**IS5151 - Information Security Policy and Management**

Semester 2 - 2018/2019



**Assignment 2**

|  |  |
| --- | --- |
| Jagadeesh Chirumamilla | A0191509B |
| Maddi Kamal Divya | A0178511E |
| Rohaizad Bin Noordin | A0195026E |
| Xu Haodi | A0191531L |
| Li Jiachen | A0194979Y |
| Yare Feng Shui | A0194951U |

# 

**Table of Content**

[**1 Introduction**](#_oyyalnumqf6i) **3**

[**2 Company Profile**](#_dx57ud6v1c0u) **4**

[**2.1 Background**](#_wtoiiqirnq26) **4**

[**2.2 Information Security Department**](#_3ha0c3qx3k6y) **4**

[**3 Company Information Security Strategy**](#_wm0r3ovpfq5y) **6**

[**3.1 Information Security Policies**](#_fxdrsre84fil) **6**

[**3.2 Information Security Technology**](#_w80h9dkqjrc3) **7**

[**3.2.1 Web Application Firewall**](#_72amosnxuon5) **7**

[**3.2.2 Point-to-point Encryption and Tokenization**](#_taff2i8yw62w) **8**

[**3.2.3 Triple Data Encryption Standard**](#_eud4jc2mjska) **8**

[**3.2.4 Two-factor Authentication**](#_68p1s5hnq6va) **9**

[**3.2.5 VPN System**](#_68epvham9fhb) **9**

[**3.2.6 Intrusion Detection and Prevention System**](#_5jv4nq7ej0nl) **10**

[**3.2.7 Access Control**](#_tdnbvivk3a9y) **10**

[**3.3 Company Security Practice**](#_2kpyaodb8n5q) **13**

[**3.3.1 Security Education, Training, and Awareness Program**](#_3yardlyu1p9c) **13**

[**3.3.2 Business Continuity and Disaster Recovery**](#_osl118vr38t6) **14**

[**3.3.3 Incident Response**](#_f1rb6dy5n0nl) **15**

[**3.4 Inadequate Behavior within the company**](#_ijr7jndrnetu) **18**

[**3.4.1 Password Policy Violation**](#_rei79rcqbmdy) **18**

[**3.4.2 Insufficient Security Layering Between Domains**](#_cz47hg3598wb) **19**

[**4 Company Risk Profile**](#_vkdx0w3l2fp) **21**

[**4.1 Three Main Leading Information Assets**](#_35s5cim93t8) **21**

[**4.2 Information Assets Vulnerabilities**](#_r2kx7q36vygx) **21**

[**4.3 Risks Assessment Process**](#_5hfyyq3rg7ir) **24**

[**5 Conclusion**](#_o33l9hxiltn2) **27**

[**6 References**](#_2kk1297o8boj) **28**

# 

# 

# 

# 

# 

# 

# 

# 1 Introduction

In the past few decades, technology has advanced tremendously, bringing convenience to different walks of life. One of the most significant improvements brought by technology is able to transact without bringing cash. Unlike the conventional cash payment, consumer will only have to bring a card or device to transact and do not have to worry about not having sufficient cash. Also, this cashless payment not only enables consumer to track their expenses from time to time, cashless payment also allowed company to understand consumer behaviour. Besides that, over the past few years, more and more cashless payment method are surfacing in the market, ranging from mobile payment, smart gadget payment, contactless card payment and etc. With the pervasive cashless payment culture, one may wonder how does card payment companies manage and keep up their cybersecurity team to ensure higher reliability and high security services to the consumer?

This report will be segmented into three portion, namely company profile, Company Information Security Strategy and Company Risk Profile. In company profile, the background and the company information security department will be discussed. In Company information security strategy, the company policies, the technology used in the company, the best practice in the company. Besides that, the inadequate behaviours in the company will also be highlighted. In the company risk profile, Threat-Vulnerabilities-Assets (TVA) will be conducted on two most important assets, followed by a drafted ranked vulnerability risk and recommendation. Last but not least, this report will end off with a conclusion to conclude on the entire report and stating the future challenge of the company.

# 

# 2 Company Profile

## 2.1 Background

The anonymous company that this report will be studying is based in U.S. and it was founded in 1960s. The business provides financial services to multinationals and to dates, the company has expanded its business worldwide in most of the countries. The company provides payment gateway services to facilitate online funds transfers with credit cards, gift cards, and debit cards.

In recent years, it was reported that the organization has nearly 15,000 staff with huge, complicated and independent infrastructure to facilitate the services 24/7 to its consumers worldwide. The organization is also said to be secured against physical and natural disasters. Since the company are in the financial services industry, the company has implemented a series of intensive fraud-detection parameters to ensure more secure transaction.

