Blackstone's third-party risk management programs relied on phone calls and spreadsheets, but this caused problems as the number of vendors grew and the number of different methodologies each used. Using CyberGRX's platform, Blackstone could develop a more efficient risk management program that helps them prioritize risk. Realizing the quantitative aspect of ranking vendors by risk is not enough, they also engage in risk-based discussions with vendors and business partners to gather qualitative data and assess how to mitigate risk [129].

A.8 External – Qualitative – Measurement

Large Technology Organization

- **ID**: 15

- **Company Name**: Alibaba Cloud

- **Filter Variables**

  Industry = Technology;

  Size = Large;

Budget = N/A;

Rationale = Compliance;

Combination = #8 External-Qualitative-Measurement

- **Narrative**

  Alibaba Cloud is one of the world's leading cloud computing service providers, and the leading cloud computing service provider in China, providing services for innovative enterprises and organizations around the world.

  Alibaba Cloud is committed to providing reliable, secure, and compliant cloud computing products and services. They need to stay compliant with more than 30 regulations, standards, framework, etc. For external view of the third parties' risk level, they regularly complete third-party audits. The organization uses a qualitative risk assessment method which calculates risk rating for changes based on potential impact. Likelihood of occurrence is also computed to ensure more additional resources and control measures are dedicated to higher risks [121].

Appendix B

Tools and Techniques

B.1 Internal

1. ***Yearly Internal Security Audit***

   ID: 1.1

   Component: Internal

   Technique/Tool name: Yearly Internal Security Audit

   Technique/Tool info: Internal Audit is the 3rd Line of Defense, which independently assess cyber risk management program effectiveness, report it to the board.

2. ***Self-assessment***

   ID: 1.2

   Component: Internal

   Technique/Tool name: Self-assessment

   Technique/Tool info: A self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts.

3. ***Control for external assessment***

   ID: 1.3

Component: Internal

Technique/Tool name: Control for external assessment

Technique/Tool info: It can be used to reduce the internal view of the organization's cyber risk.

B.2 External

1. ***Onsite/Offsite Vendor Audit***

   ID: 2.1

   Component: External

   Technique/Tool name: Onsite/Offsite Vendor Audit

   Technique/Tool info: When organizations want to understand third parties' cyber risk level, they can perform vendor audit to identify, monitor, and audit their preparedness.

2. ***US Treasury OCC: Third-Party Relationships – Risk Management Guidance***

   ID: 2.2

   Component: External

   Technique/Tool name: US Treasury OCC: Third-Party Relationships – Risk Management Guidance

   Technique/Tool info: This provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships.

3. ***Due Diligence***

   ID: 2.3

   Component: External

Technique/Tool name: Due Diligence

Technique/Tool info: An organization should have a process to evaluate the current threat landscape and identify the bad actors – external and internal – that might target the parties in the transaction. This landscape can vary by industry or region, and higher risk transactions – such as organizations in certain countries or in sectors that have suffered recent attacks – require greater diligence.

B.3 Qualitative

1. ***FFIEC Cybersecurity Assessment Tool (CAT)***

   ID: 3.1

   Component: Qualitative

   Technique/Tool name: FFIEC Cybersecurity Assessment Tool (CAT)

   Technique/Tool info: The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time.

2. ***OSFI Cyber Security Self-Assessment***

   ID: 3.2

   Component: Qualitative

   Technique/Tool name: OSFI Cyber Security Self-Assessment

   Technique/Tool info: This self-assessment template sets out desirable properties and characteristics of cyber security practices that could be considered by a FRFI when assessing the adequacy of its cyber security framework and when planning enhancements to its framework.

3. ***FSSCC Cybersecurity Profile***

   ID: 3.3

   Component: Qualitative

Technique/Tool name: FSSCC Cybersecurity Profile

Technique/Tool info: The Profile is a scalable and extensible assessment that financial institutions of all types can use for internal and external (i.e., third party) cyber risk management assessment and as a mechanism to evidence compliance with various regulatory frameworks (a "common college application for regulatory compliance") both within the United States and globally.

4. ***ICSCERT – Cyber Security Evaluation Tool (CSET)***

   ID: 3.4

   Component: Qualitative

   Technique/Tool name: ICSCERT – Cyber Security Evaluation Tool (CSET)

   Technique/Tool info: CISA assessment products improve situational awareness and provide insight, data, and identification of control systems threats and vulnerabilities. Core assessment products and services include self-assessments using the Cybersecurity Evaluation Tool (CSET®), onsite field assessments, network design architecture reviews, and network traffic analysis and verification. The information gained from assessments also provides stakeholders with the understanding and context necessary to build effective defense-in-depth processes for enhancing cybersecurity.

