Assaignement 2 Enterprise Security Portfolio Activities

Bachelor of Science | Cybersecurity Y89 | Enterprise Security and Governance

**Student :** Marco Cavani - 20003546

**Lecture:** Mohi addasd

# W1-T1: Enterprise Security Definition

Enterprise security refers to the strategies, processes, and technologies that organizations implement to protect their assets, such as data, intellectual property and physical infrastructure, from unauthorized access, theft, or damage. Enterprise security also incorporates various aspects of security, including cybersecurity, access control, and risk management (Khadraoui & Herrmann, 2007, p. 262). The ultimate goal is to mitigate security risks and ensure the confidentiality, integrity, and availability of critical resources (Ahmed et al., 2022b, p. 175). Enterprise security is often applied following the business needs offering a customized layer of protection especially in large organizations where the budget covers the cost of the analysis (Ahmed et al., 2022b, p. 64).

# W1-T2 Why should enterprises focus more on cyber security?

**Increasing Threat Landscape:** with the growing digitalization of businesses, the threat landscape is greater today than in the past, cyber threats are also evolving to become even more sophisticated and frequent (Fortinet, 2021). According with The Australian Cyber Security Centre (ACSC) and the Australian Signals Directorate (ASD) (2022), cyber-attacks registered in Australia during the 2021–22 financial year are almost 13% greater compared with the previous financial year.

**Disclosure Obligation:** Business leaders may be called upon to disclose cybersecurity risks and cyber incidents in a variety of situations, for example: after a cyber-incident or if the data stored represents material risks that could result in vast money lost and disruption of services (Press & Australian Security and Investment Commission (ASIC)), 2022).

**Reputational Damage:** A cybersecurity breach can seriously damage a company's reputation and erode customer trust. A study by IBM found that the average cost of a data breach includes not only the direct financial impact, but also the loss of equity in customers and brands (IBM, 2021).

W1-T3: Why Governance is important for cyber security even for small and medium enterprises?

Governance provides Small-Medium Size enterprises (SMEs) with a framework to establish clear lines of accountability and responsibility for cybersecurity. It also enables SMEs to comply with legal requirements and manage cybersecurity risks. According to a report by the National Institute of Standards and Technology (NIST), cybersecurity governance frameworks help SMEs identify, assess, and manage cybersecurity risks effectively (NIST, 2018). The Structure of a cyber-security framework for a SME can cover different layers of security such as processes and policies that comply with standards, regulations, network security and asset protection (Emer et al., 2021). According with The Australian Cyber Security Centre (ACSC) and the Australian Signals Directorate (ASD) (2022) the most impacted businesses within Australia during 2021-22 financial year were medium enterprises who tend to be less vigilant compared to larger corporations (The Australian Cyber Security Centre (ACSC) & the Australian Signals Directorate (ASD), 2022). According with NIST case 4 case-study on Small Enterprises (*Hotel CEO Finds Unwelcome Guests in Email Account*, n.d.) we can determinate that small businesses can avoid risks that can potentially cause harms by embracing cybersecurity. In conclusion, governance is important for medium and small enterprises as it could potentially save businesses from possible disasters providing them guidance on how to protect, mitigate or recover from cyber-attacks.

# W1-T4: Now in the event of a Ransomware attack on any of the small organizations, who should be responsible for the damages and why?

In the event of a ransomware attack on small organization that uses Second Dragon software solutions, the responsibility for the consequences of a cyberattack may be shared between the two parties. In fact, both parties should comply with common practice, guideline, and security frameworks such as ISO 27000, ISO 27001 and NIST. The user of the software should be responsible for ensuring that appropriate security measures are in place, such as cyber security awareness training, strong password policies and regular backups to prevent and mitigate cyber-attacks. Whereas Dragon Software should ensure that their products are well maintained, updated, and optimized to reduce cyber threats. Ultimately, the responsibility for damages may depend on the specific circumstances of the attack and the contractual agreements between the two parties (Australia Cyber Security Service Centre, n.d.)

W1-T5: Identify the similarity and dissimilarity between ISO 27001 and NIST CSF.

ISO 27001 and National Institute of Standards and Technologies (NIST CSF) are two well-known information security frameworks that provide guidance for managing and enhancing cybersecurity programs.

# W1-T5: Identify the similarity and dissimilarity between ISO 27001 and NIST CSF

**Similarities:** Both frameworks promote a risk-based approach to information security management. ISO 27001 requires organizations to conduct a risk assessment as part of the Security management System (ISMS) implementation process (ISO, 2005), while NIST CSF's risk management framework is a key element of its approach to cybersecurity (NIST, 2018). Both frameworks emphasize the importance of monitoring and measuring security controls. ISO 27001 mandates regular monitoring and measurement of the Information Security Management System’s performance (ISO, 2005), while NIST CSF's continuous monitoring process involves ongoing measurement and analysis of security-related activities (NIST, 2018). Additionally, they both address key components of a comprehensive security program, including asset management, access control, and incident response.

