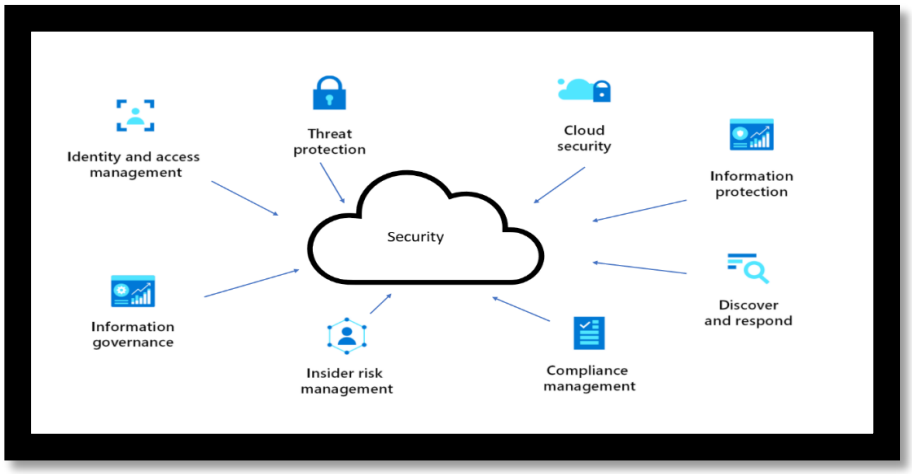
Contents

Introduction

Threat Management is an important framework designed to maintain cyber threats, protect the system from cyber-attacks, detect and react to cyber events quickly by using cyber security tools and techniques. One of the most important aspect of Threat Management is the relationship between people, technology and process (Varga et al., 2021). Cyber security professionals together with other stakeholders like employees, play an important role to ensure that they detect, respond, and protect the company's system from cyber threats. Technology such as Kali Linux, firewalls, encryption, and antivirus involves the tools that are used to respond to security events while, processes include monitoring, treat intelligence and risk management to make sure that threats and attacks are well reported and documented (Gonzalez-Granadillo et al., 2018). This report will focus on System Security domain, emphasising the importance of continuous cycle that work together to reduce cyber threats.

System Security

Ensuring that data, software, and equipment systems of the business are well protected from cyber criminals (Shukla et al., 2022) is important, as they want to steal the company's sensitive information and use it for their own gain. The vital role of system security is to protect the integrity and confidentiality of the business systems. System security will be discussed through a continuous cycle of assessment, mitigation, insurance, detection, and remediation.



[Figure 1: System Security Architecture, https://learn.microsoft.com/en-us/azure/architecture/guide/security/security-start-here]

Assessment

Assessment is an important part of cyber-threat management, involving identifying the potential risks and attacks that may cause a harm into the organization's system, allowing the business to develop strategies to prevent the attacks from happening (Inge Sebyan Black, 2010). However, while assessments are good at reducing risks, which does not mean ricks will end completely. Cyber Security professionals must understand that assessments are based on the current knowledge to minimize the risks in order for them to protect the system against cyber criminals and assessments should be continuously adapted to new risks. Two assessments that the organisation can use to identify potential risks are discussed below.

Varga et al (2021) points out the importance of vulnerability assessment which involves finding and evaluating the potential threats, weaknesses, or vulnerabilities within the systems. Tools such as Kali Linux are mainly used for penetration testing to identify these vulnerabilities and threats, assisting cyber security professionals to use what they identified and recommend strategies to prevent that. However, while these tools like Kali Linux require an extensive knowledge to utilize them, organisations must train their cyber security professionals to use these tools effectively. For example, weak password is the most identified vulnerability and threat during assessments, therefore Cyber Security professionals can introduce multifactor authentication (MFA) to strengthen the security. Thus, while assessments play a significant role, they must be held with caution.

Vinuguyathri (2023) propose that security audit is one of the most important types of assessment, involving a good analysis of IT Infrastructure of the business to ensure that there are no threats and vulnerabilities. While security audits play a significant role for companies to improve their security, it is vital to note that they can make errors or mistake. For security audit to be effective, it depends strongly on the quality of the assessments and the experience or knowledge of those conducting it. In addition, security audits detect existing risks and vulnerabilities, they may not always be on point as emerging threats increase in the cyber security space. For example, for training employees to be successful, it lies on continuous update and adapting to new risks. Furthermore, businesses must consider the expenses of regular security audits and the challenges that comes with it, even though it is crucial.

