ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 13 (2023) No. 5, pp. 525-543
DOI:10.33168/JSMS.2023.0534

A Comprehensive Cybersecurity Maturity Study for Nonbank Financial Institution

Vesa Kurnianto Hidayat, Gunawan Wang

Information Systems Management Department, Bina Nusantara University, Jakarta 11480, Indonesia

vesa.hidayat@binus.ac.id, gwang@binus.edu

Abstract. In today's era of digital disruption, information security holds paramount importance for institutions, demanding their utmost attention. Effective management of organizational information is a crucial component in achieving Good Corporate Governance. The level of protection measures serves as an indicator of an organization's cybersecurity awareness and its ability to safeguard business processes in the short, medium, and long term, especially within the realm of information and communication technology (ICT). To achieve this, organizations require a suitable security standard tailored to their specific needs, aiding them in assessing the maturity level of their cybersecurity measures and protecting their information security. This paper focuses on a case study conducted at an Indonesian Life Insurance firm, which manages critical infrastructure and digital financial transactions. The organization has already implemented several international security standards through comprehensive planning, implementation, evaluation documentation, and ICT activities. However, these initiatives have absorbed a substantial portion of the company's budget. Consequently, both management and stakeholders need to ascertain the effectiveness of these investments and gain insights into the company's preparedness to support its digitalization efforts, considering its extensive operations in the region and the prevailing cyber threats. To address these concerns, this study employs an analysis based on the NIST Cybersecurity Framework version 1.1, with a primary focus on operational effectiveness rather than mere compliance. The results and findings regarding the maturity level of cybersecurity within the organization are anticipated to inform improvements in ICT management. By conducting this analysis, the organization aims to bolster its information security posture, enhance its ability to combat cyber threats. Ultimately, this study aims to contribute to the overall advancement of information security within organizations operating in today's digitally disruptive landscape.

Keywords: Information security, Cybersecurity, NIST CSF, Security Maturity Level, Financial Institution.

1. Introduction

Digital transformation is radically changing society and the international economy, favoring new political and social interactions, as well as new economic and commercial transactions. New technologies and initiatives, such as the Internet of Things (IoT) and Industry 4.0, are leading the evolution of "net" use, introducing new users and increasing the quantity and the types of data. Financial institutions, in this case, insurance firms, also transform the method of how to sell the products. It adopts information technologies to broaden the market. Mobile applications, sales websites, and social media are being used to increase income. The adoption of new digital technologies is increasing cyberspace and, consequently, related risks (Dzolbelova, Ilaeva, 2020).

Cyber risk is the operational risk associated with organizations' economic losses caused by data and/or information systems being unavailable, lack of integrity or confidentiality failure. Its origin can be accidental (e.g., shutdown of a server) or intentional (e.g., theft of sensitive data). In the latter case, cyber-attacks represent the main threat: mainly automated actions designed to disrupt, damage, or hamper normal system operations, networks or processes (Gatzert, Schubert, 2022). Various potential consequences can be caused by a cyber-event that is either internal or external to the organization, such as interruption of activities, reputation/image damage, dissemination/violation of confidential data, violation of intellectual propriety and legal actions. Cyber-attacks are carried out using "cyber weapons": malicious software (abbreviated "malware") specifically designed to damage or modify an information system.

Cybersecurity protection is of utmost importance for life insurance institutions due to the sensitive nature of the information they handle, including personal and financial data of policyholders. The potential consequences of a cybersecurity breach can be severe, ranging from financial losses to reputational damage and legal ramifications. Here is some background information highlighting the significance of cybersecurity in life insurance institutions:

a. Growing Cybersecurity Threats: The insurance industry, including life insurance, has become a prime target for cybercriminals due to the valuable data it possesses. Cybersecurity threats such as data breaches, ransomware attacks, and phishing attempts are on the rise. According to a 2021 report by Accenture, the insurance industry experienced a 50% increase in cyber-attacks during the COVID-19 pandemic.

b. Regulatory Compliance: Life insurance institutions in Indonesia are subject to various regulations from Otoritas Jasa Keuangan (OJK). OJK has issued various regulations that address cybersecurity and data protection requirements for insurance companies, including life insurance institutions. These regulations outline the obligations, standards, and guidelines that insurers must follow to ensure the security of policyholders' data. Compliance with these regulations is essential to avoid significant financial penalties and legal consequences. Robust cybersecurity measures are crucial for maintaining compliance and protecting policyholders' privacy rights.

c. Impact of Data Breaches: A data breach can have severe financial implications for life insurance institutions. According to the 2020 Cost of a Data Breach Report by IBM, the average cost of a data breach in the financial industry was $5.9 million. This includes expenses related to incident response, legal services, regulatory fines, and customer notifications. Additionally, the reputational damage caused by a data breach can lead to customer attrition and loss of trust.

d. Examples of Cybersecurity Incidents: Several notable cybersecurity incidents have affected life insurance institutions. One such example is the 2015 Anthem breach, where hackers gained unauthorized access to the health insurer's database, compromising personal information of approximately 78.8 million individuals. Another example is the 2020 attack on Prudential, where threat actors gained access to personal information of around 17,000 customers. These incidents highlight the vulnerabilities faced by life insurance institutions and the need for robust cybersecurity measures.

To combat these challenges, life insurance institutions need to invest in comprehensive cybersecurity programs. This includes implementing robust security measures, conducting regular risk assessments, educating employees about cybersecurity best practices, and staying updated with the latest industry trends and technologies. By prioritizing cybersecurity, life insurance institutions can protect policyholder data, maintain regulatory compliance, and safeguard their reputation in an increasingly digital landscape.

In order to protect the data and information system from cyber-attacks and to pull down the cyber risk, an organization is willing to spend a huge amount of budget to purchase the infrastructure security and implement a lot of controls to protect the information from internal and external cyber risk (Romanosky, 2016). In this study case, one of Indonesian Life Insurance allocated 65 percent of a 2022 IT division budget for information security concerns. IDR 20 bio is used to perform technology refreshment, to replace all hardware and software that will reach the end of support. It is important to have support from the principal as the security patch release will be guaranteed. This organization also budgeted IDR 15 bio to renew the recurring annual license of the software including antimalware, disk encryption, e-mail/internet content scanning, intrusion preventive system, etc. IDR 2,4 bio is budgeted to rent racks in the collocation data center. This collocation data center has an international standard of physical security protection. IDR 1,8 bio is allocated to have 24x7 security officer control who monitors and responds to any security anomalies.

To explain this huge IT budget allocation to the CEO who has a non-IT background is a challenging part for the IT director. This 65 percent does not have a direct impact on the company’s profit. The effectiveness of the budget spending also cannot be measured by the company’s productivity. Hence the IT director decided to use the IT security maturity rating and level of readiness for the cyber-attack to convince the CEO of the budget allocation.

