A Cybersecurity Framework Designed for Monash Green-Field Research Management Team

FIT5129 Assignment 2 Tutorial 4 Team 2

Zhuobin Feng, Zhengyang Gu, Yusong Han, Xiao Wang, Xiaohui Ding

Executive Summary

The purpose of this report is to provide a network security framework and procedures for a special greenfield project established by Monash University Division 5057.The school used the NIST cybersecurity model to develop the program's security policy and compliance procedures. In this report, we develop a NIST-driven project management framework and guidelines for research project managers. All research software projects adopt an agile Scrum approach and adopt a DevOps perspective in their software development lifecycle efforts.

The focus of our work is to protect Monash research data from cyber-attacks, as the Australian University Research Database is part of Australia's critical infrastructure and contains very important data. The threat to research databases is twofold. On the one hand, the law is less well matched. This paper presents some suggestions for deploying a network security framework based on NIST at the technical level to defend Monash University's data. On the other hand, for cyber threats, Monash can adopt the method of background control permissions. At the same time, enhance the network security awareness of each employee. In addition, this paper uses DevOps framework and security software development framework to introduce security standards into the software programming process to ensure the security of software.

This paper analyzes and states the problem, identifies and analyzes why it is important for Monash to protect its research data from cyber-attacks, provides an objective and clear statement of the current problem Monash faces and immediate solutions to start the operation, and proposes assumptions based on the NIST cyber security framework. The problems are mainly for the technical part of the research data and equipment. This paper mainly analyzes six kinds of problems, which are respectively DDoS attack, social engineering, brute force cracking, SQL injection, malicious code to damage the computer system and human threats.

At the end of the paper, solutions to the above problems are put forward to achieve the purpose of data protection, and other relevant opinions are put forward. As for the solution, this paper deals with each small part in a classified and detailed way. First, we divide the main body into five parts based on project management. Stakeholder Management, Scope Management, Communication Management, Project Team Resource Management and Procurement

Management. Then, specific solutions are provided for each part according to its different functions, which are identification, protection, detection, response and recovery respectively.

1. Introduction

The purpose of this paper is to protect Monash University's research database on cyber security issues. Today, the network has gone deep into our lives, followed by, we are also faced with new problems, that is, the network security problem, and for the network security problem, the possibility of database attack is very high, so in many projects, protect the data security of the database is very important. Monash's research database stores many university research data, so it is very important to ensure the security of Monash's research data database for related projects.

Database security refers to the protection of database system, database server and data in the database, application, storage, and related network connection for the purpose of preventing the database system and its data from leaking, tampering or destruction of security technology. Database is often the most core data protection object of the organization, different from the traditional network security protection system, database security technology pays more attention to security from the customer's internal point of view. The purpose of this paper is to protect the security of Monash research database. The connotation of this paper includes the protection of Confidentiality, Integrity and Availability, namely the so-called CIA (Confidentiality, Integrity, Availability). Among them confidentiality means that unauthorized users are not allowed to access information; Integrity means that only authorized users are allowed to modify the data; Availability means that authorized users should not be denied access to data.

2. Problem Description

2.1 Problem Analysis

Research data exposed in the cyberattack given to the various advanced cyberattack methods, and it is obvious that the data exists in almost every aspect in this information time. The important network infrastructures in Monash university are exposed to the threat from the hackers and even managers. In this case, the security of data is very important, and personal information should be safe in case of identity theft to impact people‘s property. Additionally, hackers can steal or sabotage the data to cause great losses to Monash university. Some standards should be introduced in this case to guarantee the safety of our critical infrastructures.

One of the issues that have to be included is that the critical infrastructures should maintain safety. According to the Security Legislation Amendment Critical Infrastructure Bill 2020 brought up by Barbaschow(2021), there are some physical infrastructures related to IT, communication systems, and supplying networks that should be maintained meticulously. If these devices expired, broken, debased, the normal social operation will get impacted. Even more, the sovereignty and national security of Australia would get paralyzed. There are some mandates in terms of legislation of the critical infrastructure, the scope of laws related to cybersecurity should be dilated. “The federal government on Monday published an exposure draft on the Security Legislation Amendment (Critical Infrastructure) Bill 2020. The amendments in the Bill are aimed at enhancing the obligations in the Act, and expanding its coverage to the communications, financial services, and markets, data storage and processing, defense industry, higher education, and research, energy, food, and grocery.”(Barbaschow, 2021)

The law could mandate the universities take the implementation of critical infrastructures. Additionally, research data also regarded as a critical infrastructure in the Monash University besides some physical devices are relevant to cybersecurity. Hence, Monash university should settle down the strategies to integrate the protection of data research and devices in the law-making aspects.

The DDoS attacks and software viruses impact the great concern of international society which costs insurmountable losses. Wilczek (2021) states that malicious software, brute-force attacks, distributed denial of service attacks have a dramatic surge during the Covid-19 period. “In May 2021, a huge, distributed denial-of-service (DDoS) attack crippled large sections of Belgium's Internet services, affecting more than 200 organizations, including government, universities, and research institutes. Even parliamentary debates and committee meetings were stalled since no one could access the online services they needed to participate. A few days later, a ransomware attack shut down the main pipeline carrying gasoline and diesel fuel to the US East Coast. The Colonial Pipeline is America's largest refined-products pipeline. ”(Wilczek, 2021)

There was a case that happened at Stanford University which contains social engineering and SQL injections attacks, according to the research of Catania(2021),students register account from Link.com to socialize, and this site could not prevent the SQL injection attacking and student information get leaked. After that, the hackers get Stanford’s students email address and fake Stanford official email to send students malicious link and survey. And brute-force attacks and social engineering attacks have already become the major reason for the data breaches, one of the most distinguishing issues is that the zoom activity is easy to break. The zoom could permit any user to try the password to the zoom activities that the users do not have access times limitation, an attacker could use a python code to break the password. The human threats are more generally the cases will be shown in section four. The six-attack method will be demonstrated and analysed more scrupulously in section 4.

2.2 Problem Statement

There are two major aspects of the threats in our university, Monash university lacks the standards to satisfy the demanding of Security Legislation Amendment (Critical Infrastructure) Bill 2020. The security of the standards about management will be provided. And some suggestions could be implemented to defend the data in Monash university in the technical aspects. The NIST(Nation institution of standard) could deploy into the cybersecurity framework construction. Regarding network threats, Monash could deploy a firewall to do access-list control or remote control. Meanwhile, cybersecurity should be stipulated in the workplace and every employee should get training about cybersecurity. Secure Software Development Framework could be used to guard Monash university software safety. Meanwhile, the DevOps framework could be introduced in our case, we will discuss more a lot of the DevOps framework in this article. Ur Rahman & Willia (2016) states that the software will expose a lot of vulnerabilities if the security side and operations side do not have sufficient cooperation. The security standard could import the process of software programming which could assure the software's security.

3. Assumptions

Our project follows the PMBOK standard and integrate concepts in 5 key areas into DevOps practice, including scope management, stakeholder management, communications management, procurement management and project team resource management. In accordance with user requirements, this project will apply the NIST cybersecurity framework and adopt COBIT5 framework to solve the security problems of Monash University's research data. The detailed assumptions are as follows:

PMBOK

Project Management Body of Knowledge (PMBOK) is a knowledge system for project management that is widely recognized for its practical and scientific contributions based on years of experience accumulation and practical verification (Guide, 2001). Therefore, in our project, PMBOK has played a guiding role for finding knowledge content related to project management according to our project requirements.

5 Key areas from project management concepts

In this project, we assume that the several concepts of related fields in project management are applied to guide the team to manage the project in DevOps practice. The following are definitions and brief descriptions of these concepts from PMBOK (Guide, 2001).

