7019ICT

Workshop Document

TABLE OF CONTENTS

Module 1: Workshop Exercise Write-up

The Data Breach At ACME Corporation

Introduction

A multinational retail company, Acme Corporation experienced a data breach that disclosed the personal information of millions of customers including their names, addresses, credit card numbers and purchase history. Older security software, insufficient staff training, and failure to follow industry security standards contributed to the breach.

Security Principles and Concepts

Acme Corporation had many flaws which led to the exposing of customer's personal information.

- Outdated security software was one of the major reasons for the corporation's data breach. Older software leaves the system vulnerable to many new advanced attacks and cannot integrate with modern security tools and technologies.
- Employees needed to be adequately trained to recognise and respond to the threats. Most breaches occur because of the employees i.e. “People Behind The Keyboard”. The most common phishing attack could have been recognised and mitigated if employees were properly trained.
- Acme should have implemented industry-recognised standards which could have provided them with a framework to understand and manage risk according to the organisation's business needs.

Importance Of Aligning With Security Standards

NIST CSF is a framework that helps organisations like Acme to manage and reduce cyber risks, by providing structure to protect, identify, respond, detect and recover from cybersecurity risks. NIST CSF frameworks are flexible and can be aligned with any organisation and act as a starting point for an organisation to implement information security and cyber security risk management. (IBM, 2024)

Both NIST CSF and ISO 2700 are to protect an organisation's sensitive data but NIST CSF acts as an instruction whereas ISO 2700 is a standard where the organisation must meet the criteria to get the certificate. ACME should use NIST CSF for their early-stage in cyber security and implement ISO 2700 to strengthen their existing security programme. (*NIST CSF vs. ISO 27001: What’s the Difference? | Vanta*, 2023)

Sector-Specific Security Standards

To protect customers' personal information, the organisation should also use security standards according to the specific sector

- GDPR: GDPR helps the organisation form a regulation for collecting and processing information from individuals who live in and outside the EU. According to the GDPR, any individual record must be de-identified if no longer in use. ACME should follow the regulations and de-identify the record to protect user personal information. (Wikipedia Contributors, 2019)
- PCI DSS: PCI DSS is a collection of guidelines created to protect the secure handling of credit cards and monitor transactions to keep information safe and secure. (Tuffley & Griffith University, 2024)Acme Corporation can use PCI DSS to protect customer's payment information and reduce the risks of breaches.

Legal and Regulatory Implication

Non-compliance with data protection laws could result in fines, legal liabilities, and long-lasting damage to customer's trust and market reputation. For example, in a GDPR, fines can lead to fines up to 4% of a company's annual revenue which can cause financial risk. Additionally, a data breach can cause serious harm to customer's trust and damage the organisation's reputation which leads to a business loss and a decline in market shares.

Aligning with industry security standards like NIST and ISO 27000 series can help Acme from legal impact, protecting brand reputation and mitigating fines and legal repercussions as these standards provide comprehensive risk management and security controls. (Tuffley & Griffith University, 2024)

Recommendations

- Regular software updates will ensure all systems are up-to-date with the latest security patch.
- To provide employment training for cyber awareness and how to respond to cyber-attacks.
- Adopting industry-standard security systems to protect customer's personal information and safe from legal fines
- Conduct regular security audits to find and patch vulnerabilities before they get exploited.
- De-identifying customer's personal information when not in use.

Conclusion

The data breach in Acme Corporation is the result of not following industry-standard security like NIST CSF, ISO 27000, GDPR, and PCI DSS. Aligning with security standards ensures compliance and protects customers' data. Implementing the recommendation provided will help Acme strengthen its security measures and prevent future breaches.

References

- Tuffley, D. & Griffith University. (2024). 7019ICT Cyber Security Risk Management. In *COURSE NOTES*. https://lms.griffith.edu.au/courses/24368/files/6212968?wrap=1
- IBM. (2024). *What is NIST Cybersecurity Framework? | IBM*. Www.ibm.com. https://www.ibm.com/topics/nist
- *NIST CSF vs. ISO 27001: What's the difference? | Vanta*. (2023). Vanta. https://www.vanta.com/collection/iso-27001/nist-csf-vs-iso-27001#:~:text=Both%20NIST%20CSF%20and%20ISO
- Wikipedia Contributors. (2019, April 15). *General Data Protection Regulation*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Module 2: Workshop Exercise Write-up

Supply Chain Attack On Solarwinds

Introduction

In 2020, SolarWinds, a major IT management software company had the biggest supply chain attack where hackers infiltrated SolarWinds network monitoring and management tool and inserted a malicious code into their Orion platform. This vulnerable software was distributed to the customers which led the hackers to have an easy backdoor to all the systems who were using this software.

Risk Management Framework

The NIST RMF is a rigorous methodology that helps organisations manage information risks across their systems and operations. An organisation like SolarWinds can use NIST RMF as it has a seven-step process that covers the entire risk management process. One of the key strengths of this RMF is its emphasis on continuous monitoring, which could have detected any change in the SolarWinds platform (Tuffley & Griffith University, 2024). NIST RMF methodology is based on prioritising by impact level and taking appropriate security measures to control and monitor the security posture. Using NIST RMF could have identified vulnerabilities in the Orion platform earlier and allowed more time to mitigate the attack.

Vulnerability Management

Vulnerability management is a 5 step process that includes Access, Prioritize, Act, Reassess and Improve that helps to identify and mitigate the vulnerability found in the systems and network.

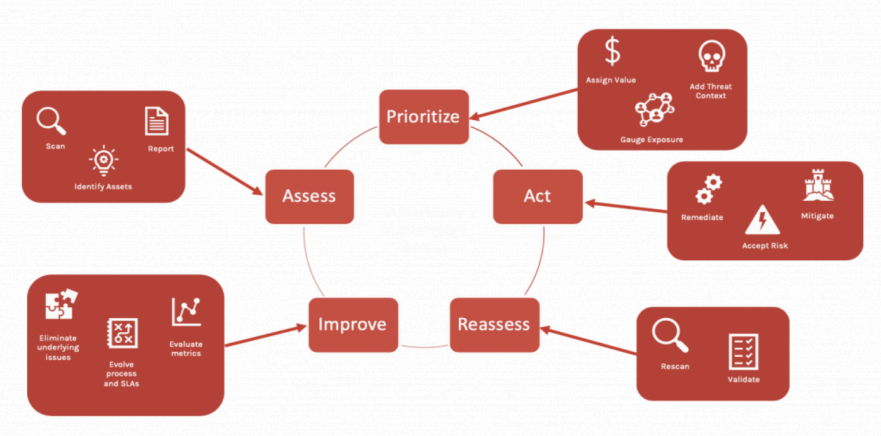

Fig. Vulnerability Management process(CrowdStrike, 2021)

SolarWinds should have robust vulnerability management that requires continuous monitoring and assessment. Effective vulnerability management helps the organisation to mitigate potential risks and comply with industry-standard

requirements. Vulnerability management mainly includes simple scanning of tools to find any flaw that can be done by having regular vendor checks and auditing the infrastructure to validate all endpoint input and interaction between exterior and interior flows, which can be implemented by using an IPS or IDS to monitor the networks and the systems. (Tita, 2023)

Third-Party Risk Management (TPRM)

The TPRM program is essential for organisations that rely on external vendors or third-party software to identify, assess and mitigate risks. Using external vendors can increase the potential risks of a supply chain attack, the TPRM program uses structured ways to tackle it by including due diligence, continuous monitoring, and establishing clear security requirements for the third-party vendors (Tuffley & Griffith University, 2024).

