Table

Description automatically generated

A picture containing text, screenshot, font, number

Description automatically generated

# **Introduction**

## 1.1 Cyber Resilient

The ability of an organisation to anticipate, respond to, and recover from cyberattacks or other incidents is referred to as cyber resilience. It entails being able to quickly resume regular operations as well as having the required processes, technology, and procedures in place to reduce the impact of a cyber assault. Organizations are using technology more and more, and as a result, they are facing more and more complex cyber attacks. As a result, cyber resilience is becoming more and more crucial (what is cyber resilience?, 2020). Cyber resilience is a multi-layered strategy that involves continuing risk assessments, frequent security testing, and continuous network activity monitoring. It also involves establishing strong incident response procedures, including trained employees. It includes organizational policies and processes, a culture of security awareness and vigilance, as well as technical solutions. To quickly identify and contain cyber risks, it also entails establishing strong incident response procedures, including trained employees (Cyber Incident Recovery, 2022).

## 1.2 Cyber Readiness

Cyber Readiness refers to the capability to detect, avoid, and quickly respond to cyber threats such as security breaches, cyber intrusions, malware attacks, phishing attacks, data theft and intellectual property theft to ensure business continuity without interruptions (Sullivan, 2016). Achieving cyber readiness is the overarching goal of the company as it is crucial to ensure that the company’s critical information assets are protected as well as preserve corporate reputation, operations, and financial standing (FTI Consulting, n.d.)For instance, a faster detection ability would aid in minimizing the harm caused by the cyberattack and reducing the time and expense of recovering from that cyberattack.

## 1.3 Reason of Cyber Resilient should be focusing more on C-suite Level

Cyber Resilient needs to pay more attention to the C-suite level because they take an important role to enhances work culture and internal processes in the organization (Security, 2019). Cyber resilience requires a culture of cybersecurity awareness and proactive risk management. The C-suite level is responsible to set the work culture of taking security seriously in the organization. Therefore, by acting responsibly regarding sensitive information and data, the C-suite level may increase staff awareness of cybersecurity and lower organizational human error rates. Additionally, the C-suite needs to prioritize cyber resilience to ensure compliance with legal and regulatory requirements, which can prevent financial and legal repercussions. Overall, Cyber Resilient should concentrate more on the C-suite level to ensure business continuity and preparedness for cyberattacks.

## 1.4 What every C-suite level need to be done to ensure the safety of their organization

C-suite executives play a critical role in ensuring the safety of an e-commerce organization's sensitive data. They need to implement strong data security measures, including firewalls and data encryption, to protect customer information. Firewalls filter traffic from unauthorized sources and prevent access to private information, while data encryption transforms it into unintelligible ciphertext. These measures make it difficult for cyber criminals to steal and use sensitive data for fraudulent activities. In summary, implementing robust security protocols is crucial for safeguarding e-commerce websites and ensuring the safety of customer data (Varghese, 2022).

# 2.0 Company Industry

## **2.1 E-commerce**

The industry of our company is e-commerce, as it's known, the word "e-commerce" means the exchange of products and services through the internet and does majority of its business online, by selling goods and services through a website or mobile application (Lutkevich, n.d.).

These business interactions can be categorized into B2B (business-to-business) which includes all forms of electronic business, trade, and transactions between two companies that relate to products and services exchange, B2C (business-to-consumer) is the most common which focuses on interactions between businesses and their customers via electronic commerce, C2B (consumer-to-business), B2A (Business-to-Administration), C2C (consumer-to-consumer) and (C2A) Consumer-to-Administration. (ipleaders, 2019)

E-commerce companies have several advantages over traditional, which is e-commerce companies can operate 24/7 allowing customers to shop at any time. Additionally, e-commerce companies can reach customers all around the world because they are not restricted by physical location, giving them a broader reach. However, our company’s industry still faces challenges such as the need to maintain a secure and reliable online platform with the increased of cybersecurity threats and attacks.

# 3.0 Best practice and specific application/systems in organization against the Cyberattack

## 3.1 Best Practice in organization

E-commerce security is a collection of procedures that guarantee businesses are operating safely. The best way to secure entire E-commerce security is implement the PCI-DSS requirements (Payment Card Industry Data Security Standard). A series of rules known as PCI-DSS serves as a roadmap for every E- commerce company that gathers, manages, and saves credit card data. (Team, 2022)

PCI-DSS works in three ways which are: Assess: determine and inventory the resources and procedures that deal with cardholder data, then examine them for weaknesses that might expose the data. Repair: Fix vulnerabilities and safeguard corporate operations. Report: Share compliance reports with the banks and credit card firms you do business with and keep records of the assessment process and remediation undertaken to address the risks. The requirement includes security measures for credit card information that must be used consistently in all payment activities. Keep in mind that security process could be differ for each company and consult cybersecurity expert to ensure that the company meet the standards. (What Is PCI DSS Compliance and How Does It Work?, n.d.)