5. ***HKMA – Cyber Resilience Assessment Framework Tool (CRAF)***

   ID: 3.5

   Component: Qualitative

   Technique/Tool name: HKMA – Cyber Resilience Assessment Framework Tool (CRAF)

   Technique/Tool info: It can be used to determine the inherent riskiness of an institution.

6. ***Building Security in Maturity Model (BSIMM)***

   ID: 3.6

Component: Qualitative

Technique/Tool name: Building Security in Maturity Model (BSIMM)

Technique/Tool info: An effective tool for understanding how organizations of all shapes and sizes, including some of the most advanced security teams in the world, are executing their software security strategies.

B.4 Quantitative

1. ***Factor Analysis of Information Risk (FAIR)***

   ID: 4.1

   Component: Quantitative

   Technique/Tool name: Factor Analysis of Information Risk (FAIR)

   Technique/Tool info: It provides information risk, cybersecurity and business executives with the standards and best practices to help organizations measure, manage and report on information risk from the business perspective.

2. ***BCG Cyber Doppler***

   ID: 4.2

   Component: Quantitative

   Technique/Tool name: BCG Cyber Doppler

   Technique/Tool info: BCG's Cyber Doppler tool builds on this insight, enabling companies to better understand their cyber risks and controls. It quantifies the likelihood of a cyber-attack occurring as well as the impact of a successful attack.

3. ***Aggregate reporting using risk appetite and Loss Exceedance Curves (LEC)***

   ID: 4.3

   Component: Quantitative

Technique/Tool name: Aggregate reporting using risk appetite and Loss Exceedance Curves (LEC)

Technique/Tool info: It can be used to assess and report on existing risk visibility and operations metrics.

4. ***ICSCERT – Cybersecurity Argument Graph Evaluation (CyberSAGE)***

   ID: 4.4

   Component: Quantitative

   Technique/Tool name: Cybersecurity Argument Graph Evaluation (CyberSAGE)

   Technique/Tool info: CyberSAGE can combine numerical information to compute quantitative security assessment results.

5. ***Lucideus – Security Assessment Framework for Enterprise (SAFE)***

   ID: 4.5

   Component: Quantitative

   Technique/Tool name: Lucideus – Security Assessment Framework for Enterprise (SAFE)

   Technique/Tool info: An Enterprise Wide, Objective, Unified, Real Time Cyber Risk Quantification (CRQ) platform which incorporates both technical and business aspects with an output for prioritized decision making.

6. ***BitSight's Security Ratings Platform***

   ID: 4.6

   Component: Quantitative

   Technique/Tool name: BitSight's Security Ratings Platform

   Technique/Tool info: It can be used to make data-driven decisions to reduce cyber risk.

7. ***UpGuard***

   ID: 4.7

   Component: Quantitative

   Technique/Tool name: UpGuard

   Technique/Tool info: It can continuously improve the organization's cybersecurity rating, detect data exposures, and control third-party risk.

8. ***SecurityScoreCard***

   ID: 4.8

   Component: Quantitative

   Technique/Tool name: SecurityScoreCard

   Technique/Tool info: Enable security and risk management teams to reduce vulnerabilities before attackers can exploit them.

B.5 Measurement

1. ***KPI conducted yearly/quarterly to track and manage cyber risk***

   ID: 5.1

   Component: Measurement

   Technique/Tool name: KPI conducted yearly/quarterly to track and manage cyber risk

   Technique/Tool info: Key performance indicators (KPIs) are an effective way to measure the success of the organization's cybersecurity program and aid in decision-making.

2. ***Periodic security goal evaluation***

   ID: 5.2

   Component: Measurement

Technique/Tool name: Periodic security goal evaluation

Technique/Tool info: Organization can conduct security goal evaluation periodically to measure cyber risk.

B.6 Management

1. ***KPI conducted yearly/quarterly to track and manage cyber risk***

   ID: 6.1

   Component: Management

   Technique/Tool name: KPI conducted yearly/quarterly to track and manage cyber risk

   Technique/Tool info: Key performance indicators (KPIs) are an effective way to measure the success of the organization's cybersecurity program and aid in decision-making.

2. ***Security Information and Event Management (SIEM) tools used daily for cyber risk management***

   ID: 6.2

   Component: Management

   Technique/Tool name: Security Information and Event Management (SIEM) tools used daily for cyber risk management

   Technique/Tool info: It can be used to review log and event data from a business' networks, systems and other IT environments, understand cyber threats, cyber risk and prepare accordingly.