A robust TPRM program could have helped SolarWinds mitigate risks by ensuring thorough vendor evaluation through due diligence and having clear contractual obligations with continuous monitoring. These security measures help the organisation to manage the risks associated with the third party.

Fig. TPRM operation process (*Third-Party Management*, 2022)

Risk Identification, Assessment and Treatment

These help the organisations identify potential risks, analyse their impact and implement security measures to manage risks.

Risk identified with the case of SolarWinds incident

- Supply chain vulnerabilities: Dependency on third-party vendors has a significant risk that the software could be compromised, which many organisations failed to recognise.

- Insufficient Monitoring of Software Updates: If SolarWinds had monitored their software updates before making it to the public, the attack could have been prevented. The public assumes that the updates from trusted vendors are secured.

Missed opportunities for the mitigations

- Risk assessment: The types of risk and assets valuation will decide a qualitative or quantitative risk assessment. A regular risk assessment should also be done which can help to mitigate the associated risks.
- Network Segmentation: A network segmentation could have been used to limit the reach of the attack within their network

Recommendations

- Using RMF: NIST RMF can help the organisation to manage information security risks.
- TPRM Program: Implement a comprehensive TPRM program with due diligence, continuous monitoring and clear security standards.
- Comprehensive risk assessment: A comprehensive risk assessment and audit should be done to identify and address potential vulnerabilities.
- Auditing: Auditing infrastructure to validate all endpoints and implement IPS or IDS.

conclusion

The SolarWinds supply chain attack needs robust risk management, including the TPRM program, better vulnerability management and risk management framework. Implementing the recommendation provided will help SolarWinds strengthen its security measures and help prevent future breaches.

References

- Tuffley, D. & Griffith University. (2024). 7019ICT Cyber Security Risk Management. In *COURSE NOTES*. https://lms.griffith.edu.au/courses/24368/files/6212968?wrap=1
- CrowdStrike. (2021, May 6). *What is Vulnerability Management? | CrowdStrike*. Crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/
- Tita, I. (2023, March 24). *How supply chain attacks work and 7 ways to mitigate them*. Pentest-Tools.com. https://pentest-tools.com/blog/supply-chain-attacks

- *Third-Party Management*. (2022). Deloitte China. https://www2.deloitte.com/cn/en/pages/risk/solutions/third-party-management.html

Module 3: Workshop Exercise Write-up

Insider Threat At Datasafe Solutions

Introduction

A data storage management company, Data Solutions, had an insider threat where a disgruntled employee had bypassed access control, tampering with security logs and transferring large amounts of customer-sensitive data into an external storage device before resigning, which resulted in a huge financial loss and legal liabilities for the organisation. (Tuffley & Senior Lecturer, School of ICT, n.d.)

ISO 27001/27002 and Insider Threats

An ISMS based on ISO 27001 describes an approach to managing sensitive information through risk assessment and security control, whereas ISO 27002 covers areas such as organisation security, and asset management. By implementing these standards Data Safe Solutions could have established a stronger access control policy that ensures only authorised personnel had access to the sensitive data. Organisations such as Datasafe Solutions can effectively translate the principles of ISO 27001 into practical security measures suited to their unique risks and operational environments by aligning with ISO 27002 and mitigating risk. (SecureSlate, 2024)

Risk Assessment and Insider Threat

Risk assessment plays an important role in addressing insider threats. Through risk assessment, an organisation can understand the control of security and take appropriate security measures that control the risk.

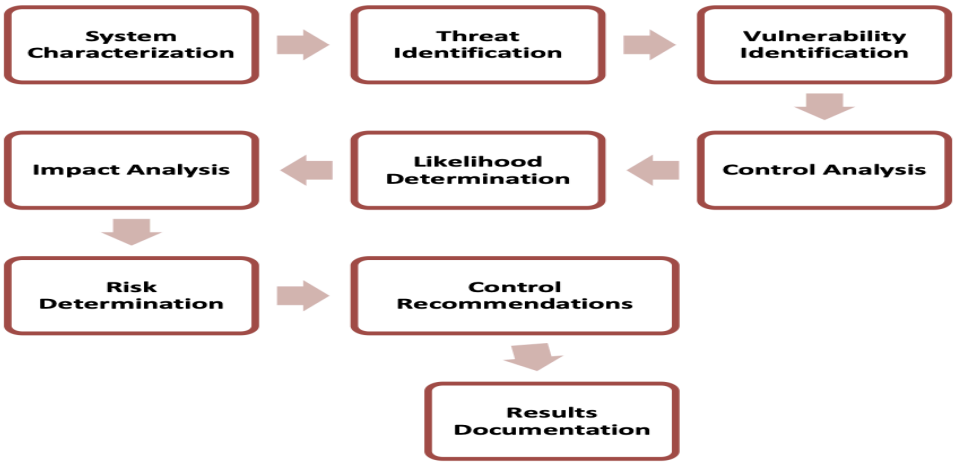

Fig. NIST model (Hashim et al., 2018)

The NIST model can improve the Datasafe solution risk assessment plan by providing a structured approach to identifying threats, evaluating control and determining risks. This helps the organisation to mitigate risk and improve overall security posture. (Hashim et al., 2018)

Security Control For Insider Threat Prevention

"Annex A of ISO 27001 lists 114 security controls divided into 14 control sets, each of which is expanded upon in Clauses 5–18 of ISO 27002" (it governance, 2016), Datasafe solutions could have been used:

- A.9 Access control: The Datasafe solution could have enforced an access control policy to restrict unauthorised access to sensitive data.
- A.16 Information Security Incident Management: Datasafe solution could have reduced the risk of insider threat by having a robust incident management plan. This control ensures effective management through established responsibilities and procedures.
- A.7 Human resource security: This control ensures that employees are aware of their job roles in safeguarding organisation data during employment. Datasafe solution can use this control as a screening to check the candidate who might pose a threat to the organisation.

Continuous Improvement and Monitoring

Continuous improvement and monitoring provide valuable insights into the effectiveness of the ISMS and point out the areas for improvement. Organisations like DataSafe have the option to implement additional controls and update policies and procedures as preventive and corrective measures (Tuffley & Griffith University, 2024).

Datasafe solution could have been leveraged by continuous improvement through regular reviews of their ISMS, updating their ISMS, incorporating the lessons from past incidents and enhancing employment training. Monitoring tools like IDS, real-time alerts and log analysis will ensure the organisation's data protection and prevent the same incident in the future.