- **Scope Management**
  Scope management is the process of managing all the tasks and requirements of the project. It aims to define and control the content of the project.
- **Stakeholder management**
  Project stakeholder management is a process to identify individuals, organizations or groups that may affect the project, analyze their expectations, and impact on the project, and formulate a process that allows stakeholders to effectively participate in project decision-making and execution.

- **Communications management**
  Project communication management helps stakeholders to communicate effectively through plans and strategies in the project to ensure that project information can be collected and transmitted.
- **Procurement management**
  Project procurement management is the process of organizing, implementing, and controlling project procurement, including analyzing potential sellers, making procurement plans and deciding procurement approaches.
- **Project team resource management**
  Project team resource management is the guidance, distribution, and control of team resources, including defining team resources, formulating distribution plans, and implementing final release.

NIST Cybersecurity framework

In the current era of highly developed information technology, to protect the country's critical infrastructure and ensure its reliability from cyber-attacks, the National Institute of Standards and Technology (NIST) in the United States has promoted a risk-based cyber security development framework. It aims to provide a more flexible, efficient, and extensive cyber security framework to improve the security and resilience of critical infrastructure (Barrett,2018).

The purpose of applying the NIST cybersecurity framework in our project is to use a risk-based approach to manage the security risks of attacks from cyberspace. Currently, the latest version of the NIST CSF framework is composed of three basic elements, i.e., the Framework Core, the Framework Implementation Tiers, and the Framework Profiles.

- **The Framework Core** provides a series of industry standards, guiding methodology and practical operations for the protection of critical infrastructure.
- **The Framework Implementation Tiers** specifically refers to the organization's recognizing level of practice for security risks.
- **The Framework Profiles** will adjust its functions, categories, and subcategories according to the organization's business needs, risk tolerance and resources.

DevOps model

The DevOps model (Ebert, Gallardo, Hernantes, & Serrano, 2016) provides a set of principles and practices for improving communication and collaboration between development and operations teams. The required information will be communicated to the operation team with higher efficiency to help them establish an effective and reliable application construction, packaging, and deployment process.

We chose the DevOps model because DevOps model has created an automated deployment channel to help teams practice continuous deployment. Relying on the early assessment of the development lifecycle and the provider of security problem solutions, the security of information can be fully guaranteed in such a continuous deployment channel.

COBIT5 framework

Controlled Objectives for Information and Related Technology (COBIT) is based on IT governance. It is not only a guide for the IT construction process, but also an audit standard (De Haes, Van Grembergen, & Debreceny, 2013). In our project, COBIT5 will be used as a comprehensive framework for the IT governance and management part of the project and support the protection of Monash University's research data.

4. Prevailing Cybersecurity Threats in Monash's Software Research Projects

The most important part of the Monash University project is the research database, which holds very important school research data and involves some level of protection and maintenance. Prior to this, we have analysed the main security risks to Monash University's research database. There are six main threats:

- Brute force
- Malicious software
- SQL injection
- Threatened by humans
- Distributed denial of service attacks
- Social engineering.

According to the analysis steps of the entire Monash project mentioned in the NIST framework, the fourth step should be "Conduct a Risk Assessment". After that, the six main risks mentioned will be analysed and illustrated respectively, and the risk assessment and the impact and judgment of the risk on the whole project will be carried out.

Brute Force

- **Risk Description**

The protection of information security is a very critical part of network security, especially in the server of a university, which stores critical research data and information, many types of attacks may occur, including brute force and DDoS attacks (Idhom, Wahanani & Fauzi, 2020). Today, the main way to protect data and personal privacy is encryption, such as RSA and DES. But many encryption methods have become less secure as computers have developed DES. The encryption is basically based on some mathematical problems, so it can be broken by brute force. Brute force is defined as an attack by a hacker using a human or computer to repeatedly try a series of password combinations to obtain a user's password (Curtin&M.,2005). This kind of attack is relatively common and common to Monash University. The main purpose is to attack some personal accounts of the school in order to gain some security permissions. But for now, defending against such attacks is relatively simple.

- **Risk likelihood description**

For the Monash University research program, this is a DevOps-based project flow. In the process of development or operation, some personal accounts will be involved. These personal accounts and passwords can often be logged into the school Intranet to obtain a certain amount of internal data. The risk is high if this information is leaked. According to Tanvi & Anurag (2015) study, it is much easier to crack a password if the user only uses Arabic numerals as the password than if the user uses letters as the password. Many organizations try to resist brute force attacks by increasing the strength of a user's password, such as by adding numbers and letters to a registry (Gautam&Jain,2015). But even if the password is fairly complex, it's only a matter of time before a brute force attack is used to crack the password. However, considering the current level of encryption and the complexity of users' passwords, the difficulty of using brute force attacks to obtain passwords is still quite high (M. Idhom et al.2020).

- **Risk impact Description**

In the case of the Monash University research project, Monash used Okta, a user authenticated login feature, to prevent malicious attacks. This approach has effectively prevented brute force attacks because users need to obtain a mobile device's verification code to log in. This way, even if the user has stolen the password, the hacker cannot successfully log in. So even if the brute force hack is successful, it will be very difficult to gain access to Monash. Relatively considering, the impact of brute force cracking is relatively low. In 2012, an eight-digit password could be obtained in six hours through a brute force hack. With the rise of cybercriminals and advances in technology, an April 2020 Kaspersky report found a 400% increase in brute force attacks against the Remote Desktop Protocol (RDP) in March and April (Kaspersky Lab debuts security awareness training, 2016). The chart below shows the trend of brute force attacks in some country in 2020. It can be clearly seen that the frequency of brute force attacks suddenly increases after April 2020.Although the encryption method is still relatively secure, but the use of brute force hackers or quite a lot. Therefore, the network security of Monash University still needs to pay attention to this problem and take corresponding measures. There are many ways to defend against brute force attacks recently, such as Honeypot deployed on the server to resist brute force attacks is very effective (Nursetyo, Setiadi, Rachmawanto & Sari, 2019).

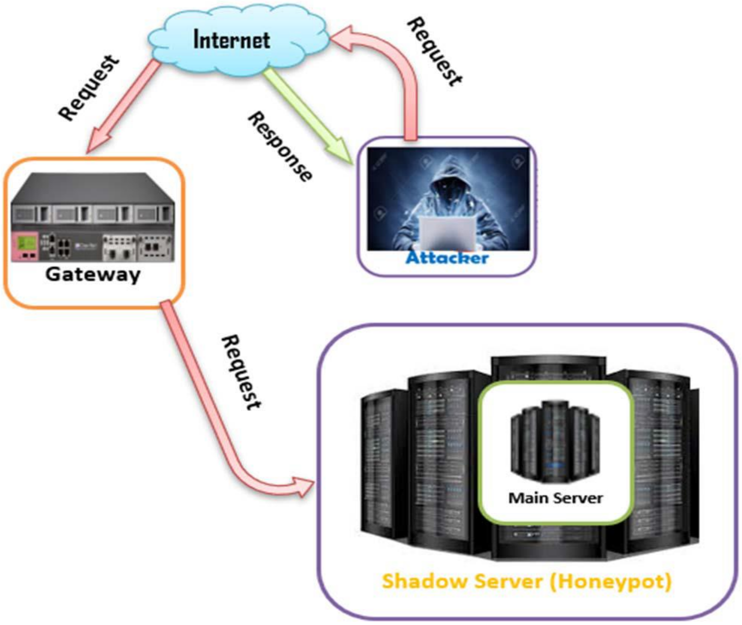


Figure 4.1 How Honeypot Works (Nursetyo, Setiadi, Rachmawanto & Sari, 2019)

Malicious software

- **Risk Description**

Malicious software refers to a series of software with malicious purposes and functions. These softwares, such as viruses, Trojans and worms, are usually installed in the system to attack or obtain confidential data and permissions in the system. Malicious software is a very serious threat in the field of network information security (Wu, Cui & Zhang,2010). From a technical point of view, Wu (2010) believes that malicious software is often attacked and cracked while the software is in progress, based on Monash University's model of DevOps.