Appendix C

System Dynamics Full Model

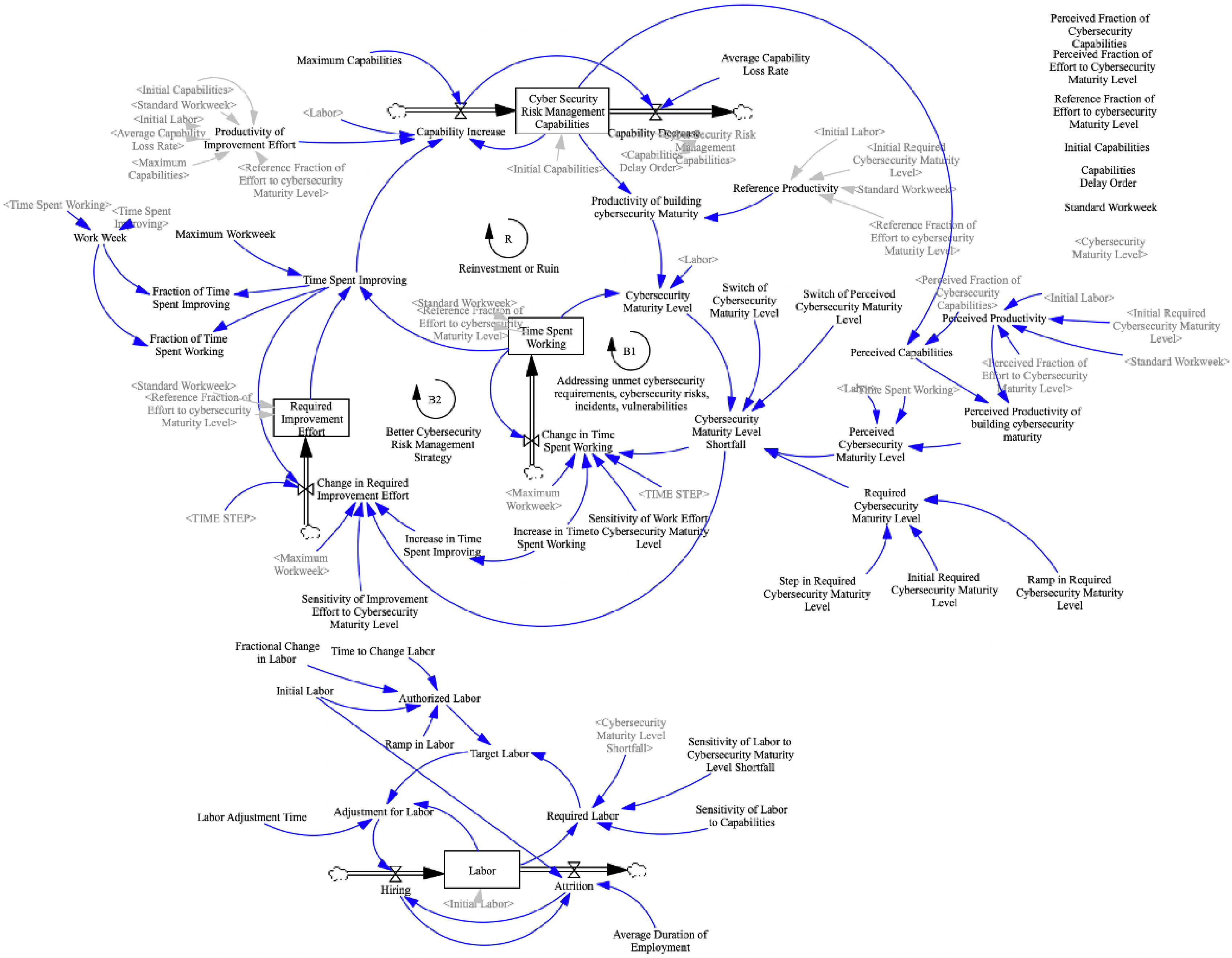

Maximum Capabilities
Cyber Security Risk Management Capabilities
Average Capability Loss Rate
<Initial Capabilities>
<Standard Workweek>
<Initial Labor>
<Average Capability Loss Rate>
<Maximum Capabilities>
Productivity of Improvement Effort
<Reference Fraction of Effort to cybersecurity Maturity Level>
<Labor>
Capability Increase
Capability Decrease
<Cyber Security Risk Management Capabilities>
<Capabilities Delay Order>
<Initial Capabilities>
Productivity of building cybersecurity Maturity
<Initial Labor>
<Initial Required Cybersecurity Maturity Level>
Reference Productivity
<Standard Workweek>
<Reference Fraction of Effort to cybersecurity Maturity Level>
Perceived Fraction of Cybersecurity Capabilities
Perceived Fraction of Effort to Cybersecurity Maturity Level
Reference Fraction of Effort to cybersecurity Maturity Level
Initial Capabilities
Capabilities Delay Order
Standard Workweek
<Cybersecurity Maturity Level>
<Time Spent Working>
<Time Spent Improving>
Work Week
Maximum Workweek
Time Spent Improving
R
Reinvestment or Ruin
Fraction of Time Spent Improving
Fraction of Time Spent Working
<Standard Workweek>
<Reference Fraction of Effort to cybersecurity Maturity Level>
Time Spent Working
<Labor>
Cybersecurity Maturity Level
Switch of Cybersecurity Maturity Level
Switch of Perceived Cybersecurity Maturity Level
<Perceived Fraction of Cybersecurity Capabilities>
<Initial Labor>
Perceived Productivity
<Initial Required Cybersecurity Maturity Level>
<Standard Workweek>
Perceived Capabilities
<Perceived Fraction of Effort to Cybersecurity Maturity Level>
B1
Addressing unmet cybersecurity requirements, cybersecurity risks, incidents, vulnerabilities
<Labor>
<Time Spent Working>
Perceived Productivity of building cybersecurity maturity
<Standard Workweek>
<Reference Fraction of Effort to cybersecurity Maturity Level>
Required Improvement Effort
B2
Better Cybersecurity Risk Management Strategy
Change in Time Spent Working
Cybersecurity Maturity Level Shortfall
Perceived Cybersecurity Maturity Level
Change in Required Improvement Effort
<TIME STEP>
<Maximum Workweek>
<TIME STEP>
Sensitivity of Work Effort to Cybersecurity Maturity Level
Increase in Timeto Cybersecurity Maturity Level
Spent Working
Increase in Time Spent Improving
Increase in Time Spent Working
Required Cybersecurity Maturity Level