Recommendations

To enhance the ISMS and prevent future incidents Datasafe solution should consider the following recommendations:

- Regular review of access control: This ensures that access control is regularly reviewed and adjusted according to employees job role.
- Employee Training Programs: Provide training and awareness for cyber threats and emphasise the importance of reporting any suspicious activity in the organisation.
- Developing Incident Response Plan: To construct a comprehensive insistent response plan that includes the most common scenarios for handling insider threats
- Implementing Monitor tools: The monitor tool will alert the organisation for any unauthorised access and tampering with the data.

Conclusion

A robust ISMS based on 27001/27002 along with a risk assessment plan of the NIST model and continuous improvement and monitoring of the Datasafe solution security could have prevented the insider threats. Implementing the recommendation provided will help the Datasafe solution strengthen its security measures and help prevent future incidents.

References

- Tuffley, D. & Senior Lecturer, School of ICT. (n.d.). Cyber Security Risk Management Workshop Exercises. In *7019ICT Cyber Security Risk Management* (pp. 1–10). https://lms.griffith.edu.au/courses/24368/files/6212950?wrap=1
- SecureSlate. (2024, July 10). ISO 27002 vs ISO 27001: The Surprising Truths Behind These Security Powerhouses. *Medium*. https://secureslate.medium.com/iso-27002-vs-iso-27001-the-surprising-truths-behind-these-security-powerhouses-2a1116077cbb
- Hashim, N. A., Zainal Abidin, Z., Zakaria, N. A., Ahmad, R., Information Security, Forensic and Networking Research Group (INSFORNET), Puvanasvaran, A. P., & Faculty of Manufacturing Engineering, Universiti Teknikal Malaysia Melaka. (2018). (IJACSA) International Journal of Advanced Computer Science and Applications. *IJACSA*, *Vol. 9*(No. 11), 126–127. https://ftp.saiconference.com/Downloads/Volume9No11/Paper_19-Risk_Assessment_Method_for_Insider_Threats.pdf
- it governance. (2016). *ISO 27002: Security Controls*. Itgovernanceusa.com. https://www.itgovernanceusa.com/iso27002
- Tuffley, D. & Griffith University. (2024). 7019ICT Cyber Security Risk Management. In *COURSE NOTES*. https://lms.griffith.edu.au/courses/24368/files/6212968?wrap=1

Module 4: Workshop Exercise Write-up

Equifax Data Breach

Introduction

In 2017 one of the largest Credit reporting agencies in the US, Equifax, had a massive data breach due to a vulnerability found in the Apache Struts web application framework, which Euqfax failed to patch despite many updates. This vulnerability causes unauthorised access to Equifax's systems and exfiltrates sensitive data for several weeks. (Tuffley & Senior Lecturer, School of ICT, n.d.)

NIST Cybersecurity Framework (CSF)

The NIST CSF provides comprehensive recommendations to improve information security and cybersecurity risk management. NIST CSF is a great place to start when implementing information security and cybersecurity risk management because it works with any organization's current security measures, regardless of the industry.(IBM, 2024)

The most relevant NIST CSF core function for Equafix would be to Identify, Protect and Detect. The risk assessment under ‘identify’ would have flagged Apache Struts' vulnerability and effective patch management under ‘protect’ would have helped in the necessary updates. The ‘detect’ would have quickly identified unauthorised access and minimised the data breach.

NIST SP 800-53 Security and Privacy Controls

NIST SP 800-53 grouped privacy and security controls into 20 distinct families, each of which prioritizes a different component of information security. Each of these families is assigned a baseline level of assurance. Based on their risk tolerance and the potential impacts of a security breach, these baselines give organizations a place to start when choosing and implementing the right controls. (Tuffley & Griffith University, 2024)

The specific families, the Equafix could have implemented

- Access Control: Implementing strict access control and multi-factor authentication would have restricted unauthorised access and limited attacker’s movement within the network
- System and Information Integrity: Regular scanning and patch updates for any bugs or errors could have prevented the exploitation of the vulnerability in Apache struts.
- Incident Response: A well-defined IR strategy would have improved Equifax's ability to manage the risk effectively and minimize the impact.

CIS Critical Security Controls

Organisations can be protected against the most frequent and harmful cyberattacks with the help of CIS controls.

CIS controls, the Equifax could have implemented

- CIS Control2 (Inventory and Control of Software Assets): Keeping up-to-date software could have identified critical vulnerabilities such as Apache Strut and addressed them promptly. (*CIS Control 2: Inventory and Control of Software Assets*, n.d.)
- CIS control4 (Secure Configuration of Enterprise Assets and Software): Regular audits and Secure configuration would have reduced the risk of the vulnerability being exploited. (*CIS Control 4: Secure Configuration of Enterprise Assets and Software*, n.d.)
- CIS Control7(Continuous Vulnerability Management): To minimise the opportunity for the attack to attack, a plan should be developed that continuously accesses and tracks vulnerability on all assets. (*CIS Control 7: Continuous Vulnerability Management*, n.d.)

Mapping Controls to Organisational Requirements

Establishing an effective cybersecurity programme requires mapping security controls to the particular needs of an organisation. It ensures that the implemented controls directly address the organization's specific risks, regulatory requirements, and operational needs (Tuffley & Griffith University, 2024). This method reduces the risk of breaches while enhancing overall security and ensuring compliance with industry standards and regulations.

Equifax could have done a comprehensive risk assessment according to their business environment. This would have identified critical areas where security measures were most needed, such as protecting against known vulnerabilities like Apache strut. Equifax could have ensured continuous monitoring, enforced stricter access controls, and prioritised essential updates by mapping security controls to these specific risks.

Recommendations

- Incident Response: A comprehensive incident response will minimise the impact in case of a data breach
- Vulnerability Management: A vulnerability management plan will allow the organisation to track vulnerability and minimise the attacks
- Patch Management: Regular patch management will ensure critical vulnerabilities are patched.
- Control Alignment: Map security control according to the organisation's business environment and specific risks.

Conclusion

The Equifax breach highlights the need for mapping controls according to the organisation's requirements. Implementing the recommendation provided will help Equifax strengthen its security measures and help prevent future incidents.

