Mayur Sejpal (C2071044)

University of Law

Data Security

Prof. Christian Dombrowski

January 17th, 2023

Table of Contents

➢ Assessment part – 1, Question No.1:

Assume that you have been invited to a committee meeting of GANT by the chairperson, who wants you to 'start the ball rolling' by explaining why it would be a good idea for GANT to think about Information Assurance. To make your points most forcefully, she has asked you to define three threats to the organization, three vulnerabilities and consequently three risks that any Information Assurance system would need to manage.

❖ Introduction and Explanation

Nowadays, when organisations are growing at a large scale, information assurance plays a very vital and crucial role, especially at the growth stage. Given that the server storing the information had no meaningful assurance, details of the group's events, people's information, their meeting sites, and other functions were recently compromised in this case study. This makes it risky for GANT to protect their data and other aspects from future loss. If at this stage GANT does not adopt the IA, they may face a security breach, the modification, duplication, or wiping of important data that might result from network flaws that may go unnoticed again in the future.

Data security and privacy are major concerns for firms in the modern world. Clients want to feel confident that their data is safe with you, so if you don't control it, you'll lose their trust. Prior to starting a company, dealing with clients, or asking for funding for charity, many clients who have access to classified information start demanding that the organisation with whom they are dealing has the strict data protection infrastructure necessary established within it.

Thus, IA is very critical as it protects the business's capacity to function. It enables applications to operate safely on the organization's IT systems. It protects the data that the business uses and acquires and also protects the institution's technology. To explain GANT in more detail, companies value information Assurance since it makes sure customer information is safe during storage and transportation. Information assurance has gained significance as a component of data security as business transactions and processes become more and more dependent on electronic handling.

Threats that organization may face if IA is not available.

- An organization's database may have to face exposure to viruses and worms, phishing attacks, ransomware, etc. These risks include fraudulent activity, data corruption, and unapproved access to confidential data – [*This can be resolved using security controls*.]
- It has to prevent cybercriminals from gaining unauthorized access to the computer systems of the institutions. – [*This can be done by endpoint or physical security, a strong password policy, or a dual authentication method*.]
- It will prevent malware or malicious software that disrupts computer operation so as to prevent a power outage. [*For this, we can use an antivirus program to scan the file or system on a periodic basis*.]

Vulnerabilities that Information Assurance system need to manage.

- It will manage to prevent the *exposure of sensitive data* to an unauthorized person or unauthorized access.
- Due to *security misconfigurations or unauthorized access*, it can create perilous security holes that expose the application and data to hacking or other attacks.
- Other forms of *cross-site request forgery* are also possible, which can lead to destroying relationships with customers, unlawful financial transfers, modifications, and data breaches, including browser cookie theft.

Risk that Information Assurance system would need to manage.

- Software attacks and data extortion from company database systems result in *financial losses to the organization or any other institution*.
- Additionally, the organization would suffer *reputational and intellectual damage* from intern sabotage, intellectual property theft, identity fraud, theft of supplies or data, or theft of equipment.
- The improper application of IA exposes institutions to a broad range of security risks, along with data leaks, *regulatory legal actions, and financial burdens*, which may lead to unauthorized access, *causing reputational damage for the organization*.

❖ Reference and Sources:

✓ "By Dominic Barton and David Court" (1st March, 2013) (Article No:4785), "*Mckinsey's – Data Driven Strategy"* viewed on – 5th January, 2023. URL access Link: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/three-keys-to-building-a-data-driven-strategy

➢ Assessment part - 2, Question No.2:

Provide a Risk assessment report for the Apple Health scenario. Identify at least five risks and mitigation strategies.

