Tabish Parkar

Formative Assessment 1:

Systems Development 2B

1.1. Using a robust information security program for a new business needs an establishing of basic rules as well as a method to employ a technical solution made for software development. It is necessary to begin with governance and policy development which uses configuration management tools to ensure that all system configurations are adhered to for basic security policies. Using a habit of security awareness can be found by implementing a basic training module into the introductory process through Learning Management Systems (LMS) and tracking completion via APIs.

Using critical risk assessments which can be automated using a vulnerability scanning tool or tools, which can be used in CI/CD pipelines to constantly fork out potential risks. Access control can also be enforced by using libraries designed for role-based access control, for example the ones found in frameworks and implementing secure identity management protocols.

To protect important data, using leveraging encryption libraries for multiple coding languages is highly critical, this ensures that data is encrypted both at rest and in transit. Furthermore, the networking of security can be improved via programmatic configuration of firewall rules and security groups in cloud systems by using an infrastructure as code practice. Endpoint security solutions should be able to integrate with APIs for an automated reaction to potential threats found on devices.

Incident response methods can be improved by using tools for incident management and using logging frameworks for the automation of incident logging. Constant supervision and logging can be introduced through centred log management systems, along with an alerting and visualization method through Prometheus and Grafana.

To ensure conformity with the relevant regulations, it can be managed using compliance as code, while actively supervising a third-party risk could involve the

use of tools to make sure that dependencies are kept safe. More importantly, advancing the continuous improvement in information security methods is highly vital and this can be managed by establishing CI or CD pipelines with tools that automate not just testing, but can also adopt security tests, such as static application security testing and dynamic application security testing.

1.2. Improving information security for a fast-growing e-commerce company needs the implementation of multiple types of security controls which are administrative, technical and physical. Each type plays an important role in protecting important information and keeping a strong cybersecurity position.

Administrative Controls - These include policies and training programs. In an e-commerce environment, this means to create a clear and precise information security policy and to provide constant training for employees on topics like phishing and data security. For example, carrying out a training session could help employees identify and avoid phishing attacks which are common threats in e-commerce. Having an incident response plan in place can also ensure the company can effectively handle its security incidents when they happen.

Technical Controls - These are based off software measures which insure protection for systems along with their data. When introducing a multi-factor authentication, it improves security drastically by making sure that only authorized or recognised users can have access to sensitive areas. Encrypting customer data both in transit and at rest is vital for protecting important information like credit card details. A great example of this is using the TLS encryption method which secures data transmission between customers and the e-commerce site. This regularly updates software which helps to close security vulnerabilities that attackers might exploit.

Physical Controls - These focus on securing physical locations in which the data is stored. This could employ the use of access controls like biometric scanners and surveillance in data centres. For an e-commerce company with servers inside its headquarters, to have aa highly strong physical security could help prevent

intrusions to highly sensitive information. Furthermore, having a constantly secure offsite backup could help in rapid recovery from data loss incidents.

All these controls together help to enhance the e-commerce business overall security by proactively reducing risks and ensuring swift responses to incidents. A great example is when using a Web Application Firewall which can protect the e-commerce site against common threats like SQL injection. Constant monitoring with intrusion detection systems helps to identify potential security issues early.

2.1. Financial Gain - The primary motivation for many cyber criminals is a way to make a financial profit. Stolen credit card information can easily be sold for money. Malicious actors could use the information to make unauthorized purchases, sell the data on a dark web forum, or use it to commit fraud. The expanding underground market for stolen financial information makes this a highly profitable method which drives attackers to intrude into platforms like Duzman Private Limited in this case.

Identity Theft – Passing instant financial concerns, malicious actors may also have the motivation along with the potential to cause identity theft. By gaining credit card information, social security numbers, or other personal data, attackers could make false identities or impersonate victims for various purposes, such as opening new credit accounts or applying for loans. This methos of cybercrime can have prolonging effects on victims, making it a lucrative and attractive option for some criminals.