However, till date, securing of transaction from data at rest, data processing and data storing remained to be a major challenge for the company as hacking techniques also evolved along the way. Despite that, the company has a very strong leadership who understand both technical and managerial needs of the organization. The leader also have a clear vision for the company’s need with respective to future technologies and their implementation such as blockchain and tap to pay also provides a promising future for the company.

## 2.2 Information Security Department

In order to ensure Cybersecurity is well taken care, the company has opened up Cybersecurity department, focusing on Cybersecurity. The Cybersecurity shares the same level as Information Technology in the organisation structure and reports directly to CEO. Besides that, the company has hired Cybersecurity team belonging to different region to cover different time zone. Generally, the company divides Cybersecurity into Cyber Defense, Cyber Engineering, Risk and Compliance, Incident Response, Cyber Investigations, Threat Detection, Access Management, Counter Threat Unit, Threat Intelligence and Security Architecture. Refer to Figure 1.0 for Organization Structure.

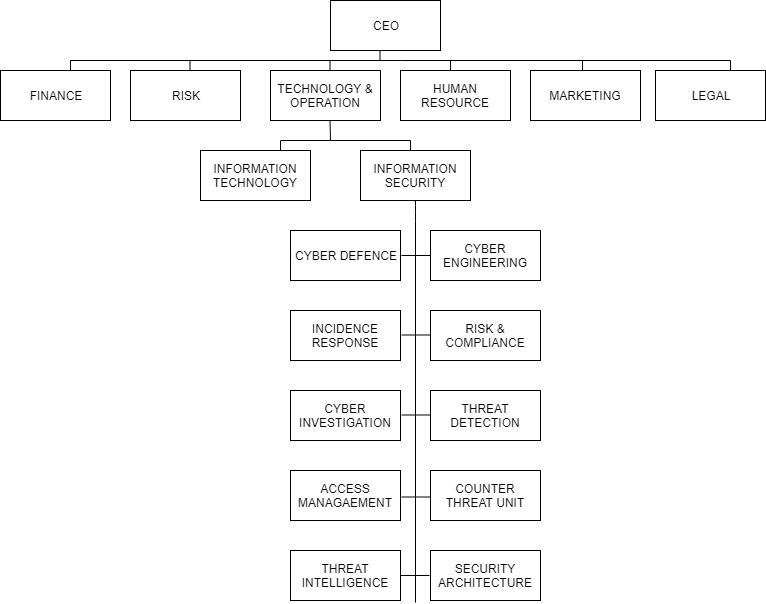


Figure 1. Organization Structure

However, given the above organisation structure, it was observed that there are some challenges in pushing through Cybersecurity initiatives or investigations within the company. Also security considerations are often absence during product design phase and several amendments might be needed during security validation before product launching, Therefore, delayed in the time-to-market.

# 

# 3 Company Information Security Strategy

## 3.1 Information Security Policies

Similar to the theory learnt in the lecture, the company has three different type of information security policies, ranging from Enterprise Information Security Program Policy (EISPP), Issue-Specific Security Policy (ISSP) and System-Specific Security Policies (SSSP), to lay out the standard and expectation for Cybersecurity. Besides that, given the profile of a multinational company, the company standardized the procedures and processes worldwide as such, publishing the details publicly within the intranet. However, as the policies get more specific, it would only be available within specific team.

Besides that, the frequency of updating for EISPP was not as high as compared to more system or issue specific security policies and EISPP was observed to be much very appropriate, comprehensive and effective. In the EISPP, it had included some of the Jargons’ with definition explained and documentation is observed to be more concise which allows reader to understand the standard and expectation of the company well.

However, on the lower level of SSSP, it had displayed an inconsistency as compared to EISPP. There were no standardization in documentation layout and there were no process or procedure owner. As a result, some of the issues faced includes outdated policy, inconsistency in documentation formatting, uncontrolled documentation updating or missing version control and etc. However, given the nature of fast changing processes and tools, it is usually very difficult to document the immediate change in processes and documents.

In order to overcome the above-mentioned issue, the company should have a documentation or process owner to be accountable for the timely updating of documents. Besides that, the owner must keep the version control of the documents and backup for the document to ensure documents are recoverable in case of data loss.

## 3.2 Information Security Technology

Apart from having information security policies, the company has also equipped various technology and tools within the company to implement the security within the company. The subsequent sections will look into the technology and tools used to safeguard the company assets.

