Architecting a Secure Enterprise with a Systems-Thinking Approach

by

Samuel J.G. Lee

B. Comp. (Hons) E-Commerce
National University of Singapore, 2010

Submitted to the MIT System Design and Management Program
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management
at the
Massachusetts Institute of Technology

June 2019

Signature redacted

Signature of Author_____
Samuel J.G. Lee
MIT System and Design Management Program
May 24, 2019

Signature redacted

Certified by_____
Donna H. Rhodes
Principal Research Scientist, Sociotechnical Systems Research Center
Thesis Supervisor

Signature redacted

Accepted by_____
Joan Rubin
Executive Director, System Design and Management Program

This page is intentionally left blank

Architecting a Secure Enterprise with a System-Thinking Approach

by

Samuel Joo Guan Lee

Submitted to the MIT System and Design Management (SDM) program on May 24, 2019 in Partial Fulfillment of the Requirements for the Degree of Master of Science in Engineering and Management.

Abstract

On April 1, 2015, President Obama issued an executive order, declaring that the increasing prevalence and severity of malicious cyber-enabled activities constitute an unusual and extraordinary threat to the national security, foreign policy and economy of the United States. He declared a national emergency to deal with this threat and included $14 billion for Cyber Security spending in his 2016 budget. On a corporate level, based on a survey conducted in 2018, 27% of IT and Cyber Security professionals said that their biggest Cyber Security challenge is that business managers don't understand or support strong Cyber Security while 27% of respondents say their biggest Cyber Security challenge is the difficulty of managing the complexity of too many disconnected Cyber Security tools. (Oltsik, 2018) From these national and corporate challenges, an apparent Cyber Security challenge exists. The national challenge is further insinuated by two key issues. First, the disconnect between business managers and security managers. Second, the complexity of too many disconnected Cyber Security tools faced at the corporate level.

"*In the past the man has been first; in the future the system must be first.*" (Taylor, 1919) As Frederick Winslow Taylor stated in his book, "Principles of Scientific Management, in the context of management, Taylor implied that developing great systems will yield greater benefits than developing great men. Similar, the author believe that the design of a cyber-security architecture should be approached with a system-thinking approach, where the sum of the system parts is greater than the parts itself, less so from an individual's perspective.

Taking this approach, the author aims to discuss the challenge in managing the evolving cyber threats, the external eco-system challenges faced by financial institutions, the differing stakeholders' needs raised to the cyber-security team, and how a systems-thinking cyber-security architecture will be more effective in dealing with threats and challenges arising from both externally and internally.

Thesis Supervisor: Donna H. Rhodes
Title: Principal Research Scientist, Sociotechnical Systems Research Center

This page is intentionally left blank

Acknowledgements

There are many people I would like to thank for supporting me as I pursued my degree and worked on this research. First and foremost is my wife, Yvonne, who knowing my passion in intellectual pursuits, supported my decision to pursue my dream to undertake a master's program in MIT, put her well-advanced career on hiatus, and selflessly dedicated her time and effort to supporting me and my three kids during our stay away from home.

I am also extremely grateful to my three young children, Belle, Dave and Chase, for even their mere presence in this journey. Even the simplest of things, like their smiles and welcome hugs I received each day as I returned from school to their appreciation for the opportunity to attend school in Cambridge, energized me to work through my research.

Next, I would like to thank my thesis advisor, Dr. Donna Rhodes, without whom this thesis would not have materialized. Her erudition and rich experience, coupled with her ever-willingness to help students despite her busy schedule, saw to me benefiting and learning much from her. I am really blessed to have her as my advisor, providing valuable, timely and sincere feedback as I developed my research.

I would like to thank Joan Rubin, the executive director of the SDM program, and other members of the SDM staff for their support and effort in making this journey such an enriching experience for me.

I would like to thank the SDM program for their initiative in offering their brightest students a teaching assistantship opportunity to give back to the future cohort by supporting the faculty in teaching, grading and motivating the subsequent SDM batch. I am thankful for this rare career-building opportunity they invest in me, as without it, my pursuit of the MIT degree will otherwise not be possible.

I would like to thank my family in Singapore, in the US, and especially those who flew in to spend quality time and warm our hearts during our stay away from home. Such times with family were precious, knowing they would be fleeting.

Last but certainly not least, I would like to thank my friends who were with me in Cambridge for this journey. I have benefitted much from them, both academically from our collaboration in team assignments, and spiritually from the friendship forged over family outings, meals and "boys' nights" at the Muddy Charles Pub.

This page is intentionally left blank

Contents

This page is intentionally left blank

List of Figures

This page is intentionally left blank

List of Tables

This page is intentionally left blank

1. Introduction

"It's true, I had hacked into a lot of companies, and took copies of the source code to analyze it for security bugs. If I could locate security bugs, I could become better at hacking into their systems. It was all towards becoming a better hacker."

- Kevin Mitnick (2013)

Kevin Mitnick is one of the most renowned hackers in the world, notoriously known for his high-profile 1995 arrest. Kevin is one of the earliest hackers known to perform social hacking. The term "hacking" generally means to have **unauthorized access** by impersonating another person's identity or finding a way to break the **authentication** system to gain access.

This thesis is concerned with the complexity involved in the design of Cyber Security architecture for financial institution required to defend the enterprise from the growing number of cyber threats and the intricacy of the interaction between the enterprise elements and ecosystem elements.

This chapter explains the motivation, needs and scope of this thesis. Subsequently, it introduces the current state of Cyber Security attacks on financial institutions with publicly known examples. Lastly, a brief explanation of the ARIES framework and the approach of this research will be explained in this chapter.

1.1. Motivation

In 2017 alone, the number of USA data breaches hit a record hit of 1,579 incidents (Generali Global Assistance (GGA), 2018). Financial institutions are 300 times more likely to be hit by such an attack (Muncaster, 2015). On average, each financial institution spent USD$18 million on Cyber Security attacks as compared to $12 million for firms in other industries (Mirchandani, 2018).

While the financial loss due to the attacks are evident, the effects of such incidents to the enterprises' staff and strategy is lesser known. In 2014, JPMorgan bank had a data breach incident that had 76 household million accounts compromised on the back of a social engineering campaign (Jessica Silver-Greenberg, 2014). A year after the breach, their CSO Jim Cummings was re-assigned to Texas (Jordan Robertson, 2015). Meanwhile, the CISO Greg Rattray was asked to take up another role in the global cyber partnerships and government strategy (Riley, 2015).

When the Target data breach incident happened in 2014, Target CIO Beth Jacob was first to step down in the wake of the massive pre-Christmas data breach (D'Innocenzio, 2014). Subsequently, CEO

Gregg Steinhafel also stepped down (O'Connor, 2014). Other than security breaches, other reasons cited for CISOs being fired include project boondoggles, system recoverability and system collapse (Yu, 2015). Often in the wake of a discovery of a hacking incident, despite being the most appropriate person who has a holistic view of the situation, CSO or CISO are requested to or chose to resign.

The Cyber Security teams often face the external challenge of managing the evolving cyber-attacks patterns ranging from technical to socio-technical and the ecosystem risk faces by financial institutions. And from within the enterprise, the Cyber Security teams often face a different internal challenge. To keep up the competition faced by the enterprise, corporate strategy often includes these two initiatives to drive up productivity: the pursuit for 1) technology innovation and 2) "always-connected" (InformationWeek, 2012). With the advent of enterprise-issued corporate mobile devices and bring-your-own-devices (BYOD) devices to support the "always connected" initiative, this corporate initiative has led to a radical change in the design of enterprise network security. Despite the technological and security challenges posed by these corporate initiatives to the Cyber Security teams, these teams are required to align their Enterprise Cyber Security Architecture to support these corporate initiatives. Inevitably, the modern challenges of designing a complex Cyber Security architecture now includes the challenge of the ever-growing technology boundary of financial institution.

These challenges are often further insinuated by the multifaceted interactions of the enterprise element, ecosystem elements and cyber-attacks. These new challenges have increased the complexity required of an effective Cyber Security architecture.

1.2. Scope

With such staggering numbers about the magnitudes of Cyber Security attacks (both frequency of attacks and the cost of addressing Cyber Security incidents) that the **financial institution** faces and the complex environment of financial institutions, the author chose to focus on the topic of Cyber Security in financial institutions.

	Research Questions
1	How can Cyber Security teams anticipate and identify the eco-system risks faced by financial institutions?
2	Given the Enterprise Cyber Security Architecture, who are the primary stakeholders and how can their needs be effectively prioritized?
3	How can emergent risks and varying stakeholders' needs be identified and be used to shape the Enterprise Cyber Security Architecture?

The research questions are shown above: With an emphasis of long-term view and for the benefit of the organisations, how can Cyber Security teams anticipate and identify the eco-system risks faced by financial institutions? Given the Enterprise Cyber Security Architecture, who are the primary stakeholders and how can their needs be effectively prioritized? Understanding that certain emergent risk can be identified, how can emergent risks and varying stakeholders' needs be identified and be used to shape the Enterprise Cyber Security Architecture?

1.3. Approach of the Thesis Framework

This section describes the approach in this thesis. The approach is adopted from ARIES Framework which was jointly developed in Massachusetts Institute of Technology by Dr. Deborah J. Nightingale and Dr. Donna H. Rhodes. The ARIES framework developed from the fundamental theory and practice of several fields, which includes, strategic management, stakeholder theory, systems architecting, ideation, scenario analysis, decision science, enterprise theory and systems engineering. Designed to provide a holistic approach to the selection of new architecture for the future enterprise, the author selected the ARIES framework after considering the various Enterprise Architecting Frameworks.

The ARIES Framework has several notable strengths, namely 1) ability to synergize, 2) future-oriented 3) methodological 4) holistic and 5) simple to apply. The strengths of the ARIES framework come from both the individual theories that it leverages upon as well as the synergies between the theories and practices. ARIES was developed with the objective to not replace existing frameworks, rather to lead and be compatible with existing formal enterprise architecture frameworks that are in practice. Another strength of the ARIES framework is its ability to effectively explore possible alternatives of enterprise futures, weigh each of the alternatives and methodically select the preferred enterprise architecture to be the baseline for the transformation.

ARIES is designed with the perspective that an enterprise is a complex sociotechnical system and therefore should be treated holistically to meet the strategic objectives. As coined by the famous philosopher Aristotle, "the whole is greater than the sum of the parts", this phase aptly reflects the reality of complex socio-technical systems due to the complexity of the interactions between the various elements of the enterprises. In the ARIES framework, there are ten unique elements defined. To reduce the complexity, the enterprise is deconstructed into elements to provide focus on each of these elements one at a time (focus approach). By having multiple perspectives through the detailed focus approach, it empowers the enterprise architect with the understanding of diverse needs of each enterprise stakeholders. As seen in Figure 1, the ARIES ten elements are as followed 1) Ecosystem, 2) Stakeholders,

3) Strategy, 4) Information, 5) Infrastructure, 6) Products, 7) Services, 8) Process, 9) Enterprise and 10) Knowledge.

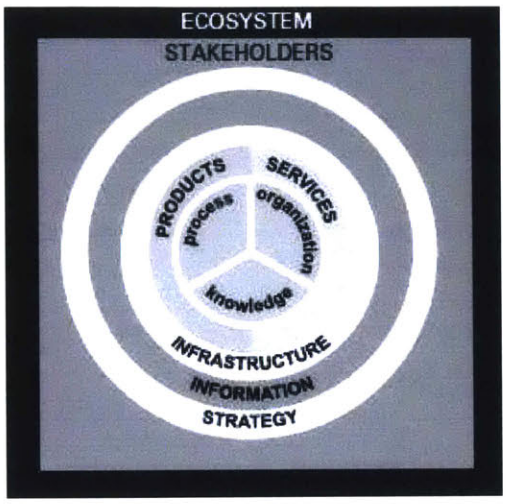


Figure 1: ARIES Enterprise Element Model

There are six steps to the thesis framework approach (Figure 2). Starting from first step (**understanding the enterprise landscape**), this step is to gather the context and necessary information about desired goals and challenges faced by both the financial institution and their Cyber Security team. Next, in the second step (**performing the stakeholder analysis**), by first defining the desirable attributes of a stakeholder will clarify and simplify the process of selecting stakeholders. With the group of selected stakeholders, both the historical and existing stakeholders' needs will be shared openly, before prioritizing the needs. To improve upon the existing Enterprise Cyber Security Architecture, a performance baseline will be subsequently collected and the metrics will be defined to measure the future improvements made. In the third step (**capturing the current architecture**), this provides the opportunity to gather the internal enterprise landscape from an enterprise elements lens approach. For each enterprise element, a SWOT analysis is performed to uncover the strengths and weakness of the element.

Subsequently, to better understand the future requirements of the stakeholders, stakeholders' narratives will be collected in the fourth step (**creating a holistic vision of the future**). With a holistic vision of the future, new meaningful metrics may emerge to measure the current architectures from a renewed perspective. In the fifth step (**generating alternative architecture**), concept ideation and generation will be performed. Subsequently, concept refinement will be done before creating and selecting feasible and optimal architectures in this step. The purpose of the concept refinement process

and architecture selection process is to tighten the alignment to the holistic vision defined in step 4 and the needs prioritized in step 2. With a list of feasible architectures, in the final step (**deciding on the future architecture**), an effective outcome of this step will require a good understanding of the stakeholders' needs to recommend an architecture. With the recommended architecture, validation will be done by obtaining expert reviews, which provides necessary feedback to accept and endorse or to further improve on the fifth step (**generating alternative architecture**).

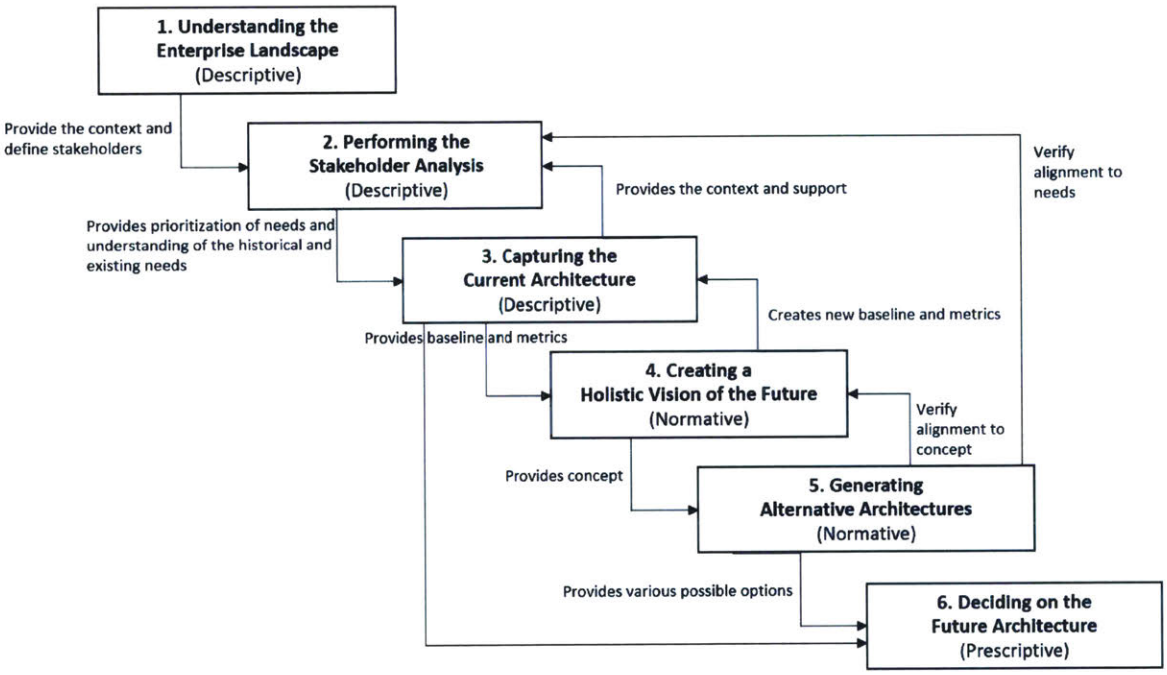


Figure 2: Approach of the Thesis Framework (Adapted from (Nightingale & Rhodes, 2015))

1.4. Research Methodology and Thesis Overview

This section describes the undertaken research methodology to perform the necessary thesis research. Each chapter of the thesis will be briefly discussed below.

Chapter 2: *Literature review.* This chapter provides the overview of the financial institutions and the risks they face. By understanding the risks faced, it provides the contexts on the need for Cyber Security enterprise architecture, systems, process and resources in place for financial institutions. Next, Cyber Security history and renowned cases are covered to provide the evolution of Cyber Security attacks and its effects. Finally, the ARIES Framework is used as the structure of a proposed reference framework; the framework will be discussed in depth. This proposed reference framework is used throughout the thesis as the main approach.

Chapter 3: *Proposal of Stakeholder-Managed Integrated & Learning Enterprise (SMILE) Reference Framework.* In this chapter, the ARIES Framework is used as the structure of a proposed reference framework. As the proposed reference framework is described, the key enterprise elements of Financial institutions are identified, along with the enterprise ecosystems. In this proposed reference framework, several other analytical models are integrated with the ARIES framework to provide additional insights. The proposed referenced framework is a six-step approach to developing several future architectures before providing an approach to decide on the future architecture.

Today, IAM's project and operational coverage spans across from technology to risk to human resource to other Cyber Security domains. Due to this extensive span across corporate functions and the operational interaction involved, IAM is considered one of the most complex Cyber Security domains as compared to the other Cyber Security domains. Challenges faced in IAM are beyond the technical challenges and often includes socio-technical challenges, e.g. acceptance of IAM attestation user-interface to perform attestation. In view of these complex challenges, the IAM is chosen for the subsequent case study out of the other Cyber Security domains.

Chapter 4: *Applying SMILE Reference Framework to a hypothetical case.* In this chapter, the SMILE Reference Framework will be applied upon a hypothetical case. Due to the sensitivity surrounding Cyber Security operations and IAM operations in financial institutions and the public publication of this thesis, a hypothetical case will be used in place of an actual case. To keep the hypothetical case as realistic as possible, the hypothetical case will be based on publicly sourced information and various known Cyber Security cases about financial institutions. In this chapter, the application of SMILE Reference Framework consist of the analyzing the landscape of a fictitious financial institution, performing the stakeholder analysis, creating the ideal holistic vision, generating alternative architecture and deciding on the future Cyber Security architecture. Finally, expert reviews are used to critique the research approach and to identify areas of strengths and improvement.

Chapter 5: *Conclusion*. This chapter discusses the research contributions, limitations and the possible areas to further the research.

2. Literature Review

This chapter introduces the context this thesis is based upon, financial institutions and Cyber Security. Today, there are various types of financial institutions; however, this was not the case in the earlier years. To add on to the span of the context, there are five broad kinds of risk that the financial institutions faces (Blackman, 2014), which has yet to include Cyber Security risk. To provide appreciation of the Cyber Security domain, the author shares the history of Cyber Security, the first cyber-attack and one of the latest and largest cyber-attack against a retail giant and a financial institution, so that the readers can see the vast difference between the attacks in terms of impact, severity and complexity.

2.1. Financial Institutions

In the early 1800s, there were only three specific types of **financial institutions**, 1) Commercial banking, 2) Thrift institution, 3) Insurance companies. Variation of financial institutions took years to mature, evolve and grow. And in 2012, as shown in Table 1, there are eight different types of financial institutions that grow from that three specific types of financial institution. (Randall Kroszner, 1996)

Table 1: Percentage Shares of Assets of Financial institutions in the United States (Randall Kroszner, 1996)

	1860	1900	1922	1929	1948	1960	1970	1980	2000	2005	2012
Commercial banks	71.4%	62.9%	63.3%	53.7%	54.5%	40.8%	42.6%	40.7%	30.5%	29.3%	32.9%
Thrift institutions	17.8	18.2	13.9	14.0	12.0	21.0	23.0	25.0	10.1	10.2	6.9
Insurance companies	10.7	13.8	16.7	18.6	26.0	24.2	19.0	16.2	15.6	15.0	14.6
Investment companies	—	—	0.0	2.4	0.3	0.7	0.7	2.0	15.8	13.7	19.8
Pension funds	—	0.0	0.0	0.7	3.8	7.7	8.0	9.5	8.8	6.2	7.6
Finance companies	—	0.0	0.0	2.0	2.7	5.2	5.7	6.2	6.9	7.3	4.8
Securities brokers and dealers	0.0	3.8	5.3	8.1	0.7	0.4	0.7	0.3	12.1	17.3	12.1
Real estate investment trusts	—	—	—	—	—	0.0	0.3	0.1	0.2	1.0	1.3
Total (%)	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Total ($ trillions)	0.001	0.016	0.075	0.123	0.218	0.500	1.079	3.140	15.93	23.80	28.68

Financial institutions, also known as **banking institutions**, are enterprises which provide financial services and serve as intermediaries of financial markets. There are three major types of financial institutions. First, the depository institutions are deposit-taking institutions that accept and manage deposits and make loans and these institution includes banks, credit unions, trust companies, and mortgage loan companies. Second, the contractual institutions are insurance

companies and pension funds institutes. Third, the investment institutions are investment banks, underwriters, brokerage firms and sovereign wealth funds institutes. (Siklos, 2001)

These eight different specific types of financial institutions (Randall Kroszner, 1996) can be classified into the three major types of financial institutions (Siklos, 2001). The evolution of financial institutions and their financial product offerings grow as the needs of their clients grow. Even today, within the specific group of Securities brokers and dealers, there are a variety of brokers managing and offering to the differing categories of clients, categorized by their net worth.

2.1.1. Risks in the Financial World

While each of these financial institutions serves a different purpose in the financial world and may have various strategies to achieve their goals, they all need to manage risk well to protect their own enterprise, the clients they serve and the society at large. There are five broad kinds of risk (Blackman, 2014).

First, **Strategy risk** - the risk of executing (or not executing) a strategy, the opportunities cost, and actual cost of the strategy.

Second, **Legal and Compliance Risk** – the risk of entering a legal case due to the lack of compliance (either intentionally or unintentionally) and having to pay for the fines. A compliance issue can also affect the strategic risk where the local authorities may issue an order in a form of a cease and desist letter to prohibit a business from continuing its current operations.

Third, **Operational Risk** – as defined by the Basel Committee, operational risk is "the risk of losses arising from problems from internal controls, systems, people and external events " (Cruz, 2002). Operational risk can appear as a **system** technical failure in the critical system of traders or even as a **human** failure, where a certain trade was accidentally performed or performed incorrectly. Operational issues can stall the business for hours or even days. In the case of Nasdaq (2013), the operational issue (technical glitch) shut down Nasdaq trading for three hours (New York Times, 2015) while New York Stock Exchange (2015) halted trading for three and a half hours due to a computer misfunction (Mamudi, 2015).

Fourth, **Financial Risk** – depending on these authors (Ontario Securities Commission, 2018) (Saunders, 2006) as seen on Table 2, there are broadly speaking eight or more financial risks, ranging from 1) interest rate risk, 2) credit risk, 3) liquidity risk to 4) foreign exchange risk and 5) sovereign risk to 6)

market risk, 7) insolvency risk and 8) off-balance-sheet risk. Though these risks are the most quantifiable risk, the challenge in quantifying these risks still remains. Due to the complexity in managing this category of risk, numerous professions are made out of the need to quantify the risk and protect the financial institution and their clients.

Table 2: Risks Faced by Financial Intermediaries (Saunders, 2006)

Interest rate risk The risk incurred by an FI when the maturities of its assets and liabilities are mismatched.
Credit risk The risk that promised cash flows from loans and securities held by FIs may not be paid in full.
Liquidity risk The risk that a sudden surge in liability withdrawals may require an FI to liquidate assets in a very short period of time and at less than fair market prices.
Foreign exchange risk The risk that exchange rate changes can affect the value of an FI's assets and liabilities denominated in nondomestic currencies.
Country or sovereign risk The risk that repayments from foreign borrowers may be interrupted because of restrictions, intervention, or interference from foreign governments.
Market risk The risk incurred from assets and liabilities in an FI's trading book due to changes in interest rates, exchange rates, and other prices.
Off-balance-sheet risk The risk incurred by an FI as the result of activities related to its contingent assets and liabilities held off the balance sheet.
Technology risk The risk incurred by an FI when its technological investments do not produce anticipated cost savings.
Operational risk The risk that existing technology, auditing, monitoring, and other support systems may malfunction or break down.
Insolvency risk The risk that an FI may not have enough capital to offset a sudden decline in the value of its assets.

Five, **Reputational Risk** – In the book by "Managing Reputational Risk: Curbing Threats, Leveraging Opportunities", (Rayner, 2004) defines reputation risk as follows: "Reputation risk is any action, even or circumstance that could adversely or beneficially impact an enterprise's reputation". This risk involves the potential loss of reputational capital created by the stakeholders for their clients or users. Reputational capital can be created via 1) emotional appeal of the company, products and services, 2) the financial performance, 3) the vision and leadership, 4) Social responsibility and lastly 5) workplace environment (Rayner, 2004). Likewise, either one of these reputation quotient attributes can negatively affect the reputational capital. Reputation risk, as compared to the four other risk mentioned above, are the hardest to quantify, largely because of its subjective nature.

2.2. Cyber Security

In this section, the historical and modern cases of Cyber Security incidents are discussed. To provide a better understanding of Cyber Security roles in financial institutions, the reporting structures for CISOs and their role requirements are discussed. Finally, the Cyber Security domains are briefly introduced to provide a high-level understanding of Cyber Security.

2.2.1. History of Cyber Security - First (harmless) worm and antivirus

The history of Cyber Security incidents often originates from a harmless research project. In 1971, Bob Thomas at Bolt, Beranek and Newman Inc realized that it was possible for a computer program to move across a network, leaving a small trail wherever it went (SentinelOne, 2018). He wrote a program in PDP-10 assembly called **Creeper** as an experiment and designed for it to travel between Tenex terminals on the early ARPANET, printing the message "I'M THE CREEPER: **CATCH** ME IF YOU CAN." (Figure 3) on the Model 33 ASR teletype (Core War, n.d.).

After Thomas demonstrated his program Creeper, Ray Tomlinson (the same person who invented email) wrote an enhanced version which replicated (the first computer worm) instead of simply moving (SentinelOne, 2018). Tomlinson then wrote another program called Reaper, which moved through the ARPANET deleting copies of Creeper, giving us the first antivirus software (Core War, n.d.).

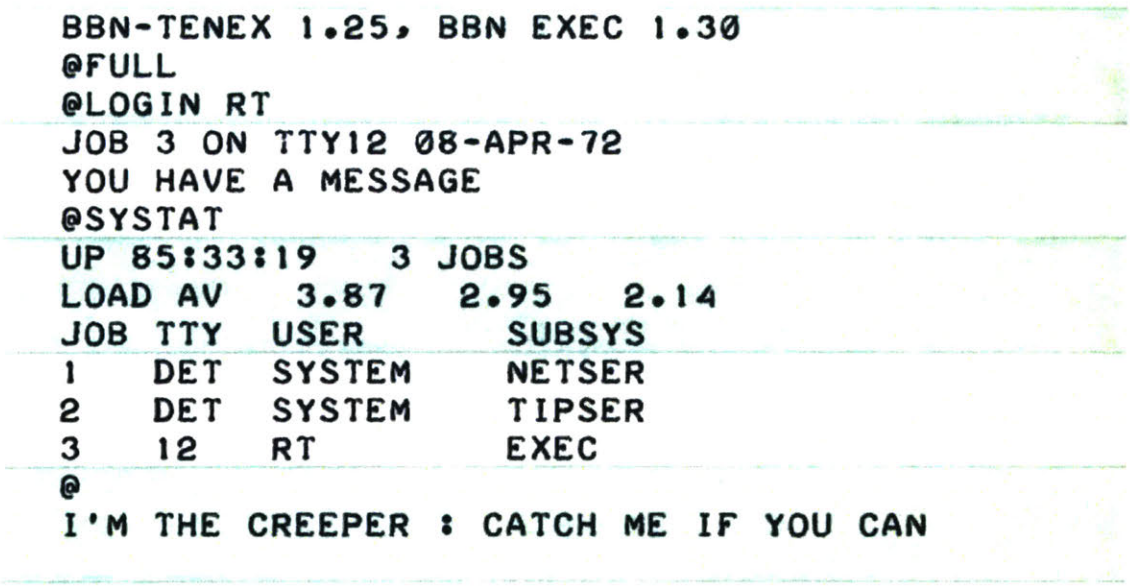


Figure 3: Bob Thomas's Creeper message (SentinelOne, 2018)

2.2.2. History of Cyber Security - First (harmful) worm

In 1989, Robert T. Morris, a Cornell University computer science graduate student who graduated from Harvard, generated what is now known as the first "computer worm" (Press, 2015). The worm was actually part of a research project, meant to measure the size of the Internet at large "*by infecting UNIX systems in order to count the number of connections throughout the web*" (Colorado Techical University, n.d.). Due to a programming error, the self-propagating worm infected machines aggressively, causing networks and systems to slow down or even crash. This became the first worm to introduce first widespread instance of a denial-of-service (DoS) attack (Julian, 2014). The Morris worm and the other attacks that came along were early cases that required cyber-security attacks responses. These incidents ultimately led to the growth of Cyber Security industry which includes the establishment of CERTs (Computer Emergency Response Teams) in government agency and corporate enterprise as the focus point for coordinating cyber-threat responses (Julian, 2014). The initial industry reaction that followed the old saying 'prevention is better than a cure' gave rise to the invocations of detective and preventative security process and products (Julian, 2014).

2.2.3. Modern and Notable Cyberattack on Consumer Store – Target

In **Error! Reference source not found.** below, this is a visualization of the list of data breaches and hacks. Each circle is a breach/hack incident. The size reflects the number of records leaked. Interestingly, while Facebook's incident has gotten a large media coverage about the data leakage of 50 million records, Marriott Hotel's incident leaked almost 8x more records than the Facebook event itself, at a record-breaking number of 383 million records.

