**Cyber Security Report**

HAN22070067

HAN22080144

HAN22080119

HAN22080358

HAN22080399

Introduction

Australian National University (ANU) is a national university locate in the capital of Australia. The first attack initiated in November 2018, leading to illegal access of the administrative system. Forensic evidence showed that high volumes of personal information were copied out of the systems. The estimated number of victims is over 200,000 people, including students and staff turned over during the past 19 years. In the following 8 domains, we will see what the role of each domain in cyber security is, and how each of them will benefit ANU, as well as the downsides when implemented.

Keywords: [Click here to add keywords.]

Contents

[Abstract 2](#_Toc139022270)

[6 primary domains 4](#_Toc139022271)

[Security & Risk Management 4](#_Toc139022272)

[Security Architecture & Engineering 6](#_Toc139022273)

[Communication & Network Security 8](#_Toc139022274)

[Identity & Access Management 9](#_Toc139022275)

[Security Assessment & Training 10](#_Toc139022276)

[Cyber operations 11](#_Toc139022277)

[2 secondary domains 12](#_Toc139022278)

[Asset Security 12](#_Toc139022279)

[Software Development Security 13](#_Toc139022280)

[**References** 14](#_Toc139022281)

# 6 primary domains

## Security & Risk Management

Security and Risk management refers to the systematic approach taken by business and organizations to evaluate risks, protect their assets and mitigate potential losses. In the context of this report, the focus of “assets” will be on information, more specifically: Sensitive Data.

The Federal Information Security Management Act (cited in Gantz and Philpott, 2013, p. 329) defines information security as “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to safeguard their confidentiality, integrity, and availability”. Security management focuses on measures to detect threats, protect data, mitigate loss, and respond to incidents. On the other hand, Risk management involves assessing and analyzing vulnerabilities’ impacts, and developing treatment. Together, Security & Risk Management can effectively develop policies, and guidelines with concise roles and responsibilities for organizations and individuals.

Within the context of ANU data breach, the main topics of discussion will be security control, risk mitigation, incident response, and compliance with laws and policies. As a result of maintaining a competent security system, ANU was able to mitigate damage and successfully regain control of compromised infrastructure. All sensitive data, including a part of personal information, were encrypted, and compressed. The system which stores said data was protected with scheduled maintenance and followed security policies. Also, the Information Security Office controls data access privileges of their employees and practices security training and awareness for all university members. Despite this, several employees, including one administrator-level privileged individual, fell for spearphishing attacks (a form of social engineering attack) as the result, the actor was able to access the network. In the worst-case scenario, ANU also had cyber insurance coverage, which covers defence cost, forensic services, and any possible damage to the organization, their employees, students, and alumni. The attack's aftermath shows that the organization had swift response during and after the incident. Another notable detail is that the Senior Management’s disclosure shows great transparency, providing helpful support for affected individuals. To give credit to ANU’s IT Security department, they handled the situation mostly with caution and professionalism, and eventually stopped the perpetrators from gaining further access to personal information, albeit there was an unknown amount of data exfiltrated.

Proper cybersecurity hygiene significantly enhances protection of data and minizes risk of data breaches. Regulatory compliance ensures the organization legality and ethical of the business, aiding business value and continuity of work. Policies, procedures, and guidelines should be followed strictly to make sure only one entity is held accountable, and accountability cannot be delegated. In the same regard, accountability and responsibility should not be confused, every entity within the organization should be responsible for preserving security. Proper treatment of risk such as avoidance, mitigation, and transfer could massively benefit the organization in case of such incident. For example, insurance, which is a form of risk transfer, can cover an immense amount. According to statistics, “In a cyber insurance claim due to a data breach, 71% of the loss falls under cyber policy coverage which is made up of insurer payments up to 44% and insured payments with retention at 27%.” (James, 2023)

Despite the benefits, implementing such robust system can be a challenge for many institutions due to limited resources, both financial and logistical. The rapid evolution of cyber threats requires expertise, continuous monitoring, and adaptation. This poses a great dilemma between usability and security; such advanced systems may cause inconveniences and affect user experience. Even in a perfect scenario, where every precaution was made, cyber-attacks still have a chance to happen, and insurance may not cover everything. In a survey in 2022 reveal that “claims grew by 100%, however only 19% of organizations have insurance beyond $600,000.” (James, 2023)

The case of ANU data breach is particularly chilling for one reason: even with extensive care, there was a large-scale attack that went undetected for many months. Fortunately, there was no imminent danger nor losses, showing how far security and risk management can protect an institution. “The fundamental message here is that cyber-security is not the sole responsibility of the Information Technology team – it is the responsibility of everyone across the organisation.” (*Unpacking modern Data Breaches: Is your data safe?* ,no date)

## Security Architecture & Engineering

Security Architecture and Engineering focuses on the design, implementation, and management of security systems and infrastructure. It covers topics such as security models, architectural frameworks, and secure system design principles. This domain aims to ensure that security is built into every aspect of ANU’s systems and infrastructure, from design to implementation and ongoing management.

While building an environment, in this case Enterprise Systems Domain (ESD), organizations often need to purchase products from vendors. It is crucial that these products are well-designed and meet the required functionality. Consumers should consider various evaluation criteria, including certification and accreditation. Common Criteria (ISO 15408) is a widely used evaluation standard that enhances trust between customers and vendors in the field *(Intertek)*.

As systems become increasingly sophisticated, vulnerabilities are inevitable. One such vulnerability is single-point-failure, where the failure of a single component can result in system-wide failure or compromise its security *(Kirvan, 2021)*. This risk can be mitigated by implementing redundancy, where backup components or systems are in place to ensure continuous operation in case of failure.

Another vulnerability arises when enormous amounts of data are placed in one location, leading to the risk of unauthorized inference. To address this, the concept of polyinstantiation can be employed. Polyinstantiation allows different versions of the same information to exist at different classification levels *(Taylor, 2020)*. This means that even if attackers gain access to the database, the information they see might not reveal the complete data, reducing the risk of data loss.

SQL injection is one of the common risks of web servers. In a web application, SQL commands are sent to a backend database to verify user identity and retrieve or store data. Attackers exploit SQL injection by passing malicious SQL commands through input fields *(Witcher, 2023)*, potentially gaining unauthorized access to the database. Input validation is the solution to this problem. The server should validate and sanitize user input by removing special characters or spaces, and never allow direct execution of SQL code.

Redundancy strengthens security by allocating systems across separate locations, making it challenging for attackers to find vulnerabilities since each one is different *(Zalox, 2022)*. Polyinstantiation is a suitable strategy for limiting unauthorized access therefore enhancing data security and preventing data loss *(Taylor, 2020)*.

Although these are all security measures, there are a few problems when it comes to putting these methods into use. Additional costs might be added not only for the duplicate products used for redundancy but also for maintenance. Furthermore, the implementation process is also more challenging due to its complexity.

Considering certification, and accreditation, addressing single-point failure through redundancy, implementing polyinstantiation for data protection, and employing input validation for mitigating SQL injection, even if they are high in cost, are essential in establishing a secure environment and protecting against potential threats.

## Communication & Network Security

Securing your network is what network security is all about. In the case of ANU data breach, hackers monitored and captured the network traffic throughout the campaign, they got an overall view of how ANU’s computer network operated. Securing network components is critical to prevent this event.

Secure network components are the hardware and software elements of a network that protect the network from unauthorized access, malicious attacks, and data breaches. There are so many essential components like network firewall, it acts as a gatekeeper between enterprises’ private network and public network (*Dynamic Solutions Group, 2021*). An intrusion detection system (IDS) detecting potential threats in real-time network traffic monitoring (*Dynamic Solutions Group, 2021*). An intrusion protection system (IPS) is similar to IDS but can also take action to block malicious traffic. Moreover, a network access control (NAC) prevents unauthorized users and devices from gaining access to corporate networks (1). Finally, security information and event management (SIEM), its role is to collect, aggregate and store log data from those sensors stated above (*Dynamic Solutions Group, 2021*). Network security follows a principle of the CIA, and aims to preserve confidentiality, integrity and availability (*Palo Alto Networks*). Confidentiality - reject unauthorized entities that want to get into assets. Integrity - make sure that data is correct and modified in an unauthorized way, and Availability - ensure that authorized users always have access to data if they need (*Palo Alto Networks*).

As previously stated, network security prevents illegal access, meaning it can keep sensitive information safe. In fact, ANU’s scheduled firewall interrupted the attackers once, even though they found a foothold in a legacy computer right after that (*Stephanie, 2019*). A secure network also has accessibility levels, the authentication will determine which level in software the user is authorized to access. The first campaign was initiated in November 2018, and they only spotted the intrusion in April 2019. By strengthening the network security compensating safeguards for legacy servers by intrusion detection or prevention security appliances, ANU could have spotted the suspicious action earlier.

Anything has downsides, installing network security solutions undoubtedly costs more. However, security is important so it must not be overlooked by any chance. Highly trained experts are also necessary to deal with any security problems in an intricate network. A network administrator is needed for a network to run well, and to meet the criterion, they must be professionally trained.

In conclusion, securing a network is a critical task, it involves many components undertaking different tasks. Implementing and improving network security may have prevented data leaks at the ANU.

## Identity & Access Management

Identity and management access (IAM) helps manage and secure access to organizations’ resources *(Microsoft).* This domain aims to give the right range of access to the right people so wrong people, like hackers, are not allowed to enter. Each subdomain inside this domain oversees a securing task, for example, conducting access restriction measures. However, this report will only focus on Managing identification and authentication of people, devices, and servicessub-domain.

Digital identity is the primary key to gaining access to any resources as it contains users’ information. Managing identification focuses on the processes and mechanisms involved in verifying the identity of individuals, devices, and services within an organization. On the other hand, authentication management includes managing user accounts, methods, and access control policies.

In ANU data breach, attackers had access to the university’s infrastructure through credentials, gained from spear-phishing emails, of people with high levels of access. Thus, the university can prevent this by increasing the level of identity and device authentication with access control services. This service includes identification, authentication, authorization, and accountability. Identification is the first step of the access control process, which asserts the identity of users based on its guideline *(Witcher, 2023)*. The following step is to verify the identity of three factors of single-factor authentication based on: knowledge (password), ownership (OTP), characteristics (fingerprint). Some multifactor authentication (MFA) solutions organizations can consider are implementing protocols, like Kerberos or SESAME, and using CAPTCHA. However, some hackers might be able to get over the authentication mentioned above, so additional session management is suggested *(Witcher, 2023)*. This helps manage users’ action and detect illegitimate users, and a method to terminate the session is using frequent re-authentication.

Implementing those security measures benefits organizations in many ways. First, the MFA enhances protection for the university in general and for each student, faculty as well *(Winbuzzer.com, 2021)*. It also includes a warning system to alert possible breaches so a defensive solution can be made on time. Secondly, re-authentication makes sure that the user remains the same person after a period of time so hackers cannot access the resource even if the user forgets to logout. Moreover, it includes stronger authentication policies and helps eliminate the threat of on-premises security.

To conclude, ANU's data breach, identity, and management access framework, will play a key role in strengthening the security of the university’s resources. Although measures in managing identification and authentication have both pros and cons, considering the results after using this method, its advantages outweigh its drawbacks.

## Security Assessment & Training

Security assessment and training are essential cybersecurity procedures that assist businesses in identifying vulnerabilities, evaluating risks, and enhancing their overall security posture. *(Smith, n.d.)*

There are two sub-domains that we need to focus on are vulnerability assessment and penetration testing. Conduct regular vulnerability assessments to identify weaknesses in systems such as vulnerabilities or misconfigurations (*Umrao et al., 2012*). Organizations may proactively detect and remedy security flaws before attackers take advantage of them by regularly conducting vulnerability assessments. This enhances overall security posture, lowers the possibility of security events, and safeguards sensitive data and priceless assets. Penetration testing, also known as ethical hacking, uses the same tool as vulnerability assessments but adds attack techniques where an assessor tries to penetrate the system by utilizing weaknesses. A few strategies that may be employed in this are war dialing, sniffing (monitor the network), eavesdropping (listening), dumpster diving, social engineering (human manipulation). The difference between these two methods is that vulnerability assessment is a high-level, automated evaluation that identifies and reports possible weaknesses whereas penetration test is a comprehensive, hands-on examination conducted by an actual individual to identify and exploit system vulnerabilities. (*Glover, n.d*.)

Pros of vulnerability assessment and penetration are identifying almost all known vulnerabilities and demonstrating at what depth vulnerabilities can be exploited. With this, organizations can define attack range, reduce, or eliminate the vulnerabilities and weaknesses of resources are now potential targets for hackers. Weakness of these methods can have a high false positive rate and be easily detected by the Intrusion Detection System firewall (*Umrao et al., 2012*).

We all know that the security systems of ANU are extremely strong, but no one had expected that a single preview of an email could cause a cyber-attack. We all understand that clicking a link can lead to cyber-attack, but no one could aware that only viewing it can also be bad. Based on my analysis, ANU did not have enough vulnerability assessment and penetration testing for cases like this. It was just a small space that the hacker could totally access to ANU systems for half a year. To enhance this, ANU and other companies or organizations should improve their cybersecurity audit model (CSAM) and improve interpretability for vulnerability assessment and emulate more real-world attack scenarios. Or in my perspective one more way is to collapse with an external red team or ethical hackers to have their view of hacking.

## Cyber operations

# 2 secondary domains

## Asset Security

Asset security includes the concepts, structures, and standards of securing and protecting valuable assets from unauthorized access. It involves instituting security measures and controls to protect assets and guarantee their availability, integrity, and confidentiality. In this domain we are going to look through asset classification. (*Infosec Resources*)

Assets classification is based on sensitivity, criticality, and the degree of protection required to ensure their security. According to Queensland law, every university must adhere to the Information Privacy Principles. There are various classifications depending on the organization, but we should focus on Information assets. Every part of institutional information must be categorized into one of three sensitivity levels: public, internal, and restricted. Basically, public information like accessible websites or promotional materials is permitted and does not contain sensitive or proprietary information. Next is internal, assets for internal use within the organization may contain sensitive or proprietary information. Access to these assets is limited, examples include internal documents, non-public financial information. Last is restricted information, which is extremely sensitive or secret. Unlike the 2 previous classifications, access to these assets is tightly controlled, and they require stringent security measures. (*Infosec Resources*)

Pros of asset classification is enhanced security. Asset classification helps improve security and protection by separating into different types of information (public, internal, and restricted).

On the other hand, it also has drawbacks, which are insider threats. Authorized users with access to classified assets may nevertheless inadvertently or willfully abuse their credentials.

For the ANU attack, after reaching the university’s system, they went into each classification, everything has been cracked. Data encryption should be added to enhance security and mitigate risks. It means adding another layer of protection, even if attackers gain access to the data, they will not be able to read or utilize it without the decryption key.

## Software Development Security

When developing any system, developers must go through a process of planning, creating, testing, and deploying that system, it is called Software Development Life Cycle (SDLC). It is essential to apply security in SDLC, which focuses on the protection of programs against attacks that exploit vulnerabilities in them (*Assal and Chiasson, 2018*). Security in developing and maintaining software is not a reason that caused the data breach, but still essential in any enterprise.

To be truly secure and being the most effective, security must be planned and initiated in every stage of SDLC. Secure Software Development Life Cycle is the most important topic when it comes to security of software.

On one hand, eliminating vulnerabilities in a program improves safety, minimizes risks and prevents further issues. Enhance efficiency and speed of development and operations release cycles.

On the other hand, securing the SDLC increases the project's time and cost. SDLC also needs technical expertise in security, coding, and testing (*Intellect Soft, 2019*). However, both downsides are too little compared to how important the security of the program brings.

In conclusion, security in software development did not directly affect the ANU data breach but is still important to the university to strengthen security and prevent further data breaches.

**References**

(No date) *Unpacking modern Data Breaches: Is your data safe?* Available at: https://griffinlegal.com.au/modern-data-breaches/ (Accessed: 28 June 2023).

Australian Government, P.S.P.F. (2022) *Policy 10: Safeguarding data from Cyber Threats*, *Protective Security Policy Framework*. Available at: https://www.protectivesecurity.gov.au/publications-library/policy-10-safeguarding-data-cyber-threats (Accessed: 28 June 2023).

Australian National University (2022) *ANU Policy Library - Procedure - Data breach response plan*. Available at: https://policies.anu.edu.au/ppl/document/ANUP\_017613 (Accessed: 28 June 2023).

Australian National University (no date) *Cyber Security Protection,* *Staff Services - ANU*. Available at: https://services.anu.edu.au/files/document-collection/cyber-protection.pdf (Accessed: 28 June 2023).

Gantz, S.D., Philpott, D.R. and Windham, D. (2013) ‘Chapter 13 - Risk Management’, in *FISMA and the Risk Management Framework the new practice of Federal Cyber Security*. Elsevier/Syngress, pp. 329–329.

Glover, G. (2023) *Pentesting vs vulnerability scanning:* *What’s the difference**?* . Security Metrics. Available at: https://www.securitymetrics.com/blog/pentesting-vs-vulnerability-scanning-whats-difference# (Accessed: 28 June 2023).

Imam, F. (2021) *CISSP domain 2: Asset security - what you need to know for the exam [updated 2021]*, *Infosec Resources*. Available at: https://resources.infosecinstitute.com/certification/cissp-domain-2-asset-security-need-know-exam/ (Accessed: 28 June 2023).

James, N. (2023) *Cyber Insurance Claims Statistics 2022-2023*, *Astra Security Blog*. Available at: https://www.getastra.com/blog/security-audit/cyber-insurance-claims-statistics (Accessed: 28 June 2023).

Smith, C. (2021) *Cybersecurity for beginners: Security assessment & testing*, *Cybersecurity for beginners: Security assessment & testing | Udemy*. Available at: https://www.udemy.com/course/cybersecurity-for-beginners-security-assessment-testing/ (Accessed: 28 June 2023).

Umrao, S., Kaur, M., and Gupta, G.K. (2016) *Vulnerability assessment and penetration testing*. Vol 7, issue 3, article 11, pp.71-74*.* Interscience Research Network. Available at: https://www.interscience.in/ijcct/vol7/iss3/11/ (Accessed: 30 June 2023).

Witcher, R. (2023) *CISSP domain 1: Security and risk management – learn this,* *Destination Certification*. Available at: https://destcert.com/domain-1-security-and-risk-management (Accessed: 28 June 2023).