Mitigation

JPMorgan (2022) emphases the importance of coming out with informed decisions that are created to minimize the identified cyber-attacks and risks, in order for the organization to protect and respond to attacks effectively. This means that while an organisation suffers from a major loss because of cyber-attack, it can reduce the possibility of future cyber-attack by implementing security measures and policies that protects the organisation's system. However, it is vital to look beyond the outcome of these measures. For example, the use of advanced technology is mainly recommended, but their success depend on how their cyber security specialist are trained to make informed decisions. Two key mitigating strategies can aid in organisation's security system: Upgrade and update software, and multi-factor authentication.

JPMorgan (2022) further suggest that regularly upgrading and updating software is crucial for mitigating in threat management. These upgrades are important because they improve systems security by fixing existing vulnerabilities and ensuring software meets the current security standards. By keeping software up to date, companies can significantly minimize the risks of software vulnerability, as cyber-attackers always targets systems that are not regularly updated and upgraded, knowing they may have weaknesses. Therefore, upgrading and updating plays a significant role in reducing risks of system vulnerability.

Multi-factor authentication is essential because password alone no longer provide that strong security due to the increasing of cyber-attacks (AC3, 2023) . MFA is when cyber security professional adds an additional layer to prevent illegal entries (Lok, 2024). The staff of SonicWall argues that while MFA improve system security by requiring an extra step to sign in, it is not enough. For example, multi-factor authentication can be overridden or bypassed through a session hijacking, meaning that if it not properly configured, can be easily bypassed. Furthermore, while this mitigation strategy can be implemented to improve the security of the system, it should be embedded into system security framework for continuous process of observing and monitoring.

Insurance

The third step is also vital after implementation of mitigation which involves measures or strategies that need to be taken to protect the system. Cyber Insurance refers to assisting the organization to respond and recover from the cyber-attacks (CFC, 2023). Onsurity Editorial (2024) shows that insurance plays a key role as it helps businesses to recover from financial loss. Cyber insurance includes the legal fees, data recovery expenses and the compensation to the individuals that may affected. However, while cyber insurance is important, it should not be taken as reliable security measures because it does not prevent cyber-attacks from happening, instead it assists with financial relief after the attack, this also include employee training and frequent testing. As a result, businesses should include cyber insurance in their strategy framework to ensure protection and data recovery.

Onsurity Editorial (2024) emphases that organisations have various options to choose from in order to protect themselves. For example, data breaches insurance, which means that it covers the organisation relating to major data loss and provide financial support. The second type of cyber insurance is network security insurance, which deals with protecting the business from harm relating to security network such as hacking incidents. While these options offer means of financial recovery, it is vital to remember that they do not prevent cyber-attacks from happening.

Detection

This refers to detecting and identifying attacks or risks from the system and it helps the company to prevent these attacks and risks before happening (Shukla et al., 2022). For example, detecting a system vulnerability early enables the organisation to implement security measures to protect the system from being attacked, which is a benefit of a good risk management. Organisations can use various tools to detect attacks and risks such as Kali Linux which provides a massive advantage in improving system security. There are two detection types that a business can utilize to detect attacks and risks.

Xcitium (2024) propose behaviour analysis as an important detecting strategy. This program is designed to identify abnormal behaviour of a system that may have an impact on the system’s endpoint by implementing baseline data that ensures it guides the user’s normal activity. For instance, this tool records user activity when

they sign in and monitors abnormal behaviour. Moreover, once a hacker tries to bypass the system, this program reports the unusual activity to security specialist who can investigate the matter by comparing norm with the baseline data. However, while behaviour analysis can detect unusual activity or potential risks, cyber-attackers may still find ways to bypass detection. Hence, it is recommended to be used with other protection measures to strengthen the system security.