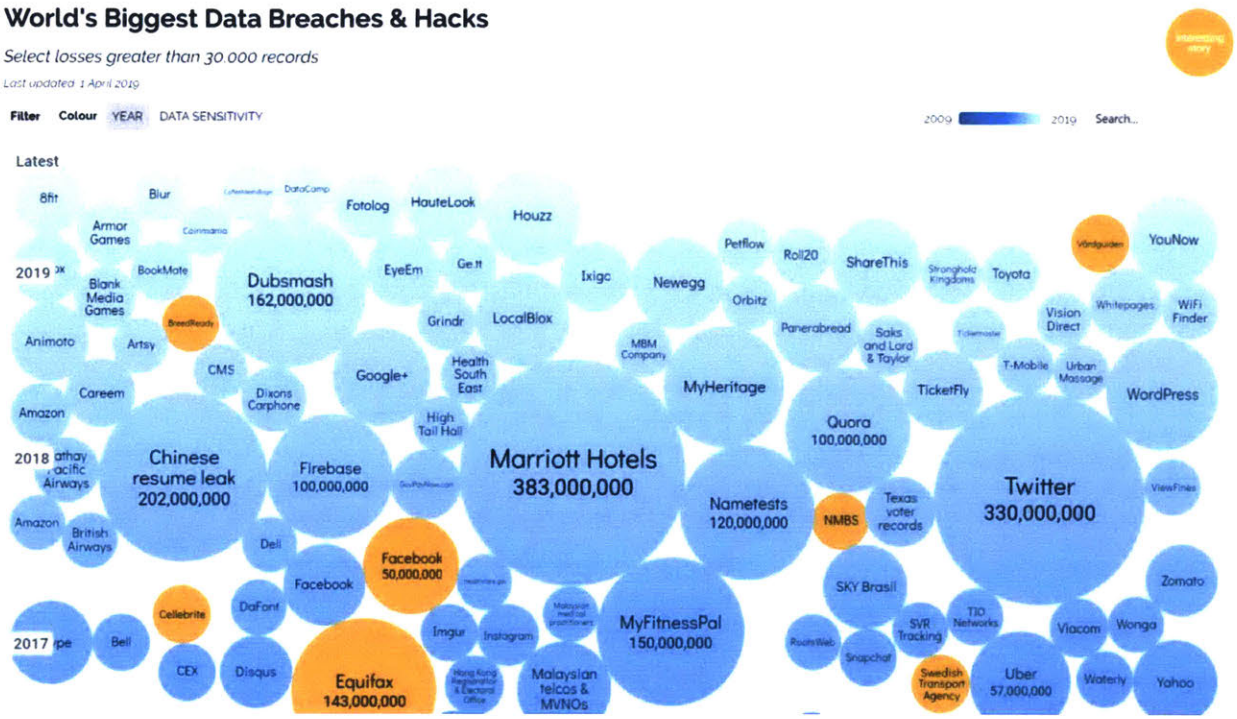


Figure 4: World's Biggest Data Breaches and Hacks (McCandless, Evans, Barton, Tomasevic, & Geere, 2019)

In 2013, forty million credit and debit card records, and seventy million email and mailing address were stolen from Target (Julian, 2014) This data breach encapsulates the nature of most Cyber Security threats today for number of reasons. With the information at hand, the hackers have the "track data," which is transmitted every time a card's magnetic strip is swiped (Wagstaff, 2013). This information consists of the cardholder's name, the credit card number, expiration date and the service code for identifying international transactions. With this information, the hackers are able to continuously purchase things online with the credit card information, especially if the company is slow to report such an incident publicly and struggles to identify the security loophole and close the gap.

As reported by security researcher Brian Krebs, the hack affected customers who shopped at Target retail stores between November 27 (Black Friday) and December 15, 2013 (Krebs, 2013). Initially, this incident was suspected to involve a Target's point-of-sale (POS) system attack where customer information was perhaps directly sent from the store's cash registers to the hackers themselves, with the means of malicious software (Wagstaff, 2013).

Eventually, the investigation showed that the compromise came through one of the heating and ventilation companies based in Pittsburgh called Fazio Mechanical Services contractors. Fazio Mechanical Services' system themselves were a victim of a spear phishing attack made by the hackers a months before

the Target attack. With the HVAC company's credentials, they installed the malware on the POS system and hid their data extraction process by conducting them during business hours. By the time Target identified the security gap, all of the stolen data had been sent to Moscow on Dec 2nd, 2013. The hackers then removed the data before the federal law enforcement could reach out to Target about the breach on December 12, 2013 (A. & T., 2014). Eventually, the retail giant Target agreed to pay $18.5 million in order to settle the claims raised by 48 states and to resolve a federal investigation of its massive data breach in late 2013. (Reuters, 2017)

2.2.4. Largest Cyber-Attack on Financial Institution – Bangladesh

SWIFT, which stands for the Society for Worldwide Interbank Financial Telecommunication, is a consortium that manages a trusted and closed network that enables their 11,000 member banks worldwide to securely communicate about financial transactions in a standardized financial message within a reliable environment. Founded in 1973, SWIFT is headquartered in La Hulpe, Belgium. Financial institutions that use SWIFT have Business Identifier Code (BIC - commonly referred to as the "SWIFT" code), which is used to identify institution as well as credentials that authenticate and verify transactions. (SWIFT, 2019)

The financial industry, being one of the top five most cyber-attacked industry, is the often the target for cybercrime due to the monetary benefits behind the corporate gates (Morgan, Top 5 Industries At Risk Of Cyber-Attacks, 2016). Cyber-attacks range from simple attacks like phishing and social hacking to systematic attacks like DDOS and vulnerability discovery to complex attacks like the organised state-run attacks where vulnerabilities are planted and exploited over time to avoid detection.

In the case of the central bank of Bangladesh Bank, which is also known as "Bangladesh Bank" locally, on February 5th 2016, there were 46 fraudulent SWIFT instructions generated to the Federal Reserve Bank of New York via the SWIFT network to transfer almost US $1 billion from the Bangladesh Bank account towards various financial institutions in Sri Lanka, Philippines, and other parts of Asia. (The Daily Star, 2019)

All these activities started on the February 5th 2016, which also happens to be a bank holiday in Bangladesh. While the bank has modernised, they still continued to have each SWIFT transaction printed in hardcopies through a dedicated printer (Hammer, 2018). Normally there would be a few dozen transactions being printed, however on that fateful day, the duty manager noticed that there were no transactions printed out that day (Zetter, 2016). The next day, which was a Saturday, he returned to the

office and tried launching the SWIFT software, only to see an error message that writes: "*A file is missing or changed.*" (Hammer, 2018). When the duty manager and his staff finally managed to get the software working, dozens of transactions started being printed (Zetter, 2016). It turns out that the Federal Reserve Bank of New York had written to the Bangladesh bank, seeking for clarifications about the suspicious 46 payment instructions which amounts to nearly to $1 billion in the past 24 hours (Hammer, 2018). As the amount and the frequency of the transfer is unusual, the Bangladesh bank team quickly verified their own record systems to find that nothing was debited and contacted SWIFT and Federal Reserve Bank of New York to no avail as it was the weekend (Zetter, 2016). It was only on the following Monday that the Bangladesh Bank found out that while most of these requests were received and processed by the Federal Reserve Bank of New York, a large number of these request were held up due to irregularities spotted by the various banking personnel involved. Some of the irregularities include 1) the transfer of a large amount to a small NGO (Hammer, 2018), 2) a spelling error which misspelled "foundation" as "fandation" (Zetter, 2016), 3) a recipient having a similar name to a company on the sanctions list, Jupiter (Hammer, 2018). Despite all these mishaps, over 900 million dollars was recovered. The remaining 81 million dollars are still lost and were transferred to a bank in Philippines, Rizal Commercial Banking Corporation (RCBC) (Hammer, 2018).

2.2.5. Enterprise Structure of Financial Institution and Reporting Structure of CSO and CISO

In the latest edition of its "Global State of Information Security Survey," PricewaterhouseCoopers (PwC) found that CISO and chief security officers (CSOs) reported to varying types of management roles, i.e. to CEOs (40%), to board directors (27%), to chief information officers (CIO) (24%), to CSO(17%) and to chief privacy officer (CPO) (15%) (Figure 5). As the numbers from PwC adds up to go beyond 100 percent and that the actual survey questions were not included, these figures likely include dotted lines of reporting on top of direct reporting. (Veltsos, 2018)

Figure 5: Distribution of CISO's Reporting Managers

This discrepancy of reporting lines reflects the varying opinions of the ownership of a Cyber Security department or team and perhaps the responsibilities of the team. The lack of a common perspective of a clear reporting line for the CISO indicates the level of uncertainty within the industry and complexity of this matter. And indeed, a F5 Ponemon CISO research report showed that the trend of CISOs reporting into the IT enterprise are fading due to these five reasons, 1) Operational Conflicts, 2) Risk, 3) Insider Jobs, 4) Effectiveness, 5) Regulations (Pompon, 2017).

These varying reporting lines and the trend reporting lines shifting shows that the stakeholders of Cyber Security are changing due to the ever-dynamic threat landscape of Cyber Security as well as the stakes on the table and true owner of these stakes. With the ARIES Framework, the framework provides a process to connect the stakeholders needs to the Cyber Security Strategy, therefore including the needs and expectation of the stakeholders into the eventual development of the Secured Enterprise Architecture.

2.2.6. CISO Roles

A To be successful in a CISO role, a CISO needs to be competent in four roles, 1) Strategist, 2) Adviser, 3) Guardian and 4) Technologist (Bell, 2015).

Table 3: Four Faces of the Chief Information Security Officer (Bell, 2015)

	Four Faces (Roles)	Functions
1	Strategist	Drive **business and cyber risk strategy alignment, innovate and investigate transformational change** to manage risk through valued investments
2	Adviser	Integrate with the business **to educate, advise and influence** activities with **cyber risk implications**
3	Guardian	**Protect business assets** by understanding the threat landscape and managing the effectiveness of the cyber risk program
4	Technologist	**Assess and implement security technologies and standards** to build organizational capabilities

With all these dimensions to consider (Business Strategy, Technology innovation and Cyber Risk), the job of a CISO is often difficult and have a typical term of 2.1 years. (Schuck, 2015)

There are two key challenges of these four roles. First, in the article (Bell, 2015), Bell shared that for a CISO to have a long tenure with a company, the CISO needs to align with the business, which the key objective of a Strategist. The challenge is that for a non-profit generating department, alignment with the business strategy is less of a profit-generating objective and more of a loss-prevention objective. However, as a non-profit department, also known as a "cost centre" to certain industry, funding is typically limited for such a department due to the lack of a tangible return (e.g. profit). Hence the challenge for most CISO is to meet a loss-prevention objective that is coupled with a pool of funding that could be limited by the business' strategy and priorities.

Second, as a guardian and an adviser to the business, the CISO has a hard requirement to protect the business assets yet the CISO often does not have real control over the various departments and their actions on their use of business assets. Henceforth the CISO can only meet his/her corporate duty and requirements by increasing the awareness of Cyber Security through the means of a soft approach to educate, advise and influence. The alternative that a CISO has, if he is reporting to the CRO, is to create strict Cyber Security policies that are shared with fully-informed employees or create mandatory corporate trainings to raise the awareness of Cyber Security and its implication to the organisation.

2.2.7. Cyber Security Domain

The International Information System Security Certification Consortium, or $(ISC)^2$ is a non-profit and globally recognized consortium. $(ISC)^2$ was formed in the 1988 by initial groups which included: the Canadian Information Processing Society, the Computer Security Institute, the Data Processing Management Association (two special interest groups), Idaho State University, the Information Systems Security Association, and the International Federation for Information Processing. (ISC2, 2019)

Prior to 2015, $(ISC)^2$ had ten domains and currently $(ISC)^2$ has revised the ten domains to eight broad domains. Below are the eight domains that every CISO needs to consider and manage in their own enterprise.

Table 4: $(ISC)^2$ Cyber Security Domains

$(ISC)^2$ 10 domains in **pre-2015**	$(ISC)^2$ 8 domains **after 2015**
1. Access Control	1. Identity & Access Management
2. Application Development Security	2. Software Development Security
3. Telecommunications and Network Security	3. Communications & Network Security
4. Operations Security	4. Security Operations
5. Security Architecture and Design	5. Security Engineering
6. Business Continuity and Disaster Recovery Planning	6. Asset Security
7. Physical and Environmental Security	7. Security and Risk Management
8. Information Security Governance and Risk Management	8. Security Assessment & Testing
9. Legal regulations, investigations, and compliance	
10. Cryptography	

While rebranding of the domains is evident, the key difference between both domains by ISC^2 is the that Identity and Access Management has become a domain by itself and includes Identity

management as part of this new domain, and the content from the domain cryptography is spread out to the remaining 8 domains.

Another perspective from an industry practitioner is that of Henry Jiang, a CISO at Diligent Corporation who created Figure 6 with 9 different security domains. The author thinks that this is a very detailed diagram to cover most of the Cyber Security aspect. The key benefit of using this diagram is understanding how the various elements of Cyber Security are related to each other and potentially inspires the Cyber Security teams who read this to consider the various stakeholders who may be related to these domains and how their functions may interact with the Cyber Security team.

Figure 6: Cyber Security Domains by CISO Henry Jiang

However, its presentation can be improved at the presentation structure. For an example, in the bottom left, SIEM, a type of tool, is seen as the same level as Protection, Prevention and Recovery which are security process.

2.3. Identity and Access Management (IAM)

This section describes Identity and Access Management (IAM), the importance of IAM and how enterprises benefit from their IAM systems.

2.3.1. IAM and its Importance and Benefits

IAM consists of four key elements, 1) the identity, 2) the access, 3) the system to assign/revoke access and 4) the systems that the user needs to have access to. For small companies with fewer employees, it is common that the IAM system is being managed by the IT administrators who create the identity, the application access and grant the application access to identity. However, as companies scale, the monolithic growth in the number of identities for application increase the amount of effort required to maintain such an IAM. A simple example of 100 employees with 20 applications would result in required to grant up to 2000 application access, and this has yet to include the revocation of access as the users move between department or leaves the enterprise.

The employee or user lifecycle (Figure 7) drives the need for IAM systems and there are three key processes.

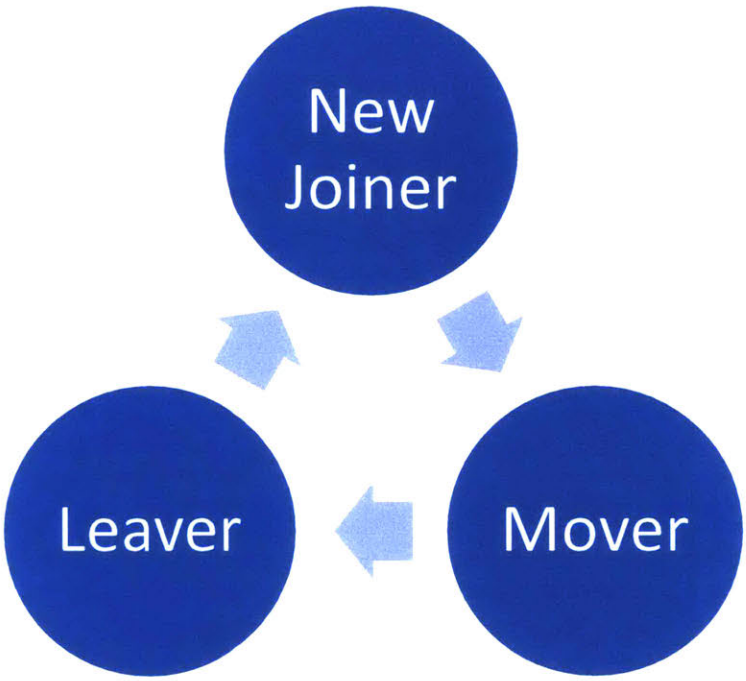


Figure 7: IAM User Lifecycle

1) Potential employee joins the enterprise as a **new joiner**, getting this access to the enterprise.
2) Over time, the employees may switch within the enterprise and this employee is known as a **mover**. During this transition, the user will need to have some of their access related to the prior department revoked and at the same time, needs to be granted access to the new department resources.

3) Eventually, all employees will leave the enterprise, triggered either by enterprise restructure, or self-attrition or even retirement. These employees are known as **leavers**. And all of the leavers' access needs to be revoked in a timely manner or at least in a manner stipulated by the industries' regulators.

2.3.2. Major Drivers for IAM Investments

There are seven business imperatives that drive the need for IAM projects. Namely, 1) Digital Transformation, 2) Mergers, Acquisitions & Divestitures, 3) Risk Management, 4) Regulatory Compliance, 5) Cloud Adoption, 6) Operational Efficiency, and 7) Mobility. Each of the seven business imperatives are well described by Figure 8 from a KPMG article (Bossardt, 2018) as shown below. Yet despite the strong and various needs for IAM, IAM projects often fail and faces numerous challenges. In the next section, the challenges will be discussed further.

Figure 8: Major Drivers of IAM investments (Bossardt, 2018)

2.3.3. Challenges of IAM

There are five key challenges, 1) Operational Challenges, 2) Compliance Challenges, 3) User Challenge, 4) Application Integration Challenges and 5) Stakeholder Challenge.

Operational challenges can arise from several scenarios. First scenario is about provisioning access, 1) granting access and 2) revoking access. Without timely access to application or systems,

enterprises will experience productivity loss and at times, it is common that a new joiner gets all the access they need in weeks instead of days. On the flip side, allowing users to hold on to access that they should not be have can lead to several issues. The first issue is data theft, where the user leak data from their previous department or enterprise. The second issue is unauthorized data manipulation, where a disgruntled employee can change the data or even deleted the crucial data required for daily operations. The third issue is related to the next category of challenge, **compliance** challenge where access that should be removed are not removed and poses a threat to the enterprise and the industry, especially financial institutions.

As the number of application increases, the number of passwords increase and the **users** face a need to find a good approach to memorize their password, leading to user password fatigue. Next, as applications are organically adopted by departments, going through pilot testing before having the enterprise adoption; this results in silo user-directories created in independent applications that are potentially not **integrated with the IAM systems**, resulting in manual provisioning of the access. And as the IAM systems or the application system receive a version upgrade, the integration between the IAM system and the application system may break, resulting in operational issues related to the department that requires the integration and eventually resulting in enterprise productivity loss.

Lastly, the lack of business buy-in is often the key cause of IAM project failure. According to an KPMG survey in 2009, 51% of the respondents stated that there was a lack of support from their **stakeholders** and management as seen in Figure 9. Finally, despite IAM being an enterprise-wide project, the IAM projects were often found as the IT or Security department's responsibility. (KPMG IT Advisory, 2009)

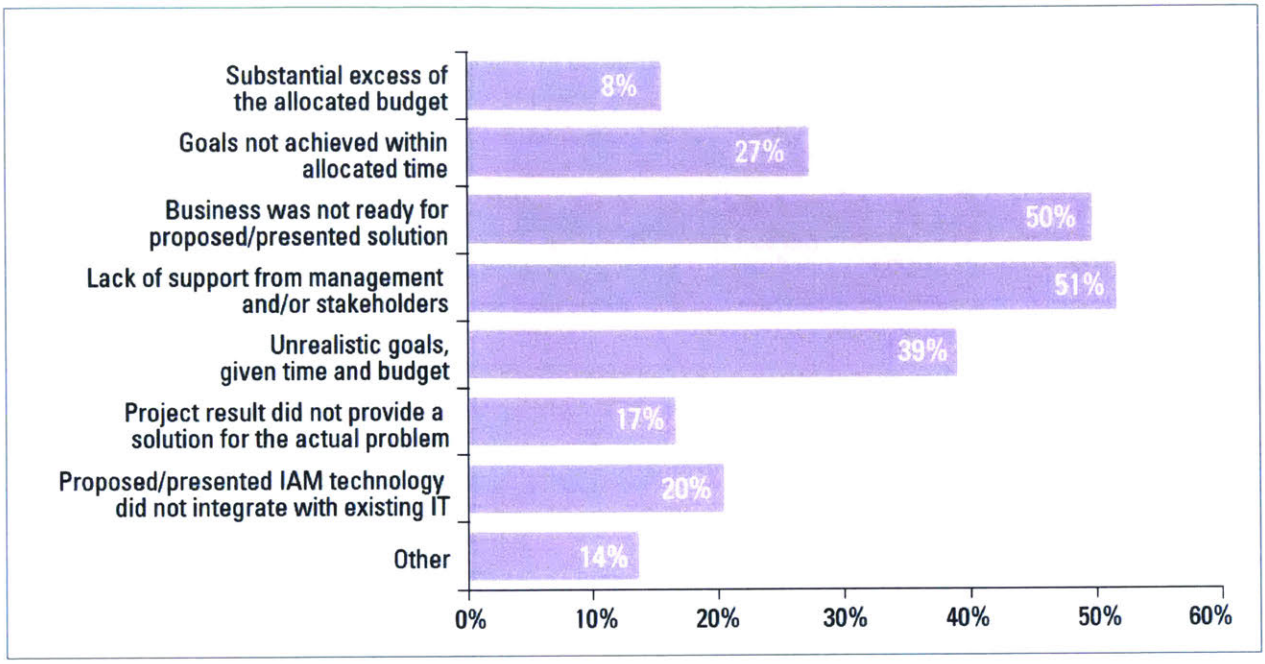


Figure 9: Cause of IAM project failure (KPMG IT Advisory, 2009)

IAM's security and operational coverage spans across from technology to risk to human resource to other Cyber Security domains. Due to this extensive span across corporate functions and the operational interaction involved, IAM is considered one of the most complex Cyber Security domains as compared to the other Cyber Security domains. Challenges faced in IAM are beyond the technical challenges and often includes socio-technical challenges, e.g. acceptance of IAM attestation user-interface to perform attestation. In view of these complex challenges, out of the other Cyber Security domains, the IAM is chosen for the subsequent case study.

2.4. Strategy

In 1962, in Alfred Chandler's book, Strategy and Structure: Chapters in the History of the Industrial Enterprise, his use of the word "Strategy" marks the inaugural mention in the business realm. In his book, Chandlers analyzed several enterprises and illustrated the phrase "Structure follows strategy" through the examples.

For enterprises, strategy management provides a general direction. The field of strategic management involves both intended and emergent activities performed by chief executives on behalf of enterprise's owners. These activities require resources to advance the firm's performance in their

environments. Part of these activities include emphasizing the enterprise's mission and vision, identifying the goals and objectives, developing plans and policies through programs/portfolio of projects.

So, if strategy management is to provide the general direction, "Taylorism" could be referred to the pillar to efficiently support the general direction. In the book, One Best Way (Kanigel, 2005), Frederick Winslow Taylor was recognized as the first efficiency industrialist who developed the original business efficiency technique that introduces the concept of time-and-motion. As the father of scientific management, his approach to rationalize and improve production speed was named ``Taylorism''. Through time studies to establish the duration a job should take, he advocated for piece-rate rates. To remove any form of judgment required by workers, he dictated that the details of each task should be prescribed by management. Considering the period that Taylor lived (1856-1915), his words seems rather reasonable given the circumstance where industrial expansion depended on increasing productivity through expertise and efficiency that helps to drive each enterprise's growth.

In the field of business administration, it is useful to talk about strategic alignment between the enterprise and its environment or strategic consistency. According to strategists, there is strategic consistency when the actions of an enterprise are consistent with the expectations of management, and these in turn are with the market and the context (Nag. et al 2007).

2.5. ARIES Framework

In this section, each of the seven processes will be discussed in deeper context with reference from the book "Architecting the Future Enterprises". (Nightingale & Rhodes, 2015)

2.5.1. Understand the Enterprise Landscape

First, the objective of the process will be explained, second the required information or inputs desired to make the process effective will be identified, third possible techniques for each process will be suggested, fourth the expected delivery or output for each process will be explained, such as why the output matters and how the users can leverage the outputs to achieve their goals.

2.5.1.1. Objective

The objective of understanding the Enterprise Landscape is to gather an outward perspective of the enterprise, uncover the eco-system that the enterprise is located within, and understand the external forces that shape the lens of the enterprise's owners, senior managers and employees. Having this outward view allows the enterprise to understand how their existing capabilities are helping or hindering

them towards their goal of transformation and also identify the required capabilities the enterprise may need to developed, so as to pivot their way towards the transformation goals.

2.5.1.2. Required Information

To ensure that this process is complete, external information such as the politics, regulations, economy, market, technology, resources, environment (as showed in **Error! Reference source not found.**) are helpful to create the complete image of the ecosystem for the enterprise to analyze their larger surrounding. Other possible information may include Social aspect, which involves the understanding of the demographics, population and even cultural trends, (e.g. for digital transformation projects, change management and/or modern technology talents are required and if the society does not have such talent within the nearby vicinity, this may pose a challenge that needs to be considered as part of the subsequent process, i.e. Capture Current Architecture).

Enterprise ecosystem factors

Ecosystem factor	Examples of shifts that may trigger enterprise transformation
Politics	• A new government comes to power, impacting investor behavior. • An anticipated election cycle affects leadership change.
Regulation	• New policies restrict countries where the enterprise may operate. • Introduction of more stringent emission standards affects products.
Economy	• A downturn in the global (or national) economy necessitates downsizing. • New venture investment funding dries up for a period.
Market	• A strong, new competitor enters the enterprise's principal market. • The signing of a trade agreement opens the potential for a new market.
Technology	• Disruptive innovation diminishes the attractiveness of the enterprise's products. • A technology innovation shifts the business model to a service-oriented model.
Resource	• Imposition of a mandatory retirement age causes rapid workforce attrition. • Availability of a new material opens new product opportunities.
Environment	• A natural disaster disrupts business in a key region. • Stakeholders begin to clamor for "green" enterprise practices.

Figure 10: Enterprise ecosystem factors (Nightingale & Rhodes, 2015)

2.5.1.3. Techniques

To analyze the Enterprise Landscape, the first step is to determine the boundary and scope of the enterprise. Next step is to identify the *major constituents* of enterprise ecosystem and *key ecosystem*

factors of the enterprise. After developing an understanding of the enterprise's ecosystem, an inward view is taken by analyzing the enterprise strategic goals and objectives. With the strategic goals and objectives, the next step is to identify the various enterprise capabilities required to meet their desired objectives. Enterprises in different industries may choose to develop capabilities that best suit their strategy to survive, compete and thrive. In **Error! Reference source not found.** , there are several definitions of enterprise capabilities that are related to the Ilities. As compared to the enterprise function where the value is realized within a short time frame (e.g. HR hiring talents), values of Ilities are realized over time. After identifying the existing needs, the enterprise can start to identify their long-term capabilities they require to meet their enterprise needs.

Definitions of enterprise capabilities

Adaptability	Ability of an enterprise to sustain value delivery by transforming itself to respond to changes in its ecosystem
Agility	Ability of an enterprise to shift rapidly from one strategy to another to sustain enterprise value delivery
Competitiveness	Ability of an enterprise to deliver products/services that provide value to stakeholders equal to or greater than that of competing enterprises
Evolvability	Capacity of an enterprise to transform by leveraging successful features of the current architecture
Replicability	Ability to reproduce enterprise entities (e.g., products/services, business units) effectively to create or sustain value delivery
Resilience	Ability of an enterprise to cope effectively with changing circumstances and recover from disruptive events
Responsiveness	Ability to respond in a timely and effective way to emergent stakeholder needs, threats, and opportunities
Robustness	Ability to sustain consistent value delivery in spite of changes and perturbations in the enterprise ecosystem
Scalability	Ability to expand or contract the enterprise to meet changing circumstances in order to sustain value delivery
Sustainability	Capacity of an enterprise to endure over time as related to environmental, economic, and/or social dimensions

Figure 11: Definitions of enterprise capabilities (Nightingale & Rhodes, 2015)

2.5.1.4. Deliverables

The expected output of analyzing the enterprise landscape is an understanding of the external landscape (the external ecosystem and major constituents) and the internal landscape (enterprise objective, goals and enterprise capabilities required). For the external landscape, a good understanding of the relationships between external eco-system factors and enterprise is essential. Monitoring key external indicators will aid the enterprise in their development and implementation of their transformation plans.

2.5.2. Perform Stakeholder Analysis

2.5.2.1. Objective

The objective of Stakeholder Analysis is to identify the key enterprise needs and design an architecture to meet most, if not all, of the stakeholder needs. This is potentially one of processes that provides the key takeaways for this thesis where the stakeholders needs are being well-considered and prioritized in the architecting of a security enterprise.

2.5.2.2. Required Information

To kickstart this process, having a good understanding of the ecosystem from the first process (Understanding the Enterprise Landscape) is crucial as it helps to provide the list of relevant stakeholders which may include collaborators beyond the enterprise and regulators whom the senior managements needs to work with to ensure compliance.

2.5.2.3. Techniques

Typically, performing a stakeholder needs analysis consist of six steps, 1) listing down all the stakeholders from both external and internal of the enterprise, 2) categorizing the stakeholders based on stakeholder saliency, 3) soliciting the stakeholder value (needs), 4) the analyzing of the stakeholder value exchange, 5) establishing the stakeholder values and the relationship with the enterprise elements, and 6) understanding the stakeholder value evolution over time.

Listing stakeholders from both external and internal stakeholders are crucial. It has been found in recent research that a greater focus on stakeholder value (including that of employee stakeholders) other than shareholder value can create more value for shareholders than focusing on shareholders alone. (Piepenbrock, 2009)

In Figure 12, this shows the three stakeholder attributes, Power, Urgency and Legitimacy. Power is the authority or influence of a stakeholder over the relationship within the enterprise. Urgency is the degree to which the stakeholder requirements call for immediate attention by the enterprise. Legitimacy is the genuineness of involvement and relevance of the stakeholder in the enterprise. (Mitchell, Agle, & Wood, 1997)

Through the various combinations of the three attributes, there are seven types of stakeholders. In the article, it is noted that legitimacy forms the basis of stakeholder needs. As such, without

legitimacy, a stakeholder with power and urgency is deemed as a dangerous stakeholder as shown in Figure 12. (Mitchell, Agle, & Wood, 1997)

Ultimately, the goal of categorizing stakeholders is to identify the stakeholder demographics in terms of saliency, and understand what this saliency comprises of. Ideally, all selected stakeholders should be definitive stakeholders. Yet in the practice, this may not always be the case. Hence, by performing the categorizing of stakeholders will provide the awareness of any gaps in stakeholder saliency and encourage the architecting team to balance the overall saliency of the stakeholder team.

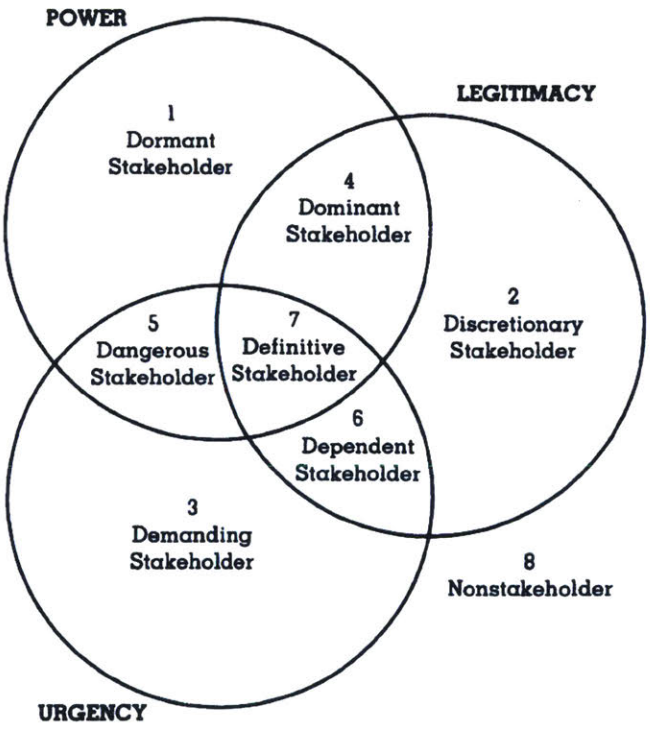


Figure 12: Stakeholder Saliency and the seven types of stakeholders (Mitchell, Agle, & Wood, 1997)

Using the list of stakeholders, the next step is to solicit their value and assess the priority of each value to the stakeholder groups and determine the enterprise's ability to delivery for each need. In Table 5Table 5: Example of stakeholder value assessment, this example shows the assessment of stakeholder value for employees, where various values are being assessed from the employees' perspective and the enterprise is being assess on its ability to provide these values to their internal stakeholder.