This study will show how to calculate the IT cybersecurity maturity level. Based on the current maturity level compared to the targeted level, this study will produce a recommendation to the company. This recommendation will become a baseline in the further study to develop a cybersecurity roadmap that is visible to be implemented in the organization. The cybersecurity maturity study will use NIST Cybersecurity Framework (CSF) version 1.1.

This study has some objectives to be achieves. The first objective is to assess the level of cyber security maturity at PT XYZ, in order to provide visibility to the company's management, who have invested in enhancing the information security aspect. This assessment aims to evaluate the existing cyber security measures and identify any gaps or weaknesses that may exist within the organization. By understanding the maturity level, the management can make informed decisions and allocate resources effectively to improve the overall cyber security posture.

The second objective is to develop a cyber security system for PT XYZ using the NIST (National Institute of Standards and Technology) version 1.1 approach. This approach follows industry best practices and guidelines for managing and securing information systems. The outcome of this development process will be a comprehensive blueprint that can be implemented within the company, ensuring that the cyber security system is optimized. The blueprint will provide a roadmap for the implementation of various security controls, protocols, and procedures to mitigate risks and protect sensitive information effectively.

By achieving these objectives, PT XYZ aims to enhance its cyber security capabilities, minimize the likelihood of cyber-attacks or breaches, and safeguard the integrity, confidentiality, and availability of its information assets. This proactive approach will not only protect the company's reputation and customer trust but also ensure compliance with relevant regulatory requirements in the ever-evolving landscape of cyber threats.

2. Literature Review

Cyber-attacks in the insurance sector are growing exponentially as insurance companies migrate toward digital channels to create tighter customer relationships, offer new products, customer experience, and expand their share of customers' financial portfolios. This shift is driving increased investment in traditional core IT systems (e.g., policy and claims systems) as well as in highly integrated enabling platforms such as agency portals, online policy applications and web- and mobile-based apps for filing claims. Although these digital investments provide new strategic capabilities, they also introduce new cyber-risks and attack vectors to organizations that are relatively inexperienced at dealing with the challenges of an omni-channel environment. What is more, the challenges are likely to become more complex as insurers embrace big data and advanced analytics that require collecting and handling vast amounts of consumer information. As insurers find new and innovative ways to analyze data, they must also find ways to secure the data from cyber-attacks.

Over the years, many insurance organizations have invested a lot of money in security tools and processes that may be providing a false sense of security. As attackers learn to leverage encryption and other advanced attack techniques, traditional tools such as firewalls, antivirus software, intrusion detection systems (IDS) and intrusion prevention systems (IPS) are becoming less and less effective. As a result, many insurers may be misallocating their limited resources to address compliance-oriented, easily recognized threats while completely overlooking stealthy long-term threats that ultimately could be far more damaging. Hence a maturity study using a cybersecurity framework is required to be done to discover the effectiveness of the budget spending.

Referring to Cybersecurity Capability Maturity Model (C2M2) Program that released by the Department of Energy (DOE) of the US (2019), the Maturity Model is a set of characteristics, indicators, or patterns representing capabilities and development in a particular science field. Maturity models can be prepared by adopting existing standards or combining several best practice standards. The cybersecurity maturity model will assist in providing direction for the Organization to undertake independent assessments.

Implementing the maturity model will provide benchmarks that can help organizations evaluate improvement organizational aspects (Rivas et all.,2020). C2M2 is on adopting and managing cybersecurity practices related to information assets, information and operating technology, and the environments. Usability model is (Sulistyowati et all., 2020):

a. Strengthening the organization's cybersecurity capabilities;
b. Allows organizations to consistently and effectively evaluate and measure cybersecurity capabilities;
c. Sharing knowledge, best practices, and relevant references across the organization;
d. Allows organizations to prioritize actions and investments to enhance cybersecurity.

There are many frameworks to be used to assists organizations to evaluate and identify areas of weakness and strength that can guide the development of a cybersecurity program. For instance, COBIT, ISO 27001, PCI DSS, NIST Cybersecurity Framework (NIST CSF), etc. But to assess the critical infrastructure, especially in financial sector, NIST CSF has unique position. The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can serve as a model for international cooperation on strengthening cybersecurity in critical infrastructure as well as other sectors and communities.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each money spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

2.1. NIST Cybersecurity Framework

The NIST Cybersecurity Framework version 1.1 is a set of guidelines, standards, and best practices developed by the National Institute of Standards and Technology. It helps organizations manage and improve their cybersecurity efforts. Originally named the Bureau of Standards, NIST's goal was to ensure a consistent standard of size and function as laboratory standards. NIST was used extensively in the cybersecurity sector in the 1970s (Sulistyowati et all., 2020). One of NIST's best practices for cybersecurity management, NIST Cybersecurity Framework (NIST CSF). NIST CSF components are more appropriate for technology organizations to use because of their scope of technical control, log analysis, and incidents. The latest update was published on April 16, 2018, through version 1.1. The current framework provides a comprehensive assessment consisting of three essential components, namely: Framework Core, Profile and Implementation Level (Sulistyowati et all., 2020).

The Framework Core is the foundation of the framework and is divided into five functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a structured approach to managing cybersecurity risks.

Profiles allow organizations to tailor the framework to their specific needs. Organizations can create a profile by selecting and customizing the framework's components based on their risk tolerance, business objectives, and requirements.

The Implementation Tiers provide a way for organizations to assess their cybersecurity maturity. Tiers range from Partial (Tier 1) to Adaptive (Tier 4), representing different levels of integration and effectiveness in cybersecurity practices.

By adopting the NIST Cybersecurity Framework version 1.1, organizations can establish a systematic approach to managing cybersecurity risks. It helps organizations identify their assets and risks, implement protective measures, detect and respond to cybersecurity events, and recover effectively. The framework's flexibility allows organizations to adapt it to their unique circumstances and improve their overall cybersecurity resilience.

2.2. Cyber Threat Landscape for Non-Bank Financial Institution

Based on the previous study by Gatzert and Schubert, there are specific cyber threat landscape for non-bank financial institution specifically in Asia. It has profiled organization’s cyber threat landscape into possible threat actors to be wary of; probable threat vectors that these groups or other criminal groups may use to target the institution; and the possible scenarios where these threats may manifest (Gatzert and Schubert, 2022).

2.2.1 Cyber Threat Actors

Cyber threat actors targeting insurance companies are generally cyber criminals from well-resourced organized crime groups with complex and wide networks of actors to leverage the information they can exploit. There are three active cyber threat actors, operating in the region, which are known to target insurance companies: FIN4, Deep Panda and Tropic Trooper.

FIN4 is an organized crime group which specializes in phishing campaigns to gain access to organizations with the interest to gain financial advantage in stock market by leveraging the healthcare data and Personal Identifiable Information (PII) obtained for extortion.

Deep Panda is a state-linked organized crime group which specializes in information and intellectual property theft for Black Market trade and financial gains via espionage. The information they target include both PII and credit card information.