- **Risk likelihood description**

Therefore, the university staff should encrypt and protect the software reasonably and safely during the OPS process. Since many computer and mobile phone systems are open source, it is more convenient to develop and attack malicious software (Zhernakov & Gavrilov, 2016). Malicious software attacks have become quite common in society. The chart below shows a list of bugs that have been found in some Android antivirus software. As you can see, the software basically acquires the user's permissions, but this provides an opportunity for hackers.

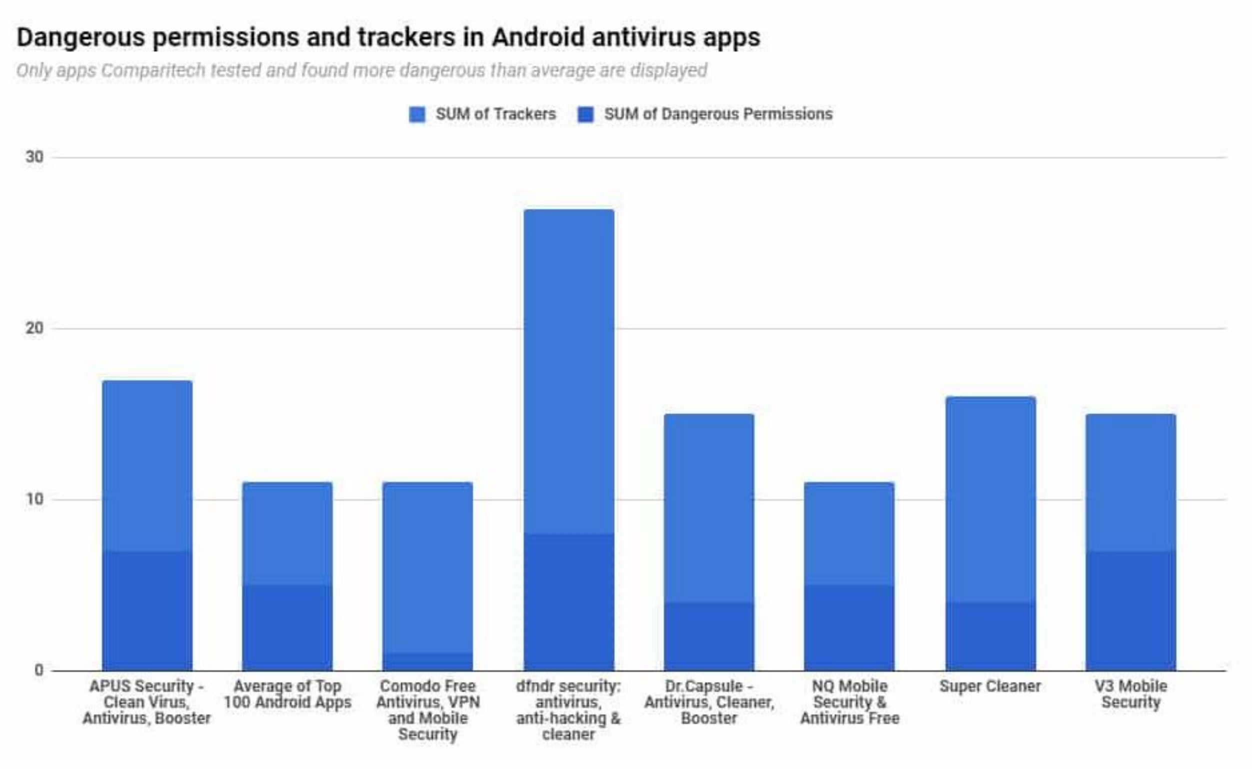


Figure 4.2 Use of Trackers in Android Anti-virus Apps (Phillips, 2019)

- **Risk impact Description**

Thus, for the Monash University research project, malicious software is very dangerous, and the probability of being attacked is very high. With the rapid development of the Internet, these malicious software become ubiquitous and good at hiding (Wu et al.2010). Monash project staff should be alert to this malicious software attack and have certain defensive measures in place. The impact of malicious software attacks on Monash University's research projects is also very dangerous. This chart shows the operation statistics of internal malicious items on the system. This figure 4.3 shows that most of the file additions and deletions (Jana&Martin,2017). If Monash University's research database and the entire university website were to be compromised by malicious software, it would be possible for hackers to exploit weaknesses in the system to gain access to research data and student and faculty account data. This is not just a matter of academic disclosure but also a matter of privacy disclosure.

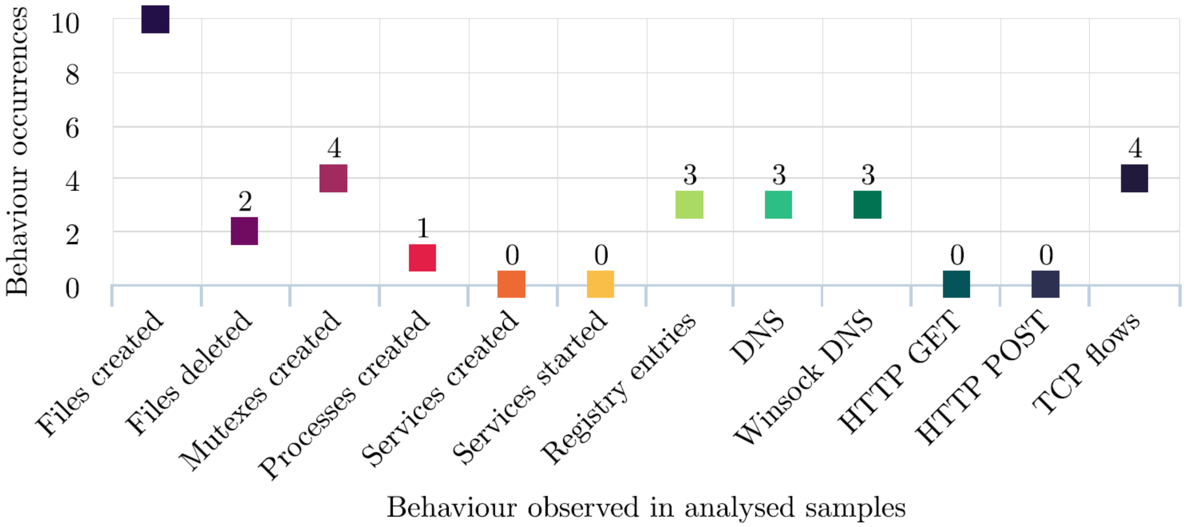


Figure 4.3 Malicious Behaviours Occurrence Diagram (Št'astná, Jana, & Tomášek, Martin. 2017)

A worm called "WannaCry" has hit 150 countries and 230,000 computers around the world. A hospital in the UK lost 92 million pounds in hospital dispatch because the worm made ambulances unable to work, causing many people to delay treatment (Kaspersky, 2021). It can be seen that malicious software is very aggressive and the harm to individual users and organizations is very high.