Competitive Advantage - In some cases, threats can also originate from corporate espionage, where a rival company could look to gain a competitive advantage through unlawful methods. If Duzman Private Limited’s important sensitive customer data includes insights into their market strategies, pricing, or customer preferences, financial competitors could be motivated to plan a breach to gather this information. Attackers that work for rival companies could also be paid to sabotage the company to gain information that could also improve their own business aspects and desires.

Political or Social Activism - Some malicious actors are influenced by theoretical achievements like political or social activism. Hacker groups may target e-commerce companies to contest against known unethical practice, social injustice, or any other grievances. By sabotaging or compromising these platforms, attackers see to draw the attention to their campaigns. If Duzman Private Limited has been found to be connected to questionable practices or interests, it could attract the attention of activists seeking to influence change with the use of interruptive methods.

Reputation Damage and Brand Sabotage - In addition to financial reasons, some hackers might target a company's reputation to damage them. A data breach can severely lose customer trust and brand recognition, which leads to a loss of business and revenue. Competitors or angry insiders could plan an attack to harm Duzman Private Limited's operational capability or market position. A great example of this is when the company had to previously go through a negative publicity or consumer dissatisfaction. Attackers using a scenario as such would be able to make strategic moves interested in exploiting weaknesses for brand sabotage.

2.2. Social engineering talks of the psychological manipulation of individuals into performing actions or broadcasting sensitive information, commonly by exploiting emotions. Straying from traditional hacking techniques that rely on technical weaknesses, social engineering is dependent on using people to get an unauthorized access to any systems, data or highly sensitive information. Techniques that are commonly used include phishing emails, pretexting, baiting and tailgating.

Recognizing Social Engineering Threats

Employees of OpenMind have to stay vigilant and aware of the signs of probable social engineering advances. A few key indicators include…

Unsolicited Requests - Individuals must be wary of unrequested contact that asks for important information, especially if they create a feeling of panic or the use of pressure tactics.

Generic Greetings - Phishing attempts commonly use general greetings instead of personal names. Actual organizations usually will address an individual by their name.

Suspicious Links and Attachments – Emails that requests you to click on links or open attachments from unknown sources should be inspected quite carefully. Hovering over the links to check the actual URL before clicking could prevent an intrusion.

Inconsistencies - Watch for differences in email addresses, grammar along with logos. Scammers often use addresses that look the same or have poorly made texts or messages.

Unexpected Calls - Be suspicious of phone calls that requests for your information or verification, especially if the caller is not aware of the basic information the company would have had at the ready.

Strategies to Manage Risks

To regulate the risks with social engineering attacks, employees at OpenMind should implement the following

Security Awareness Training - Participate in training programs that teach employees about the multiple social engineering techniques, how to identify them and the critical role of cybersecurity. Phishing exercises can also aid in learning.

Verifying Requests - Implementing a process for verifying requests for highly sensitive information could entail calling back the requester using known contact information or checking with a supervisor.

Use Multi-Factor Authentication - For sensitive accounts, OpenMind should employ multi-factor authentication to add an additional layer of protection which makes it more difficult for unauthorized users to access accounts even if the login details are compromised.

Encourage Speculation - Encouraging a culture of speculation where employees are open to feel encouraged to question strange or suspicious requests. This also includes motivating them to take their time before responding to requests that ask for sensitive information.

Report Suspicious Activity: Establish clear procedures for reporting suspicious emails, calls, or incidents. Employees should know whom to contact and feel comfortable reporting any concerns without fear of reprimand.

Regularly Update Security Practices - Keep security practices and software up to date, which ensures that firewalls, antivirus software and anti-malware programs are operating correctly. Constant updates can also help protect against known weaknesses along with new threats.

Be Cautious with Personal Information - Employees should also limit the amount of personal information shared online, especially on social media. Attackers often scan social media platforms to gather information for social engineering attacks.

3.1. Symmetric encryption is a cryptographic process that uses the identical secret key for encrypting and decrypting information or data, meaning that the sender and recipient must discreetly share this key. One of its main qualities is that the safely of the encrypted data depends on the overall discretion of the key. If the key is compromised, the secrecy of the data is at a risk. Symmetric encryption algorithms are known for their speed and efficiency, especially when tasked with handling large amounts of data. This makes it applicable to a variety of functions which are encrypting sensitive data at rest, securing remote communication and protecting the data in transit by verifying that it is encoded before transmission.

Hashing on the other hand is a one-way cryptographic method that changes arbitrary input data into constant sized strings called hash values. Hash functions are made to be irreversible which means that once the data is hashed, the original data cannot be found again. A key attribute of hashing is that it makes a constant output size regardless of the input size and robust hash functions aim to reduce the possibility of collision, where different inputs give the same hash output. Hashing is commonly used in ensuring data integrity, safely storing passwords by saving hashes rather than having plaintext and verifying the integrity of transactions via logging and auditing.

When comparing the two, symmetric encryption focuses on having a constant confidentiality by allowing data transmission to be reversible, while hashing focusses on ensuring integrity through non-reversible transformation. Symmetric encryption needs cautious key handling as the same safety key can be used for encryption and decryption, while hashing does not use key management but is dependent on the identity of hash values to verify that data remains constant. Symmetric algorithms are usually quicker, especially for large datasets, where hashing is perfect for fast data integrity checks.

3.2. Certificate revocation is a vital component of a Public Key Infrastructure as it verifies the integrity and safety of digital communication. One of its main parts is managing risks that relate to compromised keys. When a private key related to a digital certificate is compromised, stripping of that certificate becomes necessary to prevent any unauthorized access or impersonation. This step is important because it verifies that even if someone achieves access to a compromised key, they cannot use the given certificate to show trust. Furthermore, the impact of a PKI depends on the trust of its digital certificates, if revoked certificates can continue to be recognized, it undermines the entire PKI system. For this reason, strong revocation mechanisms like Certificate Revocation Lists and the Online Certificate Status Protocol are vital for having a constant trust among users and systems that rely on these certificates.

Furthermore, many industries are managed by rules and regulations that shows how sensitive data must be protected, including the handling of cryptographic keys and certificates. A highly impactful certificate revocation method helps organizations to comply with these regulations, whereby failing to comply will promptly revoke their certificates and when necessary, could lead to a lawsuit, fines or even a loss of certifications. Organizational changes also require certificate revocation, either due to employee departures, role changes or updates within system status. It is also important to strip certificates that are no longer needed. This method ensures that only authorized persons and systems have access to sensitive information and resources, overall reducing risk exposure.

4.1. Multifactor Authentication is a vital component for advancing account security by having users to compulsory provide multiple forms of verification before gaining access. The importance of MFA lies in its reliability on three main types of verification factors, knowledge factors, possession factors and inherence factors. Knowledge factors, such as passwords and PINs are known and easy to apply, but they also have significant weaknesses where passwords can be taken via phishing or keylogging and users often use weak password practices. Possession factors provide an extra layer of security by having a physical item, which makes a

significant challenge for attackers. However, they are not without its own issues, users may lose their devices and the requirement of carrying extra items can be inconvenient. Lastly, inherence factors, which include biometric verification methods are difficult to make a copy of and provide swift access. Regardless, they raise privacy issues and can be exploited to technical weaknesses, as biometric systems may fail to recognize users due to changes in their physical condition.

4.2. The concept of least privilege in the context of access control is an important security principle that shows individuals and systems should be granted only the least level of access needed to achieve their specified part or goals. This method is mandatory for minimizing the attack area of an organization's network infrastructure, as it limits the probable damage that can happen if a user's account is compromised or if a system malfunctions. By verifying that employees, contractors and systems have access that is only necessary for their functions, organizations can reduce risk to both internal and external attacks. Such small meanings of access permissions drastically minimize the risk of data intrusions because if users are given further access, it most likely will increase the risk that sensitive information could be exposed or manipulated. If an employee with access to financial records unknowingly opens a phishing email and shares their login credentials, an attacker could exploit the given access to compromise important data, although in an environment that abides to the least privilege principle, the attacker's motivation to cause damage would be unjustified.

Furthermore, using least privilege improves audit and compliance measures by making it better to monitor user actions when access is limited to necessary functions, which creates clearer audit trails for detecting unauthorized activities. Additionally, the principle helps strengthen organizational sturdiness by managing the characteristics of malware or compromised accounts to spread across the network.