Tropic Trooper is an organized crime group which specializes in using exploits against vulnerable systems and services through various malware to steal information and intellectual property for financial gains via espionage. The information they target, specific to the insurance industry, include PII, healthcare data and credit card information, both of which are traded on the black market.

2.2.2 Black Market Value of PII, Health and Credit Card Information

There is interest to obtain PII, health and credit card information for fraudulent claims or for extortion (based on health issues) especially for Politically Exposed Persons (PEPs) or Socially Influential Persons (SIPs).

The information can be used to profile the spending of the targeted individuals to monitor their location, spending behaviors, understand their health issues and target their associated persons (e.g. family members). This can be further used to blackmail or extort financial gains through coercion or influencing stock market plays for the cyber threat actors to gain legitimized income.

Additionally, PII, health and credit card information have a strong demand in the Black Market to be used as sources of funding for illegal activities by other threat actors.

2.2.3 Top Cyber Threat Vectors

The top cyber threat vectors typically used include (a) Phishing; (b) Exploiting Unpatched Systems; (c) Exploiting Vulnerable / Legacy Systems; and (d) Exploiting the cyber supply chain through vendors / business partners.

a. Phishing is typically carried out in targeted and broad sweeping Business Email Compromise campaigns to address employees of an organization as well as known associates to be able to gain a trusted access into the organization. These associates could include vendors and contractors, business partners and customers. The successful entry obtained through any one targeted party could allow for the equivalent of an insider’s access to systems.
b. Exploiting Unpatched Systems and zero-days in the technology environment generally provide opportunities to gain unauthorized access to systems and sensitive information and lead to confidentiality and integrity compromise to the information stored within these systems.
c. Exploiting Vulnerable and/or Legacy Systems is a convenient attack vector for sophisticated threat actors as organizations, due to the challenges in migrating information and operations to modern platforms, choose to continue operations using legacy systems. These systems generally have components which have run out of support and no longer receive updates to remediate newly discovered vulnerabilities, leaving them exposed for exploitation
d. Exploiting the Cyber Supply Chain is another convenient and increasingly common attack vector for sophisticated and well-resourced threat actors. Threat actors exploit access obtained through the trusted access pathways of vendors of their target organizations to achieve their nefarious objectives. Law firms, accounting firms, key outsourced services providers are constantly targeted due to their aggregated information repositories or trusted access to their final targeted organizations such as banks, manufacturing companies, and governments. The exploited weaker participants in the cyber supply chain could potentially provide means to circumventing typically strong perimeter controls.

2.3. Possible Exploit Scenario

Taking into consideration of known cyber campaigns for Sing Health (2018) and Marriott (2018), cyber threat actors target PII, healthcare data and credit card information to (a) monitoring and track PEPs and SIPs; (b) build dossiers of profiles of PEPs and SIPs for extortion; and (c) sell this information in the Black Market.

A threat actor can employ the use of social engineering techniques (e.g. phishing emails) playing on the targeted privileged users' concerns (e.g. fear of authority) to convince users to click on seemingly legitimate attachments, browse websites that has embedded malware or even submit sensitive information to infect their workstations/laptops. Equipped with privileged access, threat actors can go on to perform a variety of actions, these may include downloading additional advanced malware for deeper exploitation of the infected asset or they may choose to seek out more valuable targets or a combination of both.

The course of action depends on the motivation of the threat actor. In complex attack campaigns where threat actors go for an organization's crown jewels1, the threat actor would perform reconnaissance to understand the layout of the victim's network by seeking to propagate or laterally move through the network via exploitation of unpatched systems, zero-day vulnerabilities or misconfiguration in the technology assets. These vulnerabilities are often in commonly used communication protocols used to transfer files or manage the systems. Once the threat actor can successfully compromise a workstation with higher privileges (i.e. credentials/direct connectivity to databases) or a database server that possess sensitive data, threat actors can query databases to obtain data and proceed to exfiltrate them through these legitimate communication channels to avoid detection.

This flow of attack was adopted in both the Sing Health and Marriott breaches. The means of entry may not necessary be reliant on phishing alone and could be other vectors such as exploitation of vulnerabilities in Internet-facing systems, through the unwitting assistance by third-party vendors who possess poor cyber hygiene or even for vendors who have been deliberately compromised to provide threat actors with unauthorized access to the intended victim's network.

3. Methodology

This study adopted a three (3) phase approach for the study beginning with the Planning of Work and Discovery of Information, the Analysis of Information, and Reporting. A comprehensive assessment will be performed by following detailed steps in the NIST CSF.

Phase (1) will be Planning of work and discovery of Information that have two agendas as follows:

a. Initial planning of activities and confirming the resources and stakeholders necessary for the study
b. Collection of information. It will perform documents requests, interviews, and cyber threat landscape study for the Life Insurance Company.

The next step is phase (2), Analysis to determine maturity scoring and gaps to target state. The maturity scoring will be performed using NIST Cyber Security Framework version 1.1. The score or level determination will be explained in the chapter 3.3 Implementation Level in this paper. Then phase (3), Establishing initiatives roadmap and reporting.

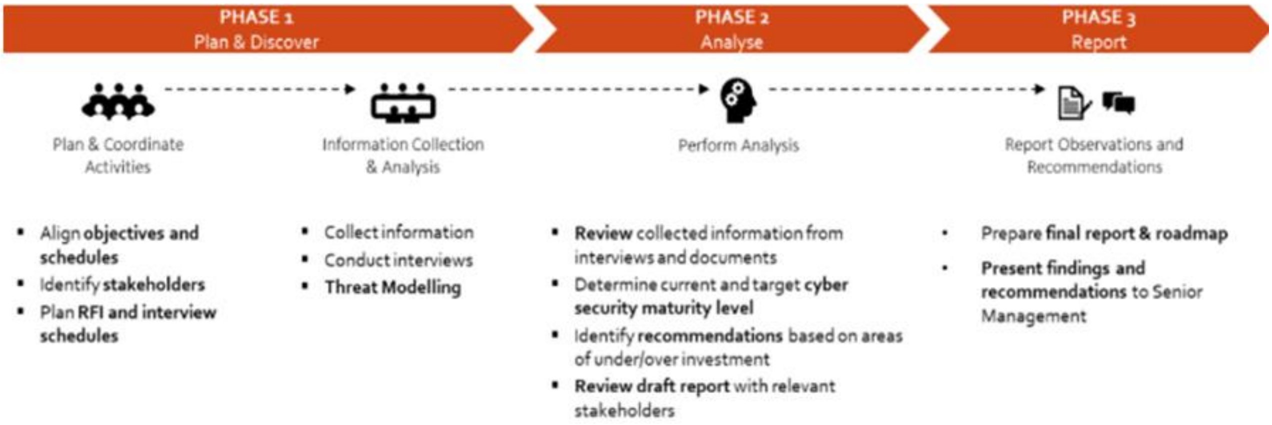

PHASE 1
Plan & Discover
PHASE 2
Analyse
PHASE 3
Report
Plan & Coordinate Activities
Information Collection & Analysis
Perform Analysis
Report Observations and Recommendations
Align objectives and schedules
Identify stakeholders
Plan RFI and interview schedules
Collect information
Conduct interviews
Threat Modelling
Review collected information from interviews and documents
Determine current and target cyber security maturity level
Identify recommendations based on areas of under/over investment
Review draft report with relevant stakeholders
Prepare final report & roadmap
Present findings and recommendations to Senior Management

Fig.1: Phase and Approach of the Study

Using NIST CSF, it contextualized the information collection and interviews across the 23 control families in the five (5) functions of IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER. In addition to the Information Collection and Interviews, a Cyber Threat Intelligence study performed on the cyber threat landscape unique to the organization. This cyber threat landscape is used to contextualize the target state for the cyber defense operations for organization to identify the gaps between the current state and the target state.