❖ Introduction and Explanation

Apple unveiled new tools for supporting loved ones as well as advanced consumer health and wellbeing insights for users. With iOS 15, users can safely share their data with significant others in their lives, such as a close relative or doctor, and gain insights into the health trends of their close ones. The new iOS 15 and iOS 16 tools use cutting-edge technology from the Apple Watch's health features app to detect, quantify, and comprehend changes in a user's health data record. Because so many people across the world are taking care of someone, the Apple team wants to offer a safe and confidential option for customers to have a reliable partner on their health journey. The Apple innovation team is thrilled to put these cutting-edge tools in people's hands.

Five risks and mitigation strategies

Risk

- Apple has a feature for sharing data with third-party apps; the information is sent directly from Health Kit to the third-party app when you choose to share health record data with it on your device. If the authenticity of a third party is not verified or the third party is not legitimate, this could create a potential exposure of data being misused by a third party.
- In addition to the risk of a person's sensitive information being disclosed in a data breach, data compromise issues, such as criminal hacking or the unintended release of sensitive user information, are a worry. For instance, fitness trackers frequently connect to a user's phone through Bluetooth, leaving personal data open to hacking.
- As fitness app data is not legally protected under local laws in the same way that health information is, neither the federal standard nor state laws classify the data that fitness trackers gather as "*health information*," which implies that personally identifiable information may be used in ways that a consumer might not anticipate. The personal data might, for instance, be shared or sold to outside parties like data brokers or law enforcement.
- The Apple devices (like the smart watch) are electronic devices, which might stop working in an emergency as they depend on periodic power charging. Therefore, the patient might not be protected from potential health risks or be able to quickly contact medical personnel. Also, the magnets and electromagnetic fields could occasionally cause medical equipment to malfunction. For instance, pacemakers and defibrillators that are implanted in the body may have sensors that react to magnets and radio waves when they are in close proximity. Apple products are required to be kept at a safe distance from other medical devices to prevent any potential interactions with these kinds of medical equipment.

- Users of mobile devices should exercise caution when sharing their location and activities with the public. Other issues with location data may also arise. a situation where a woman who needs reproductive healthcare is in a state where abortion is prohibited. According to experts, a fitness tracker with geo-location services enabled could gather data that could be used as evidence by law enforcement or that data brokers/dealers could buy and then sell to law enforcement agencies.

⟶ Mitigation Strategies

- Use a strong password to secure your account and turn on two-factor authentication for the connected app, additionally, make sure that security updates are applied and are up-to-date for the device and the app both.
- In the case of a third-party app, when you opt to share your health records with the third-party app on your smartphone, Health Kit sends the information directly to them. Thus, mostly avoid third party apps and other applications other than Apple-based secured applications in order to reduce the risk of data exposure.
- There may be chances of malfunctioning medical devices from Apple in such cases, where end-to-end encryption is used to store health data and health records in iCloud. Health record data is included in local iTunes backups if iTunes backups are configured to be encrypted. This encrypted backup can be used to restore a new Apple device if new one is purchased.
- Regular hardware maintenance is also necessary for medical equipment due to the large number of individuals who depend entirely on it for their health monitoring on a delay basis.
- Establishing appropriate local laws and frameworks by local bodies for the supervision, sharing, use, and storage of personal health data of patients and medical clients between service providers and service users to avoid potential data exposure to third parties.

❖ References and Sources:

- ✓ The Apple Website (2022), “Health Care section” viewed on 5th Jan, 2023. URL Link used: www.Apple.com - https://www.apple.com/newsroom/2021/06/apple-advances-personal-health-by-introducing-secure-sharing-and-new-insights/
- ✓ The Apple Website (2022), “Apple News room developer webpage” viewed on 6th Jan, 2023. URL Link used - https://developer.apple.com/health-fitness/works-with-apple-health/
- ✓ Chery Winokur Munk (Nov, 2022), “The Apple innovation”, “CNBC News” Published – Saturday November 26th 2022, 10:30 AM EST, viewed on 4th Jan, 2023, 4:00 PM IST.
- ✓ The Apple Website (2022), “Apple’s website support portal” viewed on 6th Jan, 2023.
- ✓ URL Link used - https://support.apple.com/en-us/HT209519

➢ Assessment part - 3, Question No.3:

Provide a discussion on data management frameworks considering the payment systems. What are the vulnerabilities and security controls for the POS case? Provide at least 4 security controls.