<Maximum Workweek>
Sensitivity of Improvement Effort to Cybersecurity Maturity Level
Step in Required Cybersecurity Maturity Level
Initial Required Cybersecurity Maturity Level
Ramp in Required Cybersecurity Maturity Level
Fractional Change in Labor
Time to Change Labor
Initial Labor
Authorized Labor
Ramp in Labor
Target Labor
<Cybersecurity Maturity Level Shortfall>
Sensitivity of Labor to Cybersecurity Maturity Level Shortfall
Labor Adjustment Time
Adjustment for Labor
Required Labor
Sensitivity of Labor to Capabilities
Hiring
Labor
Attrition
<Initial Labor>
Average Duration of Employment

Figure C-1: The full causal loop diagram of cybersecurity risk management strategy model

Bibliography

[1] S. Kemp, "Digital 2020: July global statshot," *DataReportal*, July 2020.

[2] H. Lallie *et al.*, "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, vol. 105, June 2021.

[3] T. Chiu, "90% of companies faced increased cyberattacks during covid-19," *K2 Cybersecurity*, Dec. 2020.

[4] R. Sobers, "98 must-know data breach statistics for 2021," *Varonis*, May 2021.

[5] F. Perumannil, Sabir & Haneef, "Latest trends in cybersecurity after solarwind hacking attack," *Journal of Cyber Security and Mobility*, vol. 1, Jan. 2021.

[6] Department of Financial Services, "Twitter investigation report," Oct. 2020.

[7] M. D. Rasch and A. Nixon, "How the coronavirus enabled the twitter hack (*and others too)," *Unit 221B Blog*, July 2020.

[8] L. Mathews, "For sale: Hacked data on 142 million mgm hotel guests," *Forbes*, July 2020.

[9] J. Maddison, "The problem with too many security options," *CSO Magazine*, May 2019.

[10] S. Calif, "Cybercrime to cost the world $10.5 trillion annually by 2025," *Cybercrime Magazine*, Nov. 2020.

[11] S. Acharjee, "The history of cybercrime: A comprehensive guide(2021)," *Jigsaw Academy*, 2021.

[12] T. M. Chen and J.-M. Robert, "The evolution of viruses and worms," *Statistical methods in computer security*, vol. 1, no. 16, 2004.

[13] V. Swarnakamali and D. Roshni, "Cybercrime–a threat to network security," *International Journal of Computer Science Trends and Technology (IJCST)*, vol. 5, July 2017.

[14] D. S. Griffith, "The computer fraud and abuse act of 1986: A measured response to a growing problem," *Vanderbilt Law Review*, vol. 43, no. 2, 1990.

[15] K. Hafner and J. Markoff, “Cyberpunk: Outlaws and hackers on the computer frontier,” *Simon & Schuster*, 1991.