Table 5: Example of stakeholder value assessment (Nightingale & Rhodes, 2015)

Assessing importance and value delivery for the employee stakeholder

Stakeholder group: Employees Questions to guide stakeholder conversation: *What does the stakeholder value?* *What does the stakeholder expect from the enterprise?* *What would make the stakeholder think highly of the enterprise?*	*How important is this value to this stakeholder group?* 1 = low 5 = high	*How well is the enterprise delivering this value?* 1 = low 5 = high
Fair wages	5	5
Job satisfaction	5	4
Security	2	4
Rewards	4	3
Career growth	5	2
Tools to do the job	4	1
Work facilities	3	1
Training	3	1

Next, an analysis of stakeholder value is performed to uncover stakeholder expectations of and contributions to the enterprise. In Table 6, the stakeholders' expectations are listed on the leftmost column of the table while their contributions to the healthcare system are found on the rightmost column. Having complete this table for our stakeholders, it encourages system architects to explicitly list the stakeholders' values which are essential and could overlooked. Understanding the elements (expected values) that drives their behavior (contribution) will lead system architects to design or transform the new enterprise with these values intact or design a system where stakeholders will ideally get more value from the transformed enterprises.

Table 6: Example of stakeholder value exchange in a healthcare system (Nightingale & Rhodes, 2015)

Healthcare-system stakeholder value exchange (excerpt)

Value expected from enterprise	**Stakeholders**	**Value contributed to enterprise**
Medical care when and where needed, with seamless care across regions	Clients	Client subscription to healthcare program, with payment for services
Ability to place, access, and locate accurate information in medical record regardless of region where care is received	Physicians	Medical care to eligible clients, timely updates to medical records, and ordering of tests/ treatments when/where needed
Ability to communicate with regional offices, access centralized medical record, and make timely verification of eligibility	Referral case managers	Managing care process across regions, and ensuring clients understand where to get care within regions

To improve on the stakeholder value analysis, creating a graph to illustrate the stakeholder value and delivery can help to identify gaps where enterprise can better design an enterprise architect where existing important stakeholders' needs fall below their contribution. In Figure 13, Pharmacists, PCM coordinator and Referral case manager who are viewed as providing high value to the system are not receiving the required delivered value from the enterprise. Ideally, in the new architect, these stakeholders' needs are better served than it is currently.

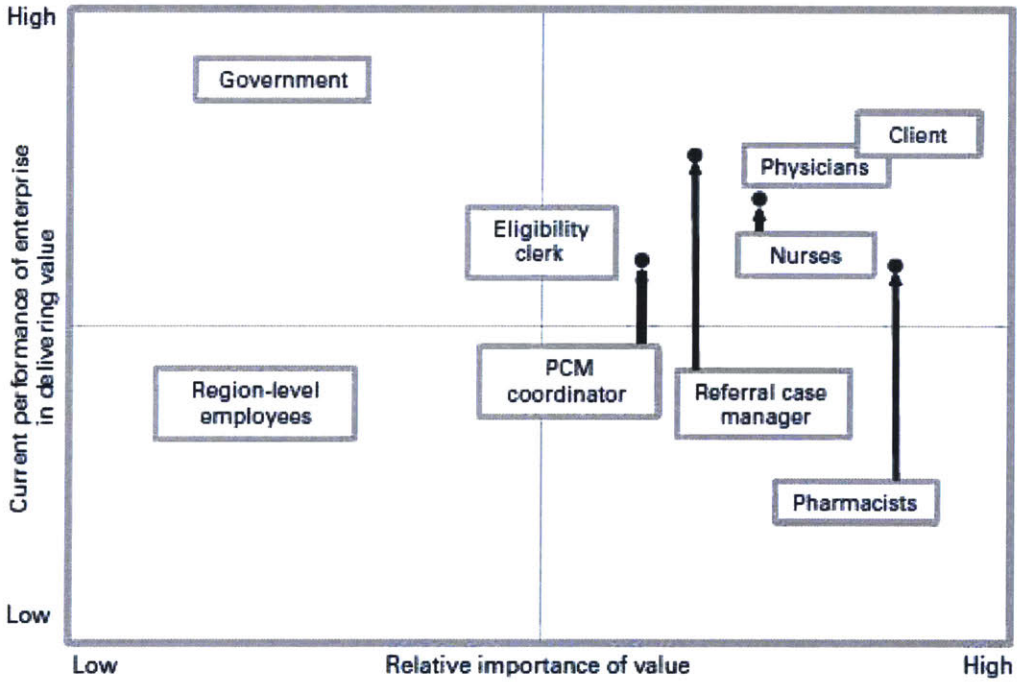


Figure 13: Consolidated stakeholder value exchange (Nightingale & Rhodes, 2015)

Subsequently, these stakeholders' views of each enterprise element are being assessed in term of importance. The key is understanding the relative importance and uncovering the enterprise elements' importance to the stakeholders. In Table 7, this table shows the stakeholders' priority for each of the enterprise elements.

Table 7: Importance of stakeholder views

Importance of views for each stakeholder (H—high, M—medium, L—low).

	Strategy	Organization	Process	Knowledge	Infrastructure
Purchasers	M	H	L	M	L
Insurers	M	H	L	M	L
Providers	H	H	M	H	M
Suppliers	M	M	L	M	L
Regulators	L	H	M	M	L

Lastly, just like all humans, our needs change per our situation and life-stages, likewise, understandably the stakeholder value may evolve over time, and it is imperative that the system architect is aware of this and plans for the stakeholder needs evolution accordingly by interviewing stakeholders and understanding their long-term goals and their potential enterprise changes.

2.5.2.4. Deliverables

Having a clear picture of the stakeholders and their prioritized needs to produce a stakeholder-weighted prioritized needs, the benefit of performing this process is to empower the system architect to design the security architecture with a good understanding of the needs and the priority of the needs, without having to be further over-concerned about the stakeholder, freeing the architect from seniority-bias and bringing the required focus to design the architecture that best meet the needs of the enterprise holistically.

2.5.3. Capture the Current Architecture

2.5.3.1. Objective

The objective of capturing the current architecture is to understand the AS-IS architecture, assess alignment between the strategic objectives, stakeholder values, key process and metrics and finally use the existing architecture as a baseline for the future architecture.

2.5.3.2. Required Information

To accurately capture the current architecture, a good understanding of both the internal elements (such as the enterprise's ARIES ten elements, strengths, weakness, stakeholder objectives and value, and internal process and metrics) and external elements (such as threats and opportunities) will be essential for this section.

2.5.3.3. Techniques

Available techniques to capture the current architecture include adopting an Enterprise Elements as Lens approach, SWOT analysis and X-Matrix analysis.

Enterprise Elements as Lens approach is used to provide a unique perspective of the enterprise to form a complete picture of the enterprise. As each of these elements are inter-related, the perspectives generated from these elements could be intertwined and reflect the interaction between these elements. Having a good understanding of these elements helps to construct an X-matrix of the enterprises, which helps to show the alignment within the enterprise. SWOT analysis which denotes Strength, Weakness, Opportunity and Weakness, is a strategic planning technique to identify the SWOT of the enterprise or industry. The X-Matrix analysis (Figure 14) is an alignment analysis to identify the strong alignments and uncover the weak alignments within an enterprise.

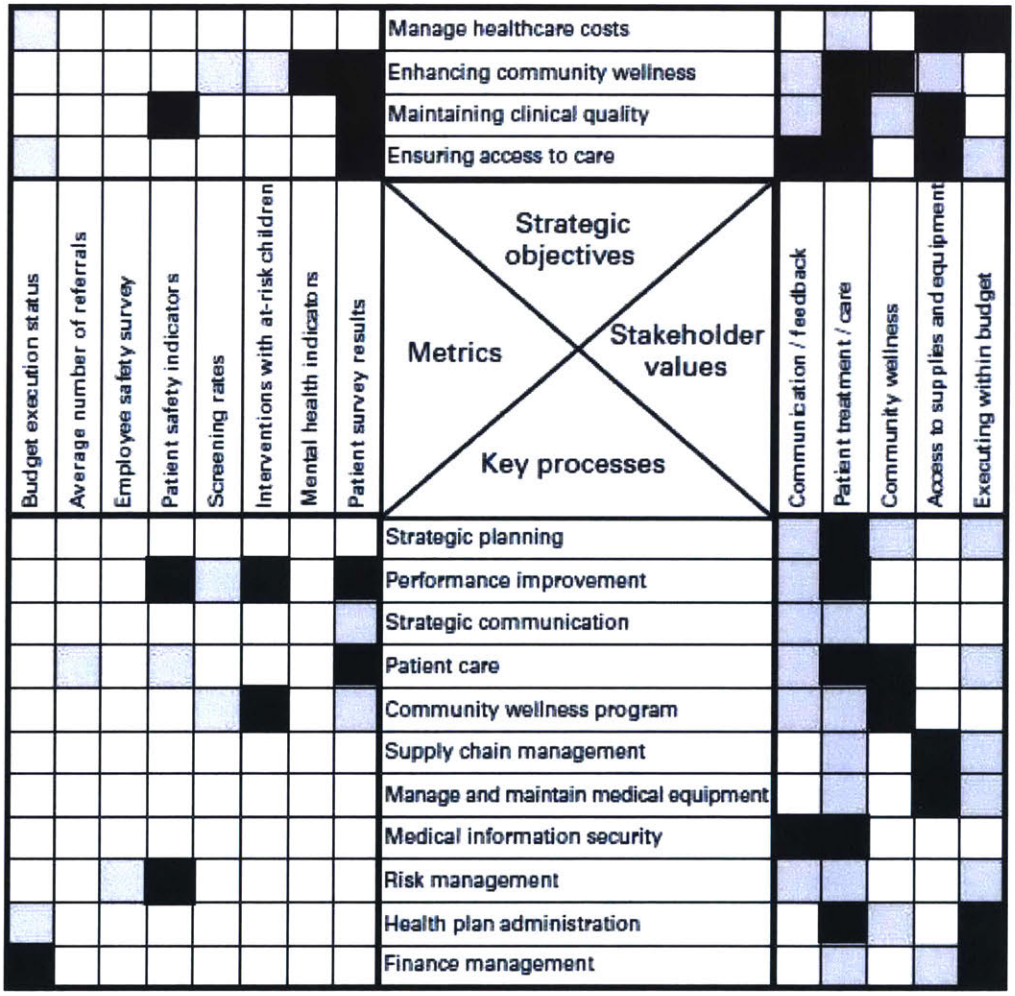


Figure 14: X-matrix for health care (Nightingale & Rhodes, 2015)

By using both tools, this enables an enterprise to identify their strengths, weaknesses, opportunities, threats, visualize internal alignments between their strategic objectives and metrics, and understand the correlation between the strengths and weakness with strategic objectives and metrics. These two tools strengthen the process of understanding and developing better alignment between strategic objectives and metrics.

2.5.3.4. Deliverables

While the key deliverables of this process are to provide the results of the SWOT analysis and X-matrix analysis, the best take-away is the insights derived from the cross-analysis of techniques, for example, through the Enterprise Elements as an element approach, the saliency of the elements and the relationship between the elements themselves, how it relates to the strengths or weaknesses of the enterprise and perhaps how the elements could be a source of leverage to tap on the future opportunities that are presented. Additional insights can be derived from the cross analysis of the outcome of SWOT analysis and X-matrix analysis, e.g. how a strength is derived from the strong alignment between certain strategic objective and the metrics or how a weakness is developed over time due to a misalignment between certain strategic objective and the metrics.

2.5.4. Create the Holistic Vision of the Future

2.5.4.1. Objective

The objective of this section is to define the ideal image of the future enterprise with the understanding of the time horizon that this vision can be achieve, identify the required capabilities to build this vision and/or the vision of capabilities to acquire. The vision can be created by generating stories, user vignettes or element-based narratives. Finally, it is essential to define the evaluation criteria that will help the enterprise architects monitor and track their progress to this vision.

2.5.4.2. Required Information

The required information to build this vision includes the needs of the stakeholders defined in the second process (Performing Stakeholder Analysis), potential future needs of the stakeholders, the enterprise elements defined in the third process (Capture the current architecture) and their elements' relationships and finally the understanding of the eco-system and how the internal enterprise elements aligns with the stakeholder needs and how the enterprise elements interact with the eco-system.

2.5.4.3. Techniques

Story Generation by creating User-Vignette and Element-based Narratives are techniques to develop the holistic vision of the future (Nightingale & Rhodes, 2015). Using the story-generation approach, it is an attempt to bring the stories alive from the user's stories, based on the lenses of each of the users. This is a very powerful technique to capture both the quantitative aspect and qualitative expectations of each users and it allows the users to share freely about their desired future without a format to fit their thoughts into. And having all the stakeholders share their desire future, overlaps will form and these becomes the common ground to build consensus of the future, rally the stakeholders together. Potentially these "common ground" will become the threshold attributes of the future enterprise or the "moonshot" of the future enterprise. (Dekker, 1995)

Another technique to use is the element-based narratives to write up a mock annual report for the coming years, focusing on each enterprise elements and what the enterprise element will become in the future. (Nightingale & Rhodes, 2015)

In consideration of time horizon, there are two approaches to this aspect. First, the present-forward approach is typically used in tactic transformation or scenario planning. As the time horizon influence the possible choices of strategies that an enterprise can partake to achieve its vision, this approach leverages on the allowable time horizon to ensure a certain level of feasibility exist for the success of enterprise transformation (Nightingale & Rhodes, 2015).

Second, the future-back approach is typically used in a strategic transformation. Understanding that the consideration of time horizon may limit the possible transformation options, leading to a limited range of possibilities, this approach overcomes the time-horizon challenge by first taking a stake in the ground and focusing on the moonshot (strategic moves) that the enterprise desires to achieve before moving backwards to connect the dots by establishing feasible stages to meet. (Anthony & Johnson, 2013).

Finally, it is crucial to develop the expected evaluation criteria and even consider adopting a stakeholder-weighted evaluation criterion. It will be advisable to discussed the possible metrics, the acceptance range for each metric and the baseline.

2.5.4.4. Deliverables

The deliverable for this process is a list of clear indicators of success, either through user vignettes or element-based narratives. These stories should be clear and inspiring to most, if not all, of the

stakeholders as this is required to lead the enterprise from the existing enterprise architecture to the future enterprise architecture. It will be ideal to have the clear metrics on how the future enterprise architecture will be measured upon and the range of metrics, such as "baseline, acceptance, and exceed expectations".

2.5.5. Generate Alternative Architectures

2.5.5.1. Objective

The objective of generating alternative architecture is to explore the possibilities by producing different architectures inspired by meaningful concepts using various techniques, before deciding on one final recommendation in the next process (Decide on the Future Architecture). Before going further, it is crucial to differentiate concept from architecture.

A concept is a vision of a product or system, idea, or mental image that maps function to form. A concept is a scheme for the system and describes how the system functions. A concept is an abstraction of the system form and provides the smooth transition from the solution-neutral to the solution-specific system. To allow high-level reasoning, a concept simplifies the system architecture. Lastly, a concept is a notional mapping between two attributes: form and function, and is not a product/system attribute. (Crawley, Cameron, & Selva, System Architecture: Strategy and Product Development for Complex Systems, 2016)

An architecture, on the other hand, "is an abstract description of the entities of a system and the relationship between those entities" (Crawley, et al., 2004). This architecture of systems represents a set of decisions and reflects how the product is organized (Crawley, Cameron, & Selva, System Architecture: Strategy and Product Development for Complex Systems, 2016).

By having alternative architectures through a range of concepts, it widens the system architect and engineer's perspectives on the available options to meet each stakeholder's needs. To produce the optimized final recommendation best suited for the given time horizon, convergence of alternative architectures may eventually be required to produce a meaningful system.

As the ideation process can last a long time, there are typically two ways to which this process ends, first is by time, where the project needs to progress to the next stage, second is by idea saturation, where each new idea is minimally better and does not bring in new benefits or insights to the existing

pool of ideas, it is essential that the system architect realize this phenomenon and move on in a timely manner. (Nightingale & Rhodes, 2015)

2.5.5.2. Required Information

To generate alternative architectures, it is useful to be deeply aware of the stakeholders' values and needs, derived from the second process (Performing Stakeholder Analysis). With the stakeholder values and needs, this information provides the goals that the system architects need to work towards.

2.5.5.3. Techniques

To generate concepts, the use of **ideation** is common. While there are no rules for ideation, it is common to use a structure to lead the ideation process. In Figure 15, this is a five-step approach where the first four steps provide the sub-approach of generating concepts through various activities (Raby, 2012). The goal of concept generation is to generate as much ideas as possible for refinement in the subsequent stages. Hence, it is vital that during the ideation process, project limitations or constraints of the realities do not come into the way of generating more concepts. The purpose is to not squash any budding ideas that could cross-pollinate potentially innovative ideas from developing. The constraints and limitations can subsequently be considered after the entire list of concepts are generated.

Figure 15: Activities for Concept Ideation (Raby, 2012)

Once the concepts and the desirable attributes and functions are generated, the next step is to generate possible architectures. An iterative SWOT analysis of the concepts can help to identify the various possible scenarios of opportunities and threats, and the required strengths to capitalize on the

potential of the opportunities and overcome the threats (Nightingale & Rhodes, 2015). To further refine the list of concepts, the concepts could be separate into three buckets of "Could be", "Couldn't be" and "Shouldn't be". "Could be" are the feasible ideas. "Couldn't be" are the obvious non-feasible ideas. The "Shouldn't be" are the "Could be" ideas that are further discovered along the way that are not suitable.

After narrowing down the list of concepts, the list is used to generate of alternative architectures as seen in Figure 16. To provide a realistic list of architectures, the enterprise elements are now being formed for each of the architectures. Subsequently, an iterative SWOT analysis of architecture by enterprise elements is used to evaluate the feasibility of each architecture.

		Alternative architectures—consultancy focus		
	Facility redesign	**Architecture flexibility**	**Human factors**	**Operational and organization design**
Ecosystem	Traditional market	Traditional + industry firms	New markets	Traditional + new markets
Strategy	Healthcare and education sectors focus	Target industry firms and labs	Focus on high tech, retail, and manufacturing	Use external networks for new markets
Process	(Same)	Scenario planning and options evaluation	Research, development, prototyping	New business development
Services	Space planning and studies on utilization	Facilities planning and studies on demand	Service design and industrial design	Enterprise design and modeling

Figure 16: Comparison of four alternative architecture (Nightingale & Rhodes, 2015)

Eventually, the goal is to have five to seven alternative architectures, ready for evaluation for the next process (Decide on the future architecture).

2.5.5.4. Deliverables

The deliverable of this process is to have a list of meaningful architectures for comparison before determining the quality of these ideas in the next process (Decide on the future architecture) based on the ability to meet the stakeholder needs.

2.5.6. Decide on the Future Architecture

2.5.6.1. Objective

The objective of this process is to move forward with the recommended architecture for the enterprise. To do so successfully, evaluation of the proposed architectures needs to be evaluated based on a set of criteria aligned to stakeholder needs of the second process and the evaluation metrics needs

to baseline to those of the stakeholder expectation. Most importantly, the stakeholders need to be on the same page for the definition of each evaluation criterion as scalability for an enterprise can refer to both the workforce and the output which are two very different criterion (Nightingale & Rhodes, 2015). Time horizon is a factor that needs to be consider while determining the right architecture to leverage upon.

2.5.6.2. Required Information

Information about the stakeholder needs and their priority is important to this process and the goal of this process is to ensure alignment between the stakeholder needs and the chosen future architecture.

2.5.6.3. Techniques

Several techniques to determine the future architecture by future proofing are, 1) Testing at the extremes, 2) Scenario-based, and 3) Model-based evaluation. Alternatively, a systematic way to evaluate the architectures is by using either an unweighted decision matrix or weighted decision matrix. (Nightingale & Rhodes, 2015)

Testing at the extremes is an approach taken to imagine the worst case and best-case scenario that an enterprise can possibly face. Taking this approach, each architecture is evaluated on their ability to withstand the challenges and leverage upon the possible upside scenarios. **Scenario-based evaluation** involves the consideration of different scenarios that the architecture will face and how it may respond. This may include a single scenario as well as a combination of scenarios to test the architecture's performance. There are several **Model-based evaluations** that spans from Macro modeling, like System Dynamics and econometric, to Meso Modeling, like agent-based modeling and network modeling. Depending on the scope of the problem space that the architecture is designed to function in, the suggested approach is to match the right modeling evaluation technique accordingly.

2.5.6.4. Deliverables

The final deliverable of this process is the recommended architecture that best aligns with the stakeholder needs and if modeling was done, it should be the architecture that produces the best results from the models used.

This page is intentionally left blank

3. Proposal of Stakeholder-Managed Integrated & Learning Enterprise (SMILE) Reference Framework

In this chapter, the focus will be on **S**takeholder-**M**anaged **I**ntegrated & **L**earning **E**nterprise (SMILE) Reference Framework. The purpose of the proposed SMILE Reference Framework is to ensure that **stakeholder's** needs are being well **integrated** into the enterprise objective, process and metrics. The continuous **learning** of stakeholder needs will relentlessly shape and refine the security enterprise architecture. Ultimately, the stakeholder's needs influences & manages the **enterprise**.

SMILE Reference Framework draws its structure from the *ARIES Framework* and several other analytic methods and approaches. For the purpose of applying the SMILE reference framework onto a domain of Cyber Security, the IAM domain has been selected due to the complexity of the its challenges. In Table 8, the table shows the framework and analytic methods that are integrated to form SMILE Reference Framework.

Table 8: Integrating ARIES Framework with other frameworks to form SMILE Reference Framework

Stakeholder-Managed Integrated & Learning Enterprise (SMILE) Reference Framework			
	Structure adapted from ARIES Framework	**Complementary Analytical Methods and Tools**	**Benefits**
1	Understand the Enterprise Landscape	PESTLE Analysis, 5C Analysis, Time-Horizon Analysis	Holistic approach to analyzing the enterprise landscape
2	Perform Stakeholder Analysis	Stakeholder-weighted Needs Prioritization Matrix	Quantitative Approach to complement the qualitative approach, to provide a proportionate representation of the stakeholder needs.
3	Capture the current Architecture	5CEPS Model - 5C analysis, Enterprise Elements, PESTLE Analysis and SWOT Analysis	Identify the correlation between the various models of different yet complement levels (Macro, Meso and Micro) and connect their elements to capture the current architecture.
4	Create the holistic vision of the future	Nil	Nil
5	Generate alternative Architectures	Bias-breaking, Kano Analysis, SWOT Analysis and Morphological Matrix	Consider alternatives by challenging the existing assumptions Categorizing the needs and building a balanced architecture with an outward view.
6	Decide on the Future Architecture	Deciding on Decision Maker	Decision-making with a neutral voice

Understanding the various multifaceted IAM challenges, this chapter is dedicated to take a system-thinking approach in attempt to better manage those challenges.

3.1. Understand the Cyber Security Enterprise Landscape

PESTLE and 5C analysis will be leverage upon to create the full picture of the Cyber Security Enterprise Landscape. Subsequently, the integration PESTLE and 5C analysis will be used to draw out the relationship between the elements in the 5C and each of the contexts in PESTLE to illustrate the interaction between these elements which may become leading indicators for enterprise to monitor their enterprise landscape.

3.1.1. PESTLE Analysis of Cyber Security in the Financial Industry

Harvard professor Francis Aguilar who wrote the book, "Scanning the Business Environment." In 1967, is believed to be the original creator of the PEST Analysis. In his book, a scanning tool called ETPS was included and this was the earliest known reference about the acronym, PEST (Aguilar, 1967). This acronym was subsequently modified to create the current acronym, PESTLE.

PESTLE is a mnemonic that denotes P for Political, E for Economic, S for Social, T for Technological, L for Legal and E for Environmental. PESTLE analysis is commonly used by entrepreneurs to analyze the markets that they have intend to enter with their products or for enterprises to perform business analysis to gather an understanding of their external landscape perspective before launching a new product or service.

PESTLE analysis will be used to initiate this process before proceeding to the subsequent techniques. From a **political** perspective, IAM is used to ensure the stability of the services that a government agency provides to its citizen, e.g. ID.me for DMV CA [1] and SingPass for Singapore government agencies[2]. From an **economic** perspective, especially in the financial industry, a nation-wide cyber breach can cause market instability which can lead to a market depression. From a **social** perspective, IAM is leveraged upon to ensure the privacy of individual's personal information. For an example, with proper IAM implemented in the public healthcare industry, it provides the patients a peace of mind that their personal identifiable information is kept safe from the hackers. Losing this information to hackers will instill a sense of distrust from the patients towards the hospital and its employees, regardless of their roles, as the affected patients and close ones may conclude that the leak was due to

[1] ID,me website - https://www.id.me/about
[2] SingPass website - https://www.singpass.gov.sg/singpass/common/aboutus

weak processes founds in the hospital. From a **technological** aspect, the new cyber threats are on always on the rise, ranging from credit card fraud to ransomware attacks. Having a good IAM system can help to prevent certain Cyber Security threats. From a **legal** standpoint, there are several compliance standards that IAM can help to meet, namely, 1) Sarbanes-Oxley Act (SOX) enacted 2002 shortly after the financial scandals, with the goal of improving investor confidence by introducing transparency into corporate practices within the Financial industry, 2) Health Insurance Portability and Accountability Act (HIPAA) which was enacted in 1996 to governed the privacy of patients and their health information, 3) Health Information Technology for Economic and Clinical Health Act (HITECH) enacted in 2009, mainly to mandate federal notification of data breach related to unencrypted health information, and 4) Payment Card Industry Data Security Standard (PCI) which is an information security standard required for enterprises that manages credit cards, with the objective of improving payment card data privacy, through mandates like requiring payment details to be encrypted during transmission (okta, 2019). And more recently, in European and the companies working with their citizens, IAM can help these enterprises to manage the GDPR requirements (Notman, 2018). As for the **environmental** aspect, there are little to no push from the regulations about reducing carbon emissions or environmental footprint. Most of the financial institutions that are doing these are primary for their own branding purposes (WorldBank, 2018) or cost-reduction reasons.

3.1.2. 5C Analysis of Cyber Security

The 5C analysis (Anderson E. , 2005) which is designed for companies to perform situation analysis to understand the Company, Customer/Client, Competitor, Collaborator and Context/Climate better. This analysis takes both an internal and an external view. As Context/Climate of the 5C covers the same analysis as PESTLE analysis, for the purpose of this section, the focus is on the first 4 C (other than Context/Climate).

In the first dimension of 5C analysis, there are two aspects to this. First, at the company level where there are macro elements affect company and second, at the Cyber Security architecting team level, where the meso elements that help to build up the 5C analysis (Zacharias, MacMillan, & Van Hemel, 2008). For the purpose of this thesis, the focus will be at the company level and cyber-security team level.

Firstly, starting from the *company* level, the company elements, such as the company's goals and objectives, their performance and their image in the market, their culture, their product or service

offerings, as well as their competitive edge, helps to distinguish and identify the company's focus and strategy.

Secondly, understanding their *customer* needs from Cyber Security and how their customer-related decision making is done is vital. For financial institutions that work closely with retail banking customers, performing market segmentation analysis will provide the information to build up 5C analysis. This customer information is particularly useful to understand elements affecting the customer, especially when there is a potential correlation between the 5C customer analysis and PESTLE analysis' *social* aspect. With regards to the Cyber Security team's customers, internal customers include the senior management whom the Cyber Security team is accountable to, for protecting the enterprise at the Cyber Security realm, as well as the internal users who needs to adhere by to the Cyber Security team's policies and guidelines.

Thirdly, the term *competitor* can refer to two groups, the first group of people who competes at the **input** stage for the same resources and the second group who competes at the **outcome** stage to ensure their own survivability. For **input** (resources) competition, at the company level, competitors can include new entrants, existing incumbents or even boutique firms who are eyeing for the same talent resources, while at the cyber-security team level, competitors can include teams who shares the same budget allowed to "support services", such as the IT team. For **outcome** (position) competition, at the company level, competitors can include any financial institutions competing for the same who are eyeing for the same market share, while at the cyber-security team level, competitors can include hackers whose goal is to the opposite of the Cyber Security team.

Next, for *collaborators*, it is essential to define a collaborator before going further. To do so, there are four elements to consider as part of evaluating and defining a collaborator, 1) Value Chain Position and the value the collaborator brings, 2) Complementary Capabilities and how the enterprise benefits from these capabilities and vice versa, 3) Compatibility of goals and trust in collaboration arrangement, and 4) Commitment level on both sides, as well as the collaboration mechanism, i.e. structure and systems (Anderson E. , 2005). Having this process of defining collaborators helps to identify and understand collaborators easier.

Finally, the *Context/Climate* dimension is covered elaborately by the PESTLE analysis, the analysis of this dimension will not be performed again.

3.1.3. Integration of PESTLE and 5C for Enterprise Landscape Planning

To understand the forces affecting the decision-making process of the company and the other parties of 5Cs, it is indispensable that an integrated analysis of the factors is performed.

Having this understanding will empower us to have the knowledge and visibility of how these factors affects them and how it eventually affects us. In order to be prepared and respond in a timely manner, these are contextual information which are the leading indicators that a company needs to monitor. In Figure 17, this illustrates the relationships between the elements of the PESTLE analysis and 5C analysis.

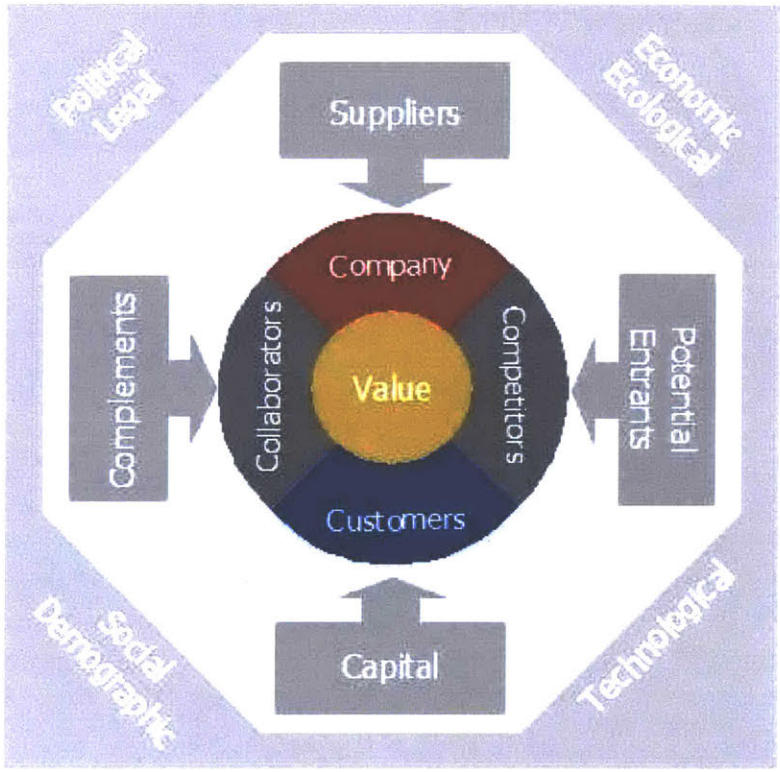


Figure 17: Overview of the Situation Analysis Framework (Anderson E. , 2005)

To perform a systematic approach to analyzing their relationship, the author proposes the use of the below Table 9 to methodically define each of the relationship between PESTLE analysis and 5C analysis elements.