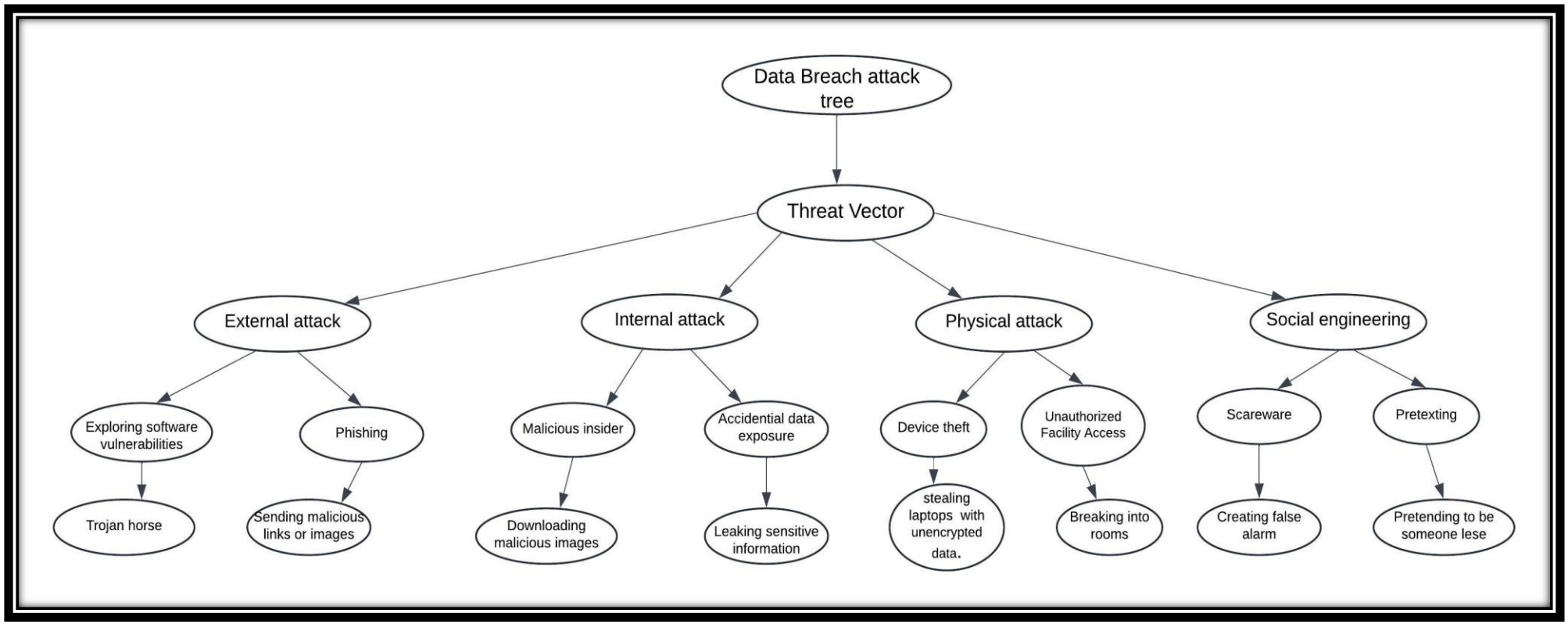
Xcitium (2024) further proposed a signature-based detection method as one of the most important methods that is used to identify malwares from the system. This method refers to detecting malicious activities and monitoring network traffic by assessing with existing signatures (Corelight, 2024). When a match is found, it reports to cyber security processionals to investigate further. On the other hand, signatured-based detection is known for detecting known risks, which means it is limited as new risks and threats arises. Thus, this method should be used with other comprehensive detection methods such as behaviour analysis to create a strong security.

Remediation

Remediation is defined as addressing cyber threats and vulnerabilities in order to reduce the damaged that may be caused to a business (Logsign, 2019). Cyber Security professionals are able to stop malicious activities such as worms, and ransomware. However, the root of the threat must be detected first. Furthermore, Logsign (2019) points out that if the business wants to stop malicious malware in the system, they first need to detect the cause of the threat.

Sumo Logic (2023) suggest that third-party integration can mitigate cyber threats and vulnerabilities, an argument that highlights the importance of protecting the organisation’s information and data, however it is crucial to note that involving third part integration can also introduce new risks, such as potential threats in the integrated systems. This means that the business must not only have a deep understanding of their own systems but also on the integrated systems they use in order to detect the weakness and respond promptly.