**Dissimilarities:** ISO 27001 is a standard, while NIST CSF is a framework. ISO 27001 provides a specific set of requirements for implementing an ISMS, while NIST CSF is a flexible set of guidelines that organizations can adapt to their specific needs (NIST, 2018). ISO 27001 is focused on confidentiality, integrity, and availability (CIA) of information assets (ISO, 2005), while NIST CSF focuses on five core functions: identify, protect, detect, respond, and recover (NIST, 2018). ISO 27001 is more prescriptive than NIST CSF, specifying detailed requirements for policy development, risk assessment, and incident management (ISO, 2005). NIST CSF, on the other hand, is more flexible, allowing organizations to tailor the framework to their specific needs (NIST, 2018).

In summary, both ISO 27001 and NIST CSF provide valuable guidance for organizations seeking to improve their cybersecurity posture, but they have different approaches and areas of focus. Organizations should evaluate their specific needs and requirements before selecting one or the other, or possibly using both in a complementary manner.

# W1 - Reference:

1. Ahmed, M., Moustafa, N., Barkat, A., & Haskell-Dowland, P. (2022a). Next-Generation Enterprise Security and Governance. CRC Press.
2. Australia Cyber Security Service Centre. (n.d.). Guidelines for Cyber Security Roles | Cyber.gov.au. Www.cyber.gov.au. <https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-cyber-security-roles>
3. Brooks, C. (2022, June 3). Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know. Forbes. <https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=14e8a4527864>
4. Emer, A., Unterhofer, M., & Rauch, E. (2021). A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises. In ieeexplore. <https://ieeexplore-ieee-org.ezproxy.ecu.edu.au/stamp/stamp.jsp?tp=&arnumber=9424999>
5. Fortinet. (2021). Global Threat Landscape Report. In https://www.fortinet.com (pp. 1–12). Fortinet. <https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-2h-2020.pdf>
6. Hotel CEO Finds Unwelcome Guests in Email Account. Retrieved February 24, 2023, from [https://www.nist.gov/system/files/documents/2020/09/30/Cybersecurity-Case-4.pdf](Hotel%20CEO%20https:/www.nist.gov/system/files/documents/2020/09/30/Cybersecurity-Case-4.pdf)
7. IBM. (2021). Cost of a Data Breach Study. Ibm.com. [https://www.ibm.com/security/data-breachMoney matters](https://www.ibm.com/security/data-breachMoney%20matters)
8. ISO. (2005). Information technology — Security techniques — Information security management systems — Requirements.
9. Khadraoui, D., & Herrmann, F. (2007). Advances in Enterprise Information Technology Security (p. 262). IGI Global.
10. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity.
11. Press, D., & Australian Security and Investment Commission (ASIC)). (2022). Cyber risk: Be prepared. Asic.gov.au. <https://asic.gov.au/about-asic/news-centre/articles/cyber-risk-be-prepared/>
12. The Australian Cyber Security Centre (ACSC), & the Australian Signals Directorate (ASD). (2022). ACSC-Annual-Cyber-Threat-Report-2022. [https://www.cyber.gov.au/. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022](https://www.cyber.gov.au/.%20https:/www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022)