References

- Wikipedia. (2020, August 2). *2017 Equifax data breach*. Wikipedia. https://en.wikipedia.org/wiki/2017_Equifax_data_breach
- IBM. (2024). *What is NIST Cybersecurity Framework? | IBM*. Www.ibm.com. https://www.ibm.com/topics/nist
- Tuffley, D. & Senior Lecturer, School of ICT. (n.d.). Cyber Security Risk Management Workshop Exercises. In *7019ICT Cyber Security Risk Management* (pp. 1–10). https://lms.griffith.edu.au/courses/24368/files/6212950?wrap=1
- Tuffley, D. & Griffith University. (2024). 7019ICT Cyber Security Risk Management. In *COURSE NOTES*. https://lms.griffith.edu.au/courses/24368/files/6212968?wrap=1
- *CIS Control 2: Inventory and Control of Software Assets*. (n.d.). CIS. https://www.cisecurity.org/controls/inventory-and-control-of-software-assets
- *CIS Control 4: Secure Configuration of Enterprise Assets and Software*. (n.d.). CIS. https://www.cisecurity.org/controls/secure-configuration-of-enterprise-assets-and-software
- *CIS Control 7: Continuous Vulnerability Management*. (n.d.). CIS. https://www.cisecurity.org/controls/continuous-vulnerability-management

Module 5: Workshop Exercise Write-up

Colonial Pipeline Ransomware Attack

Introduction

In May 2021, a U.S. fuel pipeline operator, Colonial Pipeline was hit by a major ransomware attack by a group named DarkSide which disrupted the fuel supplies across the East Coast. The attackers were able to compromise the network due to no MFA enabled on an employee VPN account. This led the Colonial Pipeline to pay $4.4 billion to recover some of its data(WALLIX, 2023).

Authentication and Authorisation Failures

The colonial pipeline failed to provide authentication for the employees to use their VPN. Authentication like MFA or Cryptographic authentication would have prevented the attacker from gaining unauthorised access to the system even after compromising the password. The absence of an authorization mechanism like least privileges or RABC would have stopped the attacker from moving within the network after the initial access.

A strong authentication mechanism like MFA, would have reduced the risks of any unauthorised access. This adds an extra layer of protection which makes it difficult for any attacker to gain access from a compromised password. If the Colonial pipeline had enabled MFA and the least privilege mechanism the attack would have been detected and prevented at an earlier stage.

Identity and Access Management (IAM) System

IAM systems provide a centralised platform for controlling user access within an organisation and ensuring that the appropriate users can access resources at the right time. The benefit of using the IAM system is that it enables the organisation to implement RBAC or PAM, which ensures only authorised users have control of the critical systems, reducing the risk of insider threat and ensuring compliance with regulatory requirements(Tuffley & Griffith University, 2024).

A system should use features of IAM like Single Sign-On for easy access to the system without having to log in again, RBAC which ensures that the user has access to the file according to the job roles and PAM which manages access to sensitive systems and resources and prevents unauthorised access

Privileged Access Management (PAM)

PAM helps the organisation to implement strict control and monitoring mechanisms which ensures privileged access is granted to the authorised individual for a specific take and for a limited time. This minimises the impact that can be caused by compromised accounts (Tuffley & Griffith University, 2024).

Colonial Pipeline could have implemented the following practices (Tuffley & Griffith University, 2024)

- Least privilege enforcement: It minimises the user access to the systems and data according to their roles.
- Session Monitoring and Recording: It monitors all the activities performed by the user with elevated privileges, allowing for audit and forensic analysis if needed.
- Credential Management: It helps in managing privileged credentials by rotating the credential, to reduce the risk of password theft or misuse.

Role-Based Access Control (RBAC)

RBAC would have limited attacker access by authorization, roles and privileges which is the core of the RBAC. This concept limits the attacker's access by defining roles and therefore restricts attackers' access levels associated with the compromised roles. The attacker could thus only use the resources to carry out actions made possible by that role. RBAC reduces the scope of what the attacker can access and do by establishing roles according to employee duties and restricting privileges to those required for each role. This effectively reduces the attack's overall impact. (*AIX 7.3*, 2023)

Recommendations

- Implement MFA: To enforce MFA in all systems and should be made must for any remote access.
- Implement RBAC: RBAC will ensure access permissions are controlled and aligned with the job roles
- Adopting IAM: It will ensure authorised users have access to critical systems, thus reducing the risk of breach.
- Implement PAM: It will help the organisation to have strict control and monitoring mechanisms.

Conclusion

The Colonial Pipelines ransomware attack highlights the importance of authentication and authorization in protecting critical infrastructure from cyber threats. Implementing the recommendation provided will help the Colonial Pipelines strengthen its security measures and help prevent future breaches.

References

- WALLIX. (2023, September 25). *What Happened in the Colonial Pipeline Ransomware Attack*. WALLIX. https://www.wallix.com/what-happened-in-the-colonial-pipeline-ransomware-attack-2/
- *AIX 7.3*. (2023, November 3). Ibm.com. https://www.ibm.com/docs/en/aix/7.3?topic=control-elements-rbac
- Tuffley, D. & Griffith University. (2024). 7019ICT Cyber Security Risk Management. In *COURSE NOTES*. https://lms.griffith.edu.au/courses/24368/files/6212968?wrap=1

Beginning of Checkpoint B

Module 6: Workshop Exercise Write-up

THE MEDIBANK PRIVATE DATA BREACH

Introduction

In October 2022, a Russian hacker Aleksandr Ermakov gained unauthorised access to Australia's largest health insurer, Medibank Private. The hacker demanded a ransom, threatening to release millions of customers' personal information, including names, addresses, dob, medical diagnoses, and credit card details if their demands were unmet. This incident severely affected Medibank's reputation and weakness in its cybersecurity measures (Turnbull, 2024).

Cryptography and Encryption Techniques

Medibank's encryption procedures were insufficient to prevent unauthorised access and protect customer data. The cryptographic technique used by Medibank has not been revealed but the breach occurred due to a misconfigured firewall for which a separate digital security certificate was not required. This vulnerability allowed hackers to exploit stolen credentials from a third-party IT provider, exposing Medibank's weaknesses in access control measures and firewall configurations (Siganto, 2024).

Medibank could have used strong encryption techniques like AES-256 which provides a high level of security. AES-256 is mostly used by organisations that handle sensitive data and even if the attacker breaches the network, the data would remain secured and unusable without the appropriate decryption key.

Public Key Infrastructure (PKI)

PKI is essential for securing sensitive data as it is used to verify digital certificates and public-private key pairs. PKI protects communication and transactions over insecure networks by verifying the identities of the parties and guaranteeing the integrity and confidentiality of the exchanged data (Tuffley & Griffith University, 2024).

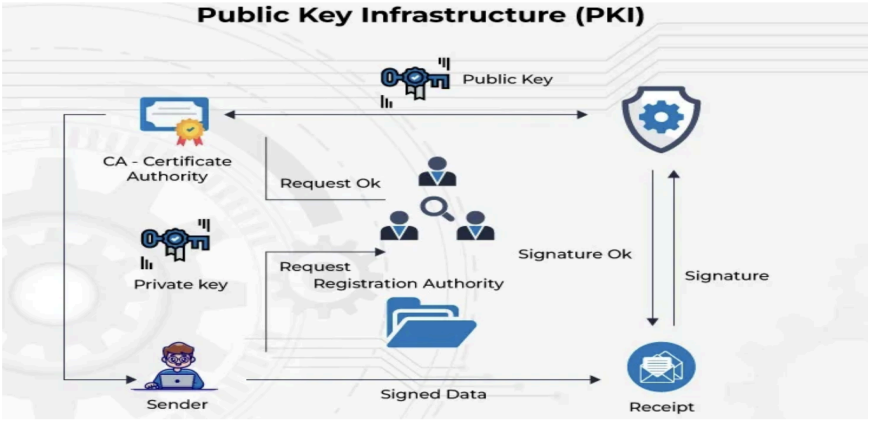

Fig. PKI workflow (SignMyCode, 2023).