Completing this table will help to explicitly call out the inter-relationships that could have be subtle or never be conceived before, providing a holistic view between the Macro (PESTLE) and Meso (5C) level.

Table 9: Integrated PESTLE and 5C Analysis

	Company	Customer	Competitor	Collaborator
Political	What are the opportunities to leverage upon or challenges faced by the **company** in the **political** aspect?	What are the opportunities to leverage upon or challenges faced by the **customer** in the **political** aspect?	What are the opportunities to leverage upon or challenges faced by the **competitor** in the **political** aspect?	What are the opportunities to leverage upon or challenges faced by the **collaborators** in the **political** aspect?
Economic	What are the opportunities to leverage upon or challenges faced by the **company** in the **economic** aspect?	What are the opportunities to leverage upon or challenges faced by the **customer** in the **economic** aspect?	What are the opportunities to leverage upon or challenges faced by the **competitor** in the **economic** aspect?	What are the opportunities to leverage upon or challenges faced by the **collaborators** in the **economic** aspect?
Social	What are the opportunities to leverage upon or challenges faced by the **company** in the **social** aspect?	What are the opportunities to leverage upon or challenges faced by the **customer** in the **social** aspect?	What are the opportunities to leverage upon or challenges faced by the **competitor** in the **social** aspect?	What are the opportunities to leverage upon or challenges faced by the **collaborators** in the **social** aspect?
Technological	What are the opportunities to leverage upon or challenges faced by the **company** in the **technological** aspect?	What are the opportunities to leverage upon or challenges faced by the **customer** in the **technological** aspect?	What are the opportunities to leverage upon or challenges faced by the **competitor** in the **technological** aspect?	What are the opportunities to leverage upon or challenges faced by the **collaborators** in the **technological** aspect?
Legal	What are the opportunities to leverage upon or challenges faced by the **company** in the **legal** aspect?	What are the opportunities to leverage upon or challenges faced by the **customer** in the **legal** aspect?	What are the opportunities to leverage upon or challenges faced by the **competitor** in the **legal** aspect?	What are the opportunities to leverage upon or challenges faced by the **collaborators** in the **legal** aspect?
Environment	What are the opportunities to leverage upon or challenges faced by the **company** in the **environment** aspect?	What are the opportunities to leverage upon or challenges faced by the **customer** in the **environment** aspect?	What are the opportunities to leverage upon or challenges faced by the **competitor** in the **environment** aspect?	What are the opportunities to leverage upon or challenges faced by the **collaborators** in the **environment** aspect?

These relationships will reveal the opportunities and threats found that the crossways of the analysis. These relationships will form the leading indicators for monitoring the enterprise landscape. Real-life examples can help to illustrate these relations.

The first example is related to the value of bitcoin (economic) and the number of ransomware attacks performed by hackers (competitor). At the junction of **Competitor** and **Economic**, the financial institute's Cyber Security team often have to deal with the hacker-introduced ransomware in the enterprise. The increase in the value of bitcoin is a cause for celebration for the Cyber Security team. As according to the article by F-Secure, the researchers found that in 2017, as the *value of bitcoin increases*, (a currency used by the hacker to prevent the tracing of fund transfer and to conceal their identity), the *number of ransomwares reduced* as the year went by. These cybercriminals who attempts to grow their pot of bitcoin, responds to the upward trend of bitcoin value by heading toward crypto-mining as an alternative to make more money. In order to process cryptocurrencies, the hackers spread crypto mining malware publicly, so as to covertly steals CPU cycles. (F-Secure, 2018)

This correlation between ransomware and bitcoin value helps Cyber Security team understand how their **competitors** behave in different **economic** scenarios. Hence, in view of times bitcoin currency devaluation, the Cyber Security ought to tighten their defense for malwares.

The second example is related to the shift of consumer's shopping preference from physical retail stores to online e-commerce stores (technology) and the change in hacking targets to obtain credit card information (competitor's interest). As the global e-commerce continues to grow by 18% from 2017 to 2018 (Young, 2019), the hacking trends follow suit. In the case of **Competitor** and **Technology,** researchers at Trustwave observed that percent of hacking incidents related to *physical retail* stores' Point-of-Sales (POS) system's **Card Track Data** has steadily declined from 41% to 36% during the period of 2017 to 2018 as seen on Figure 18. On the other hand, the percent of hacking incidents related to *online e-commerce* sites' **Card-Not-Present** (CNP) Data has grew from 18% to 25% during the same period. (TrustWave, 2019)

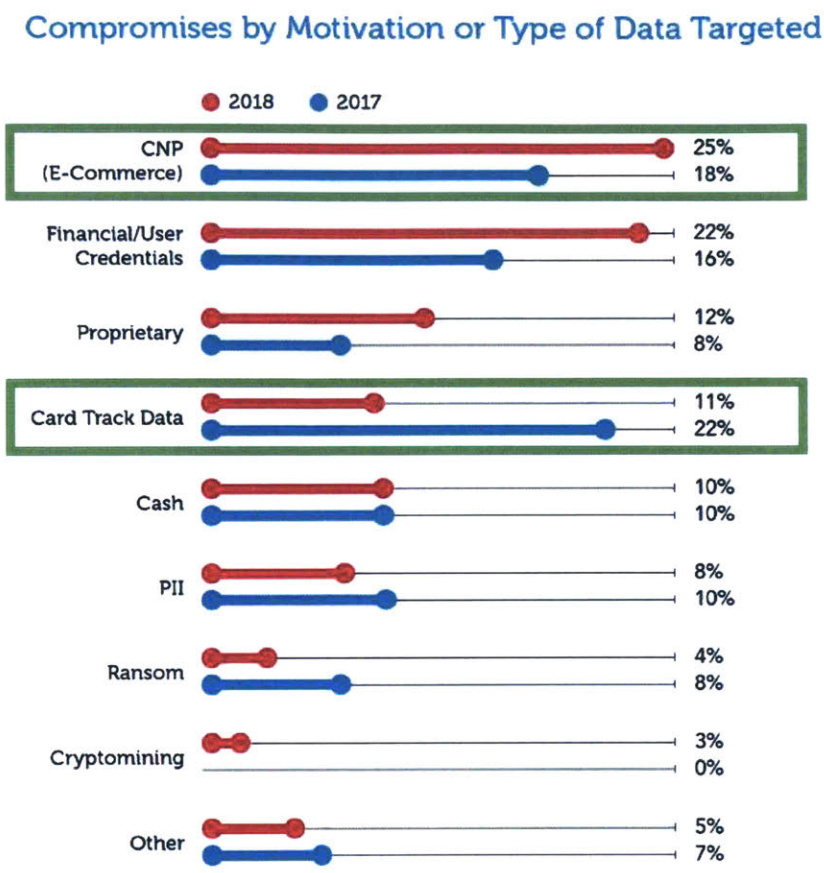


Figure 18: Motivation of Compromises (TrustWave, 2019)

As retail stores makes less money through their physical retail stores, this led to the closure of their physical stores. At the same time, the e-commerce technology improved and the number of online-retail store grew, generating more online e-commerce transactions and profits (Thompson, 2017). The hackers (competitors) started shifting their hacking targets from illegally obtaining physical Retail stores' POS **Card Track Data** to online e-commerce sites' **Card-Not-Present** (CNP) Data (TrustWave, 2019). As per the 2019 Trustwave Global Security Report, the researchers at Trustwave noted this change which reflects the hackers' awareness of the growing opportunity in the E-Commerce industry (TrustWave, 2019).

This correlation between the shift in hacking target for card data collection (competitor's interest) and shift of consumer's preference to online store (technology) can help Cyber Security team understand how their **competitors** behave in different **technology** opportunities and can tighten their defense for their customers, in view of good times of the e-commerce sites.

The third example is related to economic situations and company's budget for Cyber Security initiatives. Accord to the survey performed by KPMG, they found that during an economic crisis, 30% of the companies would reduce their Cyber Security IAM budgets due to economic pressured faced. Some of the IAM budget cuts could be as extensive as 50%. (KPMG IT Advisory, 2009)

Unfortunately for the Cyber Security teams, cyber-attacks will still happens regardless of Cyber-Security budget cuts. Hence, the key is to identify these trends and its effects, and create a forward-looking and effective Cyber Security initiatives plan that takes into consideration of these potential budget cuts.

3.1.4. Enterprise Capabilities

To determine the capabilities required for an enterprise, one possible way to start is by analyzing the potential events happening within a time horizon and the functions required to respond to the events. Keeping in line with the Cyber Security Industry standard definition of the five Cyber Security functions, the NIST Framework's five functions, namely, *Identify, Protect, Detect, Respond* and *Recover* will be used (The National Institute of Standards and Technology (NIST), 2018).

3.1.4.1. Time-horizon of Events, Functions and Enterprise Capabilities.

Taking a time-horizon approach to understanding the potential extremes that financial institute may face, below are two figures to illustrate the type of events that happen, the functions required in the stages of the event and the necessary capabilities to empower the enterprise to succeed in these events.

In Figure 19, in the normal operations (peace time), enterprise needs to identify and protect the enterprise assets. The enabling capabilities to develop are competitiveness and sustainability. Developing competitiveness is to create an edge that an enterprise has in order to survive and distinguish itself from the competitors, often this could be the image or reputation that the customers can remember them for. Within the enterprise, the IAM strategy to remain competitive include baselining their IAM capabilities to their competitors IAM capabilities, which can be done by inviting technology consultants who work across the financial industry to drive up the effectiveness of IAM deployments to provide their benching feedback. Another alternative source to obtaining competitive intelligence or benchmarking knowledge is through technology vendors who provide the IAM technology itself. Often, they are in the position of offering neutral advice and best practices to their clients.

Figure 19: Evolution of Enterprise Capabilities in Growth Scenario

Moving on to detecting these changes, the ability of remaining agility is essential to enable the enterprise to rapidly shift from one strategy to another, in order to sustain and increase their value delivery. Finally, once the teams within enterprise has committed to responding to the changes, the enterprise will start their transformation by leveraging on their existing successful features of the enterprise architecture, driving up their ability to evolve to create new ways to increase their value delivery, and scale and replicate the existing successful business units to sustain value delivery.

Next for Figure 20, this figure illustrates an additional stage, "Deadline to recover". This stage is necessary to enterprise to resume back to the normal baseline of value delivery by replicability the necessary business units that could have been affected and removed temporarily.

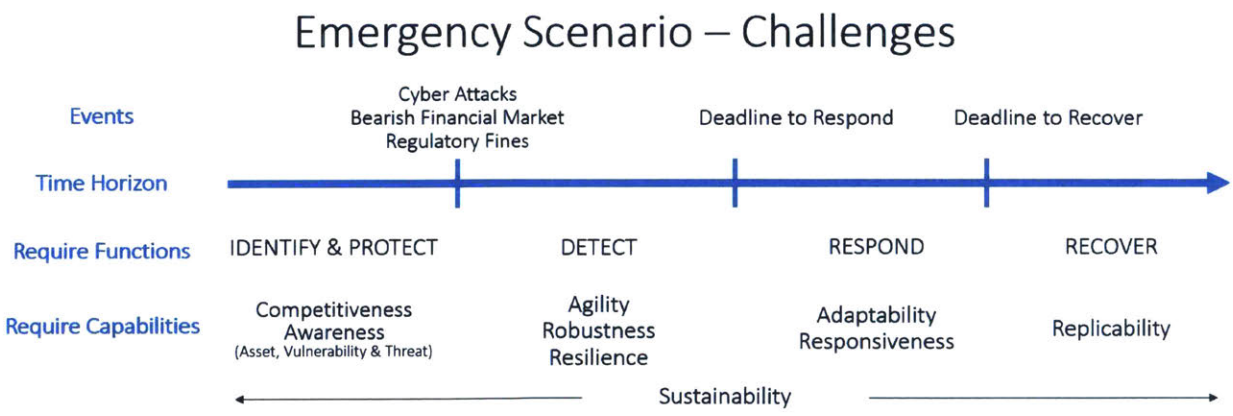


Figure 20: Evolution of Enterprise Capabilities in Emergency Scenario

In the event of detecting the impeding challenges, the enterprise needs to remain agile to switch to adopting their pre-planned strategy of dealing with these challenges. The ability to remain robust is to provide consistent value delivery despite the challenges in the enterprise ecosystem, while the ability to stay resilient is to cope effectively with the changing circumstance. In responding to these challenges, the ability to adapt by transforming the enterprise to sustain the value delivery is essential while the ability to be responsive is to provide a timely and effective approach to emerging stakeholder needs and new threats. (Nightingale & Rhodes, 2015)

3.2. Perform Cyber Security Stakeholder Analysis

In this section, stakeholder analysis will be covered, and on top of the Qualitative approach covered in the ARIES Framework and discussed extensively in chapter 2.5.3.3, a second approach, Quantitative approach, will be discussed further. Part of the Quantitative approach includes an analysis of the stakeholder's priority in the eyes of fellow stakeholders. To better understand the need for the *analysis of stakeholders*, a survey conducted in 2009 by KPMG is used to highlight a challenge.

As per the survey results (Figure 21), the greatest cause of project failures is the lack of support from management and stakeholders. Hence, to ensure that the Enterprise Cyber Security Architecture are built upon a set of needs from the *right* stakeholders, an *analysis of stakeholders* (to uncover the right stakeholders) will be performed prior to the analysis of stakeholder needs.

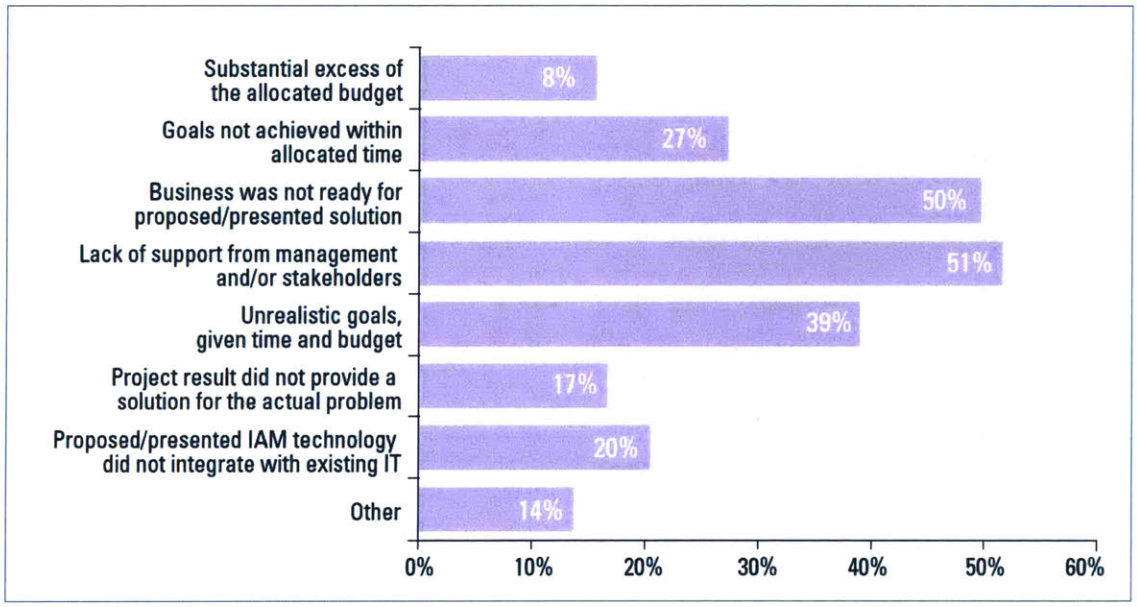


Figure 21: Causes of project failure (KPMG IT Advisory, 2009).

Typically, performing a Stakeholder Needs analysis consist of two steps, first, listing down all the stakeholders from both external and internal of the enterprise, second, after identifying the stakeholders, the stakeholder needs are being solicited and prioritized with an even-weight approach.

A potential problem with such an approach is that in most scenarios, each stakeholder holds a different priority weightage from their peer stakeholders. By evenly weighing all the stakeholders, this approach does not take into consideration of the perspective that certain stakeholder(s) may be collectively viewed more importantly by the rest of stakeholders. And in such case, this may result in an implementation based on an analysis that unaligned with reality. Potentially, such projects when going operational will require additional feature changes raised by the stakeholders of higher priority, leading to unforeseen cost increase and project delays that could have been avoided with a different approach of stakeholder prioritization.

To overcome this challenge, the author proposed a Stakeholder-weighted approach towards prioritizing the needs of the enterprise. The steps are as followed,

1) List the stakeholders
2) List the stakeholders needs
3) Perform the stakeholder prioritization exercise by filling up the stakeholder matrix

In the stakeholder prioritization exercise, each **rating** stakeholder will rate other **rated** stakeholders from 0-1 with the consideration of their own corporate objectives and the position that each **rated** stakeholder is capable of fulfilling the **rating** stakeholder's corporate objectives. Tools like the Analytic Hierarchy Process (AHP) may be consider and used to derive ratio scales from paired comparisons. The key is ensuring that the total value that each **rating** stakeholder gives to all the **rated** stakeholders must sum up to one (1). Once all the rating stakeholders complete rating the other stakeholders, the sum value of each rated stakeholder reflects the priority given to them from a holistic enterprise perspective.

This value for each of the stakeholder will be known as the **Stakeholder Priority Value.** In Figure 22, each stakeholder rates the other stakeholders in a pairwise comparison and provide their response to the system architect to complete the row related to the responding stakeholder.

	Stakeholder 1	Stakeholder 2	Stakeholder 3	Stakeholder 4	Stakeholder 5	Total (1)
Stakeholder 1	x					1.0
Stakeholder 2		x				1.0
Stakeholder 3			x			1.0
Stakeholder 4				x		1.0
Stakeholder 5					x	1.0
Actual	Stakeholder 1's Priority Value	Stakeholder 2's Priority Value	Stakeholder 3's Priority Value	Stakeholder 4's Priority Value	Stakeholder 5's Priority Value	
Normalized (x/total)	Stakeholder 1's N. Priority Value	Stakeholder 2's N. Priority Value	Stakeholder 3's N. Priority Value	Stakeholder 4's N. Priority Value	Stakeholder 5's N. Priority Value	

Figure 22: Stakeholder Prioritization Matrix

4) Perform the needs prioritization exercise by filling up the needs matrix

After completing the Stakeholder Prioritization matrix, each stakeholder will now prioritize the enterprise stakeholder needs obtained from step 2. This may include rating needs that the rating stakeholder did not state, as these needs may be derived from their peers at the enterprise. Similarly, each **rating** stakeholder will rate the needs from 0-1 with the consideration of their own corporate objectives and how each need is essential to the **rating** stakeholder's corporate objectives. Likewise, tools like the Analytic Hierarchy Process (AHP) may be used to derive ratio scales from paired comparisons. The key is ensuring that the total value that each **rating** stakeholder gives to all the enterprise **needs** must sum up to one (1). Once all the rating stakeholders complete rating the enterprise needs, the sum value of each enterprise need will reflect the priority given to them from an individual stakeholder perspective.

This value for each of the stakeholder need will be known as the **Need Value.** In Figure 23, the stakeholders will rate each of the needs, including the needs listed by other stakeholders that the responding stakeholder may not have listed. Each stakeholder rates the other needs in a pairwise comparison and provide their response to the system architect to complete the row related to the responding stakeholder.

	Need 1	Need 2	Need 3	Need 4	Need 5	Total (1)
Stakeholder 1						1.0
Stakeholder 2						1.0
Stakeholder 3						1.0
Stakeholder 4						1.0
Stakeholder 5						1.0

Figure 23: Needs Prioritization Matrix

5) Using the results of step 3 and 4, calculate the stakeholder-weighted value for each need.

Using each of the individual **needs value** from the previous process and the **stakeholder priority value** from the Stakeholder Prioritization matrix, these values are multiplied together to derive the **stakeholder-weight priority value.** In Figure 24, leveraging on the data collected from Figure 22 and Figure 23, these values will be multiplied to obtain the actual stakeholder-weight priority value.

	Stakeholder Priority Value	Need 1	Need 2	Need 3	Need 4	Need 5	Total (1)
Stakeholder 1	Stakeholder 1's N. Priority Value						Stakeholder 1's N. Priority Value
Stakeholder 2	Stakeholder 2's N. Priority Value						Stakeholder 2's N. Priority Value
Stakeholder 3	Stakeholder 2's N. Priority Value						Stakeholder 2's N. Priority Value
Stakeholder 4	Stakeholder 2's N. Priority Value						Stakeholder 2's N. Priority Value
Stakeholder 5	Stakeholder 2's N. Priority Value						Stakeholder 2's N. Priority Value
Actual	---	Need 1's Priority Value	Need 2's Priority Value	Need 3's Priority Value	Need 4's Priority Value	Need 5's Priority Value	
Normalized (x/total)	---	Need 1's N. Priority Value	Need 2's N. Priority Value	Need 3's N. Priority Value	Need 4's N. Priority Value	Need 5's N. Priority Value	

Figure 24: Stakeholder-Weighted Needs Prioritization Matrix

3.3. Capture the Current Cyber Security Architecture

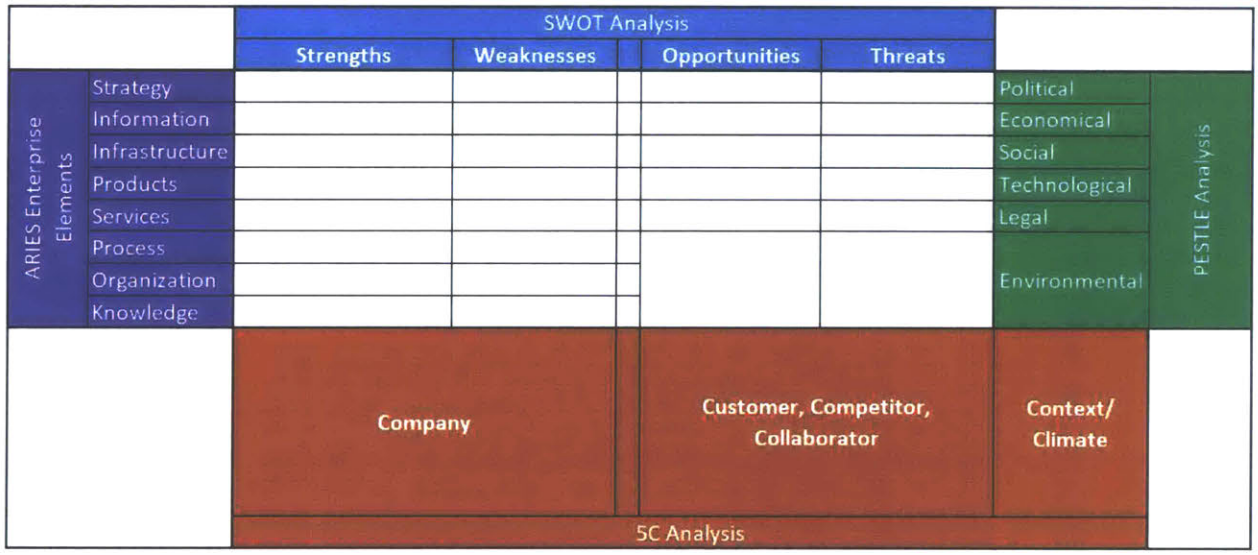
In this section, two techniques will be elaborated upon; first, the 5CEPS Model which focuses on the strategic level to scan and capture the Cyber Security Architecture, second is the X-Matrix, which is used analysis at an operational level.

3.3.1. Cyber Security SWOT, "Enterprise Elements as Lenses" and PESTLE

As the book, "Architecting the Future Enterprise" encourages us to take the approach of enriching a SWOT analysis with the "Enterprise Elements as Lenses" (Nightingale & Rhodes, 2015), the author encourages the readers to go even further by leveraging on the PESTLE analysis and 5C Analysis performed earlier for the external aspect of the SWOT Analysis (Opportunities and Threats).

As per David Marr explanation about the goal of gaining complete understanding of information processing system is that the analysis must be understood at three distinct yet complementary levels of analysis, namely the Micro, Meso and Macro, as the analysis at one level itself is insufficient. (Marr, 1982)

Table 10: 5CEPS Model



In the same approach, PESTLE analysis, 5C Analysis, ARIES Enterprise Elements Lens approach and SWOT comes together to provide this complete understanding of the enterprise. PESTLE analysis provides the *Macro* perspective, the 5C analysis provides the *Meso* perspective, and ARIES Enterprise Elements Lens approach provides the M*icro* analysis. The SWOT Analysis connects all of these three perspectives by first, identifying the opportunities and threats at both the Meso and Macro level, then identifying the strengths and weakness at the Micro level. This approach leverages on existing analytic methods to holistically view the external ecosystem and internal landscape and to enhance the perspective with

SWOT analysis. This forms the **5CEPS Model**, which denotes **5C E**lements **P**ESTLE **S**WOT, as shown in Table 10.

The author also notes that the analysis of the Strengths and Weakness does not need to align directly to the Opportunities and Strengths that are located on the same line, as such the middle blue bar is denoted to break the visual connection.

One strength of the 5CEPS model is that it helps to open up the perspectives between opportunities and threats and link that across the PESTLE analysis. One example is about hacker's motivation. Most would assume that hackers perform hack to make money. Based on a report (2018 Hacker Report, 2018) as shown in Figure 25, it shows hackers are motivated by a varying number of reasons. Some hackers are motivated to help others (socially), some are motivated to make money (economic), and some are motivated to protect and defend (political). Depending on the preconception, e.g. hackers hack for money (Economic Threat), enterprises can turn the hacking activity into a social or political opportunity by have hackathons that offer bounties reported or bragging right by publishing the hacker's ability in the mainstream paper or even offer them a full-time role.

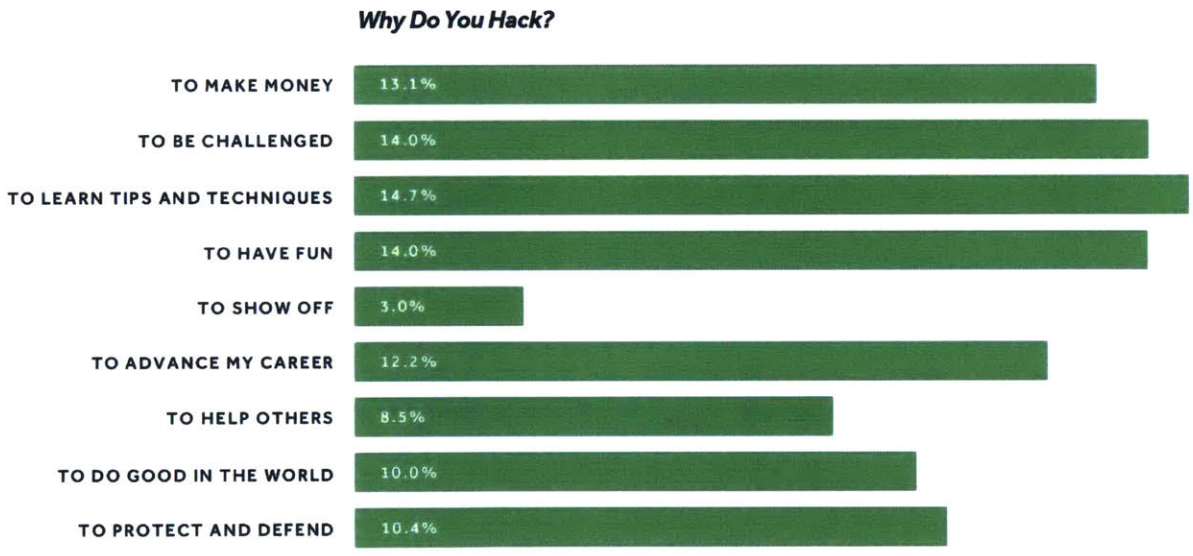


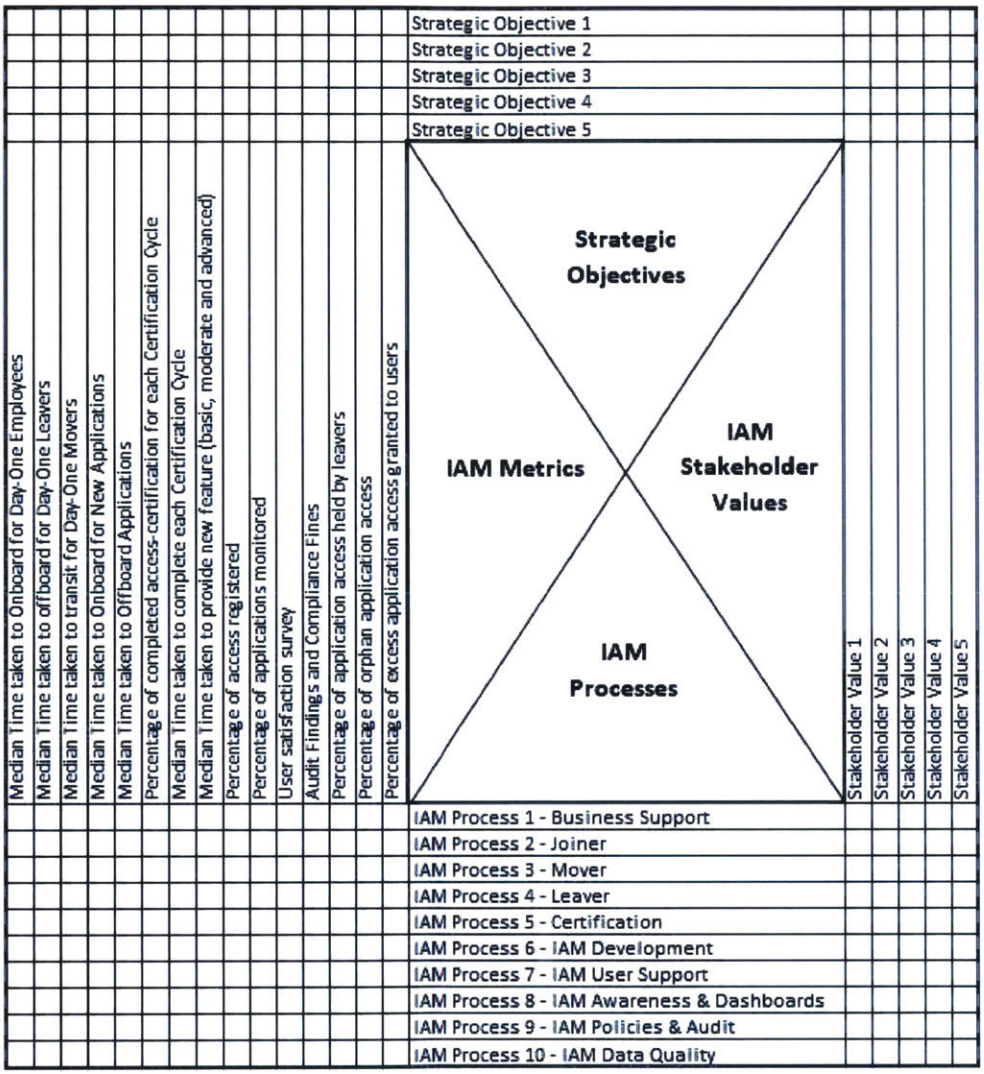
Figure 25: Hackers' Motivation

After consolidating the SWOT analysis with both frameworks, the eventual goal is to identify for each opportunity and threat, the best combination of enterprise elements to tap on the opportunity or to mitigate or remove the threats. In the event that that no enterprise elements or combinations are found to be adequate for the specific opportunity or threat, this could a be indicator of an existing enterprise weakness that waiting to be improved upon.