[16] W. Scherlis, “Darpa establishes computer emergency response team,” *DARPA Press Release*, Dec. 1988.

[17] A. Gazet, “Comparative analysis of various ransomware virii,” *Journal in computer virology*, vol. 6, no. 1, 2010.

[18] M. Lessing, “Case study: Aids trojan ransomware,” *sdxCentral*, June 2020.

[19] N. F. Macewan, “The computer misuse act 1990: lessons from its past and predictions for its future,” *Criminal Law Review*, vol. 12, 2008.

[20] L. Garber, “Melissa virus creates a new type of threat,” *Computer*, vol. 32, no. 6, 1999.

[21] P. Knight, “Iloveyou: Viruses, paranoia, and the environment of risk,” *The Sociological Review*, vol. 48, no. 2, 2000.

[22] P. Csonka, “Internet crime: The draft council of europe convention on cybercrime: A response to the challenge of crime in the age of the internet?,” *Computer Law & Security Review*, vol. 16, no. 5, 2000.

[23] J. Nazario, “Ddos attack evolution,” *Network Security*, vol. 7, no. 10, 2008.

[24] W. Haynes, “Seeing around corners: Crafting the new department of homeland security,” *Review of Policy Research*, vol. 21, no. 3, 2004.

[25] N. Swartz, “Record data breaches in 2007,” *Information Management*, vol. 42, no. 2, 2008.

[26] J. S. Cheney, “Heartland payment systems: lessons learned from a data breach,” *FRB of Philadelphia-Payment Cards Center Discussion Paper*, vol. 10, no. 1, 2010.

[27] S. Karnouskos, “Stuxnet worm impact on industrial cyber-physical system security,” *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society. IEEE*, 2011.

[28] M. John, “Israeli test on worm called crucial in iran nuclear delay,” *The New York Times*, 2011.

[29] G. M. Stevens, “Data security breach notification laws,” *Congressional Research Service Report*, 2012.

[30] N. Conway *et al.*, “Doing more with less? employee reactions to psychological contract breach via target similarity or spillover during public sector organizational change,” *Critish Journal of Management*, vol. 25, no. 4, 2014.

[31] X. Shu *et al.*, “Breaking the target: An analysis of target data breach and lessons learned,” *arXiv preprint arXiv*, 2017.

[32] N. Manworren *et al.*, “Why you should care about the target data breach,” *Business Horizons*, vol. 59, no. 3, 2016.

[33] D. E. Sanger and N. Perlroth, “Bank hackers steal millions via malware,” *The New York Times*, 2015.

[34] S. Thielman, “Yahoo hack: 1bn accounts compromised by biggest data breach in history,” *The Guardian*, vol. 15, 2016.

[35] L. Feiler, “New approaches to network and information security regulation: The eu telecoms package,” *Computer law review international*, vol. 11, no. 2, 2010.

[36] D. Y. Kao and S. C. Hsiao, “The dynamic analysis of wannacry ransomware,” *In 2018 20th International Conference on Advanced Communication Technology (ICACT)*, vol. 8, 2018.

[37] E. Newcomer, “Uber paid hackers to delete stolen data on 57 million people,” *Bloomberg*, 2017.

[38] S. Gressin, “The equifax data breach: What to do,” *Federal Trade Commission*, vol. 8, 2017.

[39] R. Smith, “Russian hackers reach u.s. utility control rooms, homeland security officials say,” *The Wallstreet Journal*, 2018.

[40] P. Voigt and A. V. dem Bussche, “The eu general data protection regulation (gdpr),” *Springer International Publishing*, vol. 10, 2017.

[41] M. Foulsham, “Living with the new general data protection regulation (gdpr),” *In Financial Compliance*, 2019.

[42] S. Larson, “Hackers take advantage of bitcoin’s wild ride,” *CNN Business*, 2017.

[43] R. Forno, “Hackers seek ransoms from baltimore and communities across the us,” *The Conversation*, 2019.

[44] E. L. Harding *et al.*, “Understanding the scope and impact of the california consumer privacy act of 2018,” *Journal of Data Protection & Privacy*, vol. 2, no. 3, 2019.

[45] T. Tam *et al.*, “The invisible covid-19 small business risks: Dealing with the cyber-security aftermath,” *Digital Government: Research and Practice*, vol. 2, no. 2, 2020.

[46] P. Wagenseil, “Zoom security issues: Here’s everything that’s gone wrong (so far),” *Tom’s Guide*, 2020.

[47] J. Arquilla and M. Guzdial, “The solarwinds hack, and a grand challenge for cs education,” *Communications of the ACM*, vol. 64, no. 4, 2021.