Medibank could have used PKI for:

- Strong Authentication: MFA can be implemented by generating digital certificates for mobile devices, these certificates can be used in addition to passwords to strengthen employee's account security.
- Secure code signing: Code signing uses digital certificates issued by a Certificate Authority to verify the software being deployed this could have helped Medibank by ensuring the integrity and authenticity of the software applications used within its network (SignMyCode, 2023).

Data Privacy Regulations (GDPR, Privacy Act)

The GDPR is a set of rules that regulates data protection implemented by the European Union in 2018. Its goal is to protect people's right to privacy and personal information inside the European Union and the European Economic Area. If Medibank had EU customers and failed to comply with GDPR, regarding personal data protection and breach notification

Fig. 10 Key GDPR Requirements (Bhatia, 2023).

within 72 hours, the organization could have faced a fine of up to 4% of its annual global revenue for GDPR non-compliance. Similarly, the Privacy Act protects people's rights but applies to personal information maintained by federal agencies but does not directly regulate the private sector (Tuffley & Griffith University, 2024). According to the Australian Information Commissioner, Medibank violated the Privacy Act 1988 by not protecting the personal information of 9.7 million Australians, resulting in a fine of up to $2.22 million per contravention (Australian Information Commissioner, 2022).

Data Protection Controls and Compliance

To prevent future breaches Medibank should include:

- Technical control: Medibank should ensure all the sensitive data are **Encrypted** using AES-256 which has resistance to brute force attack. Medbank should also implement **Access Controls** like RBAC to restrict data access on the principle of least privileges. Medibank should have a plan for **Incident response and breach notification** for detecting, responding and reporting to the data breach (Tuffley & Griffith University, 2024).
- Organisation Measures: Medibank needs to develop clear policies and procedures to protect customer data. **Security awareness and training** are critical for the employees to recognise any phishing attempts. Medibank should impose **Data masking and anonymization** in their organisational measures To hide or remove personally identifiable information (PII) from data, ensuring the privacy of the data while allowing appropriate data use (Tuffley & Griffith University, 2024).

Conclusion

Medibank's Private data breach highlights the importance of having solid data protection measures in place, especially for organizations handling sensitive health information. Implementing the recommended technical and organisational controls provided will help Medibank Private strengthen its security measures and help prevent future incidents.

References

- Turnbull, B. T. (2024, January 23). *Medibank hack: Russian sanctioned over Australia's worst data breach*. https://www.bbc.com/news/world-australia-68064850
- Siganto, J. (2024, May 9). Medibank Data breach Litigation: An update | Privacy 108. *Privacy108 | Australian Data Privacy & Security Consulting*. https://privacy108.com.au/insights/medibank-data-breach-litigation-update/
- Tuffley, D. & Griffith University. (2024). 7019ICT Cyber Security Risk Management. In *COURSE NOTES*. https://lms.griffith.edu.au/courses/24368/files/6212968?wrap=1
- SignMyCode. (2023, August 21). What is Code Signing with Public Key Infrastructure (PKI)? *Medium*. https://medium.com/@signmycode/what-is-code-signing-with-public-key-infrastructure-pki-3c60843c559e
- Bhatia, P. (2023, November 27). *10 key GDPR requirements: A short summary*. Advisera. https://advisera.com/articles/a-summary-of-10-key-gdpr-requirements/
- Australian Information Commissioner. (2022). *Medibank civil penalty action*. https://www.oaic.gov.au/__data/assets/pdf_file/0029/228980/Medibank-civil-penalty-action-overview-infographic.pdf

Module 7: Workshop Exercise Write-up

The OPTUS DATA BREACH

Introduction

In September 2022, a major Australian telecommunication company, Optus, suffered a data breach through an unprotected publicly exposed API that exposed sensitive customer data, including names, dates of birth, addresses, phone numbers, and, in some cases, identity document numbers. This incident raised concerns about identity theft and fraud, and questions about Optu's effectiveness in network and application security.

Network Security Measures

The main cause for the Optus data breach was an open API with no username and password which was accessible to anyone over the internet. Optus's existing security measures such as a firewall can block unauthorised access based on a set of rules. Still, the firewall cannot prevent the vulnerability within the application, in the case of API. IDS/IPS monitors the networks to detect and prevent any potential attack, it may have failed to detect the attack due to an inadequate match of attack signatures or anomalous activities. Vpn is a secure communication channel that acts as a tunnel between remote locations and does not protect against internal application vulnerabilities (Tuffley & Griffith University, 2024).

Strong Network security controls like Web application firewalls could have blocked any malicious request by continuously monitoring HTTPS traffic between the API and external network (Chávez, 2024).

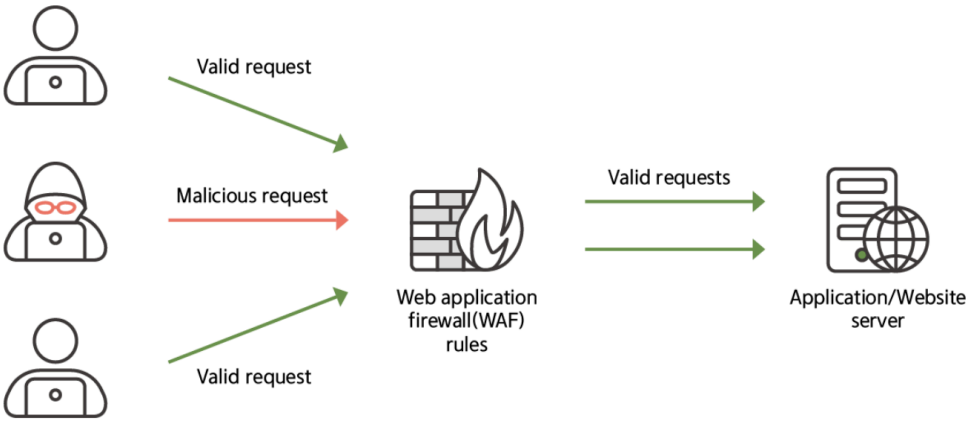

Fig. WAF in action (AIONCLOUD, 2024)

Optus could have used an IDS/IPS system with better anomaly detection which could have helped to find any malicious attacks.

Network Segmentation

Network segmentation divides a larger network into smaller zones. This is done by using network technology such as VLAN, firewalls and ACL. Network Segmentation helps to limit the spread of threats by containing the threats in a specific segment. Segmenting networks into zones with varying levels of access control could restrict the attacker's movement within the network. Network Segment also helps to separate sensitive resources on dedicated network zones with strict access controls, which reduces the risk of unauthorised access (Tuffley & Griffith University, 2024).