3.3.2. X-Matrix

The use of the X-Matrix enables the System Architect to consistently drive pair-wise alignment between the strategic objective, stakeholder, key processes and metrics. By doing so, as a whole, the enterprise becomes aligned from the beginning (strategic objectives) to the end (metrics).

Table 11: X-Matrix of IAM Security Architecture



In Table 11, this table provides an example of how an IAM X-Matrix will look like. Considering that Strategic Objective may vary among financial institutions and with different focus and values from stakeholder focus, the author had provided the typical IAM process and metrics as part of the X-Matrix above as an illustration.

3.4. Create the Holistic Vision of the Cyber Security future

The story generating techniques to apply in creating the holistic vision are 1) User-Vignette Narrative and 2) Element-based Narrative.

In the User-Vignette Narrative, it is recommended to leverage on the same list of stakeholders identified in the second process, Perform Cyber Security Stakeholder Analysis. Understanding the stakeholder needs and to develop a moon-shot perspective, asking question like "What will my stakeholder want to see in IAM in the next five year?", "What does it take to impress them?" and "What are their current challenges that should no longer appear in the next five years? "

An example will be like, a CISO sharing his vision, "Today we have so much data-issue in our IAM system, with over 5000 orphan application access belonging to no-one, potentially from the 250 leavers that we have yet to be disable their access. Due to this negligence on our part, we have been fined over $10 million dollars due to the potential threat to the enterprise and the tremendous impact on the financial industry. To help us move forward, we need to have a zero-tolerance to such incidents and have automation within the next 5 years, removing primary access within 24 hours and secondary access within the next 5 working days. A weekly alert on such access will be triggered to the Chief Risk officer and myself so that we remain accountable. Teams account or identities found to have such access will be closely monitored or disabled at the closest possible opportunity. Being able to solve enterprise-wide epidemic, we can save our enterprise $50 million or more over the next 5 years, drive up both productivity and security for our users and the investors who trusted us with their assets."

In the above paragraph, it reflects a deep challenge that many financial institutions face, the efforts required to move forward and the potential gains.

In Element-based Narrative, this approach brings the focus to the enterprise elements one at a time and for an IAM product with a renewed enterprise architecture, the following is an example.

"Five years ago, we dream of an Amazon portal for our users to shop for their required access or hardware or software, where the users can compare with our existing internal offering with real-time & updated direct offering from our strategic partners. These users can "purchase" their items, which are subjected to their "credit card clearance" (their manager approval and department budget limit). These items can come as soon as minutes (for automated installation of application access or creation of access) to days (for a new customized machine). All these with just a few clicks, saving users from the painful

paper request and manual follow of status. Today, this project automated the request management process and increased the enterprise efficiency by 500x while lowering the cost by 70% within 5 years."

The above narrative is a success story that all CISO wish to hear about their IAM projects from their customers.

With regards to the metrics, it is important to ask stakeholders, who partake in this process, about their opinions on metrics. As the saying by Rheticus in the 1500' goes, "what gets measured get done" (Henderson, 2015). If the enterprise effectiveness is measured with a wrong set of metrics, it may essentially lead even the most efficient enterprise down the wrong road of attaining an unwanted goal at a high speed. Having a diverse set of stakeholders helps to provide a holistic set of metrics that aligns them to the right set of strategic objectives. In the event that any new metric is defined or any existing metric is re-baselined in this process, it is imperative to add these new metrics to the X-matrix of the previous process.

3.5. Generate Alternative Cyber Security Architecture

Having create a holistic vision of the future, given the required capabilities and understanding the availability timeline, it is now time to generate concepts and architecture to fulfill the holistic vision. In this section, three techniques to generate alternative architectures will be discussed, 1) Bias Breaking, 2) Kano Analysis, and 3) Morphological Matrix.

3.5.1. Ideation by Bias Breaking

Bias-Breaking, as taught by Emeritus Professor Hideyuki Horii (I-School/JSIC Executive Director) of University of Tokyo, is a very effective way of generating new ideas. As per Margaret A. Boden, there are three type of creativity, combinational creativity, exploratory creativity, transformational creativity (Boden, 2004).

One possible approach is to analyze existing architectures, understand the ends and the means of the existing architecture, understand the conceptual constraints that led to the past architectural decisions and question the validity and existence of the bias in the given modern context. A real-life bias-breaking example can be illustrated by Amazon Go, where the previous bias that most held was that to check out at grocery store, the process of paying at the cashier is required, yet this is process where most of the time is wasted. Amazon Go's idea challenged this fundamental bias and broke it by using its Amazon Go app, having the users take the items they want and walk out of the store without stopping at the

cashier. All the users have to do is to scan their phone on a turnstile as they enter the store (Bhattarai & Harwell, 2018).

Amazon Go is able to achieve this by having a large, camera-friendly code on each item to help the cameras determine the item that has been picked. The Amazon Go systems combine the camera information with data from weight sensors installed in every shelf. (Bhattarai & Harwell, 2018)

3.5.2. Concept Selection through Kano Analysis and SWOT Analysis by Enterprise Elements

To understand the customer needs better, **Kano analysis** (Figure 26) was developed in 1984 by Emeritus Professor Noriaki Kano, a Tokyo University of Science (TUS) full professor who specializes in quality management. This model is used to categorize the customers' needs or preferences and identify the best way to fulfill the needs accordingly. (Kano, Seraku, Takahashi, & Tsuji, 1984)

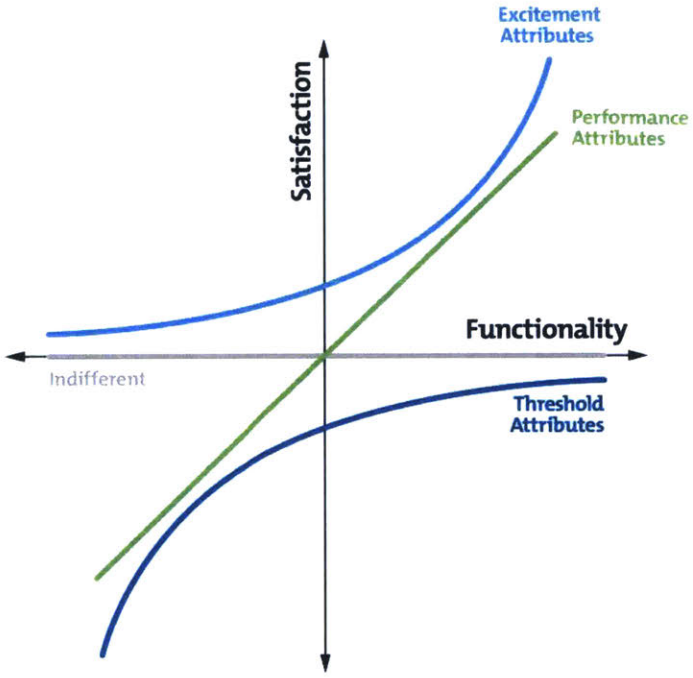


Figure 26: Kano Model Analysis (The Mind Tools Content Team, 2016)

In this model, there are three types of attributes to products and services. First, the *threshold* attributes or *hygiene* attributes comprises of the basic features that customers expect to have given the amount they have invested in the product or services. A lack of the threshold attributes will result in user dissatisfaction, in the case of an average restaurant, this can be exemplified with a clean table and clean cutleries and the lack of a clean table or cutleries will result in customer dissatisfaction. However, giving users more of a threshold attribute will plateau the satisfaction at certain degree, e.g. cleaning the table

to the last speck of visible dust is good but cleaning towards a goal of pure-white table may not significantly increase the satisfaction for all users.

Second, *performance* attributes, which consist of elements that are not necessary yet providing them increases the user satisfaction. For example, in restaurants, this could be providing free Wi-Fi or unlimited soda-refill for a fix price where normally restaurants do not provide Wi-Fi nor often provide unlimited soda.

Third, *excitement* or *delighters* attribute, where elements that are often not expected are provided, giving the users a surprise and can even increase the competitive edge of the enterprises. In the context of restaurants, a delighter attribute could be an exquisite dessert that the chef prepared specially for their customers and this is served at the end of the meal at no-cost of the customers.

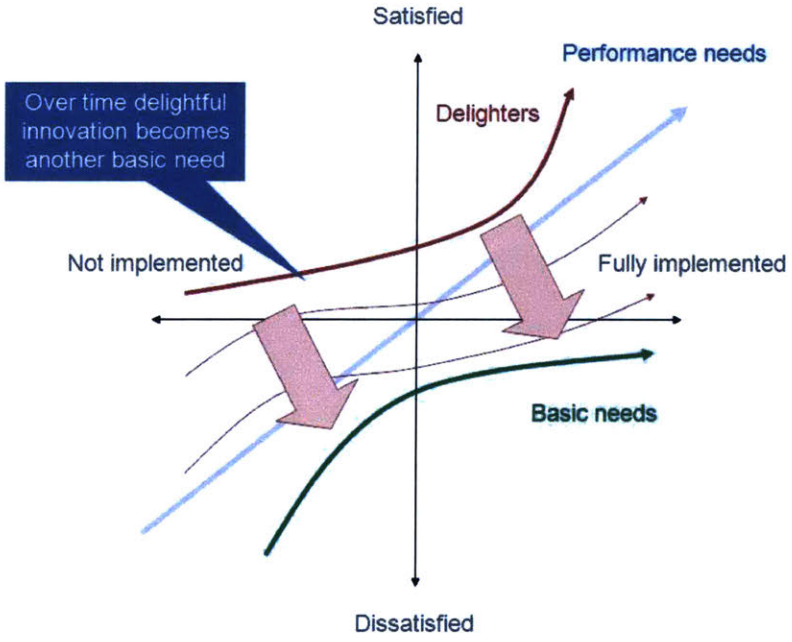


Figure 27: The natural decay of Delighter attributes to a basic need over time (Brown, 2012)

Over time, as user expectation increases, a natural decay for delight starts to occur as seen in Figure 27. For example, free Wi-Fi becoming a norm in restaurants, a performance attribute may evolve to a threshold attribute, where restaurants not having Wi-Fi may be an outlier. A classic example is the act of installing applications on PC which used takes hours, is now taking minutes as we download applications unto our mobile phones. As user's expectation increase, a new delighter needs to outdo their existing delighter, as in this case, the next revolutionary technological product for person computing

should take seconds to install applications or should have the applications already installed before the user's first login.

After categorizing the concepts' attributes with Kano analysis, the further refinement of the concepts is done by performing SWOT analysis. An iterative SWOT analysis of the concepts by the enterprise element can help to identify the various possible scenarios of opportunities and threats, and reveal the required strengths needed to capitalize on the potential of the opportunities and overcome the threats (Nightingale & Rhodes, 2015)

3.5.3. Architecture Generation by Morphological Matrix

Morphological Matrix (Figure 28) is a powerful tool to help system architects systematically generate numerous ideas and subsequently identify the innovative ideas that are the most feasible and attractive to their users. To use the morphological matrix, it is important to identify the functions required by the system that needs to be build (as seen on the left column of the Morphological matrix below).

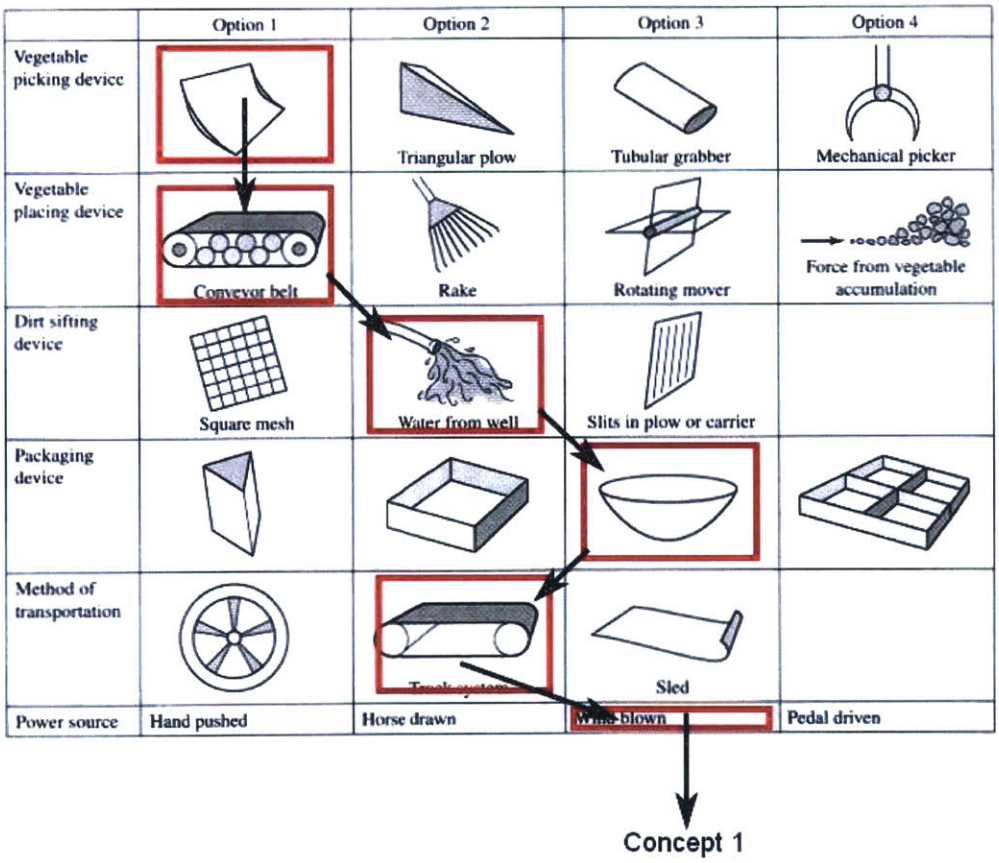


Figure 28: Morphological Matrix - Generating concepts (Sáenz, 2015)

Next, for each function determine the available options. Once the options have been provided, to generate a complete concept, an option will be selected for each function. By choosing different permutations, for the simple morphological matrix example show above, there are 2304 possible concepts to consider. It is also crucial to note that while the goal of morphological matrix is to generate numerous ideas, it is important to subsequent measure the quality of these ideas in the next process (Decide on the future architecture).

The strengths of combining the various methods together are tremendously, one example can be the use of bias-breaking to question each function that is stated as required in the morphological matrix. Such an approach of thinking will increase the creativity level of the architecting team and potentially lead to new breakthrough of idea and innovation.

The down-selection process can leverage upon the Kano Analysis to compare the concept as a first round of down-selection, to separate the "could be" options from the "couldn't be" options. (Nightingale & Rhodes, 2015) Having a good concept that has options that meet all three categories of the Kano Analysis will be ideal. Another way to perform the down-selection is by performing a SWOT of the concepts to have an understanding on how the concept interactions beyond the enterprise. Eventually, the goal is to have five to seven alternative architectures to evaluate for the next process (Decide on the future architecture).

3.6. Decide on the Future Cyber Security Architecture

In this section, the focus will be defining the right approach to decide on the right future Cyber Security architecture. Deciding on the right approach is essential as per the rule of ten. As by the time the architecture is decide upon, while only 8% of the total budget has been *spent (*Figure 29*)*, at that juncture, 80% of the budget has already been *determined* by the architecture. (Anderson D. M., 2014)

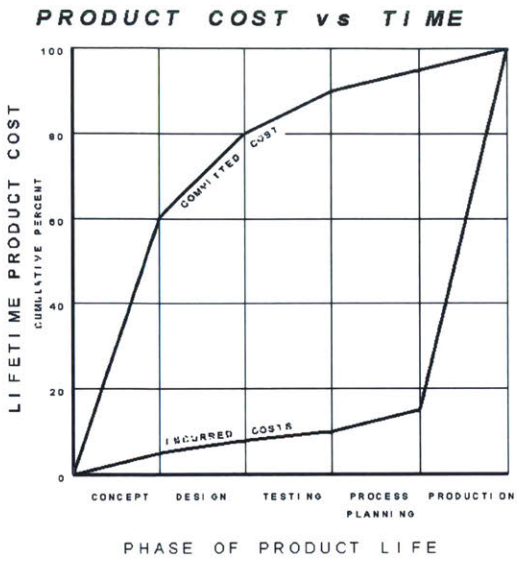


Figure 29: Product Cost vs Time (Anderson D. M., 2014)

As such, there are three required key activities that form the process to decide the future Cyber Security Architecture. First, the forming of the decision-making committee which consist of the selection of members of the committee and the definition of the evaluation criterion. Second, future proofing of the architecture to ensure that minimal changes or non-critical changes are introduced later. Third, defining the methodology taken to make the decision. With these three activities, they form the process to decide the future Cyber Security Architecture.

3.6.1. Deciding on the Decision Maker for the Cyber Security Architecture

The goal of this activity is to find "non-sponsored" neutral individuals who align themselves to the core of the enterprise more than to any functional departments. Ideally, the individuals that make up the group of decision makers are vested in the enterprises' long-term well-being and are affected by the consequence from both the short-term and long-term decisions made for the Cyber Security Architecture. These individuals should also be aware of how the enterprise functionally and culturally operates. These individuals should understand the general sentiment of the perception towards changes. These individuals should have a grounded view of the enterprises from both internal and external perspective. Ideally, they should understand Cyber Security landscape of their industry, the challenges and the opportunities in the Cyber Security landscape and have a decent understanding of the elements of the Cyber Security Architecture. Certainly, some of these individuals may not be familiar with all the Cyber Security jargon and advancements. It is at this juncture that enterprise should seek expert opinions by engaging Cyber Security Consultants who are well-versed in Cyber Security best practices for the

respective industry. Finally, these individuals should be well-respected by the employees of the enterprise as they are the key decision maker for Cyber Security Architecture that is meant to protect the enterprise.

The essence of the author's perspectives is also captured in the article, "*Salience, Credibility, Legitimacy and Boundaries, Linking Research, Assessment and Decision making*". In this article, the discussion is about managing boundaries, and in our case, different stakeholder needs and the domains of these needs. And to manage boundaries, it requires the effective linking of knowledge to action through the means of salient, credible and legitimate information. **Saliency** is the *importance or relevance* of the information. **Credible** is the degree of which the information is deemed *scientific* and the level of *technical adequacy*. **Legitimacy** refers to the *fairness* of the information or process of obtaining the information and the degree of *inclusion* of appropriate interest, values and concerns from various perspective. (Cash, et al., 2002)

To integrate *saliency* and *legitimacy* into the decision-making process, it is crucial to ensure that every member of the decision-making team have the same mental definition of the evaluating criterion by introducing the definition of metrics. Definitions of the metrics may include the context of how the metrics is defined and the relationship of the metrics to the stakeholder needs. The scope of the Cyber Security Architecture metrics should cover a wide range of metrics, not limited to Cyber Security, including those metrics affecting business, operations, risk and technology.

The evaluation metrics baseline can be adjusted as required. It will be prudent to seek the opinion of the stakeholders to understand the context in which the baselines were defined and adjusted to account for any new perspectives. New innovative capabilities may not have a well-established metrics. Three other possible consideration for determining metrics will be to adapt 1) the specific industry's **best practices** for evaluation criterion or 2) **existing** industry metrics used by other companies or 3) **new metrics** recommended by Cyber Security consultants, catered for the enterprise to measure their Cyber Security capabilities' effectiveness and efficiency.

3.6.2. Future-Proofing the Cyber Security Architecture

To future proof the Cyber Security Architecture, there are two approaches to perform this activity. The first approach is to perform the testing of extreme Cyber Security conditions. The second approach is the Scenario-based testing of Cyber Security Architecture.

For the testing of the extremes positive Cyber Security conditions, samples conditions can include the following, a Cyber Security team with unlimited budget, the company grows by 1000%, no demands

from the users, no regulations to meet and have all the staffing needs met and will continue for the same in the next 5 years. What are the potential opportunities to leverage upon and the challenges? For an enterprise to be growing so well, there will be a huge headcount of hiring from all departments, and there will be a lot of attention from the media, leading to the heightened awareness of the enterprise to the cyber-criminals who will want a part of the growing pie. The good news is that the enterprise will have sufficient analyst to monitor the cyber scene, yet with the increased number of analysts, information about existing vulnerability and potential hacks get lost in the poor quality of interaction due the vast number of Cyber Security analyst.

For the testing of the extremes negative Cyber Security conditions, samples conditions can include the following, the Cyber Security team having insufficient budget, the company does not grow well, users are demanding for new capabilities, the enterprise is failing regulations and have insufficient staff due to the retrenchment and will continue for the same in the next 5 years. For an enterprise doing so badly, there will be a huge headcount of people leaving from all departments, and there will be minimal attention from the media, leading to the reduced awareness of the enterprise to the cyber-criminals. The good news is that no one wants to hack such an enterprise and the bad needs is with reduced staffing, a lot of automation needs to be done yet automation needs time and effort, which the enterprise does not have.

Extreme conditions can consist of a mixed of the enterprise elements. Using a diverse combination of enterprise elements conditions, this can provide a wide range of extreme conditions to assess for.

Table 12: Scenario-based testing for two architectures

Existing Architecture Capabilities	**Upside Scenario**	**Downside Scenario**
Full-automated Cyber Security Capabilities	Automation of the capabilities enable the enterprise to comply to the new regulations easily and automate the monitoring process.	Cost creep for projects that are over-customized. Time to develop capabilities. Constant restructuring of talent teams may be required as the demand of capabilities from the industry evolves. High cost of labor may make automation of new Cyber Security process a challenge.
Semi-Manual Cyber Security Capabilities	Cost savings from not hiring more people previously is now being used to hire ad-hoc help.	More time and effort are needed to comply to the new regulations. Time to train the news staff is delaying the compliance needs. With increase cost of labor, this increases the cost of operations.

Next, Scenario-based testing studies how each alternative architecture will respond under different abstract futures. Scenario A is related to financial crisis (downside scenario), where regulators found that a financial scandal related to unauthorized access that allowed a trader to perform unauthorized trading. New regulations have been formed and are affected immediately. Financial institutions have 3 months to comply by building the necessary process and tools to ensure that the checks are in place. Scenario B is related to an economic growth (upside scenario), where now Cyber Security talents are demanding for more salary or risk being poached to competing firms. The consideration of the relationship between the Cyber Security Architecture and the different external scenarios (Table 12) should be included as part of the Enterprise Cyber Security Architecture evaluation criterion. By performing these two activities, it ensures alignment between the stakeholder needs and the chosen future architecture while ensuring the robustness of the chosen future Enterprise Cyber Security Architecture to withstand external conditions and scenarios.

3.6.3. Cyber Security Weighted Decision Matrix

To weigh the needs and assess each architecture decisions, there are two ways to evaluate the architecture decisions of the Enterprise Cyber Security Architecture. The first method is with an unweighted decision matrix. The second method is with a weighted decision matrix. (Nightingale & Rhodes, 2015)

Due to the complex environment with numerous stakeholders that Enterprise Cyber Security Architectures are designed for, the author recommends the use of a weighted decision matrix (Figure 30) to match the degree of enterprise complexity and to evaluate the various Enterprise Cyber Security Architectures.

In this section, it is important to reference the SMILE Reference Framework, Stakeholder-Weighted Needs Prioritization Matrix. The evaluation **criterion (Error! Reference source not found.** second column) should match the Stakeholder needs. The **criterion weightage (Error! Reference source not found.** third column) should match the Stakeholder Weighted Priority (SWP) value from Stakeholder-Weighted Needs Prioritization Matrix.

					Candidate architectures				
					As-is	Outsourcing all	Backsourcing	Outsourcing team	Process owner
Criteria	Scalability	8%	Allows growth while minimizing complexity	50%	3	4	2	5	4
			Long-term relationshop and coordination	50%	2	5	5	5	4
	Reliability	15%	Supplier excellence	75%	3	4	5	5	4
			Supplier availability	25%	4	4	5	5	4
	Manageability	22%	Use of performance metrics	50%	2	4	5	4	3
			Facilitates communications	50%	2	3	3	4	3
	Flexibility	9%	Ability to react to market conditions	100%	3	5	0	4	4
	Cost	24%	Labor costs	40%	3	5	4	4	4
			Hidden costs	20%	4	2	0	3	3
			Implentation costs	40%	5	0	0	1	4
	Cycle time	22%	Improves delivery compliance	65%	3	3	5	4	4
			Facilities lead-time reduction	35%	4	3	3	4	5
					3.1	3.41	2.86	3.89	3.81
	Ranking				4	3	5	1	2
	Risk and transformability				✔	✘	✘	★	✔

Figure 30: Weighted decision matrix for Enterprise Architecture (Nightingale & Rhodes, 2015)

Both the architecture decisions and rating (**Error! Reference source not found.** column 4 and column 5) should be defined and rated by the group of decision-making who have salient, legitimate and credible background. The architecture decisions and ratings should be determined *before* showing the various possible architectures (**Error! Reference source not found.** columns 7 to 9). This is to ensure a fair decision-making process and to avoid an unnecessary bias that may sway the weightage of a particular criterion which may be a strength of a particular architecture. In **Error! Reference source not found.**, using this use of a weighted decision matrix, this can help to evaluate the various architecture to make an informed and sound decision.

Table 13: Rating scheme relative to Reference Architecture

Relative Performance	Rating
Much worse than reference architecture	1
Worse than reference architecture	2
Same as reference architecture	3
Better than reference architecture	4
Much better than reference architecture	5

As part of the rating, Table 13 shows the rating scheme used to rate the architectures. This is a typical five-point scale commonly used to rate alternatives to a reference architecture.

In conclusion, by determining the decision-making committee, performing the future-proofing activities, as well as developing the Cyber Security weighted decision matrix will help the committee have a structured approach to consider various architecture by their strengths in each future scenario and evaluate these architectures in a manner aligned to the general agreed priorities of the decision-making committee, and finally, down-selected the most optimal Cyber Security architecture for the enterprise.

This page is intentionally left blank

4. Application of SMILE Reference Framework to a Hypothetical Case

The purpose of this chapter is to evaluate and provide an initial validation of the applicability of this thesis's proposed reference framework by using a hypothetical case. To keep the hypothetical case as realistic as possible, the hypothetical case will be based on publicly sourced information and various known Cyber Security cases about financial institutions. The hypothetical case elements will be drawn from various inferences, which include enterprise elements and Cyber Security context from real financial institutions across the world. Due to the sensitivity surrounding enterprise Cyber Security operations and IAM operations in financial institutions and the public publication of this thesis, a hypothetical case is used in place of an actual case.

In this chapter, the focus will be on a hypothetical case on the **Bank of Secured Serendipities (BOSS).** This enterprise is a global financial institution headquartered in New York, managing 5 trillion USD worth of assets, with over 500, 000 employees. BOSS provides financial products and services to over 20 million customers in over 188 countries. [3]

A new Chief Security Officer (CSO) was hired from externally due to a series of unfortunate events occur, requiring the previous CSO to step down from the role.[4] The case will be on how the new CSO will need to start from scratch to grow his influence among the key stakeholders while transforming the enterprise given the limited control he has over the entire enterprise. There will be tremendous challenges and opportunities that he will face. The case will focus on the application of the SMILE reference framework, *Stakeholder-Managed Integrated & Learning Enterprise (SMILE)* Reference Framework to BOSS's enterprise elements.

4.1. Understand the Enterprise Landscape

In this section, both PESTLE analysis and 5C analysis are used to analyze the enterprise ecosystem. The 5C analysis will be applied to BOSS to better understand their company, customer, competitor, collaborator and context/climate. The company's context will be analyzed using the PESTLE analysis.

[3] Adapted from several banks stated on https://www.doughroller.net/banking/largest-banks-in-the-world/
[4] Adapted from the case of SEC and the EDGAR breach on https://fcw.com/articles/2018/09/20/sec-cio-cyber-shuffle.aspx

4.1.1. PESTLE Analysis of BOSS

From a **political** aspect, the CSO has started to consider relocating their data warehouse abroad for cost-saving reason[5]. However, a recent bill around privacy and security has been introduced to prevent the flow of US customers' financial data from flowing out of the US to safeguard the interest of Americans' privacy[6]. The CSO has to also consider the various cross-border data flow controls as he plans for the data migration to a lower cost data warehouse as shown in Figure 31.

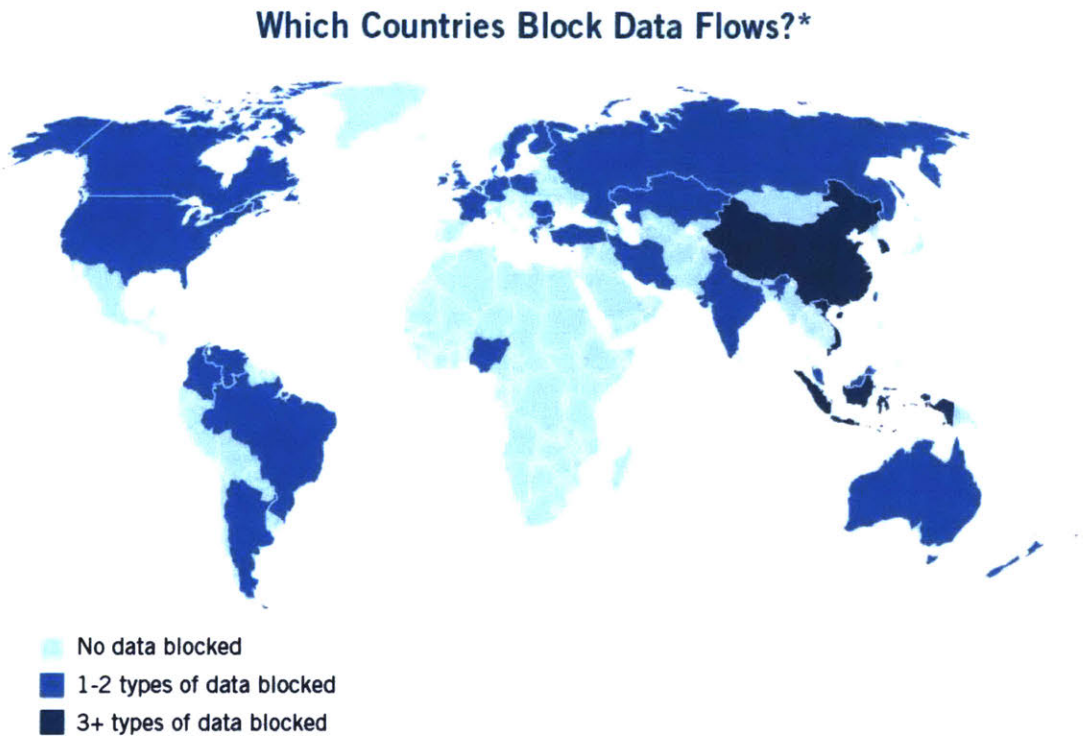


Figure 31: Data Flow control measures global comparison (Cory, 2017)

From a global **economic** perspective, the last major global economic downturn happened in 2008. Due to a subprime-mortgage crisis, this event started in US before its effects propagated across the global. And before the 2008 global financial crisis, the last major crisis was in 1997 Asian Financial Crisis that started in Thailand. Skeptics have been saying for years that "this year" is going to the year of the new financial crisis. Regardless of the skeptics, BOSS remains with its balanced perspective and will not perform any layout unless required. BOSS remains prudent in their spending, focusing primarily in long-term

[5] Adapted from Gartner's list of ways to cut cost on data centers on https://www.informationweek.com/software/7-ways-to-cut-data-center-costs-gartner/d/d-id/1080448

[6] Adapted from Cross Border Data Barrier article on https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

financial and operational investments. BOSS is estimated to continue growing at 5% each year and plans to increased their headcount at the same rate. There are no challenges funding their projects. However, during each financial crisis, the restructuring of the enterprise occurs to help the enterprise align its revenues and expenses to the market condition. The Cyber Security team, unfortunately, is also affected by such headcount cuts. The only challenge they face is to breaking the corporate and functional silos and creating organizational synergies by integrating the various Cyber Security projects.