### 3.2.1 Web Application Firewall

The studied company has employed Web Application Firewall (WAF) to implement security policies for HTTP/HTTPS. WAF provides a protection for web applications specifically by executing a series of security policies. This WAF detect HTTP requests for exceptions and reject requests that do not conform with the HTTP standards (Fernandez E B, 2004). Also, it allows only a portion of the HTTP protocol to pass, reducing the scope of the attack.

Additionally, patching web security vulnerability is difficult for web application developers as there is new vulnerability appearing or discovered everyday and the type kind of harm it will bring to the web application is usually unknown. However, with the implementation of WAFin the studied company, WAF can block the vulnerability in less than an hour after a comprehensive vulnerability scan.

The WAF of the studied company is able to determine the web browsing behaviour of the user. For instance, the entire site visiting of the user to redirected to the default login page is logged down. With the detection of the user's entire behavior, the studied company can identify attack and detect the attack. Besides that, the state management mode also allows the abnormal events detection such as login failure. This could be useful for the company to detect and response to any possible password cracking events such as password bruteforce attack when the threshold of failed password attempt within a short timespan is reached.

However, the challenge of fine-tuning the firewall rules remained to be challenge to the company, what should be blacklisted, what should be whitelisted and how could the company adjust its rules to achieve a well balance high accurate detection rate and acceptable false positive rate.

### 3.2.2 Point-to-point Encryption and Tokenization

Next, the studied company also implement a Point-to-point Encryption (P2PE) which provides protection for account number and card details during data transition for dynamic authentication. This strongly mitigates the risk for point-of-sale and cross-channel fraud. Tokenization is the subsequent steps to transform card data into a surrogate value. Please refer to Figure 2 for the transaction flow of the studied company in protecting customer data.

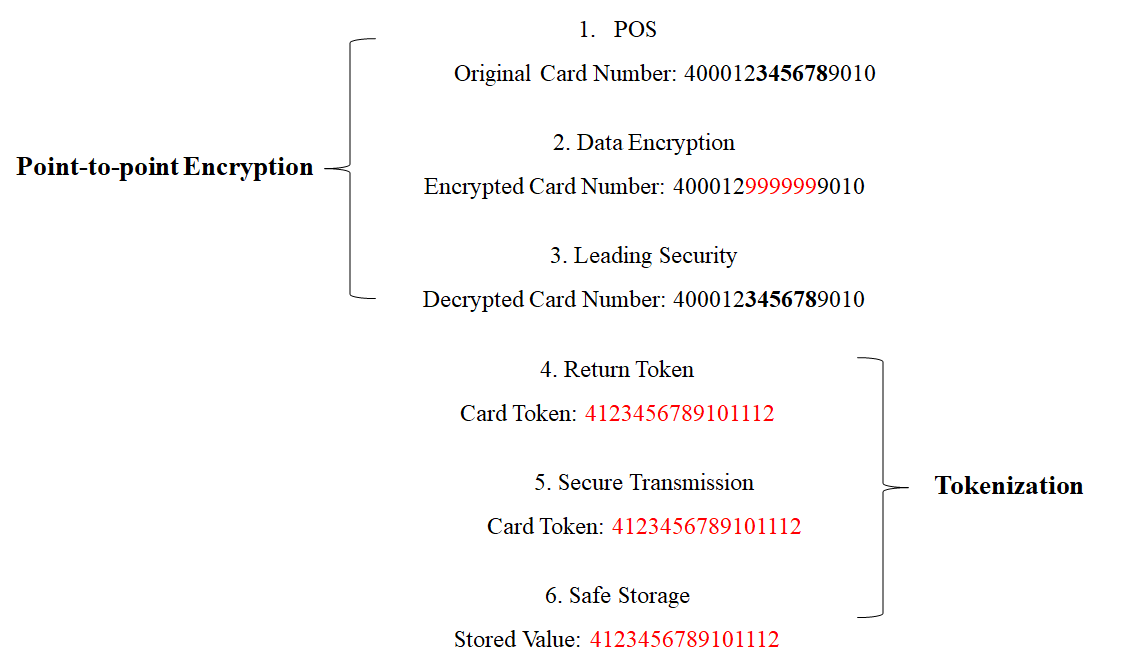


Figure 2. Point-to-point Encryption and tokenization

### 

### 3.2.3 Triple Data Encryption Standard

Besides that, triple data encryption standard (3DES) is an algorithm mode of data encryption standard (DES) encryption algorithm that uses three 64-bit keys to encrypt data three times (Singh G, 2013). DES is no longer considered a secure encryption algorithm and USES a 56-bit key that is too short to be cracked in 24 hours with modern computing power. 3DES is the encryption algorithm for the transition from DES to advanced encryption algorithm (AES), which is a more secure deformation of DES.