[48] F. Downs *et al.*, “Top cyberattacks of 2020 and how to build cyberresiliency,” *ISACA*, 2020.

[49] BBC News, “Mgm hack exposes personal data of 10.6 million guests,” *BBC News*, 2020.

[50] Check Point Software Technologies Ltd, “The new ransomware threat: Triple extortion,” *Check Point Software Technologies*, 2021.

[51] R. Browne, “Irish health service shuts down it systems after ‘sophisticated’ ransomware attack,” *CNBC*, 2021.

[52] O. Analytica, “Critical infrastructure sees rising cybersecurity risk,” *Emerald Expert Briefings*, 2021.

[53] M. May and D. Elliott, “Consortium for research on information security and policy,” *Stanford University*, 1998.

[54] D. C. Latham, “Department of defense trusted computer system evaluation criteria.,” *Department of Defense*, 1986.

[55] University of San Diego, “A brief history of cyber security standards in the us,” *University of San Diego*, 1986.

[56] S. B. Lipner, “The birth and death of the orange book,” *IEEE Annals of the History of Computing*, vol. 37, no. 2, 2015.

[57] D. S. Herrmann, “Using the common criteria for it security evaluation,” *CRC Press*, 2002.

[58] S. M. C. Téri, “Using b method to formalize the java card runtime security policy for a common criteria evaluation,” *NIST Computer Security Resource Center*, 2000.

[59] B. M. S. Shackleford, A. Proia and A. Craig, “Toward a global cybersecurity standard of care? exploring the implications of the 2014 nist cybersecurity framework on shaping reasonable national and international cybersecurity practices,” *Leg. Stud. Res. Pap. Ser*, no. 291, 2015.

[60] M. Columbia, “Nist cybersecurity framework adoption linked to higher security confidence according to new research from tenable network security,” *tenable*, 2016.

[61] E. A. Morse and V. Raval, “Payment card industry data security standards in context,” *Computer Law & Security Review*, vol. 24, no. 6, 2008.

[62] T. Greene, “Center for internet security: 18 security controls you need,” *Network World*, 2021.

[63] TripWire Inc., “Foundational controls work – a 2017 dbir review,” *TripWire Magazine*, 2017.

[64] S. G. Calder, A. & Watkins, “Information security risk management for iso27001/iso27002,” *It Governance Ltd*, 2010.

[65] Axio, “Top 5 cybersecurity frameworks to secure your organization,” *Security Boulevard*, 2020.

[66] Securicon Team, “Why a compliance-based approach to cybersecurity is not enough,” *Securicon*, 2020.

[67] J. H. Ratcliffe, “Crime mapping and the training needs of law enforcement,” *European Journal on Criminal policy and research*, vol. 10, no. 1, 2004.

[68] M. Mylrea *et al.*, “Insider threat cybersecurity framework webtool & methodology: Defending against complex cyber-physical threats.,” *2018 IEEE Security and Privacy Workshops (SPW)*, 2018.

[69] B. Center, “Cyber security task force: Public-private information sharing.,” *Bipartisan Policy Center Homeland Security Project, Washington DC*, 2012.

[70] K. Peretti, “Cyber threat intelligence: To share or not to share—what are the real concerns?,” *Privacy and security report, Bureau of National Affairs*, 2014.

[71] P. LLC, “Exchanging cyber threat intelligence: There has to be a better way,” *IID Independently conducted by Ponemon Institute LLC*, 2014.

[72] K.-J. F. Fu, Ya-Ping and C.-H. Yang, “Coras for the research of isac,” *International Conference on Convergence and Hybrid Information Technology, IEEE*, 2008.

[73] S. M. Nazli Choucri and P. Koepke, “Institutions for cyber security: International responses and data sharing initiatives,” *Cybersecurity at MIT Sloan*, 2017.

[74] A. D. Rayome, “How to choose the right cybersecurity framework,” *TechRepublic*, 2019.

[75] Apptega, “Which cybersecurity framework is right for you?,” *Security Boulevard*, 2019.

[76] Shashank, “A beginner’s guide to cybersecurity framework,” *Edureka*, 2020.

[77] C. Lago, “How to implement a successful cybersecurity plan,” *CIO Magazine*, 2019.

[78] C. Goodwin *et al.*, “A framework for cybersecurity information sharing and risk reduction,” *Microsoft Corporation*, 2015.

[79] R. Lewis *et al.*, “Cybersecurity information sharing: a framework for sustainable information security management in uk sme supply chains,” *Proceedings of the European Conference on Information Systems (ECIS)*, 2014.

[80] Deloitte Touche Tohmatsu Limited, “Cybersecurity and the role of internal audit an urgent call to action,” *Deloitte*, 2019.