Financial institutions' **social** engagements with their customers have changed dramatically over the last decade. Given the pervasiveness of online transactions and the comfort level that the millennials have with online services, new boutique online banks start to emerge. These new-age banks do not have a physical presence and only have global online presence. These banks are able to receive funds from any company or bank all over the world and allows their clients to withdraw cash at any ATM with minimal fees. The phenomenon to transact anywhere anytime with a mobile device has taken off globally. By not having a physical presence and a small number of employees, the new-age banks have a much lower cost structure and are able to provide a higher interest rates or higher promotional value for new credit cards. The existing financial institutions are rethinking on how they should engage the future society, given their vested interest in retaining their physical presence. As a retail financial institute, BOSS has been voted as the "World's most Innovative bank of the year" from 2018 and 2019 by their customers. BOSS has to manage two IAM system. One of the IAM system is for their customers logging into their online portal and the other is for their internal users. Managing this system be pivotal to BOSS's future.

For the banks with the legacy **technology**, some of these technologies are sunsetting or the employees with these skillsets are retiring. As with the programming language, COBOL, more than 80% of the ATM transactions of BOSS are still using this ancient programming language that is created in 1960 (Maack, 2017). BOSS needs to reconsider to move to the new programming language for which there are numerous developers that are able to support these technologies or to train their existing staff to manage the machines using COBOL. Finally, as technology advances and the amount of market and customer data multiples, the use of Machine Learning, Data Analytics and Artificial intelligence are on the priority list of BOSS's initiatives to revamp their security practice which includes IAM. Regarding BOSS's dual IAM systems management, there are two separate security and technology teams managing two portals. Give the large number of employees and customers, the IAM system currently manages 120 million access to 3000 applications and needs to continue scaling to meet the potential 240 million access in the next 15 years.

As BOSS is a global financial institution, one of the toughest challenges is to keep up with and comply to the stringent financial **regulations** of each country that keep evolving due to the pace of change in the financial industry. Their Enterprise Cyber Security Architecture needs to be sufficiently robust and flexible to meet the regulations from all over the world. In Figure 32, the figure shows the development of global banking regulatory requirements from 2015 to 2019, across the three key continents.

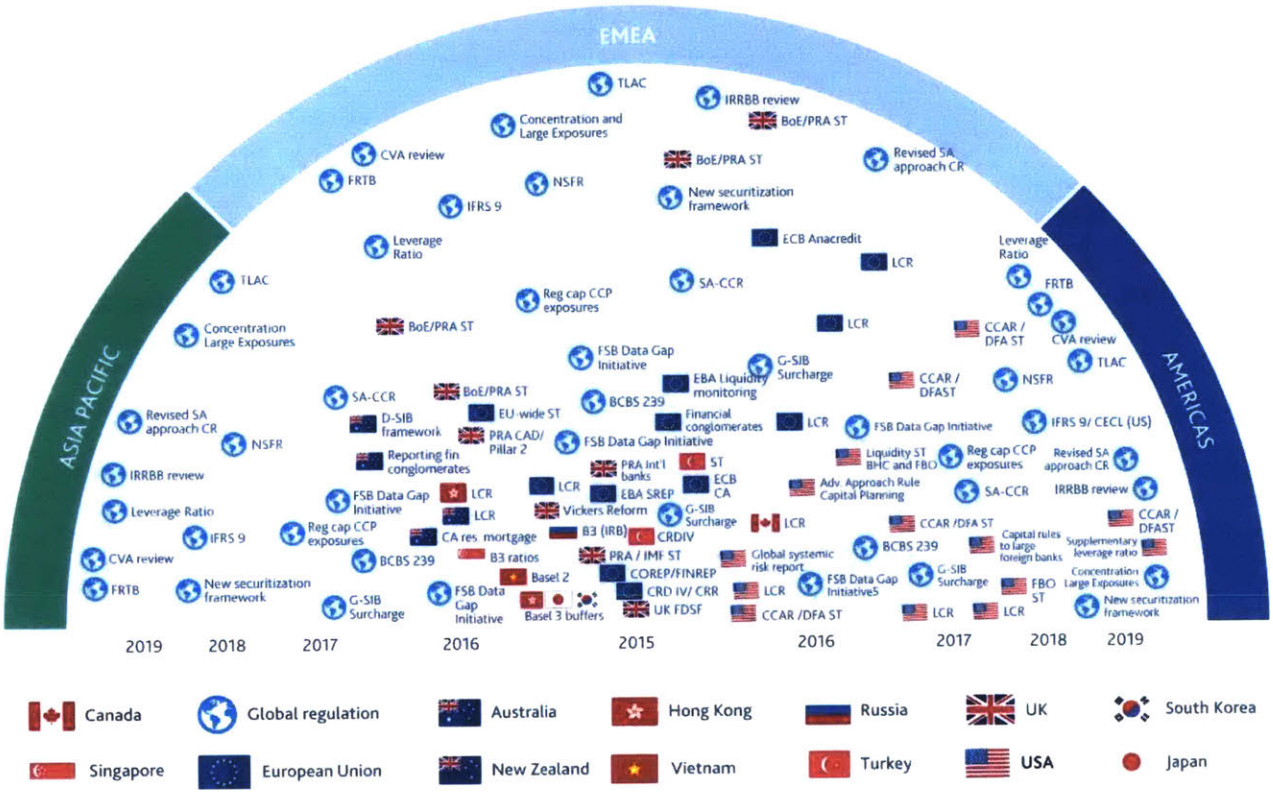


Figure 32: Global Banking Regulatory Requirements Development from 2015 to 2019 (Cañamero, 2015)

From an environmental aspect, many large enterprises have been known to own large data warehouses that consume tremendous amount energy for both powering the data warehouses and cooling the server rooms. As a result, there has been a certain degree of push from the activists and potential slated future legislation to required large enterprises in the US to reduce their carbon footprint by 50% over the next 10 years. As BOSS grows its data warehouse to support its investment into data analytics and machine learning, BOSS is considering the various opportunities to reduce its carbon footprint and minimize their impact on the **environment**. One of the three key initiatives that prioritized is the setup of Data warehouses in colder regions of each country, so as to minimize the energy required to cool these servers. Another initiative is the human less data warehouse, where in these locations, the facility will be setup with minimal lights and have no lights turned on at all times. Without humans in these

facilities, there will be minimal heating and lighting requirements, thereby reducing the energy to maintain these facilities. Lastly, these data warehouse are designed to use clean energy, sourcing from the solar panel built around the data warehouse, to the geothermal energy tapped from the nearby power plants and wind energy from the nearby wind farms. Eventually, these machines are running in the dark, cooled by and powered by natural elements.

4.1.2. 5C Analysis

In this section, the 5C analysis will be applied to BOSS to better understand the company, customer, competitor, collaborator and context/climate.

4.1.2.1. Customer

BOSS's Customers today are located all over the global. Despite having the large market share of millennials as customers, the median age of their customer is 50 years old due to the falling birth rates globally. BOSS's existing customers prefer to transact over the counter while the new customers are starting to open their account online to take advantage of the online promotion. Having a diverse group of customers and a differing level of needs, BOSS is considering how they can continue to become the bank of the world.

4.1.2.2. Competitor

As shared earlier, boutique firms are competing with BOSS for the younger customers. And at the wealthier end, asset management firms are creating private banking divisions to diversify into wealth management. Given these scenarios, BOSS faces a segment-wide competition, from asset management, to wealth-management and even to retail banking. To complicate things further, due to BOSS global presence and large asset-under-management (AUM), hackers all over the world are taking note of BOSS and are performing asynchronous hacks on a daily basis. Attacks ranges from *Distributed Denial of Services (DDOS)* to reduce BOSS's public facing website's **accessibility**, to *Website defacing attacks* to compromise BOSS's website **integrity**, and to *phishing attacks* to access internal network zone to access **confidential** data.

4.1.2.3. Collaborator

As BOSS's business model is extremely complex, due to the vast number of financial assets they own and instruments they invest in, the focus on this chapter will be on Cyber Security Collaborators. For Cyber Security, there are three key collaborators. First, the Cyber Security product vendors, who perform Cyber Security research, to share the latest attack patterns and findings to circumvent the attacks. Second,

the members of the Financial Services Information Sharing and Analysis Center (FSISAC) who provides intel about attacks they seen on their own network, help BOSS identify trends of attacks in each region. Lastly, Cyber Security academic researchers, such as MIT Sloan's "Cyber Security at MIT Sloan" (CAMS), who analyses Cyber Security trends from an academic perspective and integrates these learnings to the industry to provide a deeper explanation on certain Cyber Security attacks and possible future mitigation actions to pursue.

4.1.2.4. Climate/Context

Climate/Context analysis uses the PESTLE analysis to glean insights and this has been covered extensively in the earlier section under 4.1.

4.1.2.5. Company

This section will dive into the company's **stakeholders**, Cyber Security **enterprise**, Cyber Security **strategy**, Cyber Security **infrastructure**, **products and information**, Cyber Security **service** and **process**, and Cyber Security **knowledge**.

4.1.2.5.1. Stakeholders

From a business risk perspective, Office of the Chief Risk Officer (CRO) and Internal Audit (IA) team are key stakeholders. They are involved in the creating and shaping of Cyber Security Policies, as well as the accountable for compliance of Cyber Security policies within the enterprise and the compliance of Financial industry regulation and Cyber Security Acts. Their key objective is to ensure that all assets are **identified** and accounted for, all vulnerabilities are patched, all known threats are **prevented**, if not **detected** and have a **response** plan in place, which includes a **recovery** plan in the event of a total shutdown.

From a business resource perspective, the Human Resources (HR) team is accountable for the enterprise's employees, the employee's experiences with the company and their well-being during their time with the company. The Information Technology (IT) team is accountable for the technology assets and the well-deployment of these assets, and the technology experience of the employees. Their key objective is to ensure that all required assets are **identified** and issued to the employees on a timely basis without affecting business operations.

From a corporate communication perspective, the Corporate Communications team is responsible and accountable for the effective communications of any Cyber Security matters that affect

employees or the clients. They need to be ready to provide a satisfactory and timely response about the enterprise **recovery** status to the public in the event of an unfortunate Cyber Security attack or Cyber Security breach.

From a business operations perspective, Trading team and various Operations teams are responsible for bringing in the revenue for the enterprise. They require a seamless experience in technology and needs to work in a secure platform to perform the financial activities. Their key objective is to ensure that all required financial assets are **secured**, known threats to be **prevented** and **detected**, and that a **recovery** plan is in place to allow them to continue trading without affected by any accessibility issues that raised by a Cyber Security attack.

4.1.2.5.2. Cyber Security Enterprise

The entire current Cyber Security team is managed by the CSO. The current Cyber Security team is structured into three teams, IAM, Security Engineering, Risk Management. These teams are each lead by a Vice-President (VP).

From a functional perspective, the IAM team works closely with the HR Team to ensure effective onboarding, transfer and offboarding of staff. The Security Engineering Team works closely with the IT Infrastructure and Application teams to monitor their assets' security status. The Risk Management Team has two primary stakeholders. Their first primary goal is to work closely with the Office of CRO to create Cyber Security policies for the enterprise to keep align to the Financial industry regulation for each country. The secondary goal is to provide risk assessment of new deployment of technology, both hardware and software.

From a talent management perspective, there are three kinds of Cyber Security Professionals found in this department. First, the management which consists of the CSO and his team managers. Second, the technical program manager and product managers that drives the internal Cyber Security product innovation. Third, the Cyber Security operators and risk management team who performs routine security monitoring, standard operating procedures (SOP), and basic risk assessment of hardware and software deployments.

From a talent retention perspective, the existing Cyber Security team keeps losing talents for several push and pull reasons. First, the evil-banker image about the wall-street has been growing, many Cyber Security professionals are now leaning toward joining the technology vendor for a better career objective and better work-life balance. Second, their existing Cyber Security professionals get poached

from competing firms due to the demand for their expertise. Third, the banking industry Cyber Security work appears to be routine and non-innovative as compared to the technology vendors, as such, the best Cyber Security professionals are attracted to the technology vendors.

To aggravate the retention challenge, during the economic slowdown, often the most brilliance Cyber Security professional who are paid the most for their grade are let off to meet the budget cuts. These top-tier professionals are often the bridge of the Cyber Security team to other teams and hold the most tacit knowledge. And for those remaining Cyber Security professionals are often the operational analysts who works in their own functional area and have little understanding of the other functional teams. As they are often the operators who followed the Standard Operating Procedure (SOP), they have little tacit knowledge.

Another challenge that the Cyber Security face within the enterprise, is the issue of having the image of a police due to their work in Risk. Both the IT Infrastructure and Application teams needs to get the security and risk clearance for their new deployments by the Risk Management team. While the objective is to help the IT Infrastructure and Application teams to stay compliant by having this first round of risk assessment, the IT Infrastructure and Application teams view this assistance as a hurdle and less of a help. Due to this perspective and the potential delay arising from risk-assessment improvements, the IT Infrastructure and Application teams do not view the Risk Management team as a facilitator between them and the Internal Audit team. The IT Infrastructure and Application teams do not like the risk polices and guidelines which are there to help them.

4.1.2.5.3. Cyber Security Strategy

The key goal of Cyber Security is to ensure the Confidentiality, Integrity and Availability (CIA) of the enterprise assets.

The previous CSO has a Cyber Security strategy that focuses on detecting threats, preventing threats and recovering from threats.

Today, the new CSO has a new Cyber Security plan that spans across 3 Year plan. The plan is to have a gradual well-rounded growth of the enterprise's Cyber Security Capabilities that aligns to NIST Cyber Security Framework. (Identify, Detect, Prevent, Respond and Recover)

1) Year 1 Objectives

i. Develop a System-Thinking Risk Management Plan to identify known risk and anticipate unknown risk.
ii. Develop the missing capabilities (Identify and Respond) while retaining the existing capabilities (Detect, Prevent and Recover).
iii. Incorporate Cyber Benchmarking to measure internal capabilities and track the Cyber Security Capabilities' Improvements.
iv. Initiative Cyber-awareness program and ensure that at least 50% of the company attends this program.
v. Perform white-hat social engineering on internal users and measure cyber-risk awareness. Work with users who fall into the deception and advise them on cyber risk and its impact on the enterprise.
vi. Have a contingency cyber response contract with top Cyber Response enterprise and a cyber forensic contract in place.
vii. Perform a comprehensive cyber-attack recovery benchmarking test to determine baseline performance.
viii. Goal: Be in the top 75% category for the cyber benchmarking of Financial institutions.

2) Year 2 Objectives

i. Integrate the capabilities and identify the derived synergy from the integration
ii. Measure the capabilities maturity level and perform qualitative cyber-security benchmarking with fellow Financial institutions for future improvement.
iii. Initiative Cyber-awareness program and ensure that at least 75% of the company attends this program.
iv. Perform white-hat social engineering on internal users and measure cyber-risk awareness. Work with users who fall into the deception and advise them on cyber risk and its impact on the enterprise.
v. Have real-time updates about external attacks on other financial institutions.
vi. Develop internal cyber response capabilities.
vii. Perform a comprehensive cyber-attack recovery benchmarking test and improve by 25% from baseline performance.
viii. Goal: Be in the top 50% category for the cyber benchmarking of Financial institutions.

3) Year 3 Objectives

i. Optimize each Cyber Security capability.

ii. Perform white-hat social engineering on internal users and measure cyber-risk awareness. Work with users who fall into the deception and advise them on cyber risk and its impact on the enterprise.

iii. Real-time update of all Point-of-Entry systems with new attack vectors found from attacks happening to on other financial institutions and BOSS.

iv. Develop internal cyber forensic capabilities.

v. Perform a comprehensive cyber-attack recovery benchmarking test and improve by 50% from baseline performance.

vi. Goal: Be in the top 25% category for the cyber benchmarking of Financial institutions.

4.1.2.5.4. Cyber Security Infrastructure, Products and Information

The Cyber Security Infrastructure consists of both their products and information. The existing products support the previous Cyber Security strategy that is focused on the three capabilities, detecting threats, preventing threats and recovering from threat. The information to support these capabilities are stored in the common enterprise Data warehouse in unencrypted form. The current information consists of internally collected data of historical Cyber Security attacks to BOSS. The Cyber Security attack vectors consist of IP address, URL and email address.

4.1.2.5.5. Cyber Security Services and Process

The Cyber Security Team performs the following processes to service the enterprise:

- Risk Management
- Pen Testing
- Code Review
- IAM Onboarding
- Application Onboarding for Automation
- Cyber Security Policy Review and Regulatory Alignment
- Asset Patch Review
- Malware analysis and triaging.

Most recently, as more incidents are happening and the new CSO wants to build the Cyber Security Incident Response Capability. She found that for this new capability that everyone wants to perform, yet no-one knows how to perform as this capability requires a cross-functional understanding of the Cyber Security capabilities, which no-one has.

4.1.2.5.6. Cyber Security Knowledge

Due to the hiring and retention challenge, the average Cyber Security Employee only last for 2 years. As such most of the tacit knowledge gained by these employees are brought out when they left and does not get retained or converted into tangible notes or documentation that could be passed down. And among those who stayed behind, they are often fearful of restructuring and will held back knowledge sharing to increase their saliency to the enterprise.

As described in the earlier session, typically the longer serving Cyber Security Professionals are the low-level monitoring operators who have little tacit knowledge and does not wish to share.

4.1.3. Integration of PESTLE and 5C

To gain a wider view how BOSS's ecosystem factors interacts with BOSS and BOSS's third-parties, the integration of PESTLE and 5C analysis helps to provide this holistic perspective in Table 14.

Table 14: BOSS's integrated PESTLE and 5C Analysis

Climate	Company	Customer	Competitor	Collaborator
Political	Increase trade disputes between US and China and US and Russia creates tension both online and offline between citizens of these countries.	Increase trade disputes lower the market prices of stocks, creating an opportunity for financial institutions to capitalise upon.	Increase trade disputes between US and China and US and Russia creates tension both online, increasing the risk of cross-nation cyber-attacks on government-related agencies' websites	US Cyber Security product vendors can provide cyber-security defence products to these nations, fuelling their own growth.
Economic	The potential threat of a Financial crisis lingers on, encouraging the enterprise to remain prudent.	Customers are concerned about an impeding financial crisis and are spending lesser over the years.	The potential threat of a Financial crisis lingers on, encouraging the competing enterprise to remain prudent.	Due to prudent spending, collaborators (industry and academic) are getting less funds from BOSS and their competitors.

Social	To remain competitive, BOSS needs to analyse the social scene of fund management and compare tools like Venmo.	Customers are looking for promotions from new banking initiatives, aimed at getting new customers.	To be competitive, BOSS's competitors are providing new technology as their competitive advantage, such as social banking, to attract the millennials.	Collaborators have little consideration about the social initiatives from banks.
Technological	Due to the technological baggage, BOSS needs to strategically define their technology vision bring fore the enterprise.	Customers in developed countries embrace new technology easily, due to the trust developed over the year.	Competitor firms who are newer have lesser "baggage" and are able to be innovative at a lower cost.	Collaborators are racing to provide BOSS and their competitors the latest technology advancements before BOSS builds their own.
Legal	Both BOSS and their competitor are having a hard time keep in sync with the every-changing financial regulations. This causes internal enterprise change and unwanted stress within the enterprise.	Customers has no concern about the legal regulations.	Both BOSS and their competitor are having a hard time keep in sync with the every-changing financial regulations. This causes internal enterprise change and unwanted stress within the enterprise.	Collaborators need to be mindful for the challenges that the financial institution faces and create tools to help to meet or exceed the requirements of these financial regulations.
Environment	Due to the activist movements and potential cost savings, BOSS is considering how to move their data warehouses to cheaper locations that has abundant clean energy.	Customers have little consideration about the green initiatives from banks.	Due to the activist movements and potential cost savings, the financial institutions are considering how to move their data warehouses to cheaper locations that has abundant clean energy.	Collaborators have little consideration about the green initiatives from banks.

4.1.4. Enterprise Capabilities

In Table 14, the anticipated opportunities and threats listed there and will be used as the basis to determine the right enterprise capabilities. As per BOSS's defined Cyber Security Strategy in 4.1.2.5.3, the

plan is to have a gradual well-rounded growth of the enterprise's Cyber Security Capabilities and develop the other missing capabilities that aligns to NIST Cyber Security Framework's "Identify" and "Respond ".

Figure 33: New Capabilities required for BOSS's Growth Scenario

As seen on Figure 33 and Figure 34, the following capabilities such as organizational awareness of Assets, Vulnerability and Threats will support the required NIST Function of Identify for both growth and emergency scenarios. For **Growth** Scenarios, it is crucial that the Cyber Security Architecture is *evolvable* to take in new technology, as well as *scalable* to provide the same level of protection for a larger computing and user base. As for **Emergency** Scenarios, adaptability and responsiveness are vital for this scenario. Being *adaptable* allows the enterprise to take on a new strategy as required by the existing or impeding threat. Having a *responsiveness* architecture ensures that the enterprise is able to execute their enterprise strategy to take advantage of any opportunities gained through time.

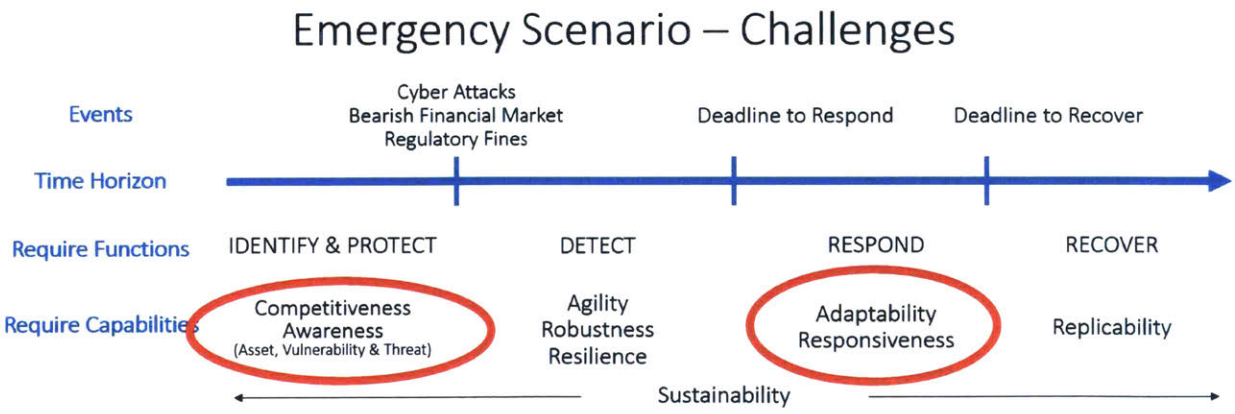


Figure 34: New Capabilities required for BOSS's Emergency Scenario

4.2. Perform Cyber Security Stakeholder Analysis

In this section, both qualitative and quantitative approach will be performed to identify the key stakeholders and their stakeholder-weighted priority value.

4.2.1. Cyber Security Stakeholder Qualitative approach

The three attributes used to characterize the stakeholders are Power, Legitimacy and Urgency. Legitimacy is defined from a Cyber Security Perspective, where the stakeholders are involved in part of shaping Cyber Security in the enterprise. Eleven stakeholders are identified and assign into the seven categories.

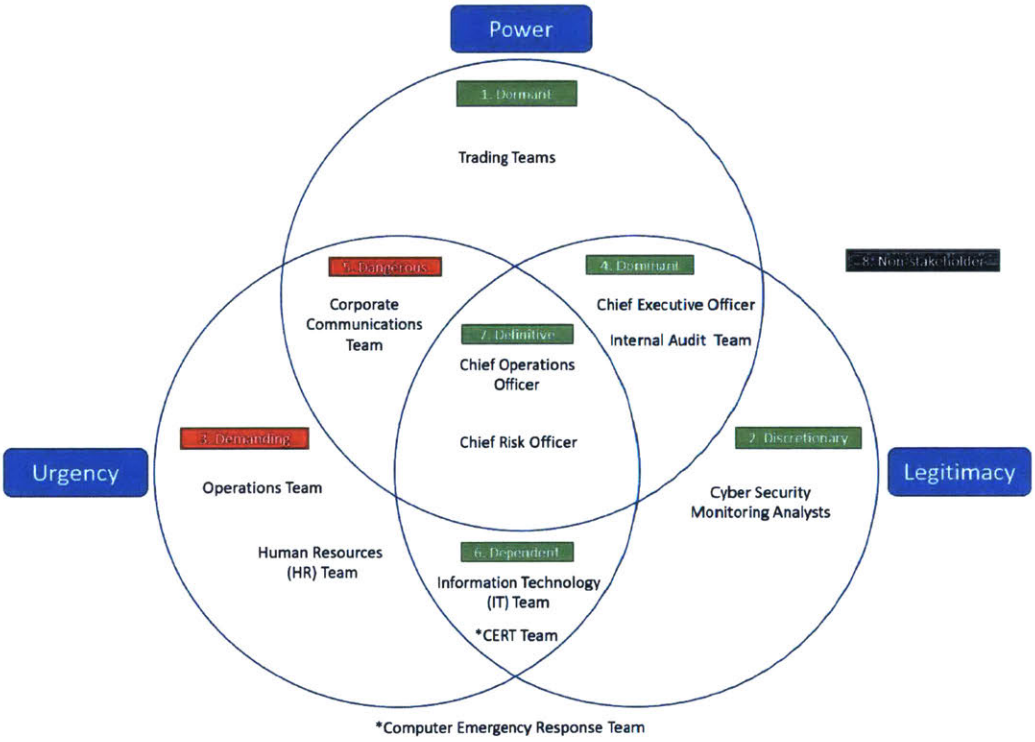


Figure 35: Stakeholder Saliency in BOSS

In Figure 35, the COO and CRO are the definitive stakeholders. To ensure that the BOSS receives progressive and constructive advice, feedback will be taken from all the stakeholders with a green label, e.g. Definitive Stakeholders, as shown in Figure 35.

4.2.2. Cyber Security Stakeholder Quantitative approach

After completing the qualitative approach, the quantitative stakeholder analysis will begin by using the list of salient stakeholders to complete the Stakeholder Prioritization Matrix (Table 15).

Table 15: BOSS Stakeholder Prioritization Matrix

Stakeholder Priority-Value	Trading Teams	Cyber Security Monitoring Analysts	Chief Executive Office (CEO)	Internal Audit (IA) Team	IT Team	Computer Emergency Response Team	Chief Operations Officer	Chief Risk Officer	Total (1.0)
Trading Teams	x	0	0.4	0.05	0.1	0.1	0.3	0.05	1
Cyber Security Monitoring Analysts	0	x	0.25	0.2	0.05	0.1	0.25	0.15	1
Chief Executive Office (CEO)	0.4	0.025	x	0.025	0.05	0.1	0.3	0.1	1
Internal Audit (IA) Team	0	x	0.3	x	0.1	0.1	0.2	0.3	1
IT Team	0.15	0.1	0.25	0.05	x	0.05	0.3	0.1	1
Computer Emergency Response Team	0	0.4	0.2	0.05	0.1	x	0.15	0.1	1
Chief Operations Officer	0.3	0.05	0.3	0.1	0.05	0.1	x	0.1	1
Chief Risk Officer	0.1	0.2	0.2	0.2	0.05	0.15	0.1	x	1
Actual Priority-Value	**0.95**	**0.775**	**1.9**	**0.675**	**0.5**	**0.7**	**1.6**	**0.9**	**8**
Normalized (x/total)	**0.11875**	**0.096875**	**0.2375**	**0.084375**	**0.0625**	**0.0875**	**0.2**	**0.1125**	**1**

Upon completing the Stakeholder Prioritization Matrix, soliciting the needs from stakeholders will form the list of stakeholders' needs. All the collated needs will be prioritized by all stakeholders, even if they did not include the need earlier. After prioritizing their needs individually, the outcome is revealed on the Needs Prioritization Matrix (Table 16).