If Optus had employed network segmentation effectively, it could have limited the attacker's access to the customer data. For example, placing customer data in a higher restricted zone can prevent attackers from accessing it, even gaining access through API and containing the attack in one network segment.

OWASP Top 10 Web Application Security Risks

The OWASP Top 10 is essential for organisations to understand the most common web application security threats. In the Optus data breach vulnerability from OWASP top 10 likely played a role. Vulnerability like **Broken Access Control** and **Insecure Design** contributed to the breach, as the API was exposed without protection, making it vulnerable by design and the API lacked proper authentication which allowed anyone to access sensitive data. To prevent future breaches Optus can use security practices like **Secure Authentication and Authorization** to ensure only authorised individuals can access the API, using **Secure Communication** protocols like TLS can help to implement a secure channel for data transmission and having **Code Reviews and Security Testing** can help to identify and address security vulnerabilities. (Tuffley & Griffith University, 2024).

Recommendations

To improve security Optus must implement a combination of technical and organisational measures:

Technical controls :

- WAFS: Implementing WAF can help filter out the incoming API traffic and block malicious requests.
- Network Segmentation: Network segmentation can help prevent access to sensitive data and lateral movement.
- API security Project: Regular reference to OWASP tAPI security project can help to identify API vulnerabilities (Kost, 2023).

Organisational measures:

- Conduct regular Audit: To find vulnerabilities review security posture regularly.
- Employee Security Training: To provide a training program on OWASp top 10 and include security coding.

- Access Control Management: Having access control reviewed and updated regularly for the employees to maintain the principle of least privilege.

Conclusion

In conclusion, for telecommunications companies like Optus, strong network and application security is essential to protect sensitive customer data. Implementing the recommendation provided will help Optus to strengthen its security measures and help prevent future incidents.

References

- Tuffley, D. & Griffith University. (2024). 7019ICT Cyber Security Risk Management. In *COURSE NOTES*. https://lms.griffith.edu.au/courses/24368/files/6212968?wrap=1
- Chávez, J. C. (2024, March 18). *Why does WAF matter in API security?* Traefik Labs: Say Goodbye to Connectivity Chaos. https://traefik.io/blog/why-does-waf-matter-in-api-security/
- AIONCLOUD. (2024, April 18). *WAF vs WAAP, Importance of API Security*. Cloud-Based Platform AIONCLOUD. https://www.aioncloud.com/waf-vs-waap-importance-of-api-security/
- Kost, E. (2023, August 4). *How to Avoid a Disaster Like the Optus Breach | UpGuard*. Www.upguard.com. https://www.upguard.com/blog/how-to-avoid-a-disaster-like-the-optus-breach

Module 8: Workshop Exercise Write-up

THE UBER DATA BREACH

Introduction

In 2016, Uber suffered a data breach that exposed the personal information of 57 million users. The attacker gained access to the Uber system by stealing login credentials for an AWS account, which allowed the attacker to download sensitive data. Uber tried to cover up the breach by paying a $100,000 ransom but the incident got exposed to the public, leading to reputational damage (Gopal, 2023).

Security Operations Center (SOC)

The SOC plays an important role in threat detection and incident response. Uber's SOC failed in several areas, including real-time monitoring and log analysis which are core SOC responsibilities. The SOC is required to continuously monitor the organisation network and detect any unusual activity in the system. Uber can improve its SOC capabilities by implementing **Enhanced Real-Time Monitoring,** here Uber needs to continuously monitor the AWS services to detect suspicious activity and utilise SIEM and XDR tools to provide better threat detection and faster response time. A robust **Log Management** system will help to identify anomalous patterns which could be analysed to detect threats at an earlier stage (IBM, 2023).

Security Information and Event Management (SIEM)

SIEM is designed to collect and analyse security-related data from sources such as firewalls, network devices and servers to identify threats and provide the security team with useful insights. The SIEM system also uses advanced analytics which includes rule-based correlations to identify anomalies and provide alerts for any unusual activities (Tuffley & Griffith University, 2024).

Uber could have leveraged SIEM to detect the breach by combining high and low fidelity which refers to the amount of context that a security alert provides. Using these alerts can help Uber's security team with better observation of the environment and attack surface which enables them to detect and respond to the breach at an earlier phase (Bains, n.d.-b).

Incident Response Planning and Execution

An IR plan defines the process and procedure that an organisation will take to detect and respond to cyber-security breaches. An effective IR plan minimises the

impact of security incidents and protects an organisation's assets and reputation (Tuffley & Griffith University, 2024). Uber's IR plan failed, both in terms of detection and recovery. The company delayed reporting the breach and also violated the terms by paying the attackers without proper legal disclosure. Uber could have used NIST SP 800-61 IR plan and execution which focuses on preparation, detection and containment of the threat. NIST focuses on continuous improvement which could help Uber learn from the incident and strengthen its defences for the future (Vaishnav, 2024).

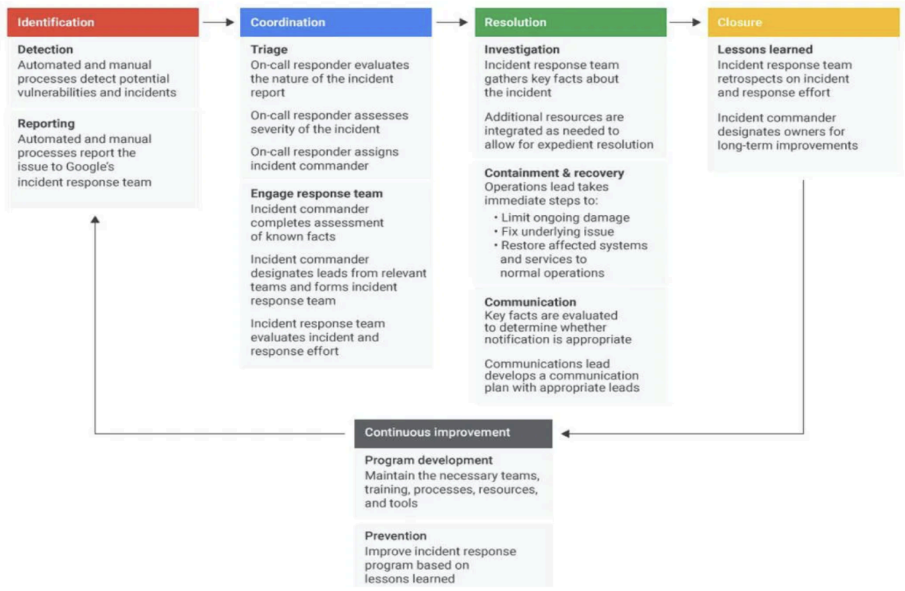

Fig. NIST IR Plan (Vaishnav, 2024)

Digital Forensics and Evidence Handling

Digital Forensics involves analysis, and interpretation of digital evidence related to the attack which helps the organisation to identify the point of entry, trace the attacker's steps and determine what data got compromised. Forensics ensures that the evidence is properly documented, transported, and stored, maintaining its integrity for legal action against the attacker. Digital forensics helps the organisation to learn from the incident and enables them to strengthen their security for future incidents (Tuffley & Griffith University, 2024). Uber could have used digital forensics to trace the attacker’s path, which involves looking through network activity and system logs to identify which data was compromised and how access was obtained. This would have provided important evidence for legal action and future security improvements.