The information collected and mapped the current and target states to derive the gaps and recommendations which would be impactful to the organization and plotted the recommended initiatives to a strategic roadmap to support the organization's growth towards a fit-for-purpose cybersecurity defense posture. These results were discussed and shared with organization's stakeholders to ensure alignment and fit and finally concluded in this study.

3.1. Framework Core

This component is divided into five risk management functions to provide a high-level overview of the organization's cybersecurity situation.

a. Identification: Development of complete knowledge about the cyber environment, particularly systems, assets, data, and capabilities. The IDENTIFY function directly relates to the alignment of the cybersecurity strategy with organizational needs, management of cyber risks as well as visibility over organizational assets. Organization fragmented asset management processes combined with its journey towards digitalization places it in a poor position to be able to have an acute understanding of its asset surface, and correspondingly the associated risks and threats.
b. Protect: Appropriate deployment and development to limit potential cybersecurity crash events. The PROTECT function directly relates to the preventive measures in place to safeguard organizational systems and data. Network segmentation has been established broadly and a basic trust model has been applied on the assets and information. Organization has implemented a three-tier network segmentation approach to separate management, user and backup traffic with an established model to managed privileged access to systems. This establishes the foundational basis for the security-by-design of systems, present and new. Organization has also established measures to protect the data residing outside of the premises network as the business gets digitalized. A roadmap has been defined to implement protective controls for data on agents' personal computing devices with solutions such as Mobile Device Management (MDM) solution and Cloud Access Security Broker (CASB) solution. In addition, plans are in place to integrate security practices into agile software development processes for new digital offerings.
c. Detection: Developing and implementing appropriate activities to identify cybersecurity events quickly. The DETECT function directly relates to the awareness and visibility of internal and

external threats to organization. The underinvestment places the company in a poor position to recover from cybersecurity incidents due to the poor awareness, agility and capability to respond and restore business operations. The organization will be exposed to higher risks in its pursuit to leverage Cloud technologies, embrace Data Sciences and proliferate digital services, which will further increase its attack surface. The organization has embarked on establishing its own threat hunting capability and is currently implementing the Endpoint Detection and Response (EDR) platform, Carbon Black, to enable internal visibility of the technology environment.

d. Respond: Develop and implement appropriate activities to avoid the unwanted impact of cybersecurity events. The RESPOND function directly relates to the agility and ability of the organization to respond to cyber threats to their systems. There is an established approach to containing incidents upon detection. Communication pathways and SLAs are also defined to ensure stakeholders are furnished with the latest information to make informed decisions. Agreements with incident response partners are also defined to ensure a contingent workforce for activation when additional expertise or resources are required.

e. Recovery: Development and recovery activities to maintain resilience plans and restore capabilities that may be compromised by a cybersecurity incident. The RECOVER function directly relates to agility and ability of the organization to recover from cyber threats. The organization had adopted recovery strategies in line with its risk appetite. These include forming forums to derive lessons learnt and workflows for public engagements to protect organizational reputation and branding.

Refer to the following figure, these five functions are divided into 23 categories and 108 sub-categories, with each sub-category, is a list of external reference materials.

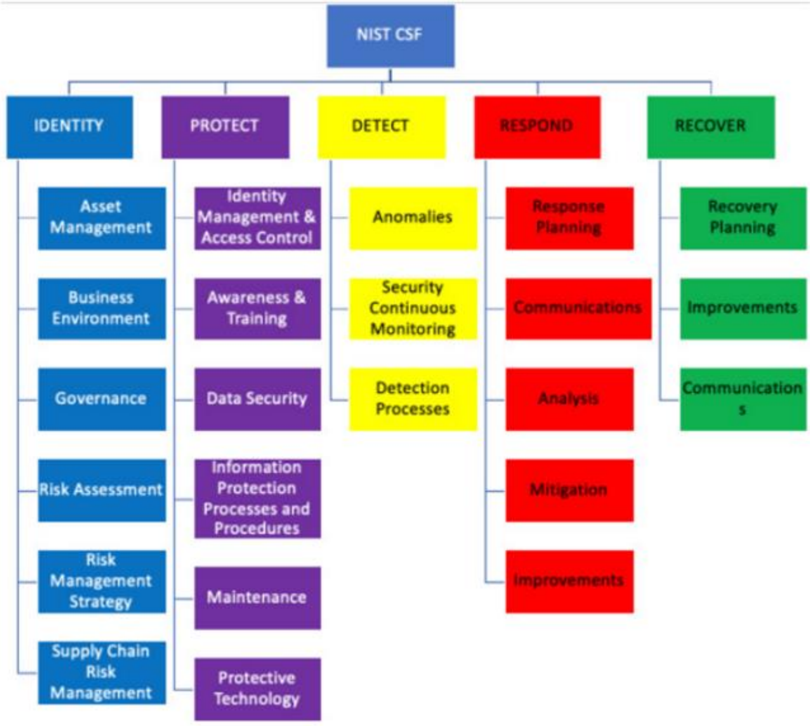


Fig.2: Function and Category NIST CSF

3.2. Profile

The framework profile represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile (the “as is” state) with a “Target” Profile (the “to be” state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization’s risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