The investigated company use it as standards-based technology to enable point-to-point encryption and tokenization to become an industry standard for encryption.

### 3.2.4 Two-factor Authentication

In addition, two-factor authentications (2FA) is added to serve as an additional layer of security to confirm users’ claimed identities. 2FA leverage on the concept of who are you, what you know and what you have to granted access with two of the combination factors to decrease the chance of impersonation. For instance, when a user entered their username and password, they will be required to provide another kind of information of themselves instead of immediately gaining access. The second factor of authentication could be something they have (credit card, smartphone, or a small hardware token) or something they are (biometric pattern of fingerprint, an iris scan or a voice print) (Singhal M and Tapaswi S, 2012).

The investigated company has pushed two-factor in authenticated transactions in order to further confirm the consumers’ identity before authorizing access. Besides that, 2FA were employed within the company for employees’ who are accessing the critical infrastructure, system and server to prevent unauthorization access.

### 3.2.5 VPN System

On the other hand, the investigated company also uses VPN system to provides a flexible yet secure solution for data communications, whether it’s for internet privacy, remote access for employees, securing IoT or networking cloud data centers. The private network has the advantage of isolating critical IT services from the internet, it is expensive and complicated to set up in different sites, devices, and users. Thus, VPN system becomes a better option to allow private connection and grant remote access while maintaining security and reducing potential risks.

In order to avoid the occurrence of unauthorized access, the investigated company provided VPN credentials targeted to both company users and third-party and thus, greatly reduces the risk of security breaches and cyber attacks, and encourages productivity.

### 3.2.6 Intrusion Detection and Prevention System

Intrusion detection and prevention systems (IDPS) are a combination concept of an intrusion detection system (IDS) to automate detect intrusion and an intrusion prevention systems (IPS) which has all the capabilities of IDS and also attempt to stop potential incidents (Scarfone K and Mell P, 2012). There are many types of IDPS technologies including network-based traffic monitoring for network segments or devices, wireless network traffic monitoring, network behavior analysis (NBA), and host-based monitoring.

According to the overall information security management framework, traditional defense technologies are constantly integrated and optimized from the space and time dimensions, forming the network security defense technology framework of unified management of echelon deployment defense in depth. The investigated company applied this defense-in-depth approach to protect the most significant resources based on their network to identify suspicious activities, especially for POS systems. Besides, segregating the payment processing network from the other non-payment processing networks in order to perform more accurate monitoring and provide stronger detection capabilities.

### 3.2.7 Access Control

Access control list (ACL) uses packet filtering technology to read information from layer 3 and layer 4 packets of the OSI seven-layer model at the router such as source address, target address, source port, target port, etc. The packets are filtered according to the predefined rules, so as to achieve the purpose of access control. ACL is a collection of rules that are applied to an interface of a router. For a router interface, the access control list goes in two directions:

Output: packets leaving the router which has been processed by the router.

Input: packets that have reached the router interface which will be processed by the router.

The investigated company makes best practices of implementing ACLs properly to avoid flat networks and review ACLs and policies to make it difficult for an attacker to pivot and traverse. Through the network partition isolated whole domain user management and access control to achieve common security threats and data security protection.

Suggestions:

1. Establish the whole life cycle vulnerability management mechanism.

In the design stage, make it clear that the security requirements should take security measures in advance. In the development stage, establish code scanning and security testing mechanism to reduce the risk of application vulnerabilities. In the operation and maintenance stage of production, conduct pre-launch access security tests, regularly conduct vulnerability scanning and permeability tests, timely discover security risks and actively rectify them.

1. Establish a multi-dimensional three-dimensional vulnerability evaluation mechanism.

It’s a good initiative to research and develop security vulnerability risk measurement standards and the platform tools to establish security vulnerability scanning system, covering all branches independently, that conduct regular vulnerability scanning and remote penetration testing work. Possibility in consideration to employ a third party independent professional institutions on a regular basis to carry out the Internet application system security evaluations, find the problem in a timely manner and rectify them. In addition, combined with the network security and intelligence, we should track Internet vulnerability information and network security risk events currently present in the industry, issuing risk alerts to the whole jurisdiction, and dealing with them in a timely manner.

1. Establish an active security situation awareness model

Based on large data and artificial intelligence technology, the investigated company should further enhance the intelligent risk control ability, implement new technologies such as cloud platform design, development and deployment of security defense system, conduct more network security technology trainings, implementation of network security risk early warnings, real-time monitoring, correlation analysis and rapid disposal of the whole control process.