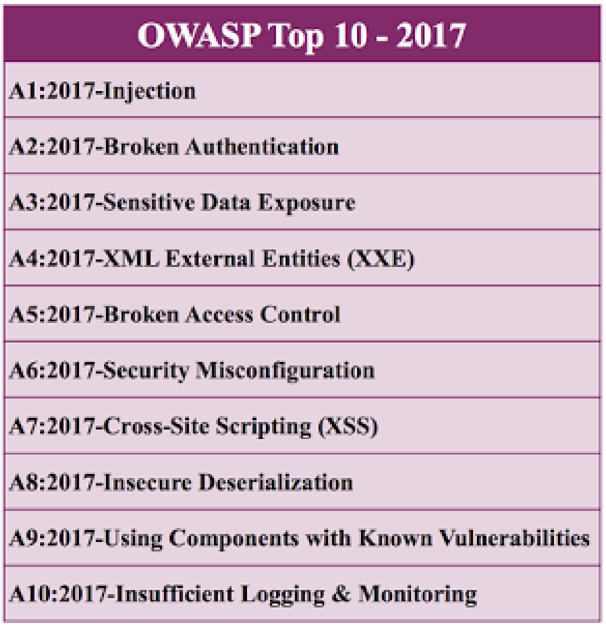
SQL injection

- **Risk Description**

With the development and popularization of the network. Demand for web services is also growing. SQL injection attacks are one of the biggest threats to Web application security today. With SQL injection attacks, an attacker can steal confidential data from web pages and software (Katole, Sherekar and Thakare,2018).

- **Risk likelihood description**

At the core of Monash University's research project is research data, which is a critical infrastructure of Australia. The protection of research data is critical to Monash University. The research data is generally stored in the server database. Monash University's database protection should be complete and secure. Although many network security companies have provided services to resist SQL Injection at present, which is still a highly threatening network attack behaviour today (Rankothge, Randeniya & Samaranayaka,2020). In 2017, the Open Web Application Security Project (OWASP), a non-profit organization, officially released the top 10 most critical Web application security risks. This is the group's first update of the top 10 security risks since 2013.As you can see, the most common attack mode in web software security is injection. To sum up, the threat of SQL injection is considerable. According to the project of Monash University, the possibility of SQL injection being attacked is still very high.



OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

Figure 4.4 OWASP Top 10 Cybersecurity Threats (OWASP, 2017)

- **Risk impact Description**

SQL injection can inject harmful code into a victim database, so that hackers can access all the information in the database or even delete the database completely, making it unusable (KARA and AYDOS,2019). Monash University's research data needs to be protected in case the database is compromised by an attack, or worse, the database is deleted. Then the Monash University data and even the website would crash. It is not just the university's data security that is affected. Even Monash's image will suffer. So, the negative impact of this attack is quite high. According to Silva & Rui (2020), ensuring the security of the database is the fundamental foundation to prevent information leakage. In the news this year, the University of California, Los Angeles, admitted that hackers had broken into a university database as early as October 2005 and that the breach was not detected until November 21, 2006.The database covers the privacy of 800,000 people (InformationWeek, 2006). The negative impact of this incident is considerable. Monash University should take appropriate measures to protect the research project database. Research data leakage caused by the consequences of the impact is very serious. It has been reported by Kim (2013) that an Indian student hacked into the database of Cornell University and he also successfully modified his own grades. The student also claims that Cornell did not design a secure system. In my opinion, this attack poses an unforeseeable risk to Cornell University if there is more to the hack than simply modifying grades. This incident is just a change of test scores. If a hacker hacked the research database of Monash and changed or deleted some data, the consequences would be very serious.

This behaviour has violated the law. And the appearance of this kind of thing will also affect the reputation of the organization.

Threatened by humans

- **Risk Description**

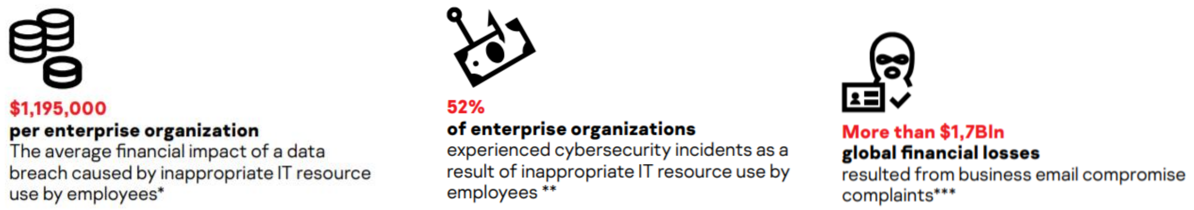
The cyber security problem of human threat is that employees have physical control over internal systems or security breach. This question relates to the responsibility and safety awareness of employees and students for system security (Stine. et al.2020). In terms of human threats, for Monash University's data security, employees' awareness and responsibility for cyber security is very important.

- **Risk likelihood description**

The Kaspersky Lab debuts security awareness training (2016) cited the theft of a Boeing employee's laptop, which resulted in the theft of information for about 382,000 employees. The occurrence of this situation also poses a great threat to network security. For Monash University. If employees are not responsible enough, this can lead to dangerous situations. And the data from Monash University are part of a critical foundation for Australia. So, its security is more important. An important part of this is the school staff's responsibility for Monash's cyber security.

- **Risk impact Description**

Recently, staff at a branch of Tesco were found guilty of discarding customers' names and credit card details. Although this event did not achieve information leakage. But this information was found at a garbage dump. If the data is obtained by a hacker or an ambitious person. Then the damage will be incalculable. Tesco could also be held liable for leaking customer information. From these cases, we can see that if university do a good job of safety awareness training, or can effectively avoid the occurrence of this situation. But once a problem has occurred, the impact of the threat on Monash is high. The seriousness of the matter can also be seen in the following statistics from the Kaspersky website. According to Kaspersky's website, more than 80% of all cyber-incidents are caused by human error, the loss suffered by the company's employees was as high as $1195,000, and the loss caused by the email leak was over $1.7billion.



$1,195,000
per enterprise organization
The average financial impact of a data breach caused by inappropriate IT resource use by employees*

52%
of enterprise organizations
experienced cybersecurity incidents as a result of inappropriate IT resource use by employees **

More than $1,7Bln
global financial losses
resulted from business email compromise complaints***

Figure 4.5 Damages Caused by Employees Mistakes (Kaspersky Lab, 2016)

Thus, it can be seen that the network security threat caused by improper management of manpower or weak security awareness is quite high. Those responsible for the research project at Monash University should pay close attention to this problem, and good staff training and management is a very important part of it.

Distribution denial of service

- **Risk Description**

The attacker will utilize the shortcomings in the transmission protocol, keeping sending a specific service request to the target and the victims cannot tackle down the normal requests of service. According to the Sumantra & Indira (2020), the devices under the DDoS attack have to deal with an insurmountable useless data packet that IP source gets fabricated, distribution denial of service attack could generate high web traffic useless data to cause network traffic congestion which could make the communication of the devices unavailable.