❖ Introduction and Explanation

Discussion on Data Management Framework in payment system.

Data Management system is the system for gathering, storing, safeguarding, and analyzing massive amounts of data throughout an organization in order to make business choices within organizational framework. This Data Management framework had become the most vital element for unorganized business and started playing crucial role across the sector or industry because data is recognized as a company asset that can be leveraged to enhance marketing initiatives, business functions, and cost-saving measures, with the aim of boosting revenue and profits.

In Payment system this data management framework enables stable and effective financial system which depends on the effectiveness and safety of the payment network, which also helps people have faith in the currency. It is necessary to incorporate the proposed payment methods into business procedures. Because every payment system, and especially a sophisticated one, has a very specific control logic, which is not easy process.

The many services offered by each payment system must be included into a border framework. End-to-end encrypted transaction information and details on payments or settlements that are gathered, transferred, or handled as part of a payment message or instruction should be included in the data management framework. Customer information (Name, Mobile Number, Email, Social Security Number, Tax ID Number, payment method, bank detail, card detail etc.) may be included among other things.

Large conglomerates already have a great amount of friction when making and receiving payments to and from one another. Making a single payment between multiple parties makes it difficulties due to the continuous reliance on outdated solutions and the increasing demand for data gathering, integration, and analytics. These relationships sometimes include frequent payments between the parties and involve intricate arrangements on prices, fees, payment terms, and other things.

Financial losses are practically certain when this process is done manually at the end of the month or financial term because of how difficult it is to manage contract compliance, mitigate conflicts, and prevent errors, which intern gives important to data management framework.

Vulnerabilities and four security controls for the POS case.

Retail firms are quickly adopting point-of-sale systems as their go-easy technology since they offer an all-in-one solution. POS systems have demonstrated their ability to deliver a strong digital database for the retail industry. POS systems have become more popular than cash due to their simplicity, increased accuracy, thorough receipts, and error-free checkouts. However, there are significant security issues raised by the POS transactions' rapid expansion in the retail sector.

- There might be threat to application system used in POS like: Security Misconfigurations, Sensitive Data Exposure, Broken Access Control or other Network Vulnerabilities. For POS transactions, a lot of shops use transfer level encryption, which secures the card data just as it travels from the Point-of-sale terminal to the payment gateway. At this point, hackers might potentially access the data and use it to their own advantage.
- Data is repeatedly exposed throughout the payment process, leaving it open to cyber-attacks like hacking. Typically, automatic malware installation is way how hackers obtain credit card details. This malware invades workstations, networks, and computer systems in search of unencrypted cardholder data.

Four Security Control for POS

1. Look for any odd activity or indications of an attack in any POS system and data operations. Any networks used by POS systems ought to be divided. Always use strong, secure credentials and two-factor verification.
2. Also, repetitive basis carry virus protection, frequently checking systems for hazardous files, keep all POS software up to date, using strong encryption, etc.
3. Put a POS monitoring program in place, monitors with cameras for surveillance, secure your POS gadget physically, regularly testing your system & database.
4. Consider physical security when designing your POS system. When customers scan their cards to make purchases, cybercriminals may try to attach card skimmers to a POS system in order to acquire their credit card details. In such exceptional case employees should receive training on how to spot these kinds of behavior of stranger.

❖ References and Sources:

✓ The Adam Hayes (2022) "*What Is a POS System and How Does It Work*", "The Investopedia" (25th September, 2022), viewed 18:07 IST, URL access link: https://www.investopedia.com/terms/p/point-of-sale.asp

✓ Kathy Haan, Toni Matthew (2023), "*Best POS Systems for Small Business January 2023*", "Forbes Advisor", (6th Jan,23, 9:15 GMT), URL access: https://www.forbes.com/advisor/business/software/best-pos-system-for-small-business/

➢ Assessment part - 4, Question No.4:

Collate the tasks completed throughout the semester and write a wrap-around cohesive report, including the above tasks. This report should have an Introduction to the tasks, the tasks themselves, and then a Conclusion and Reflection.