## 3.3 Company Security Practice

### 3.3.1 Security Education, Training, and Awareness Program

In the investigated company, the company has conducted annual security awareness training online. With the implementation of security awareness training online, this allowed employees to do it whenever they are free. Also, they ensure the employees is able to understand the training, the employees are required to answer series of questionnaire relating to the particular security topic.

Besides that, to ensure timely completion of the Security Awareness Training, the company also imposed a period of a month and failure to complete within the stipulated period will resulted in the user account being disabled. On top of that, the completion of security training was also part of each team annual KPI and this further motivates employees to complete the training. Apart from that, the investigated company conducts phishing email exercise periodically to ensure employees stay vigilant while reading email. This phishing email is considered to be effective as the scenario is similar to the real threat.

Issues:

Although the company was able to achieve great response, there are some underlying issues with this type of implementation. The questions given in the training are the same and employees who stayed for more than one year could save the answer of the previous year to answer the question. Besides that, there were little or no ownership in the security awareness training to maintain and adding of new relevant topic or update the questions bank.

Suggestions:

In order to overcome the above-mentioned issue, the investigated company must appoint an owner (preferably someone from threat intelligent, who research for new vulnerability threats on a daily basis) to maintain the questionnaire and training. Besides that, the company could include new content for the training. Last but not least, the studied company could send out new threats or at least a more prominent threats and the reporting hotline happening around the world to educate and reach out to the user effectively.

### 3.3.2 Business Continuity and Disaster Recovery

In the company, DR tests was implemented annually and the results are audited. In this process, the key consideration is to test business continuity in the time of the disaster which can be either natural or humane. Based on observation, all the locations with high availability are not tested. Only a few locations are tested in DR plan and all locations are referred in the DR report. And for most of the data centers, the secondary appliance is also on the same geographical location to avoid the latency and to ensure all the IT operations are still under the control of the same local IT team. We cannot ensure business continuity in the case of a natural disaster that happened in the geographical location. Also, hardware failure in the data centers can also cause disruption to the data.

Even though auditing is in place, they don’t consider the above scenarios and pass the test as success.

Suggestions:

1. Plan the high availability of primary and secondary appliance to be in different places.
2. Ensure the auditing meets all the compliance.
3. Test the DR for all the possible locations.

### 3.3.3 Incident Response

In case of any security incidents, our company has efficient incident response procedures as incidents will continue to occur as the sophisticated threats are increasing, the solution for this is to have an Incident Response Plan (IR Plan). This IR Plan helps to quickly recover from the incident and implements the planned strategy which in turn protects the company and compliance is maintained. If there is a violation against the security policy, unauthorized access to gain access to the systems, denial of service or unauthorized use of the system a security incident can be raised.

If the service providers, members or merchants have encountered with the security incident they have to abide PCI Security Standards (PCI DSS). The entities which are compromised will follow below actions:

1. We prevent further loss by thorough investigations within 24 hours of the raised issued. We request the compromised systems not to alter the systems like changing passwords by logging as ROOT and not to log on all machines.
2. Compromised machines will be isolated from the network i.e., just unplugging the cables but not turning off the machines.
3. Logs and electronic evidence will be preserved and whatever action is taken is recorded.
4. Monitoring all the account and transaction information on high alert.
5. Entities need to provide the incident response document to the merchant bank within the three business days of the initial report.
6. Forensic Investigation will be done by a Qualified Security Assessor (QSA) who will do the following actions
   1. Investigator will determine the cardholder information at risk and type of information at risk. On the entity’s network, if it is applicable, the team runs packet-sniffer.
   2. Incident validation and assessment are performed by questioning how the compromise has occurred, What is the source of compromise, reviewing the complete network to identify affected systems.
   3. Confirm whether the compromise has been contained.
   4. Reviewing the security endpoints and determining the risk.
   5. Performing vulnerable scans internally and externally.