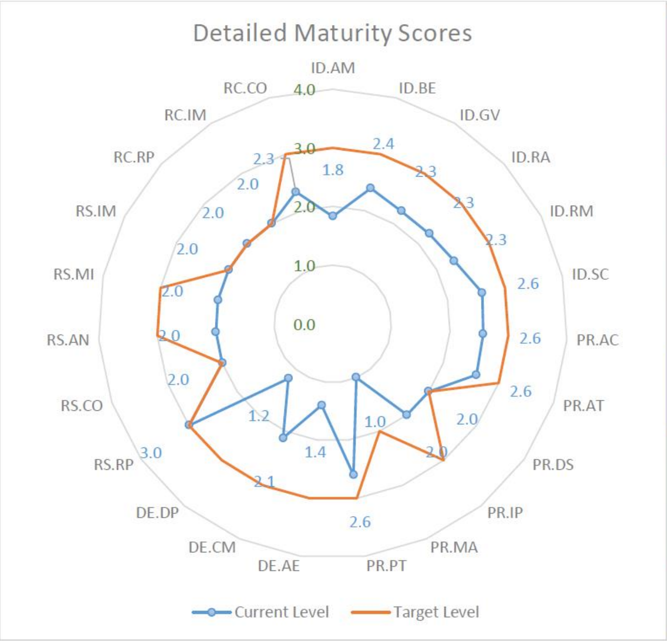
3.3. Implementation Level

The implementation level provides context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization’s practices over a range, from Partial (Level 1) to Adaptive (Level 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

a. Level 1: Partial
   At this tier, organizations have limited awareness of their cybersecurity risks, and cybersecurity activities are performed in an ad hoc manner. There is a lack of standardized policies, procedures, and controls, resulting in an inconsistent approach to cybersecurity across the organization.
b. Level 2: Risk-Informed
   Organizations at this tier have a basic understanding of their cybersecurity risks and have started to implement risk management processes. There is an ongoing effort to develop and implement cybersecurity policies, procedures, and controls. However, the implementation may not be consistent across the organization.
c. Level 3: Repeatable
   At this tier, organizations have established formalized and standardized cybersecurity processes and controls. These processes are regularly reviewed and improved based on lessons learned from previous incidents. The organization's cybersecurity practices are documented and consistently followed.
d. Level 4: Adaptive
   Organizations at this tier have an agile and proactive approach to cybersecurity. They continuously monitor their cybersecurity environment, adapt their processes and controls based on changing threats and vulnerabilities, and actively share information with internal and external stakeholders. Cybersecurity is ingrained into the organization's culture and operations.

4. Results

This section provides a view of the organization’s cybersecurity efficacy across the 23 control families in the five (5) functions: IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER.



IDENTIFY (ID)	ID.AM	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy
	ID.SC	Supply Chain Risk Management
PROTECT (PR)	PR.AC	Identity Management, Authentication and Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection Processes and Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology
DETECT (DE)	DE.AE	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes
RESPOND (RP)	RP.RP	Response Planning
	RP.CO	Communications
	RP.AN	Analysis
	RP.MI	Mitigation
	RP.IM	Improvements
RECOVER (RC)	RC.RP	Recovery Planning
	RC.IM	Improvements
	RC.CO	Communications

Fig.3: Detailed Maturity Scores and Target Scores based on the NIST Cybersecurity Framework

4.1. Key Observation

Organizations’ pursuit of IT compliance against regulations for financial services has led to the establishment of strong foundational capabilities which are clearly represented in the relatively higher maturity scores in the PROTECT, RESPOND and RECOVER functions. These are represented by significant investments in products to establish strong perimeter defense and ensure processes adhere to regulations.

Due to the focused treatment of risk management through compliance, the IDENTIFY and DETECT functions have been under-invested, exposing organization to cyber threats. The organization’s lack of cybersecurity focus beyond compliance motivation is primarily due to (i) the absence of an aligned cybersecurity strategy and centralized cybersecurity organization structure; (ii) a fragmented overview of asset surface and gaps in monitoring; and (iii) the absence of a defensible technology architecture with excessive systems diversification. The sprawl of the technological assets across the different organizational units and the lack of a centralized and detailed inventory further complicates the ability to observe and manage the asset surface, resulting in a porous resultant attack surface.

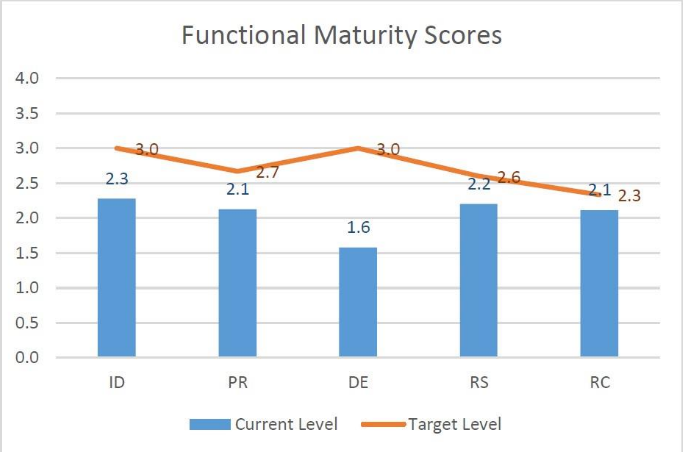


Fig.4: Functional Maturity Scores based on the NIST Cybersecurity Framework

4.1.1 IDENTIFY

The IDENTIFY function directly relates to the alignment of the cybersecurity strategy with the organization's organizational needs, management of cyber risks as well as visibility over organizational assets. The organization's fragmented asset management processes combined with its journey towards digitalization places it in a poor position to be able to have an acute understanding of its asset surface, and correspondingly the associated risks and threats.

4.1.2 PROTECT

The PROTECT function directly relates to the preventive measures in place to safeguard organizational systems and data. Network segmentation has been established broadly and a basic trust model has been applied on the assets and information. The organization has implemented a three-tier network segmentation approach to separate management, user and backup traffic with an established model to managed privileged access to systems. This establishes the foundational basis for the security-by-design of systems, present and new.

The organization has also established measures to protect data residing outside of the organization network as the business gets digitalized. A roadmap has been defined to implement protective controls for data on agents' personal computing devices with solutions such as Mobile Device Management (MDM) solution and Cloud Access Security Broker (CASB) solution. In addition, plans are in place to integrate security practices into agile software development processes for new digital offerings.

4.1.3 DETECT

The DETECT function directly relates to the awareness and visibility of internal and external threats to the organization. The underinvestment places the organization in a poor position to recover from cybersecurity incidents due to the poor awareness, agility and capability to respond and restore business operations. The organization will be exposed to higher risks in its pursuit to leverage Cloud technologies, embrace Data Sciences and proliferate digital services, which will further increase its attack surface.

The organization has embarked on establishing its own threat hunting capability and is currently implementing the Endpoint Detection and Response (EDR) platform, Carbon Black, to enable internal visibility of the technology environment.

4.1.4 RESPOND

The RESPOND function directly relates to the agility and ability of to organization to respond to cyber threats. There is an established approach to containing incidents upon detection. Communication pathways and SLAs are also defined to ensure stakeholders are furnished with the latest information to make informed decisions. Agreements with incident response partners are also defined to ensure a contingent workforce for activation when additional expertise or resources are required.

4.1.5 RECOVER

The RECOVER function directly relates to the agility and ability of the organization to recover from cyber threats to the organization. The organization had adopted recovery strategies in line with its risk appetite. These include forming forums to derive lessons learned and workflows for public engagements to protect organizational reputation and branding.