Recommendations

Uber can improve their security measures by implementing:

- **NIST SP 800-61** for incident response to ensure structured planning, detection, and recovery from incidents.
- **Continuous real-time monitoring** using advanced SIEM and XDR solutions to detect threats across internal and third-party services
- **Log management and analysis** to detect anomalies and combine the data with high and low-fidelity alerts for faster incident detection and response.

Conclusion

In conclusion, Uber's data reach shows the importance of a robust SOC and an effective incident response plan. Implementing the recommendation provided will help Uber strengthen its security measures and help prevent future incidents.

References

- Gopal, R. V. (2024c, August 14). Uber Data Breach of 2016 : Exposes data of 57 million drivers and users. *Medium*. https://medium.com/thedeephub/uber-data-breach-of-2016-exposes-data-of-57-million-drivers-and-users-1b003924f2a
- IBM. (2023). *What is a Security Operations Center (SOC)?* Www.ibm.com. https://www.ibm.com/topics/security-operations-center
- Bains, H. (n.d.-c). How to reduce the impact of a data breach with SIEM. *Defense.com™*. https://www.defense.com/blog/reduce-data-breaches-with-siem
- Tuffley, D. & Griffith University. (2024). 7019ICT Cyber Security Risk Management. In *COURSE NOTES* https://lms.griffith.edu.au/courses/24368/files/6212968?wrap=1
- Vaishnav, D. (2024, June 30). NIST SP 800–61 Incident Response Life Cycle explained. *Medium*. https://medium.com/@divyesh.vaishanv/nist-sp-800-61-incident-response-life-cycle-explained-b7b63372cd3c

Module 9: Workshop Exercise Write-up

THE TARGET DATA BREACH

Introduction

In 2013, a major U.S. retailer, Target suffered a massive data breach, resulting in the theft of payment card data from approximately 40 million customers. The breach was initiated through compromised vendor credentials, allowing attackers to install a custom "BlackPos" malware on Target's POS system which captured card data as it was swiped during transactions. This breach highlighted several vulnerabilities in Target's security measures(Gopal, 2024a).

PCI DSS Compliance

Target failed to comply with many PCI DSS requirements at the time of the breach, contributing to the attacker's success. Target did not follow **Requirement 2** which enforces the change of default usernames and passwords in the system, attackers exploited default administrative credentials i.e. **"Best1_user"**, and **"BackupU$r"** to gain control over the network. Approximately 40 million card data was stolen because **Requirement 4** was not met as the Card data collected by the POS system was stored in plain text format, which violates the PCI DSS's encryption requirements for data in transmission (Consultant, 2014b).

Target used FireEye software for security monitoring, which alerted staff about the malware detection, but no action was taken. Target failed to comply with **Requirement 10,** where Target's security team was unable to respond effectively and violated the requirement for continuous monitoring and logging (Gopal, 2024a).

Critical Infrastructure Security Standards

Critical Infrastructure Security principles like NERC-CIP and AESCSF focus on protecting organisations from cyber threats, these principles are important for retail organizations like Target. Critical security standards focus on protecting the systems through network segmentation, access controls, and incident response. Complying with the standards, organisations can enhance their cyber resilience, and maintain the trust and confidence of stakeholders and the public they serve (Tuffley & Griffith University, 2024).

Adhering to such standards could have helped Target by:

- **Network Segmentation:** Target failed to separate its assets from other parts of the network, which made it possible for an attacker to take advantage of this vulnerability. Target could have followed NERC CIP which emphasizes isolating critical systems from less secure areas (Shu et al., 2014).

- **Access control:** Limiting third-party access to critical systems would have minimised the breach's impact. The target could have followed AESCSF principles such as least privilege and RBAC to reduce access (Ross, 2024).

Zero Trust Security Model

The Zero Trust Security Model operates on the principle of "never trust, always verify", which means everything within the network scope is trusted and everything outside is untrusted. It treats all the users and devices as a threat and applies strict access controls and verifications. The target could have implemented the principle of zero trust security (Tuffley & Griffith University, 2024):

- **Least Privilege Access:** If Target had implemented the least privilege access, the third-party vendor would have had minimal access, which would have reduced the attacker's ability to exploit vendor credentials and use them to move through the network
- **Micro-Segmentation**: Dividing the network into smaller segments would have isolated Target's POS system from the rest of the network, preventing attackers from moving laterally across the network.
- **Encryption:** Encrypting card data both at rest and in transit would have protected sensitive information from being stolen by attackers, even if they managed to exploit the network.

Recommendations

To improve security Target must implement a combination of technical and organisational measures:

Technical Controls:

- **Tokenization**: Replacing sensitive customer data with irreversible tokens could have reduced the damage caused by the breach. Tokenization limits the value of stolen data, making it useless to attackers (Shu et al., 2014).
- **Network Segmentation:** Isolate critical systems (like POS) to prevent lateral movement of attackers.

Organisations control:

- **Third-Party Risk Management:** Enforce strict security standards for vendors and regularly audit their controls.
- **Security Awareness Training:** Conduct regular employee and vendor training to prevent future breaches and make them aware of the Zero Trust model.

Conclusion

In conclusion, retail companies like Target need to adopt sector-specific standards to prevent future breaches. Implementing the recommended security measures will significantly strengthen Target's defences, and reduce the risk of future breaches.

References

- Gopal, R. V. (2024a, August 14). Complete case study — Target data breach - The deep hub - medium. *Medium*. https://medium.com/thedeephub/complete-case-study-target-data-breach-2-ba4bb365a82e
- Consultant, I. G. (2014b, February 11). *The target breach and the PCI DSS*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/the-target-breach-and-the-pci-dss#:~:text=However%20it%20is%20apparent%20that,will%20never%20provide%20total%20security.
- Tuffley, D. & Griffith University. (2024). 7019ICT Cyber Security Risk Management. In *COURSE NOTES*. https://lms.griffith.edu.au/courses/24368/files/6212968?wrap=1
- Shu, X., Tian, K., Ciambrone, A., Yao, D., & IEEE. (2014). Breaking the Target: An analysis of target data breach and lessons learned. In *IEEE* [Journal-article]. https://people.cs.vt.edu/danfeng/papers/Target-Yao-unpublished.pdf
- Ross, J. (2024, July 18). *Securing Australia's Critical Infrastructure | Cybersecurity Framework and Regulations Compliance | Saviynt | SOCI*. Saviynt.com. https://saviynt.com/blog/securing-australias-critical-infrastructure

Module 10: Workshop Exercise Write-up

CYBERSECURITY SKILLS GAP AT CYBERDEFEND INC.

