NOTTINGHAM
TRENT UNIVERSITY

Module Code: COMP40491

Module Title: Information Security Management

Topic: Alleging Reckless and Negligent Cybersecurity Policies

Student Name: Venkatesh Kandula

Student ID: N1056092

Table of Contents

Description of the Identified Security Issue

According to a disclosure made by a whistleblower that CNN and The Washington Post were able to obtain, Twitter has major security flaws that pose a threat to the personal information of its users, as well as to the company shareholders, national security, and democratic processes. The disclosure, which was sent to Congress and federal agencies the previous month, claims that Twitter has a chaotic and reckless environment that allows too many staff members access to the platform's central controls and sensitive information without proper oversight (O'Sullivan et al., 2022). In addition, the disclosure claims that Twitter has violated the terms of its license to operate as a public company. It also asserts that some of the company's senior executives have been attempting to hide Twitter's vulnerabilities and that one or more of the company's current employees may be working for a foreign intelligence service. These assertions are contained in the document. Peiter "Mudge" Zatko, the person who reported inappropriate behavior on Twitter, formerly held the position of head of security at the company and reported directly to the CEO. Zatko asserts that Twitter's leadership has misled both the company's board of directors and government regulators regarding the company's security flaws, including those flaws that have the potential to open Twitter up to foreign espionage, manipulation, hacking, and disinformation campaigns.

A further allegation made by the whistleblower is that Twitter does not consistently delete user data after users cancel their accounts and, in some instances, has even lost track of the information. In addition to this, it is claimed that the company has misled authorities regarding the question of whether it deletes the data as required. Elon Musk's recent efforts to back out of a $44 billion deal to buy the company have recently made bots a central focus (although Twitter denies Musk's claims). Bots have recently become a central focus. He claims that he tried to alert

Twitter's board to the security flaws and to assist the company in addressing its technical deficiencies and alleged non-compliance with an earlier privacy agreement with the Federal Trade Commission before going public with his allegations. He also says that he assisted the company in addressing these issues.

In response to the allegations, a Twitter spokesperson stated that the company has always placed a strong emphasis on protecting its users' privacy and data and that it provides users with easy-to-understand tools to manage their data sharing preferences, ad targeting, and privacy settings. The spokesperson also claimed that Twitter has established internal workflows to ensure that when users cancel their accounts, the company deactivates the accounts and begins the process of deleting the accounts. Twitter, on the other hand, did not wish to comment on whether or not the process is typically finished (O'Sullivan et al., 2022). The spokesperson also stated that Zatko was terminated in January for ineffective leadership and poor performance and that his allegations and timing appeared to be designed to capture attention and inflict harm on Twitter, its customers, and its shareholders. Zatko was terminated in January for ineffective leadership and poor performance.

The disclosure suggests that Zatko had a contentious working relationship with Parag Agrawal, the former chief technology officer of the company who was promoted to the position of CEO following Jack Dorsey's departure in November. According to the disclosure, Agrawal and his lieutenants disregarded Zatko's repeated warnings about security vulnerabilities and his requests for additional resources to address those vulnerabilities on multiple occasions. It is also alleged that Agrawal and other executives resisted Zatko's efforts to implement fundamental security measures, such as mandating that employees use password managers and two-factor authentication. The disclosure also asserts that Agrawal and other executives resisted Zatko's efforts to increase the budget for the security team, which, in comparison to other departments, was understaffed and underfunded.

Contextualization of case study within the Information Security

Information security is the protection of digital information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Because of our ever-increasing reliance on technology, our information and our computer systems are increasingly at risk of being attacked and broken into. This poses a significant problem for individuals, organizations, and governments everywhere.

The investigation into the alleged security flaws at Twitter sheds light on the critical nature of information security in the modern era of digital technology. If the allegations are proven to be true, they suggest that Twitter has neglected its responsibilities to protect the personal information and privacy of its users, as well as the security of its systems and networks. This could result in serious consequences for the users of the company, including the theft of their identities, financial losses, and damage to the company's reputation (O'Sullivan et al., 2022). Since the financial and reputational costs of a data breach or security incident can be significant, it is also possible that it will hurt the shareholders of the company. In addition, there are allegations that Twitter misled its board as well as government regulators about the security vulnerabilities of the company, and there is also the possibility that some employees are working for a foreign intelligence service. These allegations raise concerns regarding the trustworthiness of the company as well as its potential impact on national security and democracy.