Table 16: BOSS Needs Prioritization Matrix

Needs Priority-Value	Time to Deploy/Patch	Total Cost of Ownership	Feature-Flexibility	Security	Intuitiveness	Total (1.0)
Trading Teams	0.5	0	0.2	0	0.3	1
Cyber Security Monitoring Analysts	0.1	0.1	0.35	0.35	0.1	1
Chief Executive Office (CEO)	0.1	0.3	0.1	0.2	0.3	1
Internal Audit (IA) Team	0.1	0.25	0.1	0.35	0.2	1
IT Team	0.1	0.35	0.5	0	0.05	1
Computer Emergency Response Team	0.1	0	0.2	0.5	0.2	1
Chief Operations Officer	0.2	0.3	0.1	0.3	0.1	1
Chief Risk Officer	0.2	0.1	0.1	0.5	0.1	1

Using the output of both Table 15 and Table 16, the stakeholder-weighted needs prioritization matrix is created. In Table 17**Error! Reference source not found.**, the order of priority for the needs are as followed

1) Security
2) Total Cost of Ownership
3) Intuitiveness
4) Time to deploy/patch
5) Feature-Flexibility

Table 17: Stakeholder-weighted Needs Prioritization Matrix

SH-Weighted Priority-Value	Stakeholder Priority-Value	Time to Deploy/Patch	Total Cost of Ownership	Feature-Flexibility	Security	Intuitiveness	Total (1.0)
Trading Teams	0.11875	0.059375	0	0.02375	0	0.035625	0.11875
Cyber Security Monitoring Analysts	0.096875	0.0096875	0.0096875	0.03390625	0.03390625	0.0096875	0.096875
Chief Executive Office (CEO)	0.2375	0.02375	0.07125	0.02375	0.0475	0.07125	0.2375
Internal Audit (IA) Team	0.084375	0.0084375	0.02109375	0.0084375	0.02953125	0.016875	0.084375
IT Team	0.0625	0.00625	0.021875	0.03125	0	0.003125	0.0625
Computer Emergency Response Team	0.0875	0.00875	0	0.0175	0.04375	0.0175	0.0875
Chief Operations Officer	0.2	0.04	0.06	0.02	0.06	0.02	0.2
Chief Risk Officer	0.1125	0.0225	0.01125	0.01125	0.05625	0.01125	0.1125
SH-Weighted Priority-Value		**0.17875**	**0.19515625**	**0.16984375**	**0.2709375**	**0.1853125**	
Order of Priority		4	2	5	1	3	

To validate the effectiveness of using a stakeholder-weighted needs prioritization matrix, the author created the unweighted stakeholder needs prioritization matrix to uncover any difference in the order of priority. In Table 18, the order of priority for the needs are as followed,

1) Security
2) Feature-Flexibility
3) Total Cost of Ownership
4) Time to deploy/patch
5) Intuitiveness

Table 18: BOSS's unweighted Stakeholder Needs Prioritization Matrix

Needs Priority-Value	Time to Deploy/Patch	Total Cost of Ownership	Feature-Flexibility	Security	Intuitiveness	Total (1.0)
Trading Teams	0.5	0	0.2	0	0.3	1
Cyber Security Monitoring Analysts	0.1	0.1	0.35	0.35	0.1	1
Chief Executive Office (CEO)	0.1	0.3	0.1	0.2	0.3	1
Internal Audit (IA) Team	0.1	0.25	0.1	0.35	0.2	1
IT Team	0.1	0.35	0.5	0	0.05	1
Computer Emergency Response Team	0.1	0	0.2	0.5	0.2	1
Chief Operations Officer	0.2	0.3	0.1	0.3	0.1	1
Chief Risk Officer	0.2	0.1	0.1	0.5	0.1	1
Actual Priority-Value	1.4	1.4	1.65	2.2	1.35	8
Normalized (x/total)	2	2	2.357142857	3.142857143	1.928571429	11.42857143
Order of Priority	4	3	2	1	5	

After comparing the results, the order of priority of the two approaches are different once stakeholder's priority value is taken into consideration and this is essential to the project to ensure that saliency of needs is weighted into consideration.

4.3. Capture the Current Cyber Security Architecture

In this section, to capture BOSS's current Cyber Security Architecture, there will be a four-dimensional analysis. Using ARIES framework's enterprise elements and SWOT analysis, BOSS's enterprise elements will be analyzed from their strengths and weakness. Using PESTLE and SWOT analysis's opportunities and threat perspectives, BOSS as a company, Boss's collaborators and competitors' context (opportunities and threats) will be analyzed from a PESTLE perspective.

4.3.1. 5CEPS Model of BOSS

In Table 19, this table shows the 5CEPS model of BOSS, highlighting the opportunities and threats that BOSS, BOSS's collaborators and competitors face. Having this information arrange in model, this activity helps to widen the perspective beyond BOSS and understand the potential forces that may indirectly affect BOSS.

Three insights were gained from using this model. First, BOSS **weakness** in retaining Cyber Security Professionals may have an impact on their operations, and this issue may become a significant **threat**, further aggravated by the aggressive hiring in the financial industry. Second, the political **threat** of

international trade disputes and the technological threat from Cyber-attacks drives up the needs for implement the BOSS's Cyber Security **strategy** on adopting new NIST function of identifying assets and responding to threats. Third, on top of the weakness found in BOSS where inadequate SOP and process documentation are identified, this could be furthered worsen by the changing Legal regulation, requiring changes to process and required proper documentation and storage of information.

Table 19: 5CEPS of BOSS

		SWOT Analysis				
		Strengths	**Weaknesses**	**Opportunities**	**Threats**	
7S Enterprise Elements	Organisation	A holistic team structure, covering the main functions required in cyber security teams. High compensation and large performance. As compared to other industries, as a Financial institute, BOSS is able to attract at CS talents from other industries, with a higher compensation, to support them in their new initiatives	Weak retention program of talented employee, due to internal structure of career development. Cyber Security teams are seen as cost centers or "polices" in financial firms, as compared to being seen as a revenue generator in technology firms.	**Customer**: Being a long-term investor for our clients, increased trade disputes lower the market prices of stocks, creating an opportunity for financial institutes to capitalise upon. **Collaborators**: US Cyber Security product vendors can provide cyber-security defence products to these nations, fueling the companies growth.	**Customer**: As increased trade disputes lower the market prices of stocks, some of BOSS clients may harbor fear and perform a bank run on their liquid assets, hurting the bank's ability to maintain a positive cash-flow. **Competitor**: Increase trade disputes between US and China and US and Russia creates tension both online, increasing the risk of cross-nation cyber-attacks on government-related agencies' websites.	Political
	Strategy	Strategy is to strengthen and benchmark existing capabilities of NIST functions of detecting, preventing and recovering from threats.	Strategy is to adopt new capabilities of NIST functions of identifying assets effectively and responding to threats effectively and efficiently	N/A	**Customers** are concerned about a impeding financial crisis and are spending lesser and investing lesser over the years. **Company**: Due to the upward demand for Cyber security professionals among the financial institutions due to the economical growth, BOSS is losing their Cyber Security professionals and team cultures faster than they wish for. This affects the ongoing projects' progress as some are put on halt due to lack of resources continuity. **Collaborators:** Due to prudent spending in anticipation of a financial crisis, collaborators (industry and academic) are getting less funds from BOSS and their competitors, affecting the collaborators' ability to spend in R&D.	Economical
	Infrastructure, Products & Information	BOSS has strong infrastructure and products to detecting, preventing and recovering from threats.	BOSS has no infrastructure and productsto efectively identify all existing or new assets and respond to threats effectively and efficiently The current information in BOSS are often store unencrypted in their own premises. This may become an issue when a hacker gains access to the network.	N/A	**Competitor**: New boutique financial institute firms are targeting them millenials by having a full-service online bank, leading to large market-share taken by these boutique firms. **Customers** are looking for promotions from new banking initiatives, aimed at getting new customers. **Company**: To remain competitive, BOSS needs to analyse the social scene of fund management and compare tools like Venmo.	Social
	Services & Products	Existing services and processes covers from risk management to penetration testing to IAM.	Lack of existing process and standard operating procedure to manage indcident response.	**Customers** in developed countries embrace new technology easily, due to the trust developed over the year. **Collaborators** are racing to provide BOSS and their competitors the latest technology advancements before BOSS builds their own.	**Competitor**: Due to the perception that Financial instition has a lot of funds to extract from, hackers are thinking of innovative ways to infiltrate BOSS's network to uncover such opportunities. **Competitor**: Competitng financial firms who are newer have lesser technological "baggage" and are able to be innovative at a lower cost of acquiring and adopting new technology. **Company**: Due to the technological baggage, BOSS needs to strategically define their technology vision bring fore the enterprise.	Technological
	Knowledge	Due to the last engagement with Accenture, BOSS has a vast knowledge of operating their three NIST functions, detecting, prevent and recover from threats.	While the basic knowledge have been documented by Accenture for BOSS, these actual enhanced and gained tacit knowledge have yet to be documented by the existing CS professionals due to fear of retrenchment	**Collaborators** needs to be mindful for the challenges that the financial institution faces and create tools to help to meet or exceed the requirements of these financial regulations.	**Company, Competitor and Collab**orator: Both BOSS and their competitor are having a hard time keep in sync with the every-changing financial regulations. This causes internal organization change and unwanted stress within the organization.	Legal
				Company: Due to the activist movements and potential cost savings, BOSS is considering how to move their data warehouses to cheaper locations that has abundant clean energy.	**Competitor:** Due to the large number of servers and processin power required by Financial institutions, climate change activists and those anti-Wall street may use environmental matters as a issue to take up against big financial institution, progessively leading to potential policies made against financial institution	Environmental
		Company		**Company, Customer, Competitor, Collaborator**		**Context/ Climate**
		5C Scope				

4.3.2. Cyber Security X-Matrix

In the Table 20, it shows the X-Matrix based on the information gather from the Enterprise stakeholders (Strategic objectives and stakeholder needs) and the Cyber Security Process and Metrics.

Table 20: X-Matrix of BOSS

Median Time taken to Onboard for Day-One Employees	Median Time taken to offboard for Day-One Leavers	Median Time taken to transit for Day-One Movers	Median Time taken to Onboard for New Applications	Median Time taken to Offboard Applications	Percentage of completed access-certification for each Certification Cycle	Median Time taken to complete each Certification Cycle	Median Time taken to provide new feature (basic, moderate and advanced)	Percentage of access registered	Percentage of applications monitored	User satisfaction survey	Audit Findings and Compliance Fines	Percentage of application access held by leavers	Percentage of orphan application access	Percentage of excess application access granted to users		Cyber-Resiliency	Feature-Flexibility	Executing within budget	Executing with time-frame	Tool intuitiveness
															Meet evolving cyber security threats					
															Attract Specialized Talent					
															Detect threat in a timely manner					
															prompt communications with the board					
															Protect business and client critical information					
															Asset Identification					
															Asset Maintenance					
															Asset Decommission					
															Threat Detection					
															Threat Prevention					
															Threat Response					
															Incident Recovery					
															IAM Joiner, Mover, Leaver					
															IAM Attestation					
															Threat Intelligence Research					

In this analysis, we found that there is poor alignment between Strategic objective and Stakeholder needs, Strategic objective and Cyber Security Metrics, Cyber Security Process and Metrics. Clearly much work is needed to refined the alignments in order to lead the enterprise to align with the stakeholder needs, and have supporting process and relevant metrics to measure BOSS's progress in Cyber Security endeavors.

4.4. Create the holistic vision of the Cyber Security future

Below are the narratives of several key stakeholders that were considered as salient.

Belle Rubin*[7], CEO at BOSS, "Cyber threats keep growing, and clients rightly expect us to do everything we can to **protect their information**; getting this right is critical to our success. I see a future where our work in this area will get tremendous recognition, and from now till then, I'm proud of our team's dedication **to protecting our business' and clients' critical information**. BOSS will be a shining example of leadership for the entire information security industry. As the nation's largest lender, we have plan to spend $880 million on Cyber Security in 2020 and it will the first time in 30 years of corporate budgeting where only place in the company that didn't have a budget constraint will be Cyber Security."[8]

Dave Moser*, Chief Information Security Officer at BOSS, said, "As we are aware of the benefits a holistic Cyber Security architecture brings to large enterprises, I imagine a future where we rolled out such an architecture globally by ourselves. Continuous training programs are critical to **meeting evolving Cyber Security threats.** Such an architecture will help us leverage the skills of the people at the front line of our cyber defenses and identify new talent throughout the enterprise. It will be great to see a company with the reputation of BOSS getting firmly behind one of the fastest-growing US Cyber Security success stories for the financial industry. Not only does it speak volumes of everything the Cyber Security team can achieve and also of the massive growth potential the team has." [9]

Chase Crawley*, Chief Operation Officer at BOSS, said, "Financial services sector faces the greatest economic risk related to Cyber Security. In the "Deloitte 2015 Banking Outlook", they say to improve Cyber Security, banks will be forced to devote greater resources to enhancing the security, vigilance, and resilience of their Cyber Security model and should consider: Adopting new methods, such as war gaming, **attracting specialized talent**, and **increasing collaboration with other members** of the ecosystem; Beefing up their intelligence apparatus **to detect new threats in a timely manner**; Expanding the role of the CISO to include clear and **prompt communications with the board**. This is what we will be doing at BOSS." [10]

---

[7] The names, characters, and incidents portrayed in this case-study are fictitious. No identification with actual persons (living or deceased), places, buildings, and products is intended or should be inferred.

[8] Adapted from (Bank of America, 2018)

[9] Adapted from (Immersive Labs, 2019)

[10] Adapted from (Morgan, forbes.com, 2016)

4.5. Generate Alternative Cyber Security Architecture

A Cyber Security Architecture is a process of building a system of systems, where each system focusses on a local mission to accomplish and do so in the most locally optimized manner. As BOSS requires to incorporate two more NIST Function, identify (assets) and respond (to threats), the focus will be on one of these two functions in the following sections.

4.5.1. Cyber Security Ideation by Bias-Breaking and Concept Selection through Kano-Analysis

The function of focus here is on responding to the threats. In Figure 36, the solution neutral function is to respond to the threat. The solution specific function is to reduce the effects of the threat with a Virtual LAN (VLAN). The use of VLAN reduce the possible area of maneuver by the hacker to the minimum.

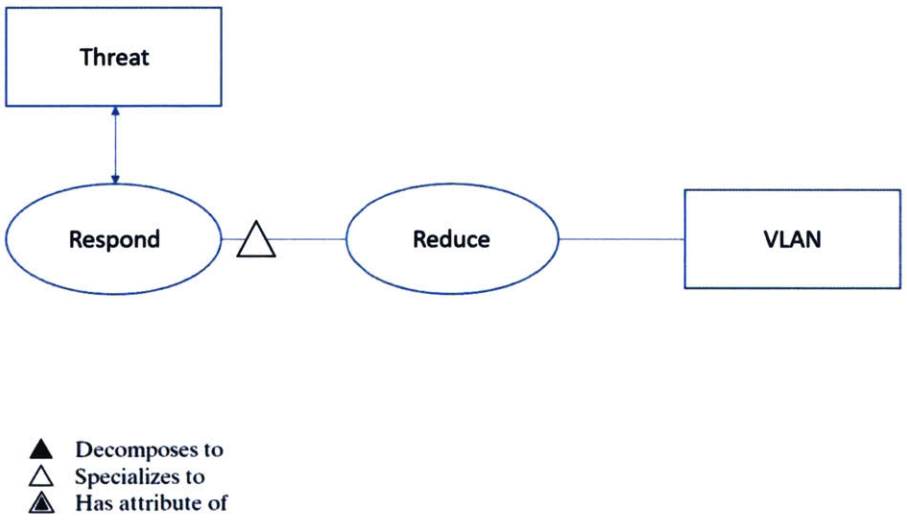


Figure 36: Concept for responding to threat before the bias-breaking session

After considering the potential bias (all threats must be reduced) that the author has, the author found three other ways threats can be managed with inspiration from risk mitigation approaches as seen in Figure 37.

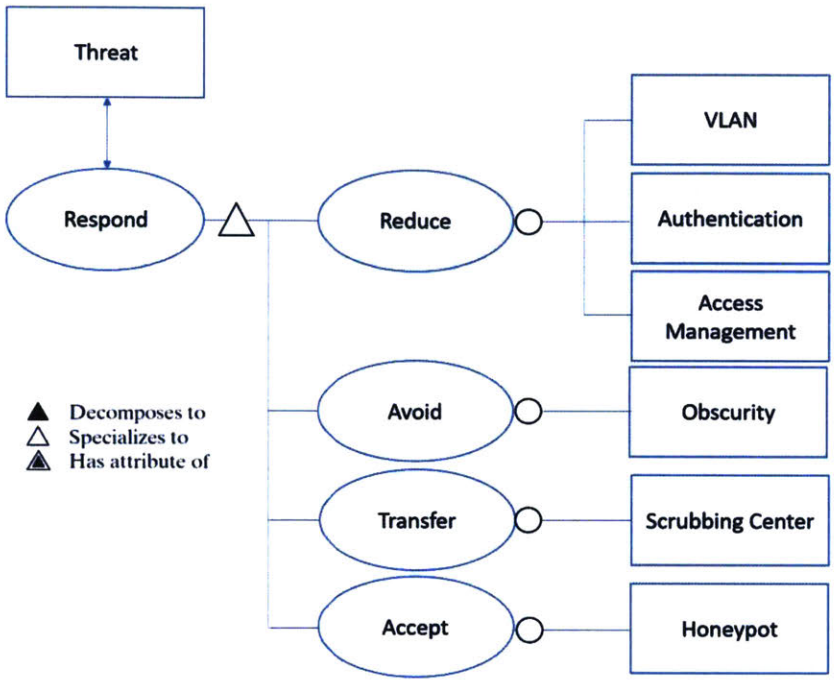


Figure 37: Concept for responding to threat after the bias-breaking session

In consider of the 4 possible concepts with Kano Analysis, a threshold concept will be "avoid". A Performance concept will be "reduce". A delighter concept will be "Transfer" and "Accept".

4.5.2. Architecture Generation by Morphological Matrix

As highlighted in the BOSS case-study that the enterprise needs to respond to both external and insider threat with a holistic Enterprise Cyber Security Architecture, the Cyber Security team created a morphological matrix (Table 21**Error! Reference source not found.**) to consider the various architecture decisions options. From 18 different architecture decisions with two to three options each, the number of possible architectures are close to three million ($2^{12} \times 3^6$). Yet in reality, a better approach for BOSS will be consider the key architecture decisions to focus upon to come up with three to five architecture, e.g. Pure **Cloud-Only** Enterprise Cyber Security Architecture, an **On-Premise** Enterprise Cyber Security Architecture or even a **Hybrid (Cloud and On-Premises)** Enterprise Cyber Security Architecture, for the decision-making team choose from. Depending on the priorities, the decision of the recommended architecture will differ.

Table 21: Morphological Matrix for Enterprise Cyber Security Architecture

Architecture Decisions	Option 1	Option 2	Option 3
Encryption types	RSA	AES	DES
Encryption Key Length	128 bits	256 bits	1024 bits
Encryption Key owned by Enterprise	Yes	No	
Hashing verification	Yes	No	
Accessible from internal network	Yes	No	
Accessible from external network	Yes	No	
Searching with encryption	Yes	No	
Allows growth while minimizing complexity	Yes	No	
Servers Uptime	99%	99.90%	99.99%
Staff Excellence	In-house	contractors	vendor
Ability to react to market conditions	Neutral	Fast	Faster
Number of NIST Cyber Security Functions	3	4	5
Servers Cost	Same	More	Less
Implementation Cost	Same	More	Less
Maintenance Cost	Same	More	Less
Time to implement	Same	More	Less
Time to patch	Same	More	Less
Time to fix	Same	More	Less

4.6. Decide on the Future Cyber Security Architecture

In this section, the case study on BOSS will move to the process of deciding the future Cyber Security architecture.

4.6.1. Cyber Security Decision-Making Committee

To identify salient, legitimate and credible decision makers, BOSS use a combination of parties. First, for saliency, key salient stakeholders such as the definite stakeholders are invited to be part of this committee. Second, for legitimacy, dominant, dependent and discretionary stakeholders are invited. Third, for credibility, consulting firms are paid to join the committee to share the industry best practices. In these scenarios, these consultants are only rewarded for their expert services in decision analysis and will have no further engagement into the implementation, to ensure no conflict of interest and to avoid bias. Subsequently, the metrics are being introduced and defined to them to ensure a common understanding of the metrics.

4.6.2. Cyber Security Future Proofing

For future proofing, scenario-based testing is used. Looking the 5CEPS model, there are four scenarios to cater for, most impactful and most likely to happen for both opportunity and threat.

Most impactful opportunity: Due to the activist movements and potential cost savings, BOSS is considering how to move their data warehouses to cheaper locations that has abundant clean energy.

When the above opportunity happens, BOSS will be able to save a large amount of expense arising from maintaining the data warehouses. Yet a potential threat may also emerge from the uncertainty of each data center location, especially if the use of geothermal energy is materialized and the risk of a volcanic eruptions potentially affecting the daily operations of these servers and BOSS

Opportunity that is most likely to happen: Being a long-term investor for our clients, increased trade disputes lower the market prices of stocks, creating an opportunity for financial institutions to capitalize upon.

When the above opportunity happens, the BOSS intends to capitalize on this opportunity and purchase all the blue-chips assets which will be sold at the peak of the market. Such returns can help to fund the necessary growth of the Cyber Security team and infrastructure.

Most impactful threat: Due to the perception that Financial institution has a lot of funds to extract from, hackers are thinking of innovative ways to infiltrate BOSS's network to uncover such opportunities.

When the above opportunity happens, on top of the potential actual financial loss, BOSS reputation risk will be at stake. The reputation loss will be hard to gain back than the actual monetary loss.

Threat that is most likely to happen: Due to the upward demand for Cyber Security professionals among the financial institutions due to the economic growth, BOSS is losing their Cyber Security professionals and team cultures faster than they wish for. This affects the ongoing projects' progress as some are put on halt due to lack of resources continuity.

When the above opportunity happens, a lot of BOSS Cyber Security projects will be on hold. Having core projects on hold will marginalize the progress of BOSS Cyber Security initiative. Potential cyber incident, that could be overcome, may in fact happen if these projects are delayed.

4.6.3. Cyber Security Architecture Weighted Decision Matrix

To evaluate the final architecture to work upon, BOSS will use a weighted decision matrix (Table 23) to assess the utility from each architecture, using the information from the stakeholder-weighted needs analysis.

Table 22: BOSS's unweighted Stakeholder Needs Prioritization Matrix

Needs Priority-Value	Time to Deploy/Patch	Total Cost of Ownership	Feature-Flexibility	Security	Intuitiveness	Total (1.0)
Trading Teams	0.5	0	0.2	0	0.3	1
Cyber Security Monitoring Analysts	0.1	0.1	0.35	0.35	0.1	1
Chief Executive Office (CEO)	0.1	0.3	0.1	0.2	0.3	1
Internal Audit (IA) Team	0.1	0.25	0.1	0.35	0.2	1
IT Team	0.1	0.35	0.5	0	0.05	1
Computer Emergency Response Team	0.1	0	0.2	0.5	0.2	1
Chief Operations Officer	0.2	0.3	0.1	0.3	0.1	1
Chief Risk Officer	0.2	0.1	0.1	0.5	0.1	1
Actual Priority-Value	**1.4**	**1.4**	**1.65**	**2.2**	**1.35**	**8**
Normalized (x/total)	**2**	**2**	**2.357142857**	**3.142857143**	**1.928571429**	**11.42857143**
Order of Priority	4	3	2	1	5	

As mentioned in section 3.6.3. Cyber Security Weighted Decision Matrix, the engagement of external experts into the decision-making process to ensure saliency, legitimacy and credibility, is highly encouraged. And in BOSS's case, based on the recommendation of industry experts, this has shaped the Stakeholders needs. The Stakeholder need, "Security" is now represented by three different needs , namely "Confidentiality, Integrity and Accessibility". Scalability and Reliability are new Stakeholder needs that are being introduced by the experts and accepted by the stakeholders. Meanwhile, the new stakeholder need "flexibility" will represent both "feature-flexibility" and previously lowest ranked stakeholder need, "intuitiveness".

Table 23: Weighted decision-making matrix for BOSS Enterprise Cyber Security Architecture

					Candidate Architectures			
	Stakeholder Needs	SWP Value	Architecture Decisions	Rating	AS-IS	Cloud-only	Hybrid Cloud	On-Premises
Criterion	Confidentiality	20%	Encryption types	30%	3	5	4	5
			Encryption Key Length	30%	3	4	4	6
			Encryption Key owned by Enterprise	40%	3	4	2	5
	Integrity	15%	Hashing verification	100%	3	4	2	4
	Accessibility	10%	Accessible from internal network	50%	3	4	5	5
			Accessible from external network	20%	3	5	5	3
			Searching with encryption	30%	3	5	2	5
	Scalability	10%	Allows growth while minizing complexity	100%	3	5	2	3
	Reliability	15%	Servers Uptime	60%	3	5	4	4
			Staff Excellence	40%	3	3	4	5
	Flexibility	10%	Ability to react to market conditions	30%	3	5	4	4
			Number of NIST Cyber Security Functions	70%	3	3	4	5
	Cost	10%	Servers Cost	30%	3	5	4	3
			Implementation Cost	10%	3	5	4	3
			Maintenance Cost	60%	3	4	4	3
	Time	10%	Time to implement	25%	3	5	2	4
			Time to patch	35%	3	5	2	4
			Time to fix	40%	3	2	2	5
			Weighted Scoring		3	4.22	3.15	4.29
			Ranking			1	3	2
			Risk and Tranformability		✓	✗	✓	✓

Despite most financial institutions attempting to move towards the cloud, for this case-study, it is found that an on-premises Enterprise Cyber Security Architecture is the recommended architecture for

BOSS enterprise. Despite rated as the second-best option, Cloud-based Cyber Security Architecture, this architecture will not be selected largely due to the risk involved as seen on Table 23.

4.7. Case Study Conclusion

The author found that by applying the reference framework to the case study, the process uncovers areas of improvement and areas of additional areas of considerations. Areas of improvements include BOSS's existing Cyber Security Architecture, alignment challenges between the strategic objectives, stakeholder needs, enterprise process and enterprise metrics and development of architecture decisions. Areas of additional considerations are the external factors that affect BOSS's constituents (collaborators, competitors, customers), possible bias and the inclusion of additional architecture options that was previously not considered, and more importantly how all these can affect BOSS in the long run. Being able to anticipate how the collaborators, competitors, customers will behave in these potential scenarios, will enable BOSS to take precautionary measures in anticipation of their actions. This so will increase BOSS's long-term survival and improve their long-term performance.

5. Conclusion

To develop a holistic Enterprise Cyber Security Architecture, this thesis examines the ecosystem **risks** that surround financial institutions, the significance of Enterprise Cyber Security Architecture **stakeholders**, the various Cyber Security **functions**, and the **complex interaction** of these three domains. Building upon the understanding of the multi-faceted risks involved and the varying needs of significant stakeholders, a stakeholder-weighted prioritization matrix was introduced to balance the prioritization of needs, that leads to the shaping of the Enterprise Cyber Security Architecture. To give a broad perspective of the enterprise ecosystem and an understanding of the possible interactions of the ecosystem elements, a 5CEPS model was developed. To create more concepts, the practice of bias-breaking and kano-analysis was included in the SMILE reference framework. To generate quality architectures from concepts, the analytical tool, morphological matrix, was used. To evaluate the final Enterprise Cyber Security Architecture, future proofing of the architecture and the final validation with a weighted decision matrix were performed. Finally, a hypothetical case was created by drawing inference from public information sources describing financial institutions and their ecosystem. The proposed reference framework was put to test with the hypothetical case to assess its initial practicality. The thesis contributions, limitations and future work are discussed in this final chapter.

5.1. Thesis Structure and Approach

This section describes the approach undertaken to perform this thesis research. Each chapter of the thesis is briefly discussed below.

Chapter 1: *Introduction.* This chapter introduces the thesis by describing the motivation and need that led to the development of this thesis. The scope and the approach of the thesis are described in this chapter, which includes the research questions. Finally, the ARIES framework's elements and processes are briefly discussed to introduce the structure of the proposed reference framework (covered in chapter 3).

Chapter 2: *Literature review.* This chapter provides the overview of the types of financial institutions and the ecosystem risks faced by financial institutions. By understanding the systemic risk faced, this provides the contexts behind the need for Cyber Security architecture, systems, process and resources in place within financial institutions. Next, Cyber Security history and renowned cases are covered to provide the understanding of the evolution of Cyber Security attacks and its effects. Finally, as

the ARIES Framework is used as the *structure* of a proposed reference framework, the framework is discussed in depth in this chapter.

Chapter 3: *Proposal of Stakeholder-Managed Integrated & Learning Enterprise (SMILE) Reference Framework.* The proposed referenced framework (Table 24) is a six-step approach to developing several future architectures before providing an approach to decide on the future architecture.

Table 24: Integrating ARIES Framework with other frameworks to form SMILE Reference Framework

Stakeholder-Managed Integrated & Learning Enterprise (SMILE) Reference Framework			
	Structure adapted from ARIES Framework	**Complementary Analytical Methods and Tools**	**Benefits**
1	Understand the Enterprise Landscape	PESTLE Analysis, 5C Analysis, Time-Horizon Analysis	Holistic approach to analyzing the enterprise landscape
2	Perform Stakeholder Analysis	Stakeholder-weighted Needs Prioritization Matrix	Quantitative Approach to complement the qualitative approach, to provide a proportionate representation of the stakeholder needs.
3	Capture the current Architecture	5CEPS Model - 5C analysis, Enterprise Elements, PESTLE Analysis and SWOT Analysis	Identify the correlation between the various models of different yet complement levels (Macro, Meso and Micro) and connect their elements to capture the current architecture.
4	Create the holistic vision of the future	Nil	Nil
5	Generate alternative Architectures	Bias-breaking, Kano Analysis, SWOT Analysis and Morphological Matrix	Consider alternatives by challenging the existing assumptions Categorizing the needs and building a balanced architecture with an outward view.
6	Decide on the Future Architecture	Deciding on Decision Maker	Decision-making with a neutral voice

In the above table, the second-left column shows the **structure** of the SMILE Reference Framework which is adapted from the ARIES Enterprise Framework. In the second-right column of the table contains the **complementary analytic methods and tools** used to enhance this research. And in the right most column, it describes the **benefits** of using the complementary analytic methods and tools.

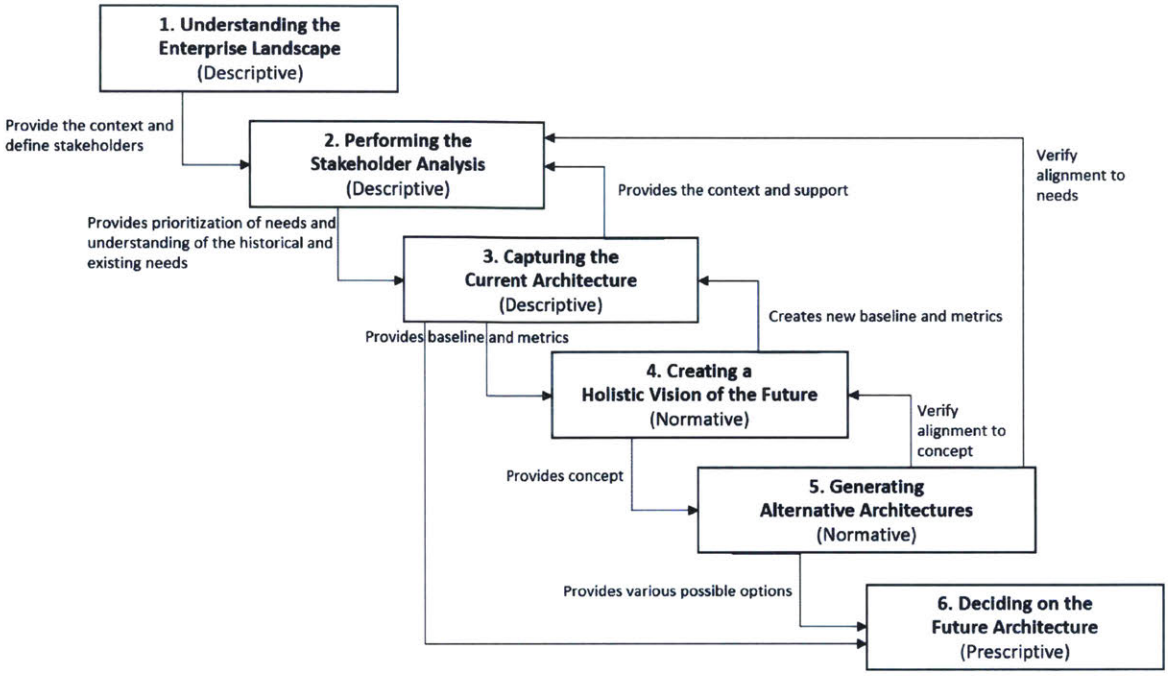


Figure 38: Proposed Reference Framework Approach

In this chapter, the ARIES Framework is used as the structure of a proposed reference framework. As part of the first step of the proposed reference framework approach (Figure 38), the PESTLE analysis is explained and demonstrated to provide a better understanding of the financial industry at a macro level. Next, the 5C analysis is performed to analyze the financial institutions at meso level (Company, Collaborator, Competitor and Client). Subsequently, the PESTLE analysis and 5C analysis are integrated to identify the effects of the macro elements (PESTLE analysis) on the meso elements (5C analysis).