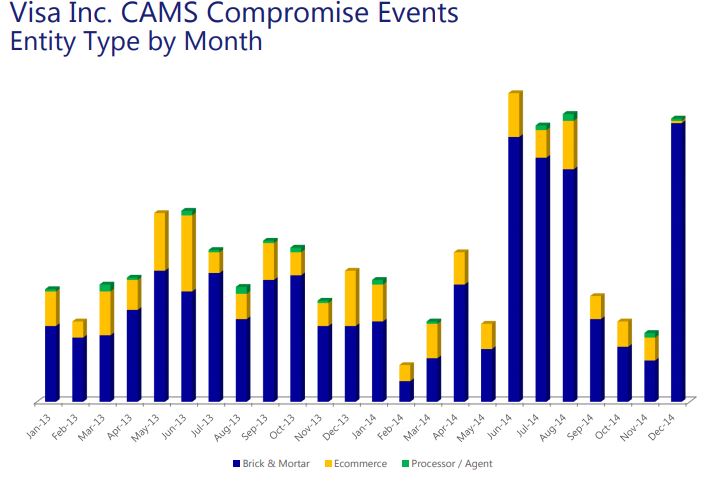


Figure 3. CAMS Compromise Events Entity Type by Month

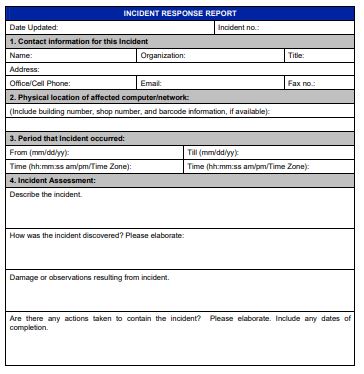


Figure 4. Incident Response Report

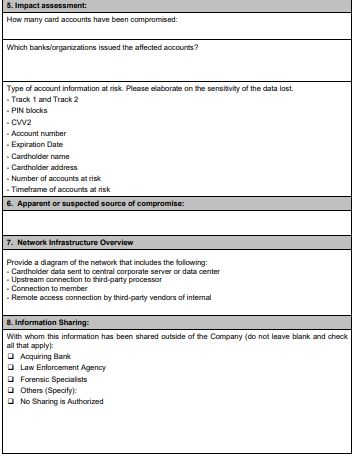


Figure 5. Incident Response Report

Suggestions:

1. Maintain separate policies for all personnel to address information security. All entities should clearly understand the incident response plan to resolve the confusions which reduce the downtime for the business, exposure of unnecessary public media and legal liabilities.
2. In day to day operations, alerts might go unnoticed or might be triggered with low priority. Need to implement monitoring in a more reliable and intelligent platform.
3. Even if the alerts are properly triggered, there are many scenarios where the employees didn’t pay attention and didn’t mitigate the impact. Qualified Professionals need to be hired without compromising on financial budget.

## 3.4 Inadequate Behavior within the company

Although there were various initiatives implemented to instill security policies, the weakest linked remained to be the internal staffs. With the trade off between efficiency and security, security is often ignored and even cybersecurity staff could be non-compliance with the policy. In the next sections, two of the non-compliance behaviours will be discussed, together with related recommendations.

### 3.4.1 Password Policy Violation

Password policy is usually in place to set the standard and characteristic of a strong password. Some of the common guideline seems are the length of the password (at least 10 characters), adding special characters (e.g. !@#$%^&\*), password must be non-English word found in dictionary, password consisting of both capital and non-capital letter. With this password policy in place, this helps to increase the difficulties in breaking the password. On the other hand, strong password also deters hacker from performing bruteforce, dictionary attack and etc.

In order to enforce the password policy, company often need to build an application layer (User Interface) to perform password validation before storing it in the System / Server. With the application layer in place, this also helped to ease non-technical staff to abide with the password policy. However, remembering and coming up with new password always impose a huge challenges to the users. Some of the behaviour observed are that a few of the technical staff with access right perform a password change at the application layer, change their password again at the lower layer. This has avoided the stringent password policy check. For instance, password is changed in the Server/System/Database directly instead of going through the Application layer.

With the above non-compliance behaviour, this will bring the company to the risk of being hacked due to weak password. The consequences could be catastrophic as the user account consists of higher privilege access and command right.

Recommendations:

In order to combat against the above behavior, it is recommended to do periodical password scan in the system to test the password strengths and flagged up to the user with the weak password for another password reset. Besides, weak password and the above non-compliance act could be brought up during the periodical Staff Security Awareness Training to prevent the similar incident from happening.

### **3.4.2 Insufficient Security Layering Between Domains**

Next, the organisation manages active directories and windows servers for the internal and external use by employees in different regions of the organisation. These servers may involve use for application development, credit and debit records and transaction as well as personal particulars of card holders. The servers are situated in various domains in the organisation’s network. It is common behaviour that employee would be able to do communication between these networks (to either transfer files or jump to different servers simultaneously to do certain tasks)

In order for communication and management amongst various networks, another network domain was set up that would able to communicate to all the existing networks. Communication between network is possible since there is are channels between networks.

Issues arises when either one of the network domains gets compromised. This could cause hackers to easily infiltrate to various domain due to this existing communication channel.