The case study also demonstrates the difficulties associated with managing information security in a digital environment that is both complicated and constantly changing. The employee who blew the whistle on Twitter claims that the company has a chaotic and irresponsible culture, with an excessive number of employees having access to sensitive data and systems without adequate supervision or training (Bushnell et al., 2019). This could result in unintentional leaks and disclosures, as well as unauthorized access by both internal staff and external parties. In addition, the case study gives the impression that Twitter has not adequately secured its internal systems and networks, which has led to successful hacks and breaches. These difficulties are faced by a wide variety of organizations and finding effective solutions to their calls for careful planning, sufficient resources, and specialized knowledge.

The case study also draws attention to the important role that whistleblowers play in addressing concerns regarding information security. Peiter "Mudge" Zatko, who formerly served as Twitter's head of security, asserts that he attempted to bring the company's board's attention to the security flaws and to assist in correcting the technical deficiencies as well as the alleged non-compliance with an earlier privacy agreement. Following his dismissal from the company, Zatko decided to blow the whistle on the allegations by going public with a whistleblower disclosure. When it comes to bringing attention to information security issues and holding organizations accountable for their actions, whistleblowers have the potential to play an important role. On the other hand, they run the risk of significant risks and challenges, such as retaliation, legal action, and harm to their careers and reputations.

In general, the case study of alleged security flaws at Twitter sheds light on the significance of information security in the modern digital age, as well as the difficulties associated with effectively managing it in an environment that is both complex and constantly changing. In addition to this, it highlights the importance of whistleblowers in the process of addressing information security issues as well as the risks and difficulties that they may encounter.

Information security

Information security is the process of keeping digital information and systems safe from people who shouldn't be able to see, use, share, disrupt, change, or destroy them. In the digital age we live in now, people, businesses, and governments depend heavily on technology and the internet to store, share, and get information. Because of this, information and systems are more likely to be attacked or broken into, which can have serious effects on individuals, businesses, and society as a whole. Hacking, phishing, malware, ransomware, and denial of service attacks are just some of the things that can hurt information security (Chaturvedi et al., 2021). Threats like these can come from many different places, like cybercriminals, nation-states, or even angry employees. Organizations and individuals need to take several steps to protect themselves from these threats, such as using strong passwords, two-factor authentication, antivirus software, firewalls, and regular updates and patches.

Information security needs more than just technical measures. It also needs strong policies, procedures, and training to make sure that employees and users know how important it is to protect sensitive information and systems. This can include rules about how to handle passwords, keep devices safe, and report security problems. For people, businesses, and governments to protect their assets, reputations, and operations, they must have good information security. It is also important for keeping trust and confidence in the digital environment and for protection against the possible effects of a security breach, such as financial losses, legal liabilities, and damage to reputation.

General Information Security Issues

In today's digital age, organizations and individuals face several general information security problems. Among these problems are:

- **Cyber threats:** Cyber threats are always changing and getting smarter, which makes it hard for organizations and people to protect themselves from them. Hacking, phishing, malware, ransomware, and denial of service attacks are all examples of these kinds of threats (Chudasama & Rajput, 2021). They can come from a variety of places, such as cybercriminals, nation-states, or even disgruntled employees.
- **Lack of knowledge:** Many people and organizations don't know about the risks and results of bad information security practices. This can lead to careless actions like using weak passwords or sharing sensitive information online, which can increase the risk of a security breach.
- **Insufficient resources:** Some organizations may not have enough money or knowledge to manage their information security well. This can be caused by a lack of money, trained staff, or up-to-date systems and technology.
- **Insiders:** People who work inside a company, like employees or contractors, can be a big threat to information security. They might have access to sensitive information and systems and might do something to break security on purpose or by accident.
- **Complex systems:** Modern organizations store, share, and access information using complex systems and networks. These systems can be hard to keep safe and can be easy to hack or break into.
- **Interconnectedness:** The more systems and networks are linked to each other, the easier it can be for threats to spread and the harder it can be to stop them. This can make it harder to keep attacks and breaches from happening.

Key elements of information security

Organizations and people should think about a few key parts of information security to protect their assets, reputation, and business operations. Among these things are:

- **Technical measures:** Tools and systems that organizations and individuals use to protect themselves from cyber threats. Strong passwords, two-factor authentication, antivirus software, firewalls, and regular updates and patches are some of the ways to do this.
- **Policies and procedures:** Organizations should have clear policies and procedures in place to make sure that employees and users know how important information security is and how to protect sensitive information and systems (Bongiovanni, 2019). These can have rules about how to handle passwords, keep devices safe, and report security problems.
- **Awareness training:** Organizations should give their employees and users awareness training to make sure they know the risks and consequences of bad information security. This can include teaching them how to spot cyber threats like phishing attacks and malware and how to protect themselves from them.
- **Risk assessment and management:** Organizations should do risk assessments regularly to find possible security holes and threats to their data. Then, they should take steps to reduce these risks and deal with them well.
- **Response to incidents:** Organizations should have a plan for how to handle security incidents like data breaches or cyber-attacks. This should include steps for figuring out what happened, stopping the damage, and getting back to normal after the event.

- **Legal and regulatory compliance:** Organizations should make sure they follow the laws and rules about information security that apply to them. This can include laws about protecting data, industry-specific rules, and standards for cybersecurity.

Overall, good information security requires a mix of technical measures, policies and procedures, training, risk assessment, and management, responding to incidents, and following the law and rules. By focusing on these key parts, organizations and people can better protect themselves from cyber threats and make sure their information and systems are safe.

Evaluation of the Responses

In the case of Twitter, the company has been accused of having major security flaws and operating in an environment that is disorganized and irresponsible, which constitutes a risk to the safety of its users, shareholders, and the nation as a whole. Peiter "Mudge" Zatko, who was formerly the company's head of security and claims to have attempted to flag these issues to the company's board before being fired in January for poor performance, is the source of these allegations. Zatko came forward as a whistleblower after he was terminated for poor performance. These allegations have been refuted by Twitter, which asserts that protecting users' privacy and data has always been a top priority for the company. They have also brought up the fact that Zatko was fired due to poor performance, as well as the fact that his allegations appear to be designed to attract attention to cause harm to the company, its customers, and its shareholders (Acheampong et al., 2020). It is imperative that organizations take seriously any allegations of security flaws, conduct thorough investigations into the allegations, and address any problems that are discovered as a result. In addition to this, businesses need to be open and honest with their customers, shareholders, and government regulators regarding the vulnerabilities and security practices of their organization.

Recommendations

Twitter could use the following suggestions to make its system more secure:

- Conduct a thorough risk assessment: Twitter should conduct a thorough risk assessment to identify any vulnerabilities or weaknesses in their systems and implement measures to address them.
- Use strong passwords and manage your passwords. To protect yourself from cyber threats, you need strong passwords and the right way to manage your passwords. Twitter should set up policies and tools for passwords to make sure that employees use strong passwords and follow best practices for managing passwords.
- Teach your employees about cybersecurity: Twitter should teach its employees about best practices for cybersecurity, such as how to avoid phishing attacks, protect devices, and report strange behavior. This can help lower the risk of threats from inside the company.
- Use encryption: Twitter should think about using encryption to keep sensitive data safe and make sure that only authorized people can access it.
- Implement access controls: Twitter should implement access controls to make sure that only authorized people can access sensitive information and systems and to track and monitor who has access to these assets.
- Update software and systems regularly: Regular updates and patches are important to fix holes and make sure software and systems are safe (Singh et al., 2022). Twitter should make sure that all of its systems have the latest updates and patches.
- Monitor and find threats: Twitter should set up systems for monitoring and finding threats so that it can find and deal with possible threats quickly.

By following these suggestions, Twitter can improve the security of its information and be better prepared for cyber threats.

Organization's Security Policy Planning

In the Twitter case, the whistleblower said there were security problems and holes. The organization could plan its security policy around the following steps:

- **Define the scope of the policy:** Twitter should define the scope of its security policy, including the assets it covers and the people and groups it covers. This could include employees, contractors, and third-party vendors, as well as information, systems, and networks.
- **Identify the risks and weaknesses:** Twitter should list the specific risks and weaknesses they face, such as any security holes or weaknesses that could allow foreign spies, hackers, or disinformation campaigns to get in.
- **Set goals and objectives:** Twitter should set clear goals and objectives for their security policy, such as making sure their users are safe and private, preventing data breaches, and following all laws and rules.
- **Create policies and procedures:** Based on its goals and objectives, Twitter should create policies and procedures to help employees and users protect sensitive information and systems in the right way (Yigitcanlar et al., 2021). This could include things like password policies, controls on who can access the data, and encrypting the data.
- **Implement technical measures:** To protect itself from cyber threats, Twitter should figure out which technical measures will work best in its environment and then put them

into place. This could be done with things like firewalls, intrusion detection systems, and virtual private networks (VPNs).

- **Train employees and users:** Twitter should make sure that its employees and users know how important information security is and how to protect themselves from cyber threats by giving them training. This could include training on things like phishing attacks, how to handle passwords, and best practices for security.

Profiles in the Security Policy

In a security policy, profiles refer to the roles and responsibilities of different people and groups within an organization. These profiles can help define the level of access and privileges that different people have to information and systems and make sure that the right controls are in place to stop unauthorized access or misuse (Yigitcanlar et al., 2021). For instance, an organization might have different profiles for employees, contractors, and third-party vendors with different levels of access and privileges based on their roles and responsibilities within the organization. In the security policy, it is important to clearly define each group's profile and the rights and access controls that go with it. This can help make sure that the policy is followed correctly and that there are proper controls in place to protect against unauthorized access or misuse.

Reference

Acheampong, F. A., Wenyu, C., & Nunoo‐Mensah, H. (2020). Text‐based emotion detection: Advances, challenges, and opportunities. Engineering Reports, 2(7), e12189. https://doi.org/10.1002/eng2.12189

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & Security, 86, 350-357. https://doi.org/10.1016/j.cose.2019.07.003

Bushnell, A., Kenny, K., & Fotaki, M. (2019). The battle for the whistleblower: An interview with John Kiriakou. Ephemera Journal, 19(4), 829-850. https://core.ac.uk/download/pdf/286359412.pdf

Chaturvedi, M., Sharma, S., & Ahmed, G. (2021, March). Study of Baseline Cyber Security for Various Application Domains. In IOP Conference Series: Materials Science and Engineering (Vol. 1099, No. 1, p. 012051). IOP Publishing. https://core.ac.uk/download/pdf/326836192.pdf

Chudasama, D., & Rajput, N. (2021). Protecting ourselves from digital crimes. National Journal of Cyber Security Law, 4(1), 1-6. https://www.researchgate.net/profile/Dhaval-Chudasama/publication/352507646_Protecting_Ourselves_from_Digital_Crimes/links/60cc3455a6fdcc01d47df059/Protecting-Ourselves-from-Digital-Crimes.pdf

O'Sullivan, D., Duffy, C., Fung, B., Wasser, Z., & Whiteside, L. (2022, August 23). Ex-twitter exec blows the whistle, alleging reckless and negligent cybersecurity policies | CNN business. Retrieved January 5, 2023, from https://edition.cnn.com/2022/08/23/tech/twitter-whistleblower-peiter-zatko-security/index.html

Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability'that needs to be fostered in information security practitioners and how this can be accomplished. Computers & Security, 92, 101761. https://doi.org/10.1016/j.cose.2020.101761

Singh, D. K. S., Nithya, N., Rahunathan, L., Sanghavi, P., Vaghela, R. S., Manoharan, P., ... & Tunze, G. B. (2022). Social network analysis for precise friend suggestion for twitter by associating multiple networks using ml. International Journal of Information Technology and Web Engineering (IJITWE), 17(1), 1-11. DOI: 10.4018/IJITWE.304050

Yigitcanlar, T., Kankanamge, N., & Vella, K. (2021). How are smart city concepts and technologies perceived and utilized? A systematic geo-Twitter analysis of smart cities in Australia. Journal of Urban Technology, 28(1-2), 135-154. https://doi.org/10.1080/10630732.2020.1753483