4.2. Key Findings

In summary, this study founded that the organization has sped up building cyber capabilities in the past few years. However, there remain areas of inadequacy considering the growing threats. They relate to foundational areas like legacy systems, cyber governance, and the ability to have constant visibility of assets. These areas reflect a broader concern for the organization – building a cogent cybersecurity strategy based on the key risks and threats identified proactively rather than adopting a reactive approach based on compliance (or regulatory) changes. Critically, this shift in focus will allow for the organization to build up operational effectiveness in cybersecurity defense. Some of the key themes of concern are as follows:

4.2.1 Legacy Systems and its Implications

The organization has 2 core systems, with some hosting as many as 5000 customer insurance policies, that have aged over time. In addition, there were several endpoints still using Windows 7. Collectively this creates substantive cybersecurity risks which range from the ability to deploy patches quickly and even stability issues as the IT system becomes cumbersome to manage. While a review of these legacy systems had been conducted before, in the light of growing cybersecurity risks and business-as-usual challenges, a more concerted effort to migrate and refresh the systems is necessary. The refresh of core systems opens the opportunity for security controls to be built-in. This will be contrary to the current practice where the fear of tampering with the legacy core systems has directed most of the security deployment on the perimeter.

4.2.2 Concept of Defense and Detection Strategy

The organization monitors its perimeter through the security operations center at its parent organization. Cyber threats in the past few years have progressed such that the most appropriate defense strategies require multiple layers of security. This begins by first identifying the key assets in the enterprise. Subsequently, the data flows across the technology estate and finally, ensuring these assets are defended by multiple layers to frustrate the attacker. As such, the organization needs to enhance its asset inventory capabilities, particularly to have an updated inventory of all assets and to monitor traffic at multiple layers. Beyond buying the best-in-class products, much value can be obtained by first reviewing the security architecture in the organization.

4.2.3 Structure and Resourcing

A key issue for the organization is the need for a dedicated Information Security Department situated in the Risk function to begin to coordinate across the organization and bring focus on cybersecurity. In the absence of which, there is a lack of knowledge and strategic vision for cybersecurity in the organization. This also means, no one person is fully responsible for the cyber risk in the organization. This results in some gaps, for example, developing and testing the organization with cyber drills, and adequately laying out the people and budgetary resources required.

Considering the themes of concern, the recommendations around the key controls of NIST and working out a proposed timeline to achieve these initiatives have been curated. The estimation of this will take between 12 and 18 months for the complete implementation of these initiatives.

4.3. Strategic Recommendation

The strategic recommendations are as follows:

4.3.1 Restructure and Resource the Cybersecurity Function in the Organization

The organization needs to establish a separate Information Security function that will be focused on the operations of cybersecurity, including monitoring and patch management. It will develop a wider strategy, interface with the regulator and ensure the cybersecurity capabilities in the organization are implemented for effectiveness. The reinforcement of the testing function under the Information Security Department amongst other new capabilities that need to be built or improved. Recommend strengthening the current people capabilities either through training, hiring or working with suitable partners who are able to provide these capabilities as required.

4.3.2 Strengthening Defenses and Development of New Strategy of Cyber Defense

The organization needs to develop a cybersecurity strategy against the growing cyber threats and risks. This requires the ability to do defense-in-depth, monitoring various layers within the perimeter of the enterprise. Monitoring and controls should also include the ability to manage identity access (where efforts are currently underway) - network access controls and privileged access management – especially in the light of the large number of agents operating with a Bring Your Own Device (BYOD) policy.

4.3.3 Build Awareness Across the Organization.

The organization needs to ensure proliferation of cybersecurity awareness across the organization as it increasingly innovates and integrates new technologies (e.g. cloud computing) and embrace new ways of working (e.g. agile development). All stakeholders (i.e. board, leaders, management and employees) need to gain an appreciation of the associated cyber threats and risks. For instance, instilling greater cyber risk ownership for business and changing perspectives that cybersecurity is an enabler will draw business closer towards understanding cyber risks and their roles in managing these risks. This will encourage tighter integration of a risk culture across the Group where cyber risks are managed early instead of as an afterthought – allowing the organization to manage the associated cyber costs sustainably.

5. Discussions

Based on the strategic recommendations above, we have organized our recommendations according to the priorities to the company.

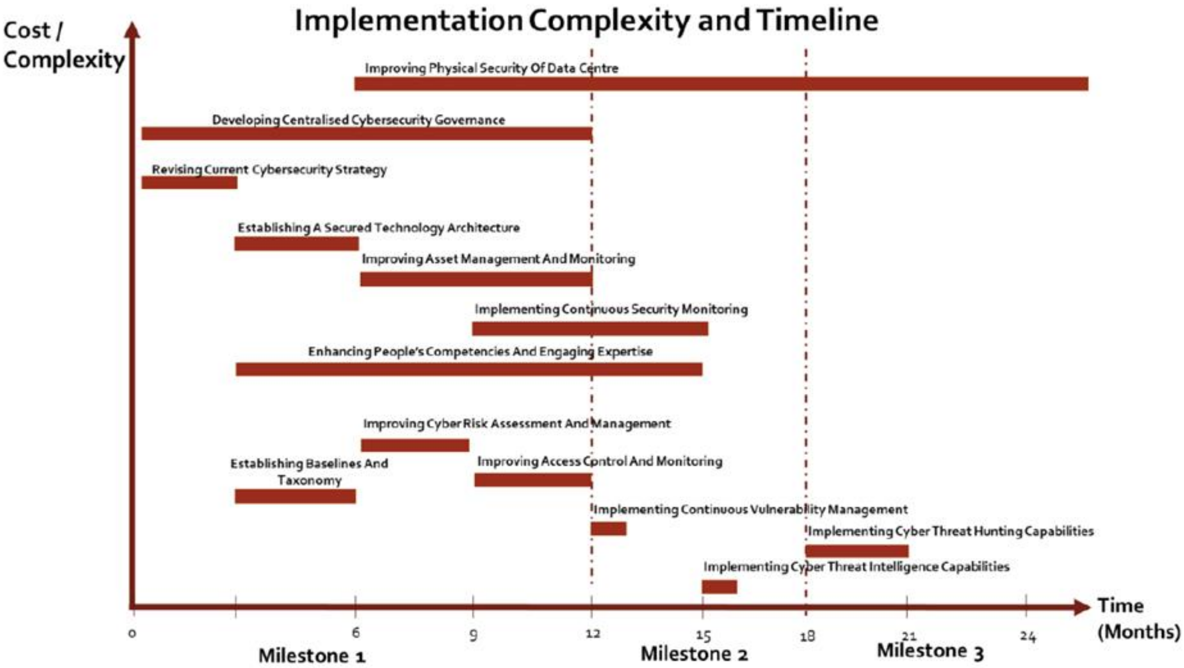


Fig.5: Initiatives Roadmap

The key recommendations are summarized into the following:

5.1 Developing Centralized Cybersecurity Governance

Cybersecurity governance in the company is held in the form of loosely coupled policies and procedures, supported by broadly defined roles and responsibilities. This results in insufficiently informed cybersecurity decision making where efforts are not optimized, and resources are not allocated appropriately. For consistent application of cybersecurity principles to the subsequent initiatives and beyond, overarching direction and guidance should be defined and provided with controls across people, process, and technology.