In the Conclusions and Reflection, you should summaries your findings and reflect on the lessons learned during this assignment and the challenges faced during this module.

❖ Introduction and Explanation

Data security in this digital age refers to the universe of data and the protection of its database. As part of this data security module, we dug deep into various aspects of security and its component [CIA], as well as aspects that would compromise CIA via various attacks on the CIA database. As security comes into picture, various attacks and defence mechanisms emerge, and various policies and procedures have implications for various security controls.

Data security is a very crucial aspect that has a direct reflection on cryptography when data is being transferred. The reliability of online data also depends on physical security, which is emphasised by its layers of security control and its application to various security validation methods. Data governance is a universal procedure to adapt for organisational effectiveness with respect to security data. Thus, master data management and data governance come into play to integrate data governance procedures. To protect against future data loss, various data governance plans are necessary, and thus data management plans have become a requirement for every organization. At the same time, information security management and risk management frameworks are critical components of physical and intangible security governance.

Under this task, we have considered all the aspects that would be aligned with security control and their implication in a real business model. The assignment done above covers all the aspects of data security and various procedures that could be adopted to prevent them. The assignment discusses the criticality of various components of data security (CIA) and the risk aspect that needs to be sorted out. Also, it briefly talks about the importance of security, both physical and online, for new products such as Apple Health Care. In order to protect client personal information and money as digitalization advances, innovation adopts a new security model (example: a payment gateway system); as a result, numerous methods are presented in the third case study.

Conclusion and Reflection

The task was based on the learning that was done throughout the semester on data security; this task will teach us at the end what information assurance is, its three pillars, and its applicability in real-life scenarios. The plan and framework for data governance, the numerous security measures to be implemented, and their relevance in various real-world circumstances are all emphasized. Also, as a part of this assignment in the first case, it teaches us what problems or challenges arise on account of information assurance not being adopted in an organization and what aspects can be considered to manage the challenges that arise on account of vulnerabilities, threats, and controls. Also, what consequences would be faced if no proper IA plan were implemented in an organization on account of various types of attacks on the CIA's data?

In the second assessment test, we learned how to account for the most recent technological advancements when considering various security aspects in a real-life scenario with respect to security defense, software control and hardware control, and encryption and decryption. Also, in this apple case study, we understood how security aspects play a crucial role when risk arises on account of weaker security aspects adopted into new, developing technology. In this Apple case study, we went deep to understand how network & physical security are considered priorities in terms of building and implementing the latest technology into branded products like Apple. Also, how mitigation strategies be developed over time to address risk elements that are typically present as a result of inadequately security controls; in this case study are all addressed.

In our third case study, we looked at the importance of a management framework based on cutting-edge technology and digitalization. We learnt how security control and data governance are being adopted, implemented, or sustained over time to integrate the latest innovation into a new business model. The new innovations such as payment gateways adapts to cyber security and physical security control as networks become more globally integrated, which has implication of cryptography. As innovation occurs, the risk factor becomes more important to be addressed with priority for the protection of client & organization personal/private data, and thus, the human brain will work upon to adapt various security measures to mitigate this risk exposure as we move ahead.

- ## Challenges and findings

The availability of data on the external platform was too vague and wide in nature, and thus, it was difficult to relate the case study to a real-life scenario. The case study discussed a situation too deep into real life, as we had never faced such a scenario previously; thus, it was difficult for us to integrate it into a practical situation for this assessment. But honestly, what we learned from our professor and the way we learned it were very unique, as we could use the same knowledge and skills to find information from an external source and implement the same knowledge directly into assessments to be integrated into a real-world model.