Data Breach attack Tree

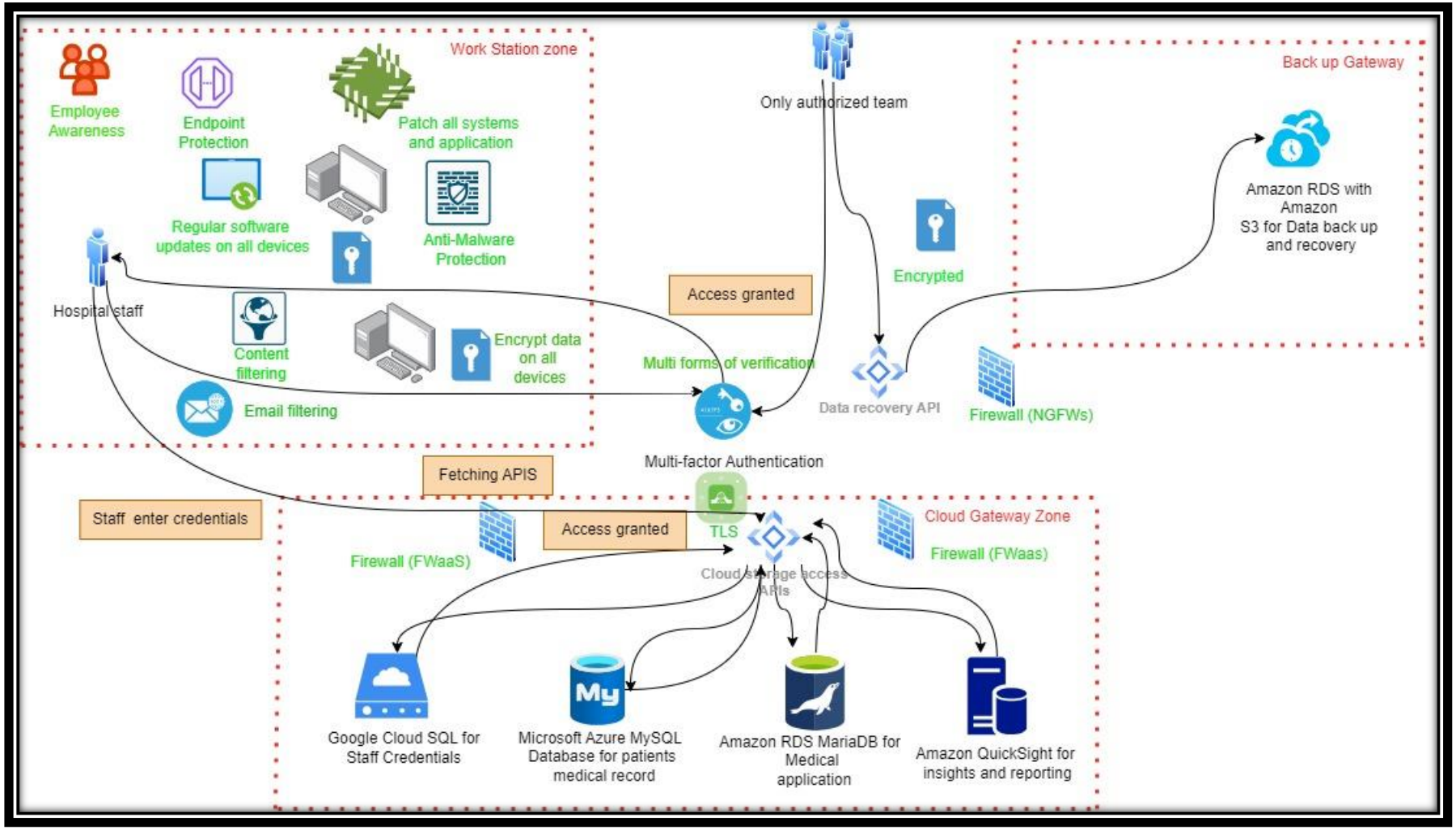


In order to design a threat model, I decided to choose an attack tree of data breach where medical records of patients can be lost or stolen by attackers. An attack tree is a component of how threat or risk is involved where attackers might gain an access to a system of the organisation (David, 2023). The purpose of this data breach attack tree is to assist healthcare facilities such as public or private hospitals to detect malicious activities to a system and this helps healthcare facilities to plan ahead, enabling them to prevent those attacks from occurring (Yuga, 2024). However, it is crucial for a hospital to produce strategies to prevent these attacks, not just drawing an attack tree.