A restructured cybersecurity structure is required to consolidate focus. This includes creation of new teams (i.e. the CISO and TISO teams) to unite existing cyber capabilities, support new capabilities, defining clear segregation of duties (a.k.a. maker-checker roles) as well as establishing and enforcing standardized cybersecurity policies and procedures.

This initiative should be performed in parallel with 5.2 Revising Current Cybersecurity Strategy for greater synergy where governance can influence cybersecurity strategy and vice versa.

5.2 Revising Current Cybersecurity Strategy

The company must establish a strategy that move beyond compliance to regulatory standards and technology-driven. As the company embrace new ways of working and innovative use of new technologies, greater alignment to changing business needs is required for cybersecurity. Nuances needs to be identified, analyzed, and addressed to ensure cybersecurity technologies are not a "one-size-fit-all" and that business environment context is considered before cyber investments are performed.

A Chief Information Security Office will be responsible to define and execute the cybersecurity strategy for the company, ensure that the strategy align with business and IT strategic goals, provide cybersecurity guidance to the management to move beyond a compliance-driven security posture

This initiative should be performed in parallel with 5.1 Developing Centralized Cybersecurity Governance for greater synergy where strategy can influence cybersecurity governance and vice versa.

5.3 Establishing a Secured Technology Architecture

Company's architectural board would need to view and assess systems beyond individual system as an aggregated overview, incorporating cybersecurity at the architectural level rather than at the security domain level. Potentially, systems are subscribed or integrated only to a subset of the available security controls that can bring a stronger cybersecurity outcome. A cybersecurity architecture blueprint which identifies and lays out the integration of technology solutions to people and processes to optimize and derive value from the investments should be defined to guide purchase of solutions and system architectural considerations. This would allow company to establish technology, information, control and detection surfaces that would optimize efforts to ensure systems and data are onboard to and offboarded from company's environment securely.

This initiative should be performed after 5.2 Revising Current Cybersecurity Strategy has been completed. This will provide guidance for existing and future cybersecurity technologies to be integrated to ensure a comprehensive view of systems and data from an architectural perspective.

5.4 Enhancing People's Competencies and Engaging Expertise

The company has a cadre of employees who naturally lead and direct the organization through cybersecurity decisions based on their experiences and professional judgement, and this has become the natural mode of operation. Due to this nature, the company has "key man risks" where the knowledge and decisions are concentrated on a select few and the absence of these employees lead to disorderly management of cybersecurity incidents due to the lack of guidance.

This initiative should be performed after 5.1 Developing Centralized Cybersecurity Governance and 5.2 Revising Current Cybersecurity Strategy to ensure that the right number of headcounts to augment existing or build new capabilities is provisioned for in line with the right roles and responsibilities of the defined cybersecurity organization structure.

5.5 Establishing Baselines and Taxonomy

Improving company's ownership over cybersecurity baselines puts it in a proactive position when multiple rounds of deliberation and forums before amendments can be made, are minimized to manage reported cyber threats. Likewise, efficacy of company's cybersecurity processes could be improved when common expectations and understandings are aligned across functional teams. For instance, definition of cyber incidents by service desk team vs incident management team.

The company currently does not baseline and profile user, system, and data activities within the network to establish the level of normalcy for anomalies detection. In addition, there is also no common taxonomy of cyber threats to establish a common understanding between incident responders, service desk teams and management.

This initiative should be performed after 5.1 Developing Centralized Cybersecurity Governance and 5.2 Revising Current Cybersecurity Strategy to ensure the baselines and taxonomy are defined in line with the right cybersecurity governance principles.

5.6 Improving Asset Management and Monitoring

Company's inventory of information and technology is maintained by the organization units independently and there are separate sets of inventories across the group. This prevents a centralized view of all the assets which exist. Furthermore, there is an absent view of the data assets across the group, i.e. the types of data and the data attributes which exist within the group. This results in the inability for assets to be baselined, correlated, and analyzed for potential threats and risks.

This initiative would require close partnership with the IT to incorporate cybersecurity considerations into IT operational practices and should be performed after 5.5 Establishing Baselines and Taxonomy.

5.7 Improving Cyber Risk Assessment and Management

Company's risk management process is currently performed in disjointed parts, preventing a centralized and complete view of the risks across its group entities and the different lines of business. Furthermore, the cybersecurity risks are aggregated into IT risks and therefore reporting is diluted.

This initiative should be performed after 5.5 Establishing Baselines and Taxonomy to ensured that the cyber risk assessment and management methodology and approach is improved based on common understanding.

5.8 Implementing Continuous Security Monitoring

Company's current security monitoring capability can be improved to ensure it is continuous. For instance, the monitoring of internal network is limited to office hours only. While the perimeter of the network is covered by security, visibility is restricted to the scope of devices monitored and does not mitigate the risk of unmonitored malicious activities within the internal network. This is compounded by the fact that not all systems and security appliances' logs and audit trails are onboarded to the SIEMs.

This initiative should be performed after 5.5 Establishing Baselines and Taxonomy and 6. Improving Asset Management and Monitoring to ensure that the baselines for monitoring are established and refined for all assets including legacy systems.

5.9 Improving Access Control and Monitoring

Company's current approach to privileged access management (PAM) compromises a mix of automated solution coupled with manual processes. However, these manual processes such as password registration, provisioning, reset and deprovisioning are manually performed by the ID Management team, resulting in risks of exploitation due to the lack of the end-to-end assurance in the integrity of these processes.

This initiative should be performed after 5.5 Establishing Baselines and Taxonomy and 5.6 Improving Asset Management and Monitoring to ensure that the baselines for access control and management are established and refined for all assets including legacy systems.

5.10 Implementing Continuous Vulnerability Management

The company has established an operational process that allows organization to have visibility into the vulnerabilities facing the organisation. However, there is a potential risk that company assets that are not aligned with their group assets (in order to receive patch advisories from CSOC) and subjected to less regular security assessments (e.g. baseline, important systems), would be overlooked in terms of patch identification and remediation.

This initiative should be performed after 5.5 Establishing Baselines and Taxonomy and 5.6 Improving Asset Management and Monitoring to ensure that the baselines for vulnerability management are established and refined for all assets including legacy systems. Likewise, all known assets should be inventoried and registered for vulnerability scanning.

5.11 Implementing Cyber Threat Intelligence Capabilities

Company's current cyber threat intelligence is heavily reliant on Group's Cyber Security Operations Centre (CSOC). As the rate of the company's digital pursuit increases, the organisation's attack surface will grow increasingly complex in terms of cyber threats and risks faced. As the current threat intelligence provided by the group's CSOC is not contextualised to company's operating landscape, there is a gap in knowledge of active threats and their associated effects to allow company to prescribe effective cyber defence measures.

This initiative should be performed after 5.4 Enhancing People's Competencies and Engaging Expertise to ensure that the right headcount with the skillset is in place to perform intelligence analysis and sense-making to identify cyber-threats against company.

5.12 Implementing Cyber Threat Hunting Capabilities

The company currently do not have any organic cyber threat hunting capabilities. As the rate of the company's digital pursuit increases, the attack surface for the organisation's technology environment will grow increasingly complex in terms of cyber threats and risks faced.

Since there is an ongoing initiative to implement Endpoint Detection and Response (EDR) solution, minimal effort would be required for company to establish cyber threat hunting capabilities by engaging competencies (i.e. people) as well as developing the processes governing the use of EDR solution.

This initiative should be performed after 5.10 Implementing Continuous Vulnerability Management and 5.11 Implementing Cyber Threat Intelligence Capabilities to ensure that the threat hunters have the enough information and context to perform their work.

5.13 Improving Physical Security of Data Centre

The current set-up of data centre for company's backend infrastructure leaves it exposed to physical threats. Ranging from car bombs, intruder infiltrations and opportunities for mischief by insiders.

While cyber defences are important, the physical defence around organisational assets where business is hosted on are as equally if not more important given the right circumstances. The company should move towards establishing a secure data centre by ensuring physical access control is strictly regulated through the principle of defence and deterrence.

This initiative has no dependency on other initiatives. However, given the complexity, it should be initiated in Milestone 1 and may leverage on the completion of 3. Establishing A Secure Technology Architecture to influence the physical security considerations.

6. Conclusion

The cybersecurity maturity recommendations are based on the information gathered in the Study and analyzed against the NIST Cybersecurity Framework. The observations have been aligned to the NIST Cybersecurity Framework version 1.1 and the recommendations are relevant to the cybersecurity posture of the organization.

After the work that was carried out between January 2023 and April 2023. The work takes into consideration of the People, Process and Technology aspects of PT XYZ's cybersecurity operations against the five (5) functions (i.e. IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER) of the NIST Cybersecurity Framework version 1.1. The overall functional maturity score of the company is 2.1. Some of the key themes of concern are as follows:

a. Legacy Systems and its Implications. The presence of aging legacy systems in organization poses significant cybersecurity risks, including the difficulty of deploying patches and the system becoming cumbersome to manage. Migrating and refreshing these systems is crucial to mitigate these risks and create an opportunity for built-in security controls.
b. Concept of Defense and Detection Strategy. PT XYZ needs to adopt a multi-layered defense and detection strategy to address evolving cyber threats. This involves identifying key assets, monitoring data flows, and implementing multiple layers of defense to frustrate attackers. Enhancing asset inventory capabilities and reviewing the security architecture are essential steps in improving the security posture.
c. Structure and Resourcing. PT XYZ lacks a dedicated Chief Information Security Officer (CISO) in the Risk function, leading to a lack of knowledge, strategic vision, and accountability for cybersecurity. Establishing a CISO position would help coordinate cybersecurity efforts across the organization, address gaps in areas like cyber drills, and allocate necessary resources effectively.

The targeted score is 2.68. Hence, there are multiple recommendations for mitigating this gap.

a. Restructure and Resource the Cybersecurity Function in the organization.
b. Strengthening Defenses and Development of New Strategy of Cyber Defense.
c. Build Awareness Across the Organization.

Based on the study conducted, it can be concluded that the utilization of NIST CSF version 1.1 has the potential to generate a maturity figure. This figure, when presented to the management level, can enhance visibility into the organization's security posture. Moreover, it can serve as a valuable tool in assisting the company in developing a comprehensive security roadmap. By leveraging the insights gained from the maturity figure, the company can effectively identify areas of improvement and prioritize security initiatives accordingly. Overall, the implementation of NIST CSF version 1.1 offers a valuable framework for establishing a robust and strategic approach to cybersecurity.

In order to enhance the depth of research, it is advisable to conduct a maturity study by utilizing alternative information security frameworks or by combining multiple frameworks. This approach would enable a more accurate and comprehensive assessment of the nonbank financial sectors, as well as other sectors. By considering a wider range of frameworks, researchers can gather a broader set of data points and insights, leading to a more robust evaluation of maturity levels. This inclusive approach would facilitate a more comprehensive understanding of the information security landscape in various industries, ultimately aiding in the development of effective strategies and safeguards.

References

Dzolbelova, V.B., Ilaeva, Z.M., (2020), Information Security Issues in the Age of Digital Economics, First International Volga Region Conference on Economics, Humanities and Sports (FICEHS 19), vol. 114

Gatzert, N., Schubert, M., (2022), Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value, Journal of Risk and Insurance

Romanosky, S., (2016), Examining the costs and causes of cyber incidents, Journal of Cybersecurity, 2-2

Sulistyowati, D., Handayani, F., and Suryanto, Y., (2020), Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS, INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION, 4-4

Rivas G., et all. 2020, “A NIS Directive compliant Cybersecurity Maturity Assessment Framework”, IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)

Putra Adyan P.G. et all, 2020, “Maturity Assessment of Cyber Security in The Workforce Management Domain: A Case Study in Bank Indonesia”, International Conference on Information Technology Systems and Innovation (ICITSI)

Overview Of The Nist Cybersecurity Framework, May 2018, available: (https://1path2020b.websitetotalcare.com/blog/overviewof-the-nist-cybersecurity-framework)

Marotta, A., & McShane, M. (2018). Integrating a proactive technique into a holistic cyber risk management approach. Risk Management and Insurance Review, 21(3), 435 ‑ 452.

McShane, M., & Nguyen, T. (2020). Time ‑ varying effects of cyberattacks on firm value. Geneva Papers on Risk and Insurance—Issues and Practice, 45, 580 ‑ 615.

National Initiative for Cybersecurity Careers and Studies (NICCS). (2018). A glossary of common cybersecurity terminology. Retrieved September 30, 2019, from https://niccs.us-cert.gov/about-niccs/glossary

Pooser, D. M., Browne, M. J., & Arkhangelska, O. (2018). Growth in the perception of cyber risk: Evidence from U.S. P&C insurers. Geneva Papers on Risk and Insurance—Issues and Practice, 43(2), 208 – 223.

L. F. Maimó, A. H. Celdrán, Á. P. Gómez, F. G. Clemente, J. Weimer, and I. Lee, ``Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments," Sensors, vol. 19, no. 5, p. 1114, Mar. 2019, doi: 10.3390/s19051114.

Straitstimes News Article. Accessed: Jan. 25, 2022. [Online]. Available: https://www.straitstimes.com/asia/east-asia/hong-kongs-healthdepartment-computers-hit-by-ransomware-planted-by-hackers

R. D. Stachel and M. DeLaHaye, ``Security breaches in healthcare data: An application of the actor-network theory," Issues Inf. Syst., vol. 16, no. 2, pp. 1_10, 2015, doi: 10.48009/2_iis_2015_185-194.