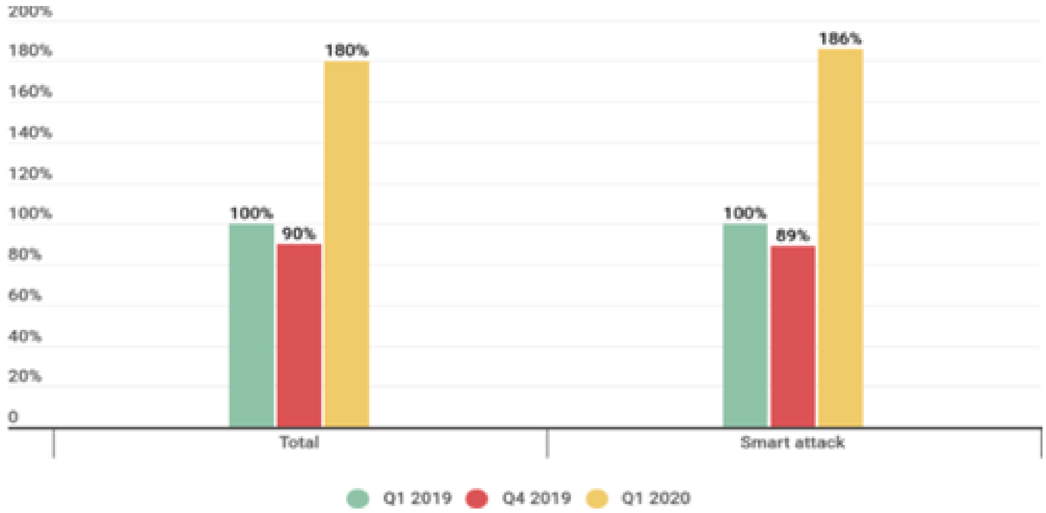


Figure 4.6 Sumantra & Indira (Kupreev et al., 2019)

- **Risk likelihood description**

Distribution Denial of service has become one of the common methods to threaten cybersecurity, there are 42% of DDoS attacks targeting video game websites, electronic commerce websites, financial websites, and government websites. And more than 70% of distributed denial of service attacks could cause the paralysis of the security system, customer service malfunction, or data disruption. The number of initializing DDoS attacks increases significantly this year. The quality and quantity of the distributed denial of attack expanded a lot compared with the number of 2019 DDoS and the increase of attacks is more than 80% of the expectation.

The small-middle size company could get a destructible loss because of distributed denial of service attacks. At the current time, the frequency of this kind of attacking ways increases more and more, the basic static defence mechanism policy could not assure cybersecurity. And given the reiterative covid-19 virus, the stability of the network is one of the more imperative priorities to assure the university operation. So, for the Monash project, the potential for risk is very high.

- **Risk impact Description**

Through analysis at the Monash university under Distribution of denial of service, the server in Monash could get impacted so that the server could not provide the service anymore. In that case, the students could not even access the site. Monash properly, there might be some services getting malfunctioned. There are some general results from DDoS attacks, the services could get disconnected, the access from students get lagged, and student users also get disconnected, even the server's manager could not log in to the service. And during the distribution of denial service attacks, the vulnerability of the network device will increase, hackers would try to get the personal information of students and teaching staff information and do some additional attack targeting the students or teaching staffs to impact their normal campus life very severely. According to the attack behaviour of DDoS, Monash University is still possible to suffer from DDoS attack, and this attack can be effectively defended by buying the equipment of network security service manufacturer. So the probability of being attacked is medium. Assuming that Monash University has suffered a DDoS attack, the result is generally an access failure. Students and staff may not be able to access the site or even access the Internet. The effect is also moderate.

Social engineer

- **Risk Description**

Social engineering is defined as the extraction of relevant safety content by contacting and dealing with relevant people. "Phishing, pretexting represents 98 and 93% of social incidents and breaches Verizon's 2018 Data Breach Incident Report states that "phishing and pretexting represent 98% of social incidents and 93% of breaches." (Crane,2021)

- **Risk likelihood description**

The social engineer has a high relevance about the breaches of the data, one of most valuable things in Monash is the intellectual property of research and academic source, social engineering can infiltrate even angles in Monash university and the technical method is getting more advanced. Every employee, students would expose the threats of social engineering at any time. In comparison with the normal cybersecurity attack, the range of social engineering is quite wide, for example, the process of social engineering could include information collection, and information or behaviour analysis, and psychology competition. The damage of the social engineering could be extremely serious, the identity theft could let the hacker access encrypted and profitable data and do whatever they want, and the scope of the social engineering led the cybersecurity to aggravate constantly.

Additionally, social engineering methods get more convenient because attackers could collect victim information from the social software. Hackers can collect data from typical software that students or educational employees generally use. Dyba, T., & Dingsoyr, T (2015) states that social network sites for socializing have potential target customers.

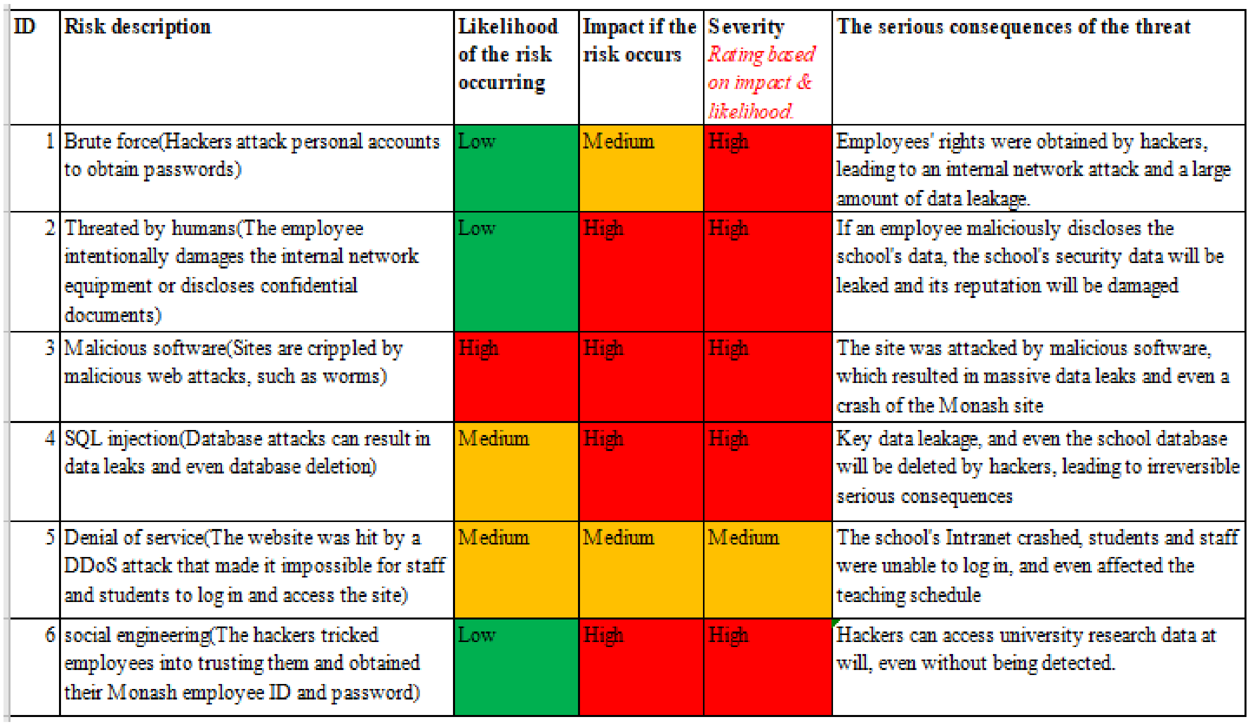
For instance, LinkedIn could help students find profession-relevant job, and Classmates.com targets setting up a campus social network. Hackers could get their information from the social software and forge the social engineering attacks according to their favourites, characters, and behaviours.

- **Risk impact Description**

When the social engineering attack towards one of the databases is accomplished, the confidential information gets leaked and the intelligence property of Monash will get violated by the hackers, hacker could edit, delete, copy the data in the Monash database if through social engineering hackers get the employees of Monash with higher authentication which provide more resource to prepare next social engineering and the damage of next social engineer could increase exponentially. Additionally, the social engineering attacks are getting simpler because of online teaching, hackers could fabricate tutor email names to send the malicious link through social engineering or make a fake login page to phish campus stuff, etc.