There are four levels in the design. The first one being threat vector which essential means how attacks find a way to gain an access to a system (SailPoint, 2023). The second level includes external attack, which means any potential threat outside the hospital (Elliott, 2024); The third level include internal attack, which means threat that originate within the hospital such as staff nurses (Shukla et al., 2022); physical attack, where attackers can steal any devices that has unencrypted data (Varga et al., 2021), and social engineering, where attackers use malicious activities to draw attention from the victims by tricking them (Lok, 2024).

The third and fourth level describe how these attacks do in order to gain an access to the system. This includes exploring software vulnerabilities through trojan horse and phishing by sending links or images that contain virus (Adam, 2014); malicious insiders, where employees download malicious images that where sent by attackers, and accidental data exposure, where employees can leak sensitive information to an outsider unintentionally (Gonzalez-Granadillo et al., 2018); device theft and unauthorized physical access, where a USB or laptop with an unencrypted data can be stolen (Iqbal & Anwar, 2020); scareware, where attackers can create a false alarm to trick victims, and pretexting, where an attacker pretends to be someone else or creates a clone website where a victim can enter their credentials(Varga et al., 2021) . Thus, it is crucial to prevent these attacks by designing a threat model which will be discussed below.

Threat Model: Protecting Patients medical records



Threat Model refers to an approach used to detect and identify risks in a system that may cause harm. By using a threat model, an organisation can be aware of security threats and how to defend against them (Adam, 2014). The threat model that is used in the above design is for protecting patient's medical records in healthcare. Healthcare facilities have an important task to ensure that the integrity and confidentiality of patients is not compromised, therefore it is crucial to have a threat model to achieve such.

Healthcare facilities must develop these strategies to prevent types of attacks mentioned in the data breach attack tree. In the model, there is a first workstation zone where employees work together to achieve a common goal, that also includes desktop computers, laptops and other end-user devices that are used in the workplace. A staff member would normally enter their credentials to access patient's medical record, however, to prevent unauthorized access, multi-factor authentication was implemented to improve security measures (Lok, 2024). Secondly, hospital organisations must ensure to regularly updates and upgrades its systems with the latest security measures (JPMorgan, 2022).

Health facilities must implement endpoint protection because it is crucial to secure devices, networks in the organisation against cyber threats. This includes antivirus and antimalware to detect and stop malicious activities. In addition, employee training and awareness are important to educate hospital staff about phishing and social engineering (Vinuguyathri, 2023). Encrypt all devices that contain sensitive information to prevent unauthorized access (Onsurity Editorial, 2024). Content filtering helps staff not to access harmful material on the internet and also prevent not to download harmful content. Similarly, email filtering is essential to ensure that staff do not download harmful images or click on links that contain viruses, as it filters them out.

Then, there is a cloud gateway zone, where health facilities can keep their records and sense information. In this threat model, there are four cloud databases that serve for different purposes to enhance security. However, using different cloud databases can introduce new challenges that must be managed carefully. It is very important to store information at different places just in case one gets exposed. Health facilities can utilize the following cloud database strategy; Google Cloud SQL

database for storing employee credentials, Microsoft Azure MySQL for keeping patient's medical records; additionally, Amazon RDS MariaDB cloud database that is used for medical application and Amazone QuickSight a database for insights and reporting to support their data analysis. Furthermore, firewalls such as (firewall as service – FwaaS) are also implemented to block suspicious network activity in the cloud, this ensures a comprehensive protection without disturbing cloud operations (Varga et al., 2021). Trasport Layer Security (TLS) is used for API communication where it's ensures data communication between API client and cloud is encrypted (Gonzalez-Granadillo et al., 2018). This encryption prevents malicious parties from interfering during data transmission.

The most important part here that healthcare facilities must also implement is data recovery or back-up. This protects against data loss, cyber-attacks, or hardware failures. Thus, Next Generation Firewall (NGFW) is also implemented to strictly safeguard back-up data with robust security measures. There is limited access to back-up data and only authorized team can access data recovery for better tracking and monitoring after the incident. Back-data have their own API to better control data recovery process and enhance security. Furthermore, Healthcare facilities must use fingerprints access and cameras to protect devices from being stolen.