[81] J. E. Justin Baxter and D. Popovic, “Cyber risk: Getting the balance right. a practical approach to making risk based decisions,” *Crowe*, 2017.

[82] D. Cope, “Cybersecurity self-assessment tool: Helps combat risk,” *ABA Banking Journal*, vol. 107, no. 4, 2015.

[83] J. Olcott, “Input to the commission on enhancing national cybersecurity: The impact of security ratings on national cybersecurity,” *NIST: National Institute of Standards and Technology*, 2016.

[84] S. B. Kahyaoglu and K. Caliyurt, “Cyber security assurance process from the internal audit perspective,” *Managerial Auditing Journal*, vol. 33, no. 4, 2018.

[85] J. Freund, “Gartner 2019 debate: Quantitative vs. qualitative cyber risk analysis,” *RiskLens*, 2019.

[86] G. Roldán-Molina *et al.*, “A decision support system for corporations cybersecurity management,” *12th Iberian Conference on Information Systems and Technologies (CISTI)*, 2017.

[87] Upguard, “Bitsight vs securityscorecard 2021 comparison and review,” *Upguard Website*, 2021.

[88] F. Curti *et al.*, “Cyber risk definition and classification for financial risk management,” *Federal Reserve Bank of Richmond*, 2019.

[89] Computer Security Division, Information Technology Laboratory, NIST: National Institute of Standards and Technology, “Nist special publication 800-30 guide for conducting risk assessments,” *NIST: National Institute of Standards and Technology*, 2012.

[90] Gartner, Inc., “Reviews for security threat intelligence products and services reviews and ratings,” *Worldwide // In: Gartner peer insights. https://www.gartner.com/reviews/market/security-threat-intelligence-services*, 2019.

[91] Gartner, Inc., “Securityscorecard vs upguard,” *Worldwide // In: Gartner peer insights. https://www.gartner.com/reviews/market/it-vendor-risk-management/compare/securityscorecard-vs-upguard*, 2019.

[92] A. Maryani *et al.*, "A system dynamics approach for modeling construction accidents.," *Procedia Manufacturing*, vol. 4, 2015.

[93] D. J. Currie *et al.*, "The application of system dynamics modelling to environmental health decision-making and policy-a scoping review.," *BMC Public Health*, vol. 18, no. 1, 2018.

[94] J. D. Repenning, N. P. & Sterman, "Capability traps and self-confirming attribution errors in the dynamics of process improvement.," *Administrative Science Quarterly*, vol. 47, no. 2, 2002.

[95] J. Lyneis, J. & Sterman, "How to save a leaky ship: Capability traps and the failure of win-win investments in sustainability and social responsibility," *Academy of Management Discoveries*, vol. 2, no. 1, 2016.

[96] D. F. Andersen *et al.*, "Preliminary system dynamics maps of the insider cyber-threat problem.," *22nd International Conference of the System dynamics Society*, 2004.

[97] T. Fagade *et al.*, "System dynamics approach to malicious insider cyber-threat modelling and analysis.," *In International Conference on Human Aspects of Information Security, Privacy, and Trust*, 2017.

[98] D. Polatin-Reuben *et al.*, "A system dynamics model of cyber conflict.," *2013 IEEE International Conference on Systems, Man, and Cybernetics*, 2013.

[99] E. Pruyt *et al.*, "From data-poor to data-rich: system dynamics in the era of big data.," *32nd International Conference of the System Dynamics Society, Delft, The Netherlands*, 2014.

[100] O. Dolezal *et al.*, "Czech cyber security system from a view of system dynamics.," *Journal of Cyber Security and Mobility*, 2018.

[101] R. M. Pinckard J. L. and R. A. Vrtis, "A mapping of the federal financial institutions examination council (ffiec) cybersecurity assessment tool (cat) to the cyber resilience review (crr)," *CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States*, 2016.

[102] L. Shen, "The nist cybersecurity framework: Overview and potential impacts.," *Scitech Lawyer*, vol. 10, no. 4, 2014.

[103] J. Freund and J. Jones, "Measuring and managing information risk: a fair approach.," *Butterworth-Heinemann*, 2014.

[104] S. Ramachandran *et al.*, "A smarter way to quantify cybersecurity risk," *BCG Website: https://www.bcg.com/capabilities/digital-technology-data/smarter-way-to-quantify-cybersecurity-risk*, 2019.

[105] L. SAFE, "Security assessment framework for enterprise (safe)," *Lucideus SAFE*, 2012.

[106] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA), "Cyber security evaluation tool (cset)," *CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA)*, 2019.