Introduction

A cybersecurity firm, CyberDefend Inc., faces a skill gap that affects its ability to attract and retain qualified cybersecurity professionals, while current employees struggle to keep up with the evolving threat landscape. This gap hinders CyberDefend's ability to deliver effective services and remain competitive in the market.

Cybersecurity Capability Maturity Assessment

Essential Eight frameworks will be used to evaluate CyberDefend capabilities which are based on the maturity of ACSC mitigation strategies that deal with important areas such as restricting administrative privileges, patching applications, and MFA. The Essential Eight Maturity Model defines three maturity levels for each strategy i.e. Partially Adhered (Maturity Level 1), Largely Adhered(Maturity Level 2), and Fully Complied(Maturity Level 3). By addressing the maturity level for each strategy, CyberDefend can reduce the risks of cyber threats and build up a strong cybersecurity foundation according to their business needs. CyberDefend can use the maturity model to improve its **Structured Approach** to access and improve cybersecurity practices, **Benchmarking** the company security against industry standards, this creates a roadmap for **Continuous Improvement**, that ensures the organisation stays aligned with best practices and regulatory requirements (Tuffley & Griffith University, 2024).

Career Development Plan

A well-structured career plan development plan is essential for closing the skills gap at CyberDefend and ensuring the employees can grow within the company and stay aligned with the industry standards. Cybersecurity professionals can demonstrate their knowledge and expertise by pursuing industry-recognised certificates. In addition to the certificates, Cybersecurity professionals can uplift their career opportunities by going to networking events, cyber conferences, and online communities. Each participant shares their knowledge and skills to stay updated on the latest trends. These events and certificates can boost the self-confidence of an individual and motivate them to learn new skills continuously (Tuffley & Griffith University, 2024).

Some industry-recognised certificates CyberDefend employees can acquire (Admin, 2024):

- **OSCP:** Employees who want to deepen their technical skills in penetration testing and offensive security techniques can acquire this certificate.

- **CISM**: Employees who want to advance their understanding of organizational information security management can acquire this certificate.

Many certificates in the field of cybersecurity can be pursued by the employees in the interest of their domains.

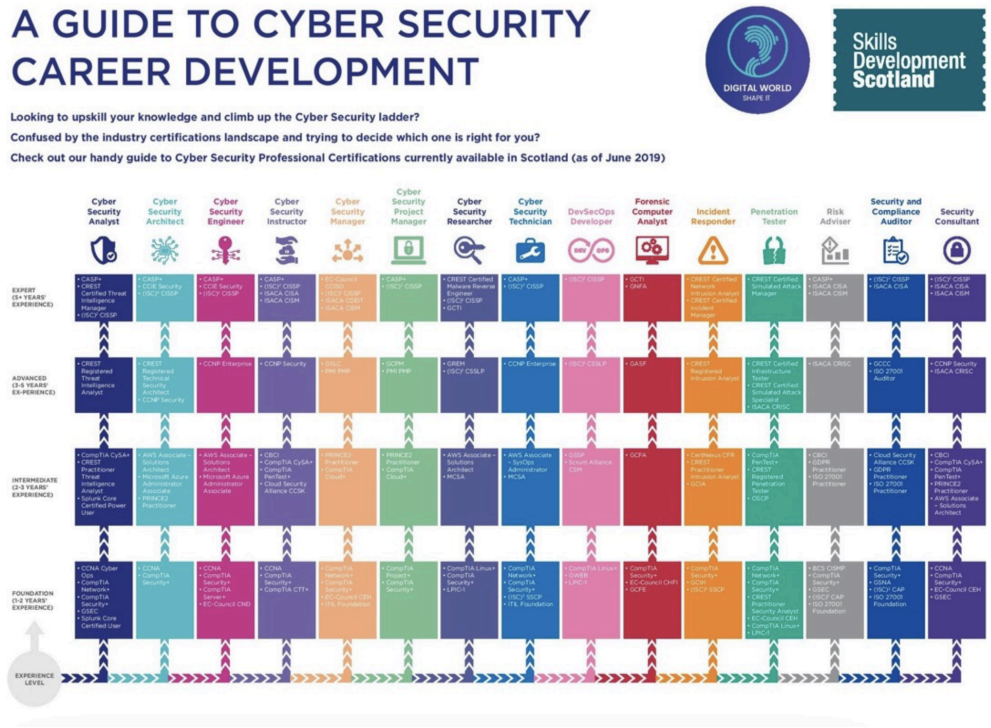

Fig. Roadmap for Career Development (Admin, 2024)

Ethical Considerations and Professional Codes of Conduct

Ethical considerations are important in cybersecurity, as professionals often access databases and possess the tools and knowledge that could cause significant harm if misused. Employees at CyberDefend must adhere to strict ethical guidelines to ensure the integrity, responsibility, and trustworthiness of the services they provide. Cybersecurity professionals can follow the **CIA Triad** to protect data confidentiality, integrity, and availability, **Responsible Disclosure** ensures vulnerabilities are reported responsibly before public disclosure, The **(ISC)² Code of Ethics** and **SANS Code of Ethics** guide professionals to act honorably, maintain technical excellence, and protect society's digital assets, ensuring trust and security. Employees can show their commitment to ethical practices, and contribute to a more secure and responsible digital landscape by upholding the ethical principles (Tuffley & Griffith University, 2024).

Strategies for Attracting and Retaining Talent

CyberDefend can use the following strategies for attracting and retaining qualified cybersecurity professionals (Delanoche, 2024):

- **Offer Competitive Compensation**: To ensure salaries and benefits are competitive with industry standards, and include incentives like certification reimbursements.
- **Flexible Work Arrangements**: Employee's work-life balance can improve by having remote work options and flexible schedules.
- **Enhance Engagement Opportunities**: Providing continuous professional development through training, certifications, and career growth programs can motivate employees to learn new skills.
- **Foster a Safe and Inclusive Culture**: Create a diverse and inclusive workplace by promoting fairness, equity, and diversity in hiring and leadership roles, and ensuring employees feel valued and respected.

Conclusion

In conclusion, CyberDefend must address its skills gap to maintain competitiveness. Implementing the recommended career development strategies, adhering to ethical standards and enhancing recruitment efforts will significantly strengthen CyberDefend's capabilities to deliver effective services and remain a competitive edge in the market.

References

- Tuffley, D. & Griffith University. (2024). 7019ICT Cyber Security Risk Management. In *COURSE NOTES*. https://lms.griffith.edu.au/courses/24368/files/6212968?wrap=1
- Admin. (2024, June 17). *Certifications that can boost a Cybersecurity Leader's Career*. Consultia. https://www.consultia.co/certifications-that-can-boost-a-cybersecurity-leaders-career/
- Delanoche, R. (2024, June 4). *8 Effective Strategies for attracting and retaining top cybersecurity talent*. Cyber Security District. https://www.cybersecuritydistrict.com/8-effective-strategies-for-attracting-and-retaining-top-cybersecurity-talent/