Conclusion

Threat management is crucial in organisations to ensure that they implement robust strategies to prevent cyber-attacks and to safeguard the organisation's systems. By implementing these security measures, hospital facilities can ensure confidentiality of patients. This includes training staff about social engineering and phishing, using endpoint protection, regularly updating software and most importantly implementing a data backup regularly. As cyber-attacks continuously evolve, cyber security professional must run a regular IT security audit to detect vulnerabilities and stay up to dates with cyber threats. Thus, the importance of staying alert is very important in cyber security.

References

AC3. (2023). *Essential Eight: Mitigation Strategy—Multi-Factor Authentication* [Australian Centre for Advanced Computing and Communication Pty Ltd]. https://www.ac3.com.au/resources/essential-eight-mitigation-strategy-multi-factor-authentication

Adam, S. (2014). *Threat Modeling: Designing for Security*. https://ieeexplore.ieee.org/book/9932141

CFC. (2023). What is cyber insurance and why do you need it? *CFC*. https://www.cfc.com/en-gb/knowledge/resources/articles/2023/12/what-is-cyber-insurance-and-why-do-you-need-it/#:~:text=An%20essential%20part%20of%20cyber,harm%2C%20regulatory%20fines%20and%20more.

Corelight. (2024). *What is signature-based detection?* https://corelight.com/resources/glossary/signature-based-detection

David, T. (2023). *What You Need to Know About Attack Trees* [E-Councel Cyber Security exchange]. https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/attack-trees-cybersecurity/

Elliott, G. (2024). *What are internal cyber security threats?* [Aspire]. https://www.aspirets.com/blog/what-are-internal-threats-cyber-security/

Gonzalez-Granadillo, G., Dubus, S., Motzek, A., Garcia-Alfaro, J., Alvarez, E., Merialdo, M., Papillon, S., & Debar, H. (2018). Dynamic risk management response system to handle cyber threats. *Future Generation Computer Systems*, *83*, 535–552. https://doi.org/10.1016/j.future.2017.05.043

Inge Sebyan Black. (2010). *The Professional Protection Officer*. https://doi.org/10.1016/C2009-0-19898-7

Iqbal, Z., & Anwar, Z. (2020). SCERM—A novel framework for automated management of cyber threat response activities. *Future Generation Computer Systems*, *108*, 687–708. https://doi.org/10.1016/j.future.2020.03.030

JPMorgan. (2022, September 29). 12 tips for mitigating cyberattacks. *JPMorgan Chase & Co*. https://www.jpmorgan.com/insights/cybersecurity/ransomware/12-tips-for-mitigating-cyber-risk

Logsign. (2019). *What is Remediation in Cyber Security?* https://www.logsign.com/blog/what-is-remediation-in-cyber-security/

Lok. (2024). *A complete guide to the Essential Eight and Strategies to Mitigate Cyber Security Incidents* [Usecure]. https://blog.usecure.io/a-complete-guide-to-the-essential-eight-and-strategies-to-mitigate-cyber-security-incidents

Onsurity Editorial. (2024). *What is Cyber Insurance: Types, Coverage and Benefits* [Onsutity]. https://www.onsurity.com/blog/what-is-cyber-insurance/

SailPoint. (2023). *What is a threat vector? Examples in cybersecurity* [SailPoint]. https://www.sailpoint.com/identity-library/threat-vector

Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K., & Weldehawaryat, G. K. (2022). System security assurance: A systematic literature review. *Computer Science Review*, *45*, 100496. https://doi.org/10.1016/j.cosrev.2022.100496

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security*, *105*, 102239. https://doi.org/10.1016/j.cose.2021.102239

Vinuguyathri, C. (2023). *What Is Cyber Security Audit and How Is It Helpful for Your Business?* [Indusface]. https://www.indusface.com/blog/what-is-cyber-security-audit-and-how-it-is-helpful-for-your-business

Xcitium. (2024). *What are Three Main Detection Types? Explained*. https://www.xcitium.com/what-are-three-main-detection-types/

Yuga. (2024). *Guide to Threat Modeling using Attack Trees* [Practical-devsecops]. https://www.practical-devsecops.com/threat-modeling-using-attack-trees/