Recommendations:

The solution to this issue is to set up a security protocols/policies such as firewalls between two different network domains.The connection between those network domain and the management network domain should also be protected with a layer of firewall as well.

Another solution is to create a separate duplicate of the network map seen in one region for untrusted regions. Untrusted regions due to organisation expansion should have their own network system that is separated from the main organisation network map. However, a communication between these two network map should also be established, monitored and protected with firewalls to ensure only the right people with the right access is able to communicate between those two network systems.

# 4 Company Risk Profile

## 4.1 Three Main Leading Information Assets

Given the business nature of the company, i.e. a financial institution, and the above analysis, the team feels that the three main leading information assets are:

* Data
  + Data is seemed to be a very important asset as data includes company future strategy planning, card holder information, employee information, contracts with merchants and banks, etc.
* Procedure
  + Procedure is considered as another main leading information asset as the company has its own proprietary tools and ways of implementing payment services to ensure seamless and more efficient payment.
* People
  + This organisation relies heavily on people (employees, contractors and external people from other organisation such as merchants, bank institutions and third-party vendors).

## 4.2 Information Assets Vulnerabilities

Data (servers):

1. Vulnerabilities on the storage servers are inevitable. There are many opportunities for the adversaries to launch DDoS attacks or malware attacks or injection attacks on the organisation’s storage and data servers. The vulnerabilities can also be caused by design flaw or the implementation flaws of network security devices such as firewalls between the domains.
2. Security Misconfiguration is done by overboarding the servers with unnecessary features, components and documentation. It is always suggested to remove the unused features and frameworks or do not install the features that are not required while processing.

Procedure:

1. Compliance training: Lack of compliance training matching with enterprise standards. Even though there are many internal and external compliance trainings as part of project operations for every quarter, there is still a gap in the implementation with lack of proper management of the funds. Employees feel trainings as burdens instead of as an accomplishment. The right domain trainings has to be identified and scheduled for every employee and additional perks or mandatory trainings for employment progression may encourage to attend and complete these trainings.
2. Insufficient Logging, Tracking and Monitoring: Auditable events, Warnings and errors inadequate information, or unclear log messages are not given importance. For most of the end user machine, there is no centralized log management. When there is a suspicious activity, the alert triggered is usually suppressed considering it as low or medium critical because of the huge alerts triggered. A proper explanation has to be mandated before suppressing the alerts so that the sensitive or unidentified incident alert is not misidentified.

People:

1. Human is considered as the weakest link chain in terms of security. Social engineering, and stolen or loss physical assess cards that can be used to enter the organisation’s premises. Lost cards has to be immediately reported and disabled without any penalty considering the security threats that this scenario may pose. Remote agent's proficiencies to deal with complaints from users is decreased due to less access to communication, mentoring, knowledge transfer
2. As part of the business, there are many external agents,vendors and supporters in the organisation. We have to define the access levels of all the people that the organisation need to interact with. The vendors may work with the company in both online and with physical devices to serve the customers.
3. Technological obsolescence. Workstations of employees may not be updated and should be refreshed every 2-3 years. This may cause employee’s workstation to be vulnerable. Forced updates or patches has to be mandated after reminding the employees for certain time. A realistic target has to be maintained to update or change the employees machine considering the budget criteria. While disposing the discarded machines, care has to be taken to format the data properly and a team or person has to be accountable for these operations.

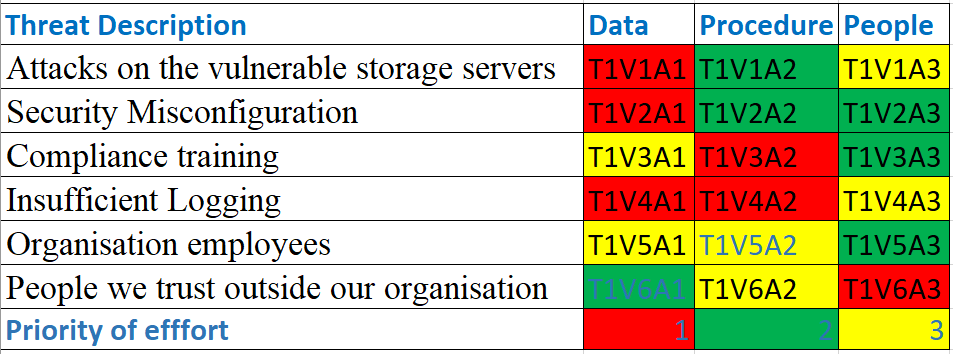


Table 1. Threat Vulnerability Assessment

## 

## 4.3 Risks Assessment Process

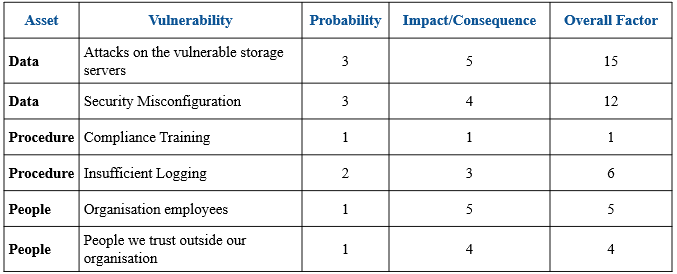


Table 2. Risk Assessment

**4.4 Risk control measures**  
We want to apply the risk control measures for the identified threats/vulnerabilities and focus that would mitigate risks.

Defense

* Attacks on the vulnerable storage servers - Patches has to be immediately applied and vulnerable machines should not be deployed in critical production environment. Also, the responsible team should keep track of the CVE and patches that are released. For instance, Microsoft releases its patches on second Tuesday of every month.
* Security Misconfiguration - Hardening the existing setup, and not using the default authentication credentials will help to defend the security misconfigurations.
* Compliance training - Identifying and training the employees based on their job role is more fruitful.
* Insufficient Logging - As we are in financial services, we have to Ensure high-value transactions have an audit trail with integrity controls.
* Organisation employees - The organisation employees are trusted in the organisation and continuous efforts are put in to make sure the employees understand the compliance standards of the organisation.
* People we trust outside our organisation - Minimal privileges should be given to the people we trust outside the organisation.

Transference

* Attacks on the vulnerable storage servers - Architectural planning has to define that the critical servers should not face the external environment and should not have internet access. The environments has to be divided into trusted and demilitarized zone. Honey pots or traps will also transfer the risk.
* Security Misconfiguration - automating the process for a new setup will reduce the risks of misconfiguration

Mitigation

* Attacks on the vulnerable storage server - An IR team to respond to the incident and BC&DR team to recover and reduce the impact of loss caused by an incident or disaster
* Insufficient Logging - Incident Response team is highly dependent on the logging. An effective monitoring and alerting suspicious activities will mitigate the risk impact.
* People we trust outside our organisation - Partners are inevitable as the organisation serves a large number or customers. All partners organisations hold accountability and SLA has to clearly define the consequences of violation of company’s policies.

Acceptance

Given the limited budget in the company and it is infeasible to cover all the threats in the company, it is important for the company to prioritize the threats through a series of threat assessment. The company determine the priority through assessing the risk impact and event occurrence. Also, the company is required to identify the risk acceptance levels and cost benefit analysis before implementing a new risk management policy. Above all of this comes the reputation of the company, so the company has to maintain high standards as it provides financial and technological services.

Termination

Equipment and asset disposal is also considered as a high priority in this organisation. All the outdated versioned machines are discarded and workstations refresh are done every 4 years in order to improve the security of the employee’s workstation in the organisation. The termination of the old services and introduction of the new services by this organisation is widely published and advertised to make sure the customers are informed about the change in the terms and policies.

# 

# 5 Conclusion

With the increasing usage number of attack surfacing in the recent years, companies have realized the importance of information technology management, paying more attention to securing information assets and making an effort to manage potential risks to the greatest extend.

Similarly, the investigated company also constructed a larger and well supported information security department and effective reporting structure. A lot of information strategies including security policy, technology, and practices were conducted in this company for the purpose of ensuring better secure information flow, strengthening the management capabilities and for preparing for contingencies. In particular, risk management, risk mitigation and uncertainty analysis used for this company to identify the risk factors and maintain essential risk controlling strategies.

However, there are still a lot of challenges, such as insider threats, unsecure transaction, more combatting with more sophisticated hacking tools, faced by the company and also many other financial institutions. Thus, cybersecurity remained to be a prolonged continuity effort for all institutions and required high level of commitment in fine-tuning processes to achieve a well-balance between detection rate and at the same time acceptable risk level.

# 

# 6 References

1. Fernandez, Eduardo B. "Two Patterns for Web Services Security." International Conference on Internet Computing. 2004.
2. Singh, G."A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." International Journal of Computer Applications 67.19 (2013).
3. Singhal, M. and Tapaswi, S. "Software tokens based two factor authentication scheme." International Journal of Information and Electronics Engineering 2.3 (2012): 383-386.
4. Scarfone, K. and Mell, P. Guide to intrusion detection and prevention systems (idps). No. NIST Special Publication (SP) 800-94 Rev. 1 (Draft). National Institute of Standards and Technology, 2012.