[107] R. Bannam, "Cyber scorekeepers: A growing number of ratings firms aim to help companies and their insurers assess and manage cybersecurity risks.," *Risk Management*, vol. 64, no. 10, 2017.

[108] A. Nag A. K. & Chennamaneni, "A survey on emerging trends of cyber threats to academic research.," *AMCIS 2020 TREOs*, 2020.

[109] H. Lee, "The cyber resilience assessment framework," *Hong Kong Monetary Authority*, 2016.

[110] NIST, "Success story: University of kansas medical center," *NIST Website: https://www.nist.gov/cyberframework/success-stories/university-kansas-medical-center*, 2019.

[111] B. Kiani *et al.*, "Using causal loop diagram to achieve a better understanding of e-business models.," *International Journal of Electronic Business Management*, vol. 7, no. 3, 2009.

[112] Sushil, "System dynamics: A practical approach for managerial problems," *New Delhi: Wiley Eastern Publication*, 1993.

[113] J. D. Sterman, "Business dynamics: Systems thinking and modeling for a complex world," *Irwin: McGraw-Hill*, 2000.

[114] A. T. Tunggal, "What is cybersecurity performance management?," *UpGuard Website: https://www.upguard.com/blog/cybersecurity-performance-management*, 2020.

[115] H. HOSN, "Cybersecurity perception vs reality: Is your organisation actually secure?," *Secureworks Website: https://www.secureworks.com/blog/cybersecurity-perception-vs-reality-is-your-organization-actually-secure*, 2018.

[116] J. B. Copeland, "Fair breakfast case study: Lpl financial realigns risk management around fair (video)," *FAIR Institute Blog: https://www.fairinstitute.org/blog/fair-breakfast-case-study-lpl-financial-realigns-risk-management-around-fair-video*, 2019.

[117] Digital Defense, Inc., "Digital defense, inc. helps investors bank enhance their information security posture," *Digital Defense Website: https://w2k5c134qwx2vutib80kg2a7-wpengine.netdna-ssl.com/wp-content/uploads/2019/02/DigitalDefense-Investors-Bank-Case-Study-122818F.pdf*, 2019.

[118] securityscorecard, "Case study: Axcient," *securityscorecard Website: https://securityscorecard.com/resources/case-study-axcient*, 2019.

[119] T. Maze, "Case study: Tech company quickly identifies top cyber risks with quantitative analysis," *RiskLens Website: https://www.risklens.com/resource-center/blog/case-study-tech-company-quickly-identifies-top-cyber-risks-with-quantitative-analysis*, 2020.

[120] LogRhythm, "Mccoll's retail group remains pci compliant with the logrhythm nextgen siem platform," *LogRhythm Website: https://logrhythm.com/case-studies/uk-mccolls/*, 2018.

[121] Alibaba Cloud, "Alibaba cloud security whitepaper," *Alibaba Cloud Website: http://alicloud-common.oss-ap-southeast-1.aliyuncs.com/Alibaba%20Cloud%20Security%20Whitepaper*$_v$2$_0$12017*.pdf*, 2017.

[122] Standard Chartered Bank, "Standard chartered annual report," *Standard Chartered Bank Website: https://av.sc.com/corp-en/content/docs/risk-review-and-capital-review-2018.pdf*, 2018.

[123] S. Lisbon and E. Rice, "Case study: Information security risk assessment for a small healthcare clinic using the security risk assessment tool provided by healthit. gov.," *Midwest Instruction and Computing Symposium, La Crosse, WI*, 2017.

[124] S. Lisbon, "A comparative analysis of hipaa security risk assessments for two small dental clinics," *St. Cloud State University Website*, 2018.

[125] BitSight, "Global financial firm reduces risk of third party breach with bitsight security ratings," *BitSight Website: https://info.bitsight.com/bitsight-case-study-global-financial-firm*, 2019.

[126] securityscorecard, "Case study: Farm credit," *securityscorecard Website: https://securityscorecard.com/resources/farm-credit*, 2019.

[127] securityscorecard, "Children's minnesota case study," *securityscorecard Website: https://s3.amazonaws.com/ssc-corporate-website-production/documents/resources/ChildrensMN-Case-Study-c04-1.pdf*, 2017.

[128] securityscorecard, "Liquidnet case study," *securityscorecard Website: https://s3.amazonaws.com/ssc-corporate-website-production/documents/resources/Liquidnet-Case-Study-c03.pdf*, 2017.

[129] CYBERGRX, "Blackstone case study, a force multiplier for third-party cyber risk management," *CYBERGRX Website: https://www.cybergrx.com/resources/case-studies/blackstone-case-study*, 2020.