On top of the qualitative approach of the ARIES Framework to perform stakeholder analysis, the author proposes a *quantitative* approach to complement this analysis. The *quantitative* approach's goal is to gather the proportional representation of the individual needs for closer alignment with the stakeholders, by identifying both the stakeholder priority value and the needs value, using a stakeholder-weighted prioritization matrix. The quantitative approach consists of 5 steps which includes listing the stakeholders and needs, performing both stakeholder and needs prioritization and finally deriving the stakeholder-weighted value for each need as shown in Figure 39.

	Stakeholder Priority Value	Need 1	Need 2	Need 3	Need 4	Need 5	Total (1)
Stakeholder 1	Stakeholder 1's N. Priority Value						Stakeholder 1's N. Priority Value
Stakeholder 2	Stakeholder 2's N. Priority Value						Stakeholder 2's N. Priority Value
Stakeholder 3	Stakeholder 2's N. Priority Value						Stakeholder 2's N. Priority Value
Stakeholder 4	Stakeholder 2's N. Priority Value						Stakeholder 2's N. Priority Value
Stakeholder 5	Stakeholder 2's N. Priority Value						Stakeholder 2's N. Priority Value
Actual	---	Need 1's Priority Value	Need 2's Priority Value	Need 3's Priority Value	Need 4's Priority Value	Need 5's Priority Value	
Normalized (x/total)	---	Need 1's N. Priority Value	Need 2's N. Priority Value	Need 3's N. Priority Value	Need 4's N. Priority Value	Need 5's N. Priority Value	

Figure 39: Stakeholder-Weighted Needs Prioritization Matrix

To capture the current architecture, the enterprise lens approach of the ARIES framework is used to identify and describe the key enterprise elements of Financial institutions. As per Marr, the key about gaining complete understanding of information processing system is that the analysis must be understood at three distinct yet complementary levels of analysis, namely the *Macro, Meso and Micro*, as the analysis at each level itself is insufficient. (Marr, 1982)

In the same approach, to gather the complete understanding of the enterprise, PESTLE analysis, 5C Analysis, ARIES Enterprise Elements Lens approach and SWOT are used to form this integrative view. **PESTLE analysis** provides the *Macro* perspective, the **5C analysis** provides the *Meso* perspective and **ARIES Enterprise Elements Lens approach** provides the M*icro* analysis. The SWOT Analysis connects all of these three perspectives by first, identifying the opportunities and threats at both the Meso and Macro level, then identifying the strengths and weakness at the Micro level. This approach leverages on existing analytical methods of viewing the external ecosystem and internal landscape holistically, and enhances the perspective with SWOT analysis. The author developed the **5CEPS Model (**Figure 40), which denotes **5C E**lements **P**ESTLE **S**WOT, with the intention of viewing enterprise in a holistic yet concise approach. The 5CEPS Model, along with the X-Matrix, are used to provide a complete view of the current architecture and an analysis of the degree of enterprise architecture alignment between the enterprise objectives, values, process and metrics.

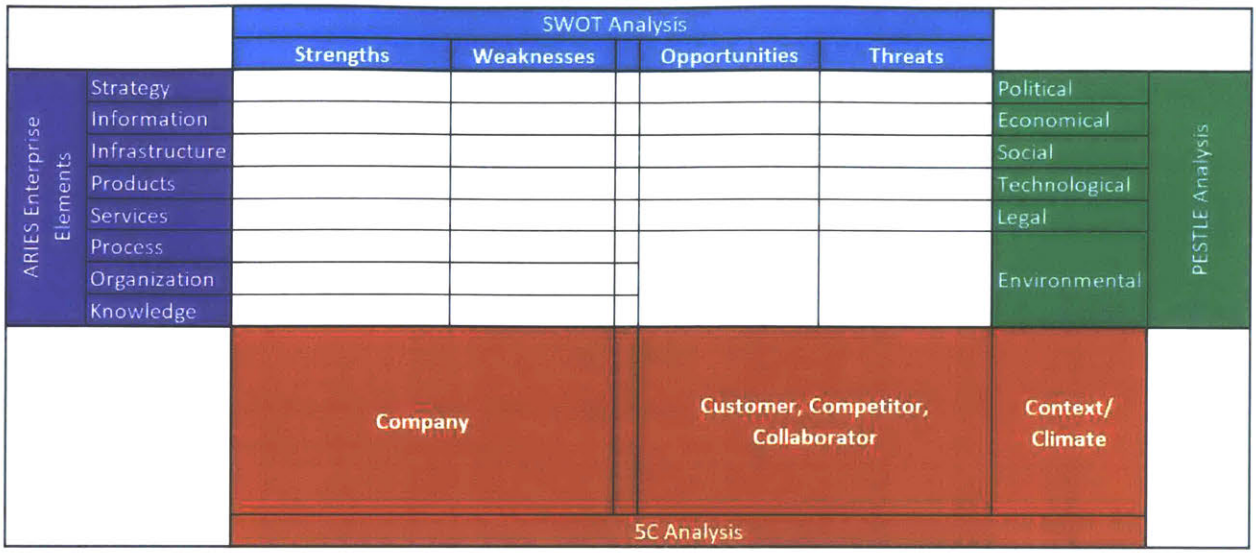


Figure 40: 5CEPS Model

For the fourth step, this step entails the creation a holistic vision of the future. The author adopts the same approach recommended by the ARIES framework, using the stakeholder narratives to shape the holistic vision.

In the fifth step, to generate alternative architectures, the author introduces three sub-approaches. First, the author introduces the practice of bias-breaking to analyze existing bias that could prevent the system architects from conceiving refreshed ideas related to developing a new Enterprise Cyber Security Architecture. Second, the author introduces Kano analysis to refine the concept by ensuring the new Enterprise Cyber Security concept consists of threshold, performance and delighter attributes. Finally, to convert the concept to the architecture, the author recommends the use of a morphological matrix to systematically identify the various possible architectures.

In the final step, the focus in this step is on determining the recommended architecture. The author covers three areas, 1) Deciding on the Decision Makers, 2) Future Proofing of Architecture, 3) Validation of new Enterprise Cyber Security Architecture with a weighted decision matrix. In this proposed SMILE reference framework, several analytical models are integrated with the ARIES framework to provide additional insights.

Chapter 4: *Applying SMILE Reference Framework to a hypothetical case.* In this chapter, the SMILE Reference Framework will be applied upon a hypothetical case. Due to the sensitivity surrounding Cyber Security operations and IAM operations in financial institutions and the public publication of this thesis, a hypothetical case will be used in place of an actual case. To keep the hypothetical case as realistic as

possible, the hypothetical case will be based on publicly sourced information and various known Cyber Security cases about financial institutions. In this chapter, the application of SMILE Reference Framework consist of the analyzing the landscape of a fictitious financial institution, performing the stakeholder analysis, creating the ideal holistic vision, generating alternative architecture and deciding on the future Cyber Security architecture. Finally, expert reviews are used to critique our approach and to identify areas of strengths and improvement.

Today, IAM's project and operational coverage spans across from technology to risk to human resource to other Cyber Security domains. Due to this extensive span across corporate functions and the operational interaction involved, IAM is considered one of the most complex Cyber Security domains as compared to the other Cyber Security domains. Challenges faced in IAM are beyond the technical challenges and often includes socio-technical challenges, e.g. onboarding of new joiners, the mover process, and the acceptance of IAM attestation user-interface (UI) to perform attestation. Out of the several other Cyber Security domains, the IAM is chosen for the subsequent case study in view of these complex challenges and its functional coverage across the enterprise.

Chapter 5: *Conclusion*. This chapter discusses about the research contributions, limitations and the possible areas to further the research.

5.2. Research Questions and Contributions

The research contributions of this thesis are focused on the process of developing an Enterprise Cyber Security Architecture that includes the anticipation the risk faced by financial institutions and the complexity of managing stakeholders from varying contexts while ensuring that the Cyber Security functions are still be performed. This led to the development and proposal of the SMILE reference framework. To manage the known financial institution risks, the stakeholders' interest and expectations, this reference framework is design to form a holistic view that serves as the foundations of the Enterprise Cyber Security Architecture.

Table 25: Research Contributions addressing research questions

	Research Question	Research Contribution answering the question
1	How can Cyber Security teams anticipate and identify the eco-system risks faced by financial institutions?	Integration of the PESTLE Analysis of Cyber Security in the Financial Industry for Enterprise Landscape Planning (Section 3.1.3.) can be used to anticipate and identify the eco-system risks faced by financial institutions.
2	Given the Enterprise Cyber Security Architecture, who are the primary stakeholders and how can their needs be effectively prioritized?	To identify the stakeholders, the proposed approach can be used to understand the Enterprise Structure of financial institution and reporting structure of CSOs and CISO. (Section 2.2.5.) To effectively prioritize the stakeholders' needs, a proposed approach can be used to perform both qualitative analysis (Section 2.5.3) and quantitative analysis (section 3.2) of the stakeholders' needs.
3	How can emergent risks and varying stakeholders' needs be identified and be used to shape the Enterprise Cyber Security Architecture?	By using the Stakeholder-Managed Integrated & Learning Enterprise (SMILE) Reference Framework (Chapter 3.), emergent risks and varying stakeholders' needs can be used to identify and shape the Enterprise Cyber Security Architecture. In Chapter 4, a demonstration of the application of SMILE Reference Framework to a Hypothetical Case is performed.

5.3. Limitation

In reviewing the thesis, the author identifies three key limitations about the SMILE Reference Framework and discusses them in the following subsections.

1) 5CEPS model input sources

While the 5CEPS model is great for converging perspectives from 5C Analysis, ARIES Enterprise Elements view analysis, PESTLE Analysis, SWOT Analysis, this analysis is highly dependent on the individual researcher's subjective ability to recognize the converging elements. To maximize the potential of the 5CEPS modes, it is recommended that this model is built upon the knowledge of a group of stakeholders. This group should collectively possess a vast understanding of the eco-system that evolves around the enterprise.

2) Selection of scenarios for future proofing

Currently, the selection of scenarios (to future proof for) is done qualitatively by the author and the effectiveness of the future proofing approach depends a lot on the individual researcher. In view of emergent effects, this approach may be limited and does not account for the emergence of both extreme positive and negative cases that can arise from previously unidentified scenarios. Alternatively, these potentially extreme scenarios could be linked to existing scenarios that are *not* considered as extreme. Due to the lack of study into the effects and impact of possible emergence, the selection of scenarios could be flawed if performed by an individual who does not have complete understanding of the enterprise or lack the ability to foresee potential impactful scenarios.

3) Partial validation of framework with hypothetical case

The feedback for validating the SMILE reference framework comes from industry practitioners who are either Cyber Security Consulting or Cyber Security team members managing a Financial institution Cyber Security functional team. Given the approach of applying the SMILE reference framework to a hypothetical case and the limited number of qualitative feedbacks performed, these efforts can at best achieved an initial and partial validation of the proposed reference framework.

5.4. Future Work

The author identifies five possible areas of future work,

1) Cyber Security Future Proofing

For each of the various scenarios, the feedback received is about the rating of each scenario found on the 5CEPS. The rating will be on the risk scenario's impact and probability to happen, akin to a risk matrix. Having such a matrix helps to systematically identify the opportunities and threats' impact (risk/reward) and probability, leading to a better selection of scenarios to plan for.

2) Quantifying the 5CEPS model effects with System Dynamics Modeling

The 5CEPS model is a qualitative analysis of enterprise's external and internal landscape and provides insightful awareness of the elements. This model does not provide the quantitative insight of the full impact upon the enterprise, upon the potential interactions of the elements. To better understand the impact, there are two possible quantitative approach. The first approach focusses on the defining an impact (risk/reward) rating for each intersection found on the right half of the 5CEPS model by placing a probability and impact value on each interaction. The second approach can be a meso-level modeling approach such as system dynamics modeling to uncover the potential impact of these effects.

3) Sensitivity and Connectivity analysis of the Architecture Decisions (AD)

To appropriately select a combination of AD, performing a sensitivity and connectivity analysis will provide the understanding of each AD's relevance to the metrics of the system and the inter-dependency of AD.

4) Emergent effects of increased or decreased utility for each combination of Architecture Decision

With the knowledge gained from the 5CEPS model, this can provide the understanding about potential emergence and how each combination of AD will provide a degree of synergy (or negative synergy) in the event of these emergent scenario.

5) Inclusion of Reflexivity awareness as an enterprise capability

Reflexivity is described as circular relationships between cause and effect that are often embedded in human belief structures. With both the cause and the effect affecting one another in a manner where neither can be assigned as causes or effects, a reflexive relationship is bidirectional and

hard to analyze. Further analysis on this topic can provide the researcher and enterprises a better appreciation of the causal relationship between enterprise elements and the ecosystem.

Bibliography

2018 Hacker Report. (2018, Dec 31). Retrieved May 13, 2019, from hackerone.com: https://www.hackerone.com/sites/default/files/2018-01/2018_Hacker_Report.pdf

A., C., & T., R. (2014). *Infiltrating the Target network*. Retrieved from Target Security Breach: https://people.carleton.edu/~carrolla/story.html

Aguilar, F. (1967). *Scanning the business environment.* New York: Macmillan.

Anderson, D. M. (2014). *Design for Manufacturability: How to Use Concurrent Engineering to Rapidly Develop Low-Cost, High-Quality Products for Lean Production.* Boca Raton: CRC Press.

Anderson, E. (2005). *Framework for marketing planning.* Michigan: Michigan Business school.

Anderson, E. (2005, March 1). *Framework for Marketing Planning.* Retrieved May 4, 2019, from www-personal.umich.edu: http://www-personal.umich.edu/~aandrea/Emrich%20Visioning/framework_for_marketing_planning.doc

Anthony, S. D., & Johnson, M. (2013, May 14,). *What a Good Moonshot Is Really For*. Retrieved from hbr.org: https://hbr.org/2013/05/what-a-good-moonshot-is-really-2

Bank of America. (2018, April 19). *Bank of America's Cyber Team Named Best by SC Magazine*. Retrieved from bankofamerica.com: https://newsroom.bankofamerica.com/press-releases/awards-and-recognition/bank-americas-cyber-team-named-best-sc-magazine

Barnett, W. P. (2008). *The Red Queen among Organizations: How Competition Evolves.* Princeton: Princeton University Press.

Bell, T. (2015, November 5). *How to not get fired as CISO*. Retrieved from CSOonline: https://www.csoonline.com/article/3000854/it-careers/how-to-not-get-fired-as-ciso.html

Bhattarai, A., & Harwell, D. (2018, January 23). *Inside Amazon Go: The camera-filled convenience store that watches you back*. Retrieved from chicagotribune.com: https://www.chicagotribune.com/business/ct-biz-amazon-go-cashierless-store-20180123-story.html

Blackman, A. (2014, Dec 8). *The Main Types of Business Risk*. Retrieved from envatotuts+: https://business.tutsplus.com/tutorials/the-main-types-of-business-risk--cms-22693

Boden, M. A. (2004). *The Creative Mind: Myths and Mechanisms.* London: Routledge.

Bossardt, M. (2018, May 15). *Identity and Access Management.* Retrieved May 3, 2019, from kpmg.com: https://assets.kpmg/content/dam/kpmg/ch/pdf/ch-identity-and-access-management.pdf

Brown, C. W. (2012, December 20). *File:Kano model showing transition over time.png.* Retrieved from wikimedia.org: https://commons.wikimedia.org/wiki/File:Kano_model_showing_transition_over_time.png

Cañamero, M. C. (2015, December 1). *Global Banking Regulatory Radar*. Retrieved May 12, 2019, from moodysanalytics.com: https://www.moodysanalytics.com/risk-perspectives-magazine/risk-management-decade-ahead/regulatory-spotlight/global-banking-regulatory-radar

Cash, D., Clark, W., Alcock, F., Dickson, N., Eckley, N., & Jäger, J. (2002, November). Salience, Credibility, Legitimacy and Boundaries: Linking Research, Assessment and Decision Making. *Faculty Research Working Papers Series*. Cambridge, Massachusetts, United States of America: John F. Kennedy School of Government, Harvard University.

Colorado Techical University. (n.d.). *The History of Cybersecurity*. Retrieved from Colorado Techical University: https://www.coloradotech.edu/degrees/studies/information-systems-and-technology/cybersecurity-history

Core War. (n.d.). *Creeper & Reaper*. Retrieved from Core War: http://corewar.co.uk/creeper.htm

Cory, N. (2017, May 1). *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* Retrieved May 20, 2019, from itif.org: http://www2.itif.org/2017-block-global-data-flow-960.jpg?_ga=2.240733632.2147133920.1558379618-751579218.1558379618

Crawley, E., Cameron, B., & Selva, D. (2016). *System Architecture: Strategy and Product Development for Complex Systems.* Hoboken: Pearson.

Crawley, E., de Weck, O., Eppinger, S., Magee, C., Moses, J., Seering, W., . . . Whitney, D. (2004). *The Influence of Architecture in Engineering Systems.* Cambridge: The ESD Architecture Committee.

Cruz, M. G. (2002). *Modeling, measuring and hedging operational risk (pp. 19-2).* New York: John Wiley & Sons.

Dekker, D. (1995). Engineering design processes, problem solving and creativity. *Proceedings Frontiers in Education 1995 25th Annual Conference. Engineering Education for the 21st Century.* Atlanta: IEEE.

D'Innocenzio, A. (2014, March 5). *Target's Chief Information Officer Resigns*. Retrieved Jan 3, 2019, from nytimes.com: https://www.nytimes.com/2014/03/06/business/targets-chief-information-officer-resigns.html

Drinkwater, D. (2016, April 20). *These CISOs explain why they got fired*. Retrieved from NetworkWorld: https://www.networkworld.com/article/3058985/security/these-cisos-explain-why-they-got-fired.html

Financial Times. (n.d.). *Glitch resets multiple Nasdaq tech stocks to same price*. Retrieved from Financial Times: https://www.ft.com/content/fbb44c3e-6053-11e7-91a7-502f7ee26895

F-Secure. (2018, 5 1). *The Changing State of Ransomware.* Retrieved 5 5, 2019, from fsecurepressglobal.files.wordpress.com: https://fsecurepressglobal.files.wordpress.com/2018/05/ransomware_report.pdf

Generali Global Assistance (GGA). (2018). *The impact of cybersecurity incidents on financial institutions .* Bethesda, MD: Generali Global Assistance (GGA).

Gonsalves, A. (2014, June 13). *Target top security officer reporting to CIO seen as a mistake*. Retrieved from CSOonline: https://www.csoonline.com/article/2363210/data-protection/target-top-security-officer-reporting-to-cio-seen-as-a-mistake.html

Hammer, J. (2018, May 3). *The Billion-Dollar Bank Job*. Retrieved from New York Times: https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html

Henderson, R. (2015, June 8). *Henderson*. Retrieved May 6, 2019, from forbes.com: https://www.forbes.com/sites/ellevate/2015/06/08/what-gets-measured-gets-done-or-does-it/#1adff43e13c8

Immersive Labs. (2019, January 15). *Goldman Sachs Leads Investment In Cyber Security Platform*. Retrieved May 17, 2019, from marketsmedia.com: https://www.marketsmedia.com/goldman-sachs-leads-investment-in-cyber-security-platform/

InformationWeek. (2012, April 4). *Banks May Not Be Able to Resist BYOD*. Retrieved from InformationWeek.com: https://www.informationweek.com/wireless/banks-may-not-be-able-to-resist-byod/d/d-id/1104033

ISC2. (2019, 2 28). *About ISC2*. Retrieved 2 28, 2019, from isc2.org: https://www.isc2.org/About

Jessica Silver-Greenberg, M. G. (2014, October 2). *JPMorgan Chase Hacking Affects 76 Million Households*. Retrieved December 17, 2018, from The New York Times: https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0

Jordan Robertson, M. R. (2015, November 4). *JPMorgan's Security Chief Jim Cummings Reassigned to Texas*. Retrieved Sept 15, 2018, from Bloomberg: https://www.bloomberg.com/news/articles/2015-11-04/jpmorgan-chief-security-officer-jim-cummings-reassigned-to-texas

Julian, T. (2014, December 4). *Defining Moments in the History of Cyber-Security and the Rise of Incident Response*. Retrieved from Infosecurity-magazine: https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/

Kanigel, R. (2005). *The One Best Way.* Cambridge: MIT Press Books.

Kano, N., Seraku, N., Takahashi, F., & Tsuji, S.-i. (1984, April 15). Attractive Quality and Must-Be Quality [in Japanese]. *Journal of the Japanese Society for Quality Control*, 147-156.

KPMG IT Advisory. (2009). *2009 European Identity and Access Management Survey.* Netherlands: KPMG .

Krebs, B. (2013, December 13). *Sources: Target Investigating Data Breach*. Retrieved from KrebsonSecurity: https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/

Maack, M. M. (2017, April 10). *Ancient programming language COBOL can make you bank, literally*. Retrieved from thenextweb.com: https://thenextweb.com/finance/2017/04/10/ancient-programming-language-cobol-can-make-you-bank-literally/

Mamudi, S. (2015, July 8). *NYSE Suspends Trading in All Securities*. Retrieved from Bloomberg : https://www.bloomberg.com/news/articles/2015-07-08/new-york-stock-exchange-suspends-trading-in-all-securities

Marr, D. (1982). *Vision: A Computational Investigation into the Human Representation and Processing of Visual Information.* Cambridge: MIT Press.

McCandless, D., Evans, T., Barton, P., Tomasevic, S., & Geere, D. (2019, April 1). *World's Biggest Data Breaches & Hacks*. Retrieved May 13, 2019, from informationisbeautiful.net: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Mintzberg, H. (1987). The Strategy Concept I: Five Ps for Strategy. *California Management Review*, 11–24.

Mirchandani, B. (2018, Aug 28). *Laughing All The Way To The Bank: Cybercriminals Targeting U.S. Financial Institutions*. Retrieved from forbes: https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#4e06ba746e90

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who. *Academy of Management*, October.

Morgan, S. (2016, Jan 30). *forbes.com*. Retrieved May 17, 2019, from Why J.P. Morgan Chase & Co. Is Spending A Half Billion Dollars On Cybersecurity: https://www.forbes.com/sites/stevemorgan/2016/01/30/why-j-p-morgan-chase-co-is-spending-a-half-billion-dollars-on-cybersecurity/#72af0b9e2599

Morgan, S. (2016, May 13). *Top 5 Industries At Risk Of Cyber-Attacks*. Retrieved from Forbes: https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#597459ba715e

Muncaster, P. (2015, June 24). *Finance Hit by 300 Times More Attacks Than Other Industries*. Retrieved from Infosecurity-magazine: https://www.infosecurity-magazine.com/news/banks-hit-300-times-more-attacks/

Natasha Nelson, S. M. (2017). Studying the Tension Between Digital Innovation and Cybersecurity. *Twenty-third Americas Conference on Information Systems* (pp. 1-11). Boston, MA: MIT Cybersecurity Interdisciplinary Systems Laboratory (CISL).

New York Times. (2015, JULY 8). *A History of Stock Exchange Failures*. Retrieved from New York Times: https://www.nytimes.com/interactive/2015/07/08/business/dealbook/history-of-stock-exchange-failures.html#/#time380_11063

Nightingale, D. J., & Rhodes, D. H. (2015). Architecting the Future Enterprise. In D. J. Nightingale, & D. H. Rhodes, *Architecting the Future Enterprise* (p. 185). Cambridge: The MIT Press.

Notman, J. (2018, August 15). *Identity and Access Management is pivotal for GDPR compliance*. Retrieved from opentext.com: https://blogs.opentext.com/identity-and-access-management-is-pivotal-for-gdpr-compliance/

O'Connor, C. (2014, May 5). *Target CEO Gregg Steinhafel Resigns In Data Breach Fallout*. Retrieved from Forbes: https://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/

okta. (2019, May 4). *Setting Up IAM: Managing Permissions to Ensure Compliance*. Retrieved May 4, 2019, from okta.com: https://www.okta.com/identity-101/iam-compliance/

Oltsik, J. (2018, September 19). *5 biggest cybersecurity challenges at smaller organizations*. Retrieved February 2, 2019, from csoonline.com: https://www.csoonline.com/article/3307476/5-biggest-cybersecurity-challenges-at-smaller-organizations.html

Ontario Securities Commission. (2018, June 14). *9 types of investment risk*. Retrieved from Ontario Securities Commission: https://www.getsmarteraboutmoney.ca/invest/investing-basics/understanding-risk/types-of-investment-risk/

Piepenbrock, T. (2009). Towards a Theory of Evolution of Business Ecosystems: Enterprises Architecture, Competitive Dynamics, Firm Performance and Industrial Co-Evolution. *doctoral dissertation*. Cambridge, Massachusetts, United State of America: MIT.

Pompon, R. (2017, September 7). *CIO or C-Suite: To Whom Should the CISO Report?* Retrieved 2 28, 2019, from darkreading.com: https://www.darkreading.com/partner-perspectives/f5/cio-or-c-suite-to-whom-should-the-ciso-report/a/d-id/1329807

Porter, M. (1996). What is Strategy. *Harvard Business Review*, 61-78 Nov-Dec.

Press, G. (2015, November 1). *This Week In Tech History: The Birth Of The Cybersecurity And Computer Industries*. Retrieved from Forbes: https://www.forbes.com/sites/gilpress/2015/11/01/this-week-in-tech-history-the-birth-of-the-cybersecurity-and-computer-industries/#258488275bcd

Raby, M. A. (2012, May 11). Architecting the Future Enterprise: A Framework for Supporting Decision Making in the Selection of Future States. *Master's Thesis*. Cambridge, MA, United States of America: MIT.

Randall Kroszner, A. S. (1996). *The Evolution of Universal Banking and Its Regulation in Twentieth Century America.* Burr Ridge, IL: Irwin.

Rayner, J. (2004). *Managing reputational risk: Curbing threats, leveraging opportunities (Vol. 6).* John Wiley & Sons.

Reuters. (2017, May 24). *Target Settles 2013 Hacked Customer Data Breach For $18.5 Million*. Retrieved from NBC News: https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031

Riley, J. R. (2015, June 30). *JPMorgan Reassigns Security Team Leader a Year After Data Breach*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2015-06-30/jpmorgan-reassigns-security-team-leader-a-year-after-data-breach

Sáenz, H. H. (2015, April 10). *The magic of a morphological matrix.* Retrieved from medium.com: https://cdn-images-1.medium.com/max/400/1*kc5N4N8bIy2isgR8156i6g.gif

Saunders, A. C. (2006). *Financial institutions management: A risk management approach.* New York: McGraw-Hill/Irwin.

Schuck, H. (2015, February 5). *HIGH CIO AND CISO TURNOVER: WHAT IT MEANS FOR IT SALES*. Retrieved from DiscoverOrg: https://discoverorg.com/blog/high-cio-and-ciso-turnover-what-it-means-for-it-sales/

SentinelOne. (2018, March 10). *the history of cyber security — everything you ever wanted to know.* Retrieved from SentinelOne: https://www.sentinelone.com/blog/history-of-cyber-security/

Siklos, P. (2001). Money, Banking, and Financial Institutions: Canada in the Global Environment. In P. Siklos, *Money, Banking, and Financial Institutions: Canada in the Global Environment* (p. 40). Toronto: McGraw-Hill.

SWIFT. (2019). *Introduction to SWIFT*. Retrieved from SWIFT: https://www.swift.com/about-us/discover-swift

SWIFT. (2019). *Messaging and Standards*. Retrieved from SWIFT: https://www.swift.com/about-us/discover-swift/messaging-standards

Taylor, F. W. (1919). *The principles of scientific management.* New York and London: Harper and Brothers Publishers.

The Daily Star. (2019, February 5). *BB Cyber Heist: JP's Chunnu demands finance minister's statement in House*. Retrieved from The Daily Star: https://www.thedailystar.net/politics/bangladesh-bank-heist-jatiya-party-mp-demands-finance-ministers-statement-1697344

The Mind Tools Content Team. (2016, November 16). *Kano Model Analysis*. Retrieved April 1, 2019, from mindtools.com: https://www.mindtools.com/pages/article/newCT_97.htm

The National Institute of Standards and Technology (NIST). (2018, April 16). *Cybersecurity Framework Documents.* Retrieved from nist.gov: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Thompson, D. (2017, April 10). *What in the World Is Causing the Retail Meltdown of 2017?* Retrieved May 6, 2019, from theatlantic.com: https://www.theatlantic.com/business/archive/2017/04/retail-meltdown-of-2017/522384/

TrustWave. (2019, May 6). *2019 Trustwave Global Security Report.* Retrieved May 6, 2019, from Trustwave.com: http://go.trustwave.com/a0300l0VCR0z002MCFcRTiq

Veltsos, C. (2018, January 9). *Where the CISO Should Sit on the Security Org Chart and Why It Matters*. Retrieved 2 28, 2019, from securityintelligence.com: https://securityintelligence.com/where-the-ciso-should-sit-on-the-security-org-chart-and-why-it-matters/

Wagstaff, K. (2013, December 19). *Massive Target credit card breach new step in security war with hackers: experts*. Retrieved from NBC News: https://www.nbcnews.com/technology/massive-target-credit-card-breach-new-step-security-war-hackers-2D11778083

WorldBank. (2018, October 1). *Environmental and Social Framework*. Retrieved May 12, 2019, from worldbank.org: https://www.worldbank.org/en/projects-operations/environmental-and-social-framework

Young, J. (2019, January 21). *Global e-commerce sales grow 18% in 2018*. Retrieved May 6, 2019, from digitalcommerce360.com: https://www.digitalcommerce360.com/article/global-ecommerce-sales/

Yu, M. (2015, Feb 26). *Four Reasons Why CIOs Get Fired*. Retrieved from CIO.com: https://www.cio.com/article/2889326/it-strategy/four-reasons-why-cios-get-fired.html

Zacharias, G. L., MacMillan, J., & Van Hemel, S. B. (2008). *Behavioral Modeling and Simulation: From Individuals to Societies.* Washington: National Academies Press.

Zetter, K. (2016, May 17). *That insane, $81m bangladesh bank heist? Here's what we know*. Retrieved from WIRED: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/