To protect sensitive customer data and retain customer confidence in the online buying experience, e-commerce enterprises must achieve and maintain PCI compliance. PCI standards non-compliance can lead to significant fines, legal action, and reputational harm. (Chavis, 2022)

## 3.2 Specific applications/systems in organization against the Cyberattack in E-Commerce industry

### 3.2.1 Firewalls

In the e-commerce industry, firewalls is an application that works by comparing a large number of publicly available lists of harmful websites to prevent harmful websites from accessing e-commerce company networks. They can recognize and filter out various unwanted web traffic elements. The firewall can be set up to keep track of and restrict traffic depending on certain parameters. Firewalls utilize various methods to identify and monitor website traffic, including IP addresses, domain names, website categories, and keywords present in URLs or website content and detect changes in behaviour including sudden data deletion. (How firewalls protect your business from cyber attacks, 2019).

### 3.2.2 SSL

SSL (Secure Sockets Layer) is needed to secure and encrypt financial information between devices and payment processors. When an e-commerce website employs SSL, HTTP becomes HTTPS, which is the industry standard for internet security and is safer for users. Not using SSL not only provides poor security but could also turn off visitors to our company’s e-commerce website. In some browsers, pop-up warning pages indicating that the page is not safe are available. The industry standard for e-commerce security moving forward should always be SSL and HTTPS. (Team, 2022)

# **4.0 Conclusion**

In summary, E-commerce companies have the advantage of being able to operate without stopping and reach customers over the world. However, they face challenges such as maintaining a secure online platform full of cybersecurity threats.

Moreover, cyber resilience is important for e-commerce companies because they deal with a large amount of personal data to ensure that their information assets are protected, and business continuity is maintained. Cyber resilience should focus more on the C-suite level because they are responsible for enhancing the internal processes in the organization. They play a crucial role in making sure that their e-commerce organization has strong data security measures such as firewalls and SSL. In order to prevent unauthorised access, they must keep an eye on and manage incoming and outgoing traffic according to pre-set security criteria.

In conclusion, e-commerce companies are faced with unique challenges that require them to have strong cyber resilience. This involves having the necessary processes, technology, and procedures to reduce the impact of a cyber-attack, therefore maintaining business continuity. The C-suite level executives need to ensure that the organization is compliant with legal requirements while ensuring the security of their customers’ personal data. Therefore, e-commerce companies can maintain a secure online platform and continue to reach customers globally.



# **5.0 Workload Matrix**



A document with signature on it

Description automatically generated with low confidence

# 6.0 References

Chavis, J. (17 January, 2022). Retrieved from https://www.spreedly.com/blog/pci-compliance-for-e-commerce-platforms#:~:text=PCI%20Compliance%20in%20E%2DCommerce,place%20to%20protect%20cardholder%20data.

*Cyber Incident Recovery*. (2022). Retrieved from Kyndryl: https://www.kyndryl.com/gb/en/services/cyber-resilience/incident-recovery/cyber-recovery?utm\_content=SRCWW&p1=Search&p4=43700066997797601&p5=e&gclid=Cj0KCQjwgLOiBhC7ARIsAIeetVAuagwSR0RCp1gShISGoszKqmeqvsYQkU4gN6U010jDDdYzWrcDPTsaAiTvEALw\_wcB&gclsrc=aw.ds

FTI Consulting. (n.d.). *Cyber Readiness*. Retrieved from fticonsulting: https://www.fticonsulting.com/services/cybersecurity/cyber-readiness

*How firewalls protect your business from cyber attacks*. (30 October, 2019). Retrieved from totality services: https://www.totalityservices.co.uk/how-firewalls-protect-business-cyber-attacks/

ipleaders. (12 November, 2019). *Introduction to E-commerce : An ultimate guide*. Retrieved from ipleaders: https://blog.ipleaders.in/introduction-to-e-commerce-an-ultimate-guide/

Lutkevich, B. (n.d.). *What is e-commerce*. Retrieved from techtarget: https://www.techtarget.com/searchcio/definition/e-commerce

Security, R. (14 August, 2019). *What Is Cyber Resilience and Why Is It Important?* Retrieved from RSI Security: https://blog.rsisecurity.com/what-is-cyber-resilience-and-why-is-it-important/

Sullivan, P. (August, 2016). *Achieving cybersecurity readiness: What enterprises should know*. Retrieved from techtarget: https://www.techtarget.com/searchsecurity/tip/Achieving-cybersecurity-readiness-What-enterprises-should-know

Team, A. C. (10 July, 2022). Retrieved from https://business.adobe.com/blog/basics/get-a-list-of-ecommerce-security-tips

Varghese, J. (3 July, 2022). *Ecommerce Security: Importance, Issues & Protection Measures*. Retrieved from Astra Security Blog: https://www.getastra.com/blog/knowledge-base/ecommerce-security/

*what is cyber resilience?* (2020). Retrieved from IBM: https://www.ibm.com/topics/cyber-resilience

*What Is PCI DSS Compliance and How Does It Work?* (n.d.). Retrieved from synopsys: https://www.synopsys.com/glossary/what-is-pci-dss-compliance.html