# W2-T1 / W2-T2: Supplemental Document to Information Security Policy – Human Factor

|  |
| --- |
| **1.Disclaimer**  The security of company data and resources is a top priority. By adhering to these guidelines, employees can help to ensure that the company's information remains secure, and potential security risks are mitigated. Any violations of this policy may result in disciplinary action, up to and including termination. This document was written following NIST Cyber Security Framework (CSF) 2.0 and use the risk assessment to mitigate Human-Factor related cyber security threats.  **2.Introduction**  This supplemental document to the information security policy outlines the guidelines and best practices for the use of personal devices and social media accounts within the enterprise.  **3.Purpose**  The purpose of this document is to ensure that the company's data, network, and resources are protected from potential security threats.  **4.Scope**  The scope of the policy covers the appropriate use of employee self-phone, social media platform and access of company’s resources outside work area.  **5.Policy**  **5.1.BYOD (Bring Your Own Device)**   * Devices must be password-protected and encrypted to prevent unauthorized access to company data (Boeckl et al., 2022). * Devices must have up-to-date antivirus and anti-malware software installed (Boeckl et al., 2022). * Only authorized individuals may access company data on personal devices ((Boeckl et al., 2022)). * Devices must be registered with the company's IT department before they can be used for work-related tasks ((Boeckl et al., 2022)). * The company reserves the right to remotely wipe any device that is lost or stolen or that contains company data ((Boeckl et al., 2022)).   **5.2.Use of Personal Social Media Accounts**   * Employees must maintain separate personal and professional social media accounts (Etue, 2013). * Employees must not share any confidential or proprietary company information on their personal social media accounts (Etue, 2013).   Employees must adhere to the company's code of conduct when using social media, including but not limited to, avoiding discriminatory, harassing, or offensive content (Etue, 2013).  **5.3.Accessing Company’s Data Outside Work**   * Employees must not save any company data on personal devices (Greene, 2020). * Employees must log out of company accounts and disconnect from VPNs when finished with work-related tasks (Greene, 2020). * Employees must Enable Multi-Factor-Authentication to access company resources (Greene, 2020).   **6.Policy Compliance**  All employees are expected to comply with this supplemental document to the information security policy. Failure to comply with the policy may result in disciplinary action, up to and including termination. The company reserves the right to monitor employees' use of personal devices and social media accounts to ensure compliance with this policy. If an employee becomes aware of any violations of this policy, they must report it to their supervisor or the IT department immediately. Any unauthorized access, sharing, or dissemination of company information may result in legal action being taken against the employee. By adhering to this policy, employees can help to ensure the security of the company's data, network, and resources.  **Related Standards**  ISO 27000  NIST  **Terms and Definitions**  **BYOD:** refers to any employee’s personal device such as personal phone, tablet, computers as well as smart watch or any other smart objects that could potentially use at work. |

# W2-T3: What are the key strategies to address cyber-attacks launched by social engineering attacks especially via Facebook Marketplace?

Social engineering attacks are a common way for cybercriminals to gain access to sensitive information, and Facebook Marketplace is a popular target. The key strategies that could address cyber-attacks launched by social engineering attacks are:

* Educate people using their platforms and devices through appropriate cyber-security Awareness Training.
* Enache Multifactor Authentication using google authenticator on all devices.
* Strictly avoid exchanging images, documents, or URLs through Facebook Market place.

**Educate employees and users: Educating employees and users about the risks associated with social engineering attacks is critical. Ensure that all employees are trained on how to identify and avoid social engineering attacks, especially when using Facebook Marketplace. This could include training on how to spot phishing emails, how to recognize fraudulent Facebook Marketplace listings, and how to avoid clicking on suspicious links.**

**Use multi-factor authentication: Implementing multi-factor authentication can help protect user accounts from being compromised by social engineering attacks. By requiring an additional form of identification, such as a code sent to a user's phone, attackers are less likely to be able to gain access to sensitive information.**

**Monitor and respond to suspicious activity: Implementing monitoring tools that can identify and respond to suspicious activity is critical in identifying and stopping social engineering attacks. This could include monitoring for unusual login attempts, unusual activity on Facebook Marketplace listings, or suspicious links.**

**Limit user access: Limiting user access to sensitive information can help reduce the risk of social engineering attacks. This could include restricting access to certain Facebook Marketplace listings or limiting access to sensitive company information.**

**Implement security controls: Implementing security controls such as firewalls, intrusion detection systems, and anti-malware software can help protect against social engineering attacks launched via Facebook Marketplace. Regularly updating security controls and monitoring their effectiveness is also critical.**

**Report suspicious activity: Encourage employees and users to report any suspicious activity they encounter while using Facebook Marketplace. This could include reporting suspicious listings or messages, or reporting any unusual activity on their accounts. This can help identify and respond to social engineering attacks more quickly.**

**W2 - References**

* Boeckl, K., Grayson, N., Howell, G., Lefkovitz, N., Ajmo, J., McGinnis, M., F.Sandlin, K., Slivina, O., & Ward, P. (2022). Mobile Device Security: Bring Your Own Device (BYOD). In NIST (pp. 55–58). <https://www.nccoe.nist.gov/sites/default/files/2022-11/mdse-nist-sp1800-22-supplement-draft-2.pdf>
* Etue, D. (2013). SOCIAL MEDIA: LEVERAGING VALUE WHILE MITIGATING RISK. In *NIST*. <https://csrc.nist.gov/CSRC/media/Presentations/HIPAA-2013-Social-Media-Leveraging-Value-While/images-media/etue_day1_315_leveraging_social_media_while_mitigating_risk.pdf>
* Greene, J. (2020, March 18). Telework Security Basics. NIST. <https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics>