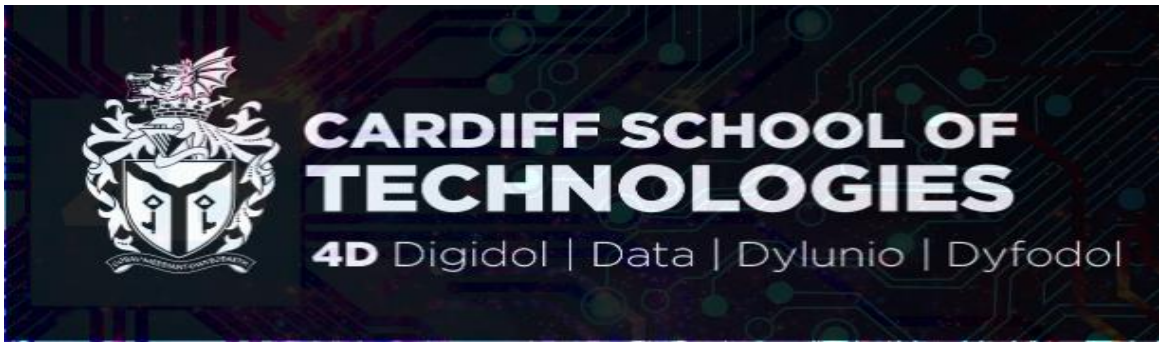

Cardiff Metropolitan University	
Cardiff School of Technologies	
Academic Year: 2023/2024	
Term: 2	
Module Name: Information Security	
Module Code: CIS7028	
Module Leader: Dr Liqaa Nawaf	
MSc Programme: Information Security	
Assignment Title: Information Security Assignment	
Student Name: Vignesh Alluri	**Student ID:20288240**

Table of Contents

Chapter 1

Integrating Data Protection and Security Standards

1.1 Data Protection by Design and Default

The Data Protection by Design and Default Principles are the building blocks that make the data protection methods to be constructed into the technological systems from the start. This approach incorporates the preventive dimension of privacy and confidentiality, which is taken into account at the initial stage of the design and development of the surveillance and contact apps (Stalla-Bourdillon et al. 2020). The Data Protection by Design requirement obligates the incorporation of security and privacy elements into the development and operation of these applications as an integral part of the solution, not as an add-on or only as a post-implementation measure. Such a goal can be realized by incorporating these principles in the very foundation of the system. Consequently, the risks will decline and the data management systems' resilience against any threats will improve (Tamburri 2019).

A multifaceted approach to abide by Data Protection by Design and Default should be adopted while implementing surveillance and contact tracing applications. The initial step entails understanding the purpose and working of every application. This consequentially provides an opportunity to catch the privacy and security risks that may originate from any of the stages in the data life cycle, such as data collection, processing, and storage. Organizations can proceed by implementing technical tools such as encryption, access controls, and data minimization methods to address risks efficiently (Habbal, Ali & Abuzaraida 2024). Similarly, privacy and security principles should be systematically integrated into the software development cycle instead of being introduced and under surveillance without any improvement. To do so, Privacy Impact Assessments (PIAs) and Threat Modeling methods are viable solutions.

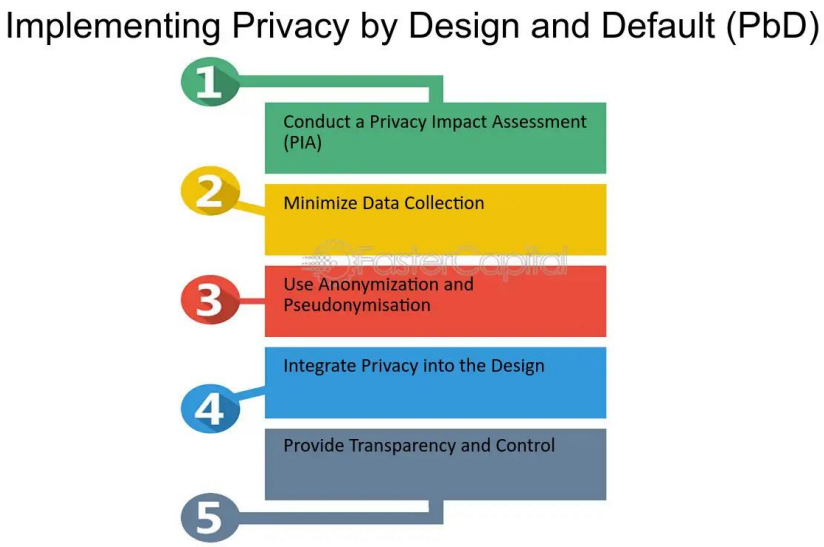

Figure 1: Implementing Privacy By Design And Default from faster capital (2024)

The need to include data protection by design and default principles in implementing surveillance and contact tracing applications cannot be emphasized enough. In a world where we are becoming increasingly interconnected and data becomes crucial, security violations and privacy breaches are serious threats to individuals and organizations (Ou et al. 2022). In such a situation, the preventive measures are critical. Through a proactive rather than a reactive approach to data protection, organizations can build trust with the users, show that they have met the requirements of the Data Protection Act in the UK, and, in general, increase the security level of their applications. Hence, applying these principles from the beginning is not only a legal and ethical obligation but also a strategic advantage in the contemporary digital environment.

1.2 Compliance with Regulations

Data Protection by Design and Default are the two basic principles that must be applied to all the systems already in use and the preventive measures for data protection at the time of introduction. This for preserving privacy and security rights from the planning and development phase of the surveillance and contact tracing apps. Privacy and security considerations are the core of Data Protection by Design, which requires that the application's architecture, features, and infrastructure contain these features from the beginning and not as an afterthought. In the process, organizations can give their systems capacities that make them resilient to any risk that might negatively affect their data-handling functions.

The use of Data Protection by Design and Default principles in the surveillance and contact tracing application is an issue that should be given a close view from a holistic angle. First, it demands a certain amount of information and data understanding. The knowledge enables a comprehensive investigation of the privacy and security risks present at every stage of data processing, which includes the data collection, processing, and storage phases (Kumar Tyagi et al. 2020). Through here, institutions can incorporate technical measures like encryption, access control as well as data minimization to effectively deal with risks (Thapa & Camtepe, 2021). Furthermore, approaches like Privacy Impact Assessments (PIAs) and Threat Modeling can be implemented into the process of the software development life cycle to make sure that they are not only included in the system but also monitored and improved continuously.

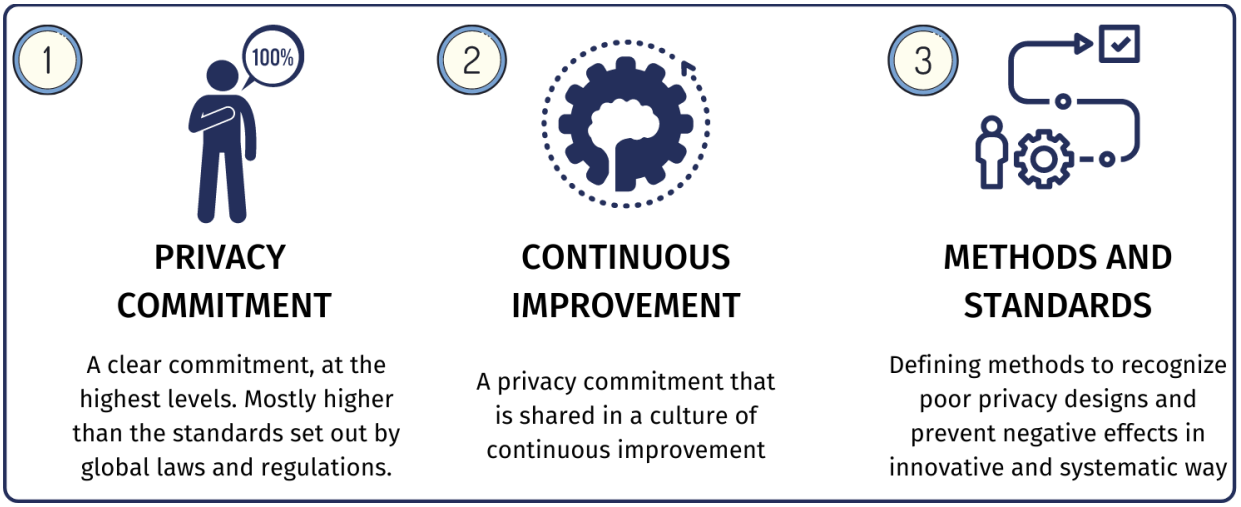

Figure 2: Implementation of Data Protection by Design and Default from data privacy (2020)

The necessity of encompassing Data Protection by Design and Default principles into the stage of designing surveillance and contact tracing software is paramount. In a world today that is closely connected and uses data as a driver, privacy breaches and security incidents that risk people and organizations are on the rise (Cremer et al. 2022). Hence, preventive measures are a must. Through the implementation of a preventive rather than a curative strategy, the data security of organizations can be improved, users can be trusted, and compliance with the UK GDPR can be demonstrated. Moreover, the application security can be strengthened as a whole. Therefore, incorporating those principles from the onset is not only a legal and moral obligation but also a smart business strategy in the digital world that exists today (Hsiao et al. 2022).

1.3 User Privacy

User privacy is a central principle that must be followed by data handling ethics in surveillance and contact tracing applications. Protecting user privacy is a task that involves the implementation of measures that ensure that individual data is being accessed by unauthorized persons, neither misused nor exploited (Daalen 2023). Organizations must comply with privacy aspects from the beginning of the design and during the application development process and use privacy-enhancing technologies and methods within the project itself. Organizations will take a privacy-by-design approach to avoid data breaches, build users' trust, and mitigate the risks of data privacy violations.

Organizations should employ data minimization principles by collecting just the data required for the particular intended use and restricting the level and time of data retention (Ribeiro-Navarrete, Saura & Palacios-Marqués 2021). Also, combining anonymization and pseudonymization methods can give extra protection to users' privacy but still help with data analysis and use. Through the application of a minimalist philosophy in regard to databases, organizations can diminish the threat of data misuse and improve user trust regarding the privacy and security of their applications (Ren et al. 2021).

Regarding user-oriented privacy strategy, the essential tools are clear consent mechanisms and transparency. Organizations may ensure that only users who have consented correctly share their data by informing them about the reason for data collection, data processing activities, and if there is any third party involved (Reuter, Iacono & Benlian 2022). Transparent data privacy policies and friendly user interfaces also make users conscious of the data they are sharing and can put them in a place where they can manage their user privacy. Nevertheless, companies should be working on how consumers may check, review, and alter the data choices they have made to create an environment where data processing is transparent and accountable (Javaid et al. 2022). Organizations shall strive to build a culture of trust and accountability by ensuring that consent is their number one priority and practicing transparency. Thus, they will not lose the users' trust and demonstrate that privacy is one of their priorities.

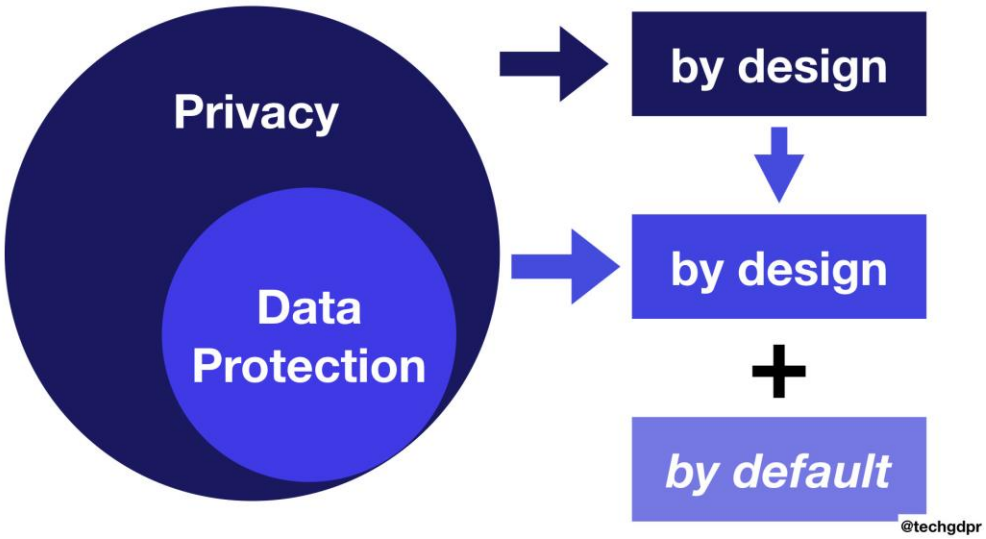

Figure 3: GDPR, Blockchain, and the Principles of Privacy by Design and Default from springer (2019)

1.4 Security Measures

Security measures are the core factors of data protection and privacy which normally entails data collection in surveillance and contact tracing. The risk and vulnerability assessment of the data environment is a targeted scanning of the environment. Encryption like end-to-end, and encryption-at-rest could be the tactical tool that protects data from being read by unauthorized people while it is transmitted and stored (Ramadan et al. 2021). Besides that, there are other access controls and authentication methods also which can be used such as multi-factor authentication and role-based access control. This sensitive information can be limited in reading, and unauthorized users are not able to change or extract it due to its nature (Atiewi et al. 2020).

Unauthorized penetration and access are prevented by implementing technical and procedural measures. Organizations should set and follow strong safety protocols, which include firewalls, intrusion detection systems, and network segmentation, to make sure that no attacker is able to get access to the infrastructure (Sayyed et al. 2023). The regular performing of security audits and vulnerability tests is an effective way to detect before the actual cyber-attack, reinforce the system, and increase the failure of attacks. With continuous validation of the incident response plans, the effectiveness of the actions taken for the security incidents would be as fast and accurate as it can be. This helps to preserve the integrity of the data and the organization's operations. It is

recommended to run a process that duplicates data and sets up a disaster recovery system to prevent data corruption and loss caused by breaches. Additionally, companies must pay attention to potential new cyber threats and ensure that their security and processes align with the fast-changing cybersecurity landscape.

1.5 Data Retention and Deletion Policies

Data retention and deletion standards are the core components of the data governance frameworks, and without following those, the applications used for surveillance and contact tracing are useless. The data censorship and evasion laws at the same time require a proper balance between data retention for practical needs and the data protection principles and rules. The retention time for the data from the organizational authorities is assessed according to the data nature, the sensitivity of the collection, and the purpose for which the data was collected (Janssen et al. 2020). Companies take data protection seriously, which involves limiting the risk of holding the data for a long period and ensuring the security of the data from any data privacy breaches by setting and defining retention periods for various types of data.

The most crucial thing to consider when designing either data retention or data deletion policies is how the data can be accessed and disappear in compliance with existing data protection legislation and rules. Organizations must guarantee that their policies do not break the law, which states that subjects' data should be destroyed when they are not needed for the purpose they have been collected (Gunnell 2024). Nevertheless, organizations often use technical tools such as data anonymization and pseudonymization to reach a higher level of privacy protection of personal data. With the adoption of an ethical data management policy having retention and deletion, the organizations are able to prove that they are ready to work according to the law and protect data subjects from any risk possible..

As for data retention, a balanced line that includes the factors that can harm the rights and freedoms of individuals is crucial in this case. Companies should come up with clear records retention policies for users indicating how their data is kept, and users should be informed that they have the right to access, modify, or delete their personal information (Ducato 2020). Privacy and accountability should be a basic requirement for data storage processes. In this regard, there is a chance of the enterprise being trusted by the users and a culture of responsible data stewardship will become prevalent.

1.6 Ethical Considerations

Ethical issues are therefore critical considering the surveillance and contact tracing technology's effect on privacy and civil liberties. The ethical concerns are explored through a critical assessment of the risks and concerns involved in the large-scale use of such technologies, including issues like consent, transparency, and misuse of the data collected. It is inevitable that the ethical difficulties posed by surveillance and tracing should be recognized, especially in the issue of the balance between public health interests and the individual's right to privacy and autonomy.

To address the possible risks and privacy issues, companies should make transparency, accountability, and user consent their main priorities during development and deployment (Wylde et al. 2022).

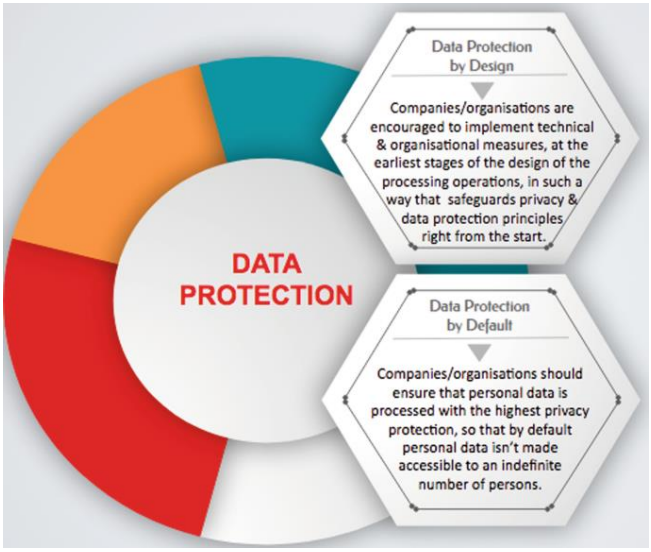

Figure 4: Ethical Principles for data protection from springer (2020)

Chapter 2

Analysis of a Recent Information Security Incident

2.1 Overview of the Information Security Incident

In the early October 2023, there was a data security breach involving 23andMe, a genetic test service company, has made many people question the security of their personal data. The issue was unearthed when the cybercrime website advertised a huge amount of customer data purported

to be from 23andMe. In the company's own words, this data was "the most valuable data you'll ever see." It was a sample of "20 million pieces of data" and was something the public should be worried about as it raised user privacy and security issues (Vicens 2023).

These account hacks were the direct result of unauthorized access to personal 23andMe.com accounts. The attacker is said to have obtained the account by using old passwords, which had been found on other platforms. The hacker capitalized on the flaw of using the same username and password combination to breach 23andMe customer accounts where users reused their login details on other sites. This vector of vulnerability shows the problem of password reuse and emphasizes the need to build strong authentication mechanisms in order to protect user accounts as well as confidential data.

The victim of the breach is 23andMe, a DNA testing company that is among the leaders in the genetic testing and ancestry exploration area. The company issued the statement saying that there are no data security breaches in its systems, but it acknowledged that individual accounts might have been abused by an unauthorized user. The case shows that 23andMe and other similar companies need to protect their security processes and remind users to create unique and strong passwords in order to decrease the possibility of unauthorized access and data leaks.

2.2 Impact on the Organization

The aftermath of the 23andMe information security breach, which affected a certain organization, is twofold in terms of either tangible or intangible consequences. The effect of the incident becomes clear once the damage is evaluated, and it shows that user privacy, data security, and the company's name can be at risk. Facing a massive amount of customer data allegedly breached, 23andMe will have to take on the repercussions of the mishap and mitigate the damage as much as possible.

A security breach may affect the organization's operations and reputation. Technologically, 23andMe needs to allocate resources to investigate the breach, assess the extent of the data compromise, and put measures in place to enhance security and avoid such incidents in the future. Alternative expenditures could adversely affect the normal course of business production and burden the financial capabilities of the company. In addition, such a breach may damage consumer confidence in 23andMe's ability to safeguard confidential user data, thus reducing customer acquisition and retention rates (team 2023). Furthermore, the case could be subjected to regulatory

scrutiny and legal consequences, and on top of that, it might make the recovery process even more difficult for the company.

Over the reputation, the hack ruins 23andMe's status as a reliable provider of DNA testing services. Due to unauthorized access to customer accounts and potential exposure of personal data, which are the main components of privacy and security, the company is unable to honor its commitment to them. The aftermath of the scandal may hurt the brand's reputation and credibility, thus repelling potential customers to the detriment of the existing ones, who will turn to other service providers. Developing trust with stakeholders, including customers, regulators, and investors, will remain the toughest task as 23andMe proceeds with the aftermath of the data security breach and tries to regain confidence in its data protection policies.

2.3 Vulnerability Exploited and Attack Manifestation

The vulnerability that underlies the attack on 23andMe seems to be the reuse of login credentials acquired by other sites. Notwithstanding the fact that particular CVE details have not been disclosed, it can be seen that the perpetrators took advantage of the prevalent practice of password reuse among the users. By using exposed credentials from other sources, the intruders were able to circumvent the company's authentication process and penetrate the accounts of the users without authorization. Thus, their personal information was compromised.

Consider the scenario where Jane has a 23andMe account in which she has the same password and username as the one that she uses on her email account. In case Jane's email account credentials are stolen by various data breaches, the attackers can enter her 23andMe account with the use of these login details. During entry, however, the hackers can steal all crucial personally identifiable information linked to Jane's account, which, in the end, is a privacy threat (Dwivedi et al. 2023).

Hackers will try to bypass weak password behaviors and authentication processes at all times. Therefore, strong authentication measures and proper password behaviors should be employed to keep safe user accounts and data. If you use the exact login details on multiple sites, this means that you increase your attack surface and hence, you become vulnerable to attacks. Moreover, it will require you to spend more time and energy to restore your account in case you forget your password and the effects of this will get heavier (Yusuf et al. 2020). It turns out that the perpetrators discovered that there was a vulnerability through the user's password reuse which helped them to access the sensitive personal information of 23andMe. This example gives us a better idea of a

policy that requires a strong and unique password and a multi-factor authentication process for the prevention of unauthorized access to confidential information and the real avoidance of data breaches.

2.4 Tools Employed by the Attackers

The hackers who attacked the fictitious 23andMe accounts were most likely equipped with a set of techniques, tools, and procedures to conduct their attack. The limited information about hacking methods may indicate that the perpetrators used automated scripts or botnets to find the user logins with the stolen credentials systemically. These functionalities not only allowed them to easily discover and overcome accounts whose passwords were reused or weak but also gave them access to users' private data.

The maturity and depth of the attack can be estimated by analyzing the mass and damage caused by it. It is clear from the hackers' declaration that they had "20 million of data" for sale and that the attack was targeted against all account holders, not a specific account. With the aid of automation tools and techniques that exploit repeated passwords, it follows that this is an easy but effective way to victimize accounts. In the opposite direction, these attacks can cause privacy and reputational issues at 23andMe as a result of them, which illustrates the seriousness of this issue, but its implementation might seem to be very simple.

2.5 Preventive Measures and Risk Management

After the comprehensive assessment of the risk management processes after the 23andMe incident, some areas of improvement that could have helped in preventing or lessening the consequences of similar risks in the future are identified. Recognizing and solving deficiencies in the systems and processes of the organization beforehand is the main issue of risk management. This event means that the security of the login credentials is at stake, and it also provides the necessity of putting into place resilient authentication mechanisms and promoting a good password management culture among users. Organizations should make it a routine to run security assessments and audits regularly, which will help uncover vulnerabilities that can be prevented from being exploited by unauthorized access or data breaches.

MFA (Multifactor authentication), which is supplementary to password-based authentication, should be used by organizations as a security measure to prevent such threats that were not

prevented before. The MFA technology incorporates a multi-factor authentication approach based on a second-factor verification system, such as a one-time password sent to the user's mobile phone in addition to the primary password (Suleski et al. 2023). This forces hackers to work more since the login credentials are now more difficult to crack, even when they are compromised, because the hackers have to proceed through another barrier. In addition to this, stricter policies on passwords will have to be put in place so that users will be motivated to create strong, unique passwords, and they will be discouraged from using the same passwords across different accounts. Users are also instructed about the need for a strong password and the features of the tools for password management. The implementation will help to mitigate the risk of credential-based attacks.

Moreover, systems have to be checked for any unacceptable behavior in advance in order to carry out the prompt detection and response to security incidents as they occur. Implementing IDS and SIEM systems, which are designed to detect malicious activities and issue real-time alarms in case of security incidents, will allow the company to quickly respond to a data breach and thus minimize its negative consequences (Mohsan et al. 2023). Security technologies that are well-established and incident response protocols allow organizations to detect, handle, and recover from security incidents in a timely manner.

Besides that, it is also essential to emphasize employee training and awareness programs so that the staff can learn about cybersecurity best practices and the crucial role of data protection. Employees contribute to the security of the organization’s systems and data, and therefore, ensuring that they are aware of and can identify security issues is very important. Employees should be made aware of phishing awareness, password security, and Incident reports in incidences so that they can be active participants in the organization's security stance (Hijji & Alam 2022). Also, the organization can conduct security awareness training sessions on a regular basis and try to perform simulated phishing exercises to reinforce the principles of cybersecurity and cultivate a security-aware culture within the organization. By investing in employee awareness and education and creating a security-conscious workforce, organizations can increase their security posture and thus reduce the probability of human errors resulting in security incidents. The joint use of technical controls and risk management processes, together with employee training, makes up a set of measures for the cyber security strategy that aims to mitigate the effect of possible threats and prevent access to sensitive data by unauthorized people.

In addition to this organizations should run through security assessments and penetration tests to get an idea about the vulnerabilities in their systems and applications and then remediate them. Frequent evaluations enable organizations to stay one step ahead of attackers by helping them pinpoint the gaps in their security stance before the malicious actors are able to take advantage of them (Ravindran & Potukuchi 2022). The organizations can carry out in-depth penetration tests to know how a real-world attack could be simulated, and the efficiency of their security controls in mitigating and detecting threats can be assessed. In addition, vulnerability scanning tools can be used to scan networks and applications for known security vulnerabilities that can be categorized and fixed in order of priority. A robust vulnerability management program is aimed at discovering and responding quickly to vulnerabilities that could otherwise render systems accessible to cyberattacks and data breaches. Via the strategic use of security audits and vulnerability management, organizations are able to boost their security posture and ensure the security of their infrastructure as well as their data assets.

Chapter 3

Reflective Report

Applying the 8 Cisco Cyber Essentials lessons in a real-world setting is very important because it consists of awareness training and practical exercises. These factors strongly impacted my perception of cybersecurity challenges. The labs were the best learning experiences for me because they combined theory and practice in a way that allowed to me put theories into practice. The process of learning was gradual. It was reflected through the coursework completion of the chapter life. Throughout the course, I received training on threat detection, incident response, and risk management, among other cybersecurity-related topics.

Cisco Cyber Essentials labs and hands-on activities have allowed me to acquire indispensable competencies in dealing with cybersecurity vulnerabilities. Through this interactive learning process, I created scenarios typical of actual cyber incidents and used best practices to minimize the cyber risks and protect the organizational resources. Moreover, the practical element of the training enabled interactive participation and cooperation that translated into a higher level of understanding of cybersecurity ideas and the development of critical thinking competencies. Generally, the real-world experience of these activities has been an incredible tool that has helped me present solutions to the increasing cyber threats competently.

Reference list

Atiewi, S, Al-Rahayfeh, A, Almiani, M, Yussof, S, Alfandi, O, Abugabah, A & Jararweh, Y 2020, 'Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography', *IEEE Access*, pp. 1–1.

Cremer, F, Sheehan, B, Fortmann, M, Kia, AN, Mullins, M, Murphy, F & Materne, S 2022, 'Cyber risk and cybersecurity: A systematic review of data availability', *The Geneva Papers on Risk and Insurance - Issues and Practice*, vol. 47, no. 3.

Daalen, OL van 2023, 'The right to encryption: Privacy as preventing unlawful access', *Computer Law & Security Review*, vol. 49, p. 105804.

Ducato, R 2020, 'Data protection, scientific research, and the role of information', *Computer Law & Security Review*, vol. 37.

Dwivedi, YK, Nir Kshetri, Hughes, L, Rana, NP, Baabdullah, AM, Arpan Kumar Kar, Koohang, A, Ribeiro-Navarrete, S, Belei, N, Balakrishnan, J, Basu, S, Behl, A, Davies, GH, Dutot, V, Dwivedi, R, Evans, L, Felix, R, Foster-Fletcher, R, Mihalis Giannakis & Gupta, A 2023, 'Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse'.

Gunnell, M 2024, *Why You Should Always Destroy Your Own Data*, viewed 6 May 2024, <https://www.techopedia.com/why-you-should-always-destroy-your-own-data>.

Habbal, A, Ali, MK & Abuzaraida, MA 2024, 'Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions', *Expert Systems with Applications*, vol. 240, no. 122442, p. 122442.

Hijji, M & Alam, G 2022, 'Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees', *Sensors*, vol. 22, no. 22, p. 8663.

Hsiao, WW-W, Lin, J-C, Fan, C-T & Chen, SS-S 2022, 'Precision health in Taiwan: A data-driven diagnostic platform for the future of disease prevention', *Computational and Structural Biotechnology Journal*, vol. 20, pp. 1593–1602.

Janssen, M, Brous, P, Estevez, E, Barbosa, LS & Janowski, T 2020, 'Data governance: Organizing data for trustworthy Artificial Intelligence', *Government Information Quarterly*, vol. 37, no. 3, p. 101493.

Javaid, M, Haleem, A, Singh, RP, Suman, R & Khan, S 2022, 'A review of Blockchain Technology applications for financial services', *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, vol. 2, no. 3, p. 100073.

Kumar Tyagi, A, Manoj Nair, M, Niladhuri, S & Abraham, A 2020, *Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead*.

Mohsan, SAH, Othman, NQH, Li, Y, Alsharif, MH & Khan, MA 2023, 'Unmanned Aerial Vehicles (UAVs): Practical aspects, applications, Open challenges, Security issues, and Future Trends', *Intelligent Service Robotics*, vol. 16, no. 1.

Ramadan, RA, Aboshosha, BW, Alshudukhi, JS, Alzahrani, AJ, El-Sayed, A & Dessouky, MM 2021, 'Cybersecurity and Countermeasures at the Time of Pandemic', in M Arif (ed.), *Journal of Advanced Transportation*, vol. 2021, pp. 1–19.

Ravindran, U & Potukuchi, RV 2022, 'A Review on Web Application Vulnerability Assessment and Penetration Testing', *Review of Computer Engineering Studies*, vol. 9, no. 1, pp. 1–22.

Ren, W, Tong, X, Du, J, Wang, N, Li, S, Min, G & Zhao, Z 2021, 'Privacy Enhancing Techniques in the Internet of Things Using Data Anonymisation', *Information Systems Frontiers*.

Reuter, C, Iacono, LL & Benlian, A 2022, 'A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead', *Behaviour & Information Technology*, pp. 1–14.

Ribeiro-Navarrete, S, Saura, JR & Palacios-Marqués, D 2021, 'Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy', *Technological Forecasting and Social Change*, vol. 167, no. 120681, p. 120681.

Sayyed, T, Kodwani, S, Dodake, K, Adhayage, M, Solanki, R, Bhaladhare, P & Tech, B 2023, 'Intrusion Detection System', *International Journal of Aquatic Science*, vol. 14, p. 2023.

Stalla-Bourdillon, S, Thuermer, G, Walker, J, Carmichael, L & Simperl, E 2020, 'Data protection by design: Building the foundations of trustworthy data sharing', *Data & Policy*, vol. 2.

Suleski, T, Ahmed, M, Yang, W & Wang, E 2023, 'A Review of multi-factor Authentication in the Internet of Healthcare Things', *Digital Health*, vol. 9, no. 1, p. 205520762311771-205520762311771.

Tamburri, DA 2019, 'Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation', *Information Systems*, vol. 91, no. 2, p. 101469.

team 2023, *The impact of data privacy on customer acquisition and retention*, AIContentfy.

Thapa, C & Camtepe, S 2021, 'Precision health data: Requirements, challenges and existing techniques for data security and privacy', *Computers in Biology and Medicine*, vol. 129, no. 1.

Vicens, AJ 2023, *DNA testing service 23andMe investigating theft of user data*, CyberScoop.

Wylde, V, Rawindaran, N, Lawrence, J, Balasubramanian, R, Prakash, E, Jayal, A, Khan, I, Hewage, C & Platts, J 2022, 'Cybersecurity, Data Privacy and Blockchain: A Review', *SN Computer Science*, vol. 3, no. 2.

Yusuf, N, Marafa, KA, Shehu, KL, Mamman, H & Maidawa, M 2020, 'A survey of biometric approaches of authentication', *International Journal of Advanced Computer Research*, vol. 10, no. 47, pp. 96–104.