Risk quantification and rating conclusion

According to the above analysis and arrangement, I can get the following table of risk quantification and rating (Table4.1). Based on these six risks, I have listed the possible attacks as examples. And according to the previous analysis, we can get the possibility of the occurrence of these risks, the impact of the occurrence of risks and the severity of the risks. And described the risk after the occurrence of the possible serious consequences as an example.



ID	Risk description	Likelihood of the risk occurring	Impact if the risk occurs	Severity *Rating based on impact & likelihood*	The serious consequences of the threat
1	Brute force(Hackers attack personal accounts to obtain passwords)	Low	Medium	High	Employees' rights were obtained by hackers, leading to an internal network attack and a large amount of data leakage.
2	Threated by humans(The employee intentionally damages the internal network equipment or discloses confidential documents)	Low	High	High	If an employee maliciously discloses the school's data, the school's security data will be leaked and its reputation will be damaged
3	Malicious software(Sites are crippled by malicious web attacks, such as worms)	High	High	High	The site was attacked by malicious software, which resulted in massive data leaks and even a crash of the Monash site
4	SQL injection(Database attacks can result in data leaks and even database deletion)	Medium	High	High	Key data leakage, and even the school database will be deleted by hackers, leading to irreversible serious consequences
5	Denial of service(The website was hit by a DDoS attack that made it impossible for staff and students to log in and access the site)	Medium	Medium	Medium	The school's Intranet crashed, students and staff were unable to log in, and even affected the teaching schedule
6	social engineering(The hackers tricked employees into trusting them and obtained their Monash employee ID and password)	Low	High	High	Hackers can access university research data at will, even without being detected.

Table 4.1 Risk rating table

To sum up, brute force, human threats and social engineering are less likely to occur. Because Monash University already protects against some of these attacks, the likelihood of an attack is generally low. The possibility of Monash being attacked by SQL Injection and DDoS is relatively high, because these attacks are still very common and commonly used in the society. At the top of the list is malware, which updates very quickly and is difficult to defend against. And the impact of these risks, as we can see from the previous analysis, the impact of each attack is relatively scary. Relatively speaking, DDOS may be a network impact, relative to the database security or impact is low.

5. Solution Proposal – NIST-Aligned Cybersecurity Instructions

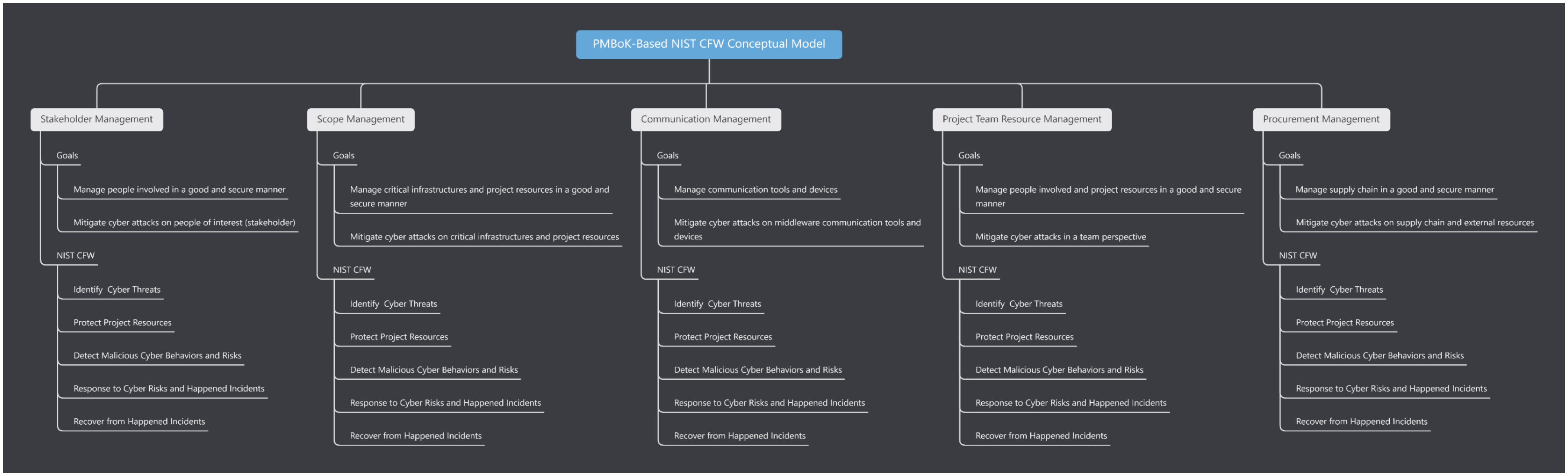
Out of concerns brought up in Section 2 and analysis about the severity of threats proposed in Section 4, we have formulated a series of procedural solutions for this Monash project. These solutions are all based on the assumptions mentioned in Section 3 which you can refer to see all the definitions and details of these assumptions. By applying our solutions to Monash project management, the project team will obtain a series of secure procedural guidelines to protect their research data which is part of university's critical infrastructure by law.

PMBoK-Based NIST Cybersecurity Framework and Guidelines for Monash Project Resources

Now we will present our detailed solution for this Monash project. The solution contains two parts which are PMBoK-based NIST cybersecurity conceptual model and the procedural guidelines.

a) Conceptual Model

The conceptual model mainly focuses on the 5 selected key areas of PMBoK that have already been defined in Section 3. Based on these key areas, the NIST cybersecurity framework is applied. The classical 5 steps of this framework are refined in order to fit the key areas better, so each of the management will have these 5 actions aiming to protect their respective fields. The goals of the NIST CFW in each of the key areas are also demonstrated in the conceptual model. Below is our diagram.


PMBoK-Based NIST CFW Conceptual Model
Stakeholder Management
Goals
Manage people involved in a good and secure manner
Mitigate cyber attacks on people of interest (stakeholder)
NIST CFW
Identify Cyber Threats
Protect Project Resources
Detect Malicious Cyber Behaviors and Risks
Response to Cyber Risks and Happened Incidents
Recover from Happened Incidents
Scope Management
Goals
Manage critical infrastructures and project resources in a good and secure manner
Mitigate cyber attacks on critical infrastructures and project resources
NIST CFW
Identify Cyber Threats
Protect Project Resources
Detect Malicious Cyber Behaviors and Risks
Response to Cyber Risks and Happened Incidents
Recover from Happened Incidents
Communication Management
Goals
Manage communication tools and devices
Mitigate cyber attacks on middleware communication tools and devices
NIST CFW
Identify Cyber Threats
Protect Project Resources
Detect Malicious Cyber Behaviors and Risks
Response to Cyber Risks and Happened Incidents
Recover from Happened Incidents
Project Team Resource Management
Goals
Manage people involved and project resources in a good and secure manner
Mitigate cyber attacks in a team perspective
NIST CFW
Identify Cyber Threats
Protect Project Resources
Detect Malicious Cyber Behaviors and Risks
Response to Cyber Risks and Happened Incidents
Recover from Happened Incidents
Procurement Management
Goals
Manage supply chain in a good and secure manner
Mitigate cyber attacks on supply chain and external resources
NIST CFW
Identify Cyber Threats
Protect Project Resources
Detect Malicious Cyber Behaviors and Risks
Response to Cyber Risks and Happened Incidents
Recover from Happened Incidents

b) Procedural Guidelines

Scope Management

<Step 1> Identify for Scope Management

- Identify project resources that need to be protected. For example, those resourced defined in NIST Identification categories: asset, environment, governance, risk assessment and its Strategies.
- Determine the methods to protect the project resources. For example, access control, awareness training, etc.
- Determine the risk detection scheme for project resources. For example, detection for anomalous events.
- Determine the response scheme for project resources. For example, analysis and defence mechanism.
- Determine the recover measures when university's critical infrastructures facing loss, modification, damage.

<Step 2> Collect Client Requirements

- Collect client requirements about resources securing.
- Collect client requirements about their trusted protection methods.
- Collect client requirements about their trusted risk detection mechanism.
- Collect client requirements about their trusted risks response mechanism.
- Collect client requirements about their trusted infrastructures recovery mechanism.

<Step 3> Define Project/Product Scope

- Identify which project assets are exposed to danger in product design phase.
- Implement protection in both functional and non-functional features of product.
- Detect the code kill-switch in product design phase.
- Design response to code kill-switch in product design phase.
- List the recovery plan for university in the situation when code kill-switch is turned on.

<Step 4> Build Work Breakdown Structures (WBS)

- Build WBS for identifying project resources that need to be protected.
- Build WBS for determining the methods to protect the project resources.
- Build WBS for determining the risk detection scheme for project resources.
- Build WBS for determining the response scheme for project resources.
- Build WBS for determining the recover measures for university critical infrastructures.

<Step 5> Test Scope

- Make Test plan for efficiently and completely identifying project resources.
- Write test scripts for testing project resources protection.
- Write test scripts for testing risk detection.
- Write test scripts for testing risk response.
- Write test scripts for testing recovery of research data from disaster.

<Step 6> Control Scope

- Manage changes to project resources.
- Manage changes to project resources protection methods.
- Manage changes to risk detection scheme.
- Manage changes to response methods.
- Manage changes to recovery mechanism.

Stakeholders Management

<Step 1> Identify for Stakeholders Management

- Identify people involved in the project and their resources.
- Identify the vulnerability brought by people's lack of awareness of cybersecurity and list the potential chances that people can be hacked by social engineering.
- Identify the detection scheme to detect potential external hacking on employees and employers. Specify how to detect social engineering.
- Identify the risk response to social engineering.
- Identify the recovery mechanism after being attacked by social engineering or other people perspective cyber attacks.

<Step 2> Recruit Stakeholders

- Recruit employees that already have some sense and awareness of cybersecurity.
- Recruit cybersecurity specialist to train the general employees and protect potential vulnerability caused by general employees.
- Recruit cybersecurity specialist to implement the detection mechanism
- Recruit cybersecurity specialist to analyze and respond to the happening cyber attacked that goals for stakeholders.
- Recruit cybersecurity specialist and assets manager that can quickly recover the critical infrastructures of university.

<Step 3> Manage Stakeholders

- Train employees and managers regularly on cybersecurity awareness and mitigation methods.
- Train employees and managers regularly on the procedure of protecting project resources.

- Train employees and managers regularly on detecting potential social engineering risks.
- Train employees and managers regularly on reporting the cyber attacks for cybersecurity specialist to respond to the attacks.
- Train employees and managers regularly on how to recover the critical infrastructures and project resources after a high impact incident already happened.

<Step 4> Monitor Stakeholders

- Monitor and record any malicious or suspicious behaviour of internal stakeholders and any vulnerability of people management.
- Monitor and record the whole protection process on preventing cyber attacks on people involved.
- Monitor and record any detected suspicious logs from internal people.
- Monitor and record responses of social engineering attacks from stakeholders.
- Monitor and record the recover operation from stakeholders each time.

Communication Management

<Step 1> Identify for Communication Management

- Identify reliable communication tools and do due diligence check for them.
- Determine protection scheme for any vulnerability exposed from communication tools.
- Determine detection scheme for detecting potential risks from communication tools.
- Determine response scheme for responding to the data leakage from communication tools.
- Determine recovery scheme for recovering from any damage of data integrity caused by communication methods.

<Step 2> Manage Communication

- Manage changes to communication tools. Do due diligence check before change to another communication tools.
- Manage changes to protection methods for communication tools. Check the effectiveness for protection methods each time when you change it.
- Manage changes to detection scheme for communication tools. Test if the detection scheme work each time when you change it.
- Manage changes to response scheme for communication tools and test effectiveness.
- Manage changes to recovery scheme for communication tools and test effectiveness.

<Step 3> Monitor Communication

- Monitor and record any malicious behaviours in communication perspective. For example, the unsafe communication about research data outside university.
- Monitor and record the protecting history.
- Monitor and record the detection for any research data leakage from communication tools.
- Monitor and record response behaviours for any data leakage or damage from communication tools.
- Monitor and record recovery of communication tools. For example, the message recovery should be stored in case another damage happens.

Project Team Resource Management

<Step 1> Identify for Project Team Resource Management

- Identify the definition of team resources, the allocation of personnel in different situations, the management plan within the team, and resource release based on roles and responsibilities of individuals.
- Identify the staffs responsible for risk protection and distribute the team resources(e.g., tools, equipment, and supplies).
- Identify the staffs responsible for risk detection and security vulnerabilities that may be caused by internal personnel's improper behavior.
- Identify staffs and resources will be deployed to response to cyber risk.
- Identify staffs and resources for executed recovery processes and procedures.
- Identify the information security roles and responsibilities of the team members, aligned with internal roles and external partners.
- Identify which team resources will be allocated to staff who is responsible to protect including maintenance, organizational assets, controlled tools, vulnerability management.
- Identify which team resources will be allocated to staff who is responsible to detect cybersecurity incidents.
- Identify which team resources and staffs will be deployed when cyber risks occur.
- Identify which team resources and staffs will be applied for recovery strategies after a cybersecurity incident.

<Step 2> Estimate Activity Resources

- Estimate the type and quantities of resources necessary to specific cyber risk.
- Team resources for protection of certain risk should be estimated.
- Team resources for detecting vulnerabilities should be estimated.
- Estimate how much the deployment of respond plan would cost.
- Estimate how much would the recovery strategies cost.

<Step 3> Estimate Recruit Resources

- Analyze and organize the requirement list of team resources for different cyber risks.
- Obtain open-source software and useful data resources from reliable third parties.
- Check the effectiveness of the tools and resources used in the vulnerability detection plan.
- Ensure that the recruited staffs involved in the response work have sufficient capabilities to deal with different cybersecurity incidents.

<Step 4> Train the Team

- Train staffs to identify security risks and get familiar with different functional tools and resources
- Provide the staffs with cybersecurity awareness education, cybersecurity- related duties and responsibilities consistent with related policies, procedures, and agreements.
- Teach staffs how to use various tools to analyze and detect possible vulnerabilities.
- Teach staffs how to deal with different cybersecurity incidents, and incorporate the lessons learned into the plan.
- Train staffs on the use of repair tools and methods of executing repair plans.

<Step 5> Manage the Team

- Allocate staffs to related department and team resources are inventoried.
- Set the content related to team discipline in the team charter and clarify the sensitive information and resources that need authenticated access.
- Monitoring for unauthorized personnel, connections, devices, and software is performed.
- Establish good connection with the detection department to ensure that cybersecurity incidents can be reported to the response department in time.
- Ask staffs to use storage devices that comply with the organization's specifications in a safe manner for data backup when necessary.

Procurement Management

<Step 1> Identify for Procurement Management

- Identify if the procured resources have lower cyber risk.
- Identify the resources are procured from a secured seller.
- Identify security vulnerabilities of procured resources.
- Identify the efficiency of procured resources in response to cybersecurity incidents.
- Identify the recovery capabilities of procured resources.

- Identify the organization’s requirements for reasonable cybersecurity resources and potential sellers.
- Identify the necessary protection level of procured software and hardware.
- Identify the necessary tools and data resources for detection.
- Identify what equipment can guarantee an efficient response to cybersecurity incidents and third-party services that can be relied on.
- Identify the secured and reliable storage devices for the recovery.

<Step 2> Do due diligence check for procurement

- Choose a trusted seller to trade, identify the potential business impacts and likelihoods.
- Make sure the procured resources comply with cybersecurity standards.
- Make sure the seller has not concealed product defects and potential vulnerabilities.
- Make sure the seller can response with necessary security risk information in time.
- Make sure the procured resources could be recovered.

<Step 3> Monitor procurement

- Confirm that the content in the contract complies with laws and standards, and analyze whether the seller’s product has cyber risks.
- Confirm that the product has passed the integrity check mechanism in the contract.
- Clarify possible security vulnerabilities in the seller’s products and the attribution of responsibilities in the contract.
- Clarify that the seller should agree with voluntarily share information about security risks and respond to the purchaser in time in the contract.
- Reach an agreement with the seller on after-sales service to guarantee the maintenance and repair of the procurement.

We also include a solution matrix in an Excel file as an attachment. You can check more details in the Excel.

6. Conclusion & Recommendation

To protect the Monash university research of database security, this paper first analyses they may face problems and description, threats to network, this paper lists the six kinds of problems, DDoS attacks, social engineering, brute force, SQL injection, malicious code damage computer systems and human threat, and the six problems are analysed in detail. In addition, the legal aspects are also elaborated to a certain extent.

In the process of the project information construction, it is necessary to ensure that the database network security problems have been solved, because the network is the foundation of the information construction. However, with the development of information technology, network security has been subjected to more and more threats, for the storage of important data database there are huge security risks, once lost, damaged or leaked will bring huge losses to the organization. Therefore, a perfect network security solution is very important for a project.

For a project, in the process of implementation, it may face many unpredictable problems. Often, the impact of a network security-related issue on a technical level can be extremely serious, as it faces two problems, external attacks and internal leaks.

Against external attacks, we can only defend against problems that we can predict and know to analyse and respond. However, some issues may be unknown and not easy to explore. These problems often lead to major problems, and the cost of finding and fixing them can be significant.

While internal leaks may be a more terrible problem, because each contact projects have a certain understanding of the project, although we in the process of project management planning and selecting talents are strictly controlled, but the reality is more complex, and the resulting a series of related issues on the technology involves network is difficult to solve.

Reference

A. Katole, S. S. Sherekar and V. M. Thakare, "Detection of SQL injection attacks by removing the parameter values of SQL query," 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 736-741, doi: 10.1109/ICISC.2018.8398896.

A.Nursetyo, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto and C. A. Sari, "Website and Network Security Techniques against Brute Force Attacks using Honeypot," 2019 Fourth International Conference on Informatics and Computing (ICIC), 2019, pp. 1-6, doi: 10.1109/ICIC47613.2019.8985686.

Barbaschow, A. (2021). *Australia's critical infrastructure definition to span communications, data storage, space | ZDNet*. ZDNet. Retrieved 13 May 2021, from https://www.zdnet.com/article/critical-infrastructure-definition-to-span-communications-data-storage-and-space/.

Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity version 1.1.

Catania, S. (2021). *Vulnerability in 'Link' website may have exposed data on Stanford students' crushes | The Stanford Daily*. The Stanford Daily. Retrieved 14 May 2021, from https://www.stanforddaily.com/2020/08/13/vulnerability-in-link-website-may-have-exposed-data-on-stanford-students-crushes/.

Crane, C. (2021). *80 Eye-Opening Cyber Security Statistics for 2019 - Hashed Out by The SSL Store™*. Hashed Out by The SSL Store™. Retrieved 2 May 2021, from https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/.

Curtin, M. (2005). Brute Force Cracking the Data Encryption Standard (1st ed. 2005. ed.).

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, *27*(1), 307-324.

Dyba, T., & Dingsoyr, T. (2015). Agile Project Management: From Self-Managing Teams to Large-Scale Development. *2015 IEEE/ACM 37Th IEEE International Conference On Software Engineering*. https://doi.org/10.1109/icse.2015.299

Ebert, C., Gallardo, G., Hernantes, J., & Serrano, N. (2016). DevOps. *Ieee Software*, *33*(3), 94 -100.

Guide, A. (2001). Project management body of knowledge (pmbok® guide). In *Project Management Institute*.

H. Rankothge, M. Randeniya and V. Samaranayaka, "Identification and Mitigation Tool for Sql Injection Attacks (SQLIA)," 2020 IEEE 15th International Conference on Industrial and Information Systems (ICIIS), 2020, pp. 591-595, doi: 10.1109/ICIIS51140.2020.9342703.

KARA and M. AYDOS, "Detection and Analysis of Attacks Against Web Services by the SQL Injection Method," 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2019, pp. 1-4, doi: 10.1109/ISMSIT.2019.8932755.

Kaspersky Lab debuts security awareness training. (2016). *Pivotal Sources*, pp. Pivotal Sources, 2016-06-01.

Kim Arora. (2013). Indian student in Cornell University hacks into ICSE, ISC database. *The times of India (Bombay, India)*, pp. The times of India (Bombay, India), 2013-06-06.

Kupreev, O., Gutnikov, A., & Badovskaya, E. (2019, November 11). *DDoS report Q3 2019*. Securelist English Global securelistcom. https://securelist.com/ddos-report-q3-2019/94958/.

M.Idhom, H. E. Wahanani and A. Fauzi, "Network Security System on Multiple Servers Against

Brute Force Attacks," 2020 6th Information Technology International Seminar (ITIS), 2020, pp. 258-262, doi: 10.1109/ITIS50118.2020.9321108.

Phillips, A. (2019, August 26). *We tested 21 Android antivirus apps and found these serious vulnerabilities*. Comparitech. https://www.comparitech.com/antivirus/android-antivirus-vulnerabilities/

Šť'astná, Jana, & Tomášek, Martin. (2017). Characterising Malicious Software with High-Level Behavioural Patterns. *SOFSEM 2017: Theory and Practice of Computer Science*, 473-484.

Sumantra, I., & Indira Gandhi, S. (2020). DDoS attack Detection and Mitigation in Software Defined Networks. *2020 International Conference On System, Computation, Automation And Networking (ICSCAN)*. https://doi.org/10.1109/icscan49426.2020.9262408

T.Gautam and A. Jain, "Analysis of brute force attack using TG — Dataset," 2015 SAI Intelligent Systems Conference (IntelliSys), 2015, pp. 984-988, doi: 10.1109/IntelliSys.2015.7361263.

UCLA Admits Massive Data Hack; UCLA is alerting approximately 800,000 people that a hacker broke into a university database as long ago as October 2005; the intrusion wasn't detected until Nov. 21, 2006. (2006). *InformationWeek (Manhasset, N.Y.)*, InformationWeek (Manhasset, N.Y.), 2006-12-12.

Ur Rahman, A., & Williams, L. (2016). Software security in DevOps. *Proceedings Of The International Workshop On Continuous Software Evolution And Delivery*. https://doi.org/10.1145/2896941.2896946

US university notifies 800,000 of database hack. (2007). Computer Fraud & Security, 2007(1), 3.

V. Zhernakov and G. N. Gavrilov, "Malicious software detection in operating system (OS) for mobile devices (the case of Android OS)," 2016 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE), 2016, pp. 163-165, doi: 10.1109/APEIE.2016.7806438.

Wilczek, M. (2021). *Critical Infrastructure Under Attack*. Dark Reading. Retrieved 14 May 2021, from https://www.darkreading.com/attacks-breaches/critical-infrastructure-under-attack-/a/d-id/1340960.

Yunlong Wu, Dong Cui and Qiang Zhang, "A malicious software evaluation system based on behavior association," 2010 International Conference on Optics, Photonics and Energy Engineering (OPEE), 2010, pp. 258-260, doi: 10.1109/OPEE.2010.5508137.