Resubmission June 2022 C

Incident Risk Management | Question 2

Tutor: Stephanie Itimi

Risk Assessment

Risk assessment is a critical component of any security analysis, as it helps to identify potential threats and vulnerabilities that could impact the security of an organization. Technology boosts the performance of the business which is a recommendable strategy. However, technology comes with some risks, which the management should foresee (Ridley et al., 2018). As businesses move from the brick-and-mortar setting to e-commerce, they should do risk assessments to ensure that measures are taken to mitigate the risks (Fraser & Simkins 2016; Marks, 2019). There are a variety of risk assessment methodology options available, each with its strengths and weaknesses. After careful consideration, I have selected the Open FAIR methodology to help with my analysis. Open FAIR is a comprehensive risk assessment framework that offers a structured approach to identifying and quantifying risks. It is based on the principle of FAIR (Factor Analysis of Information Risk), which is a well-established methodology for analyzing risk. This holistic approach to risk assessment ensures that all potential risks are considered and that the final risk assessment is as accurate as possible.

Common Weaknesses and Attacks

When conducting a risk analysis, it is important to consider both qualitative and quantitative approaches to get a comprehensive understanding of the risks involved. For each of the risks identified in the previous section, I will now explain whether I am using a qualitative or quantitative approach, and justify my decision. Network vulnerabilities are a key issue associated with software or hardware that exposes them to unauthorized party intrusion. A typical example is poorly configured firewalls which may attack eCommerce websites (Upadhyay & Sampalli, 2020). Operating system vulnerabilities are fundamental weaknesses that attackers exploit to access the asset on the e-commerce website or damage it (Adil et al. 2020). Lack of comprehensive security policies and procedures. This is because the main driver of this risk is the organization's culture and values around security, which is difficult to quantify. By conducting interviews with employees and management, I can get a better understanding of the organization's stance on security and what, if any, policies and procedures are in place.

Inadequate security training for employees. This risk involves identifying the number of employees who have received security training, which can be easily measured. I can also look at the organization's training records to see how often security training is provided and how comprehensive it is. additionally, a Lack of an incident response plan is another risk. The main driver of this risk is the organization's culture and values around security, which is difficult to quantify. By conducting interviews with employees and management, I can get a better understanding of the organization's stance on security and what, if any, policies and procedures are in place.

Lack of security awareness among employees: identifying the number of employees who are aware of security risks and how to protect themselves, which can be easily measured. I can also look at the organization's training records to see how often security awareness training is provided and how comprehensive it is. Inadequate security controls. The organization's culture and values around security, which is difficult to quantify. By conducting interviews with employees and management, I can get a better understanding of the organization's stance on security and what, if any, policies and procedures are in place. Most attacks are usually in defacement situations intending to send clear messages.

Risk	weight	score	Recommendation	Mitigation Approach
Inadequate security controls	High	9	Increase	Improve security controls
Lack of incident response plan	High	9	Develop	Develop a plan
Lack of comprehensive security policies and procedures	High	9	Retain	Adopt strict comprehensive policies
Inadequate security training for employees	High	9	Retain	Offer training to employees
Lack of security awareness among employees	Medium	8	Retain	Enhance security among employees

The Recovery Point Objective (RPO) is the maximum amount of data that your company can afford to lose. The Recovery Time Objective (RTO) is the maximum amount of time that your company can afford to be without its systems. We decided to use an RPO of 12 hours and an RTO of 24 hours. This means that our company can afford to lose up to 12 hours of data, and we can afford to be without our systems for up to 24 hours. Our risk appetite aligns with this decision because we are willing to accept the risk of losing up to 12 hours of data and being without our systems for up to 24 hours.

A resilience solution should help an organization recover from incidents and continue operating despite them. Network security solutions should help an organization protect its data and systems from unauthorized access and breaches. Vendor provision and lock-in solutions should help an organization avoid being locked into a single vendor or solution. Some benefits of using a resilience solution include the ability to recover from incidents quickly and continue operating despite them. Network security solutions include the ability to protect data and systems from unauthorized access and breaches. Using a vendor provision and lock-in solution includes the ability to avoid being locked into a single vendor or solution.

Some strengths of using a resilience solution include the ability to recover from incidents quickly and continue operating despite them. Some weaknesses of using a resilience solution include the need for specialized skills and knowledge to implement and maintain the solution and the potential for increased complexity and cost. Some strengths of using a network security solution include the ability to protect data and systems from unauthorized access and breaches. Some weaknesses of using a network security solution include the need for specialized skills and knowledge to implement and maintain the solution and the potential for increased complexity and cost. Some strengths of using a vendor provision and lock-in solution include the ability to avoid being locked into a single vendor or solution. Some weaknesses of using a vendor provision and lock-in solution include the need for specialized skills and knowledge to implement and maintain the solution and the potential for increased complexity and cost.

Impacts of a Successful Exploit on a Web Application’s Weakness

The impact of a successful exploit on a web application’s weakness can be catastrophic. Depending on the nature of the weakness, an attacker could gain access to sensitive information, execute malicious code on the server, or even take over the entire website (Adil et al., 2020). In some cases, the impact could be even worse, leading to a loss of data or a complete loss of service. In all cases, a successful exploit can have a serious impact on the security and stability of a web application.

Summary

Some weaknesses and attacks associated with eCommerce and social networking applications include SQL injection, cross-site scripting (XSS), Cross-site request forgery (CSRF), session hijacking, and man-in-the-middle attacks. Identifying the weaknesses and attacks helps the business decide on a dedicated vulnerability management service as it will be easy to manage and deploy (Sutton 2021). It will be critical as it will eliminate additional internal staff, which may increase the cost of vulnerability management. The business will have an appropriate management service with robust tools for handling weaknesses to patch management plans for build-outs. Identifying attackers' motivation in the development process will help the business pinpoint practical approaches to protecting the eCommerce website. It will also inform the business of the capability of the attackers and what the attackers are after in their target network.

Disaster Recovery Solution Design

Role of I.T. Professionals and Administrators

The role of IT professionals and administrators in disaster recovery solution design is to ensure that the organization's data and IT infrastructure are protected in the event of a disaster. They must design a solution that meets the organization's needs and budget, and that can be implemented quickly and easily in the event of a disaster (Aven, 2016. The solution must be able to restore the organization's data and IT infrastructure to a usable state promptly (Varshney & Alemzadeh, 2017). System administrators take part in developing strategies, design, and advising to mitigate system disruption and user errors. They are instrumental in managing and building comprehensive information for managing the whole Brick-and-mortar retailer.

Quality assurance analysts will play a critical role in mitigating process vulnerabilities of the eCommerce model to ensure that all the controls are reliable and functional. They will provide regular monitoring efforts to track the progress of mitigation of attacks and weaknesses to resolve issues efficiently (Aven, 2016). The security engineer will be critical in addressing network vulnerabilities by ensuring confidentiality, sensitivity, and security of data (Aven 2016). They will frequently analyze security systems to mitigate software issues or threats. Developers address operating system vulnerabilities by maintaining and producing new software programs with better results. They continue modifying the system and monitoring its performance as technology evolves.

Incident Response Protocol

Despite the adoption of measures to ensure the system’s safety, it is not guaranteed that the users will be safe. For this reason, frequent feasibility tests are recommended to ensure that all loopholes are identified and addressed. However, if an instance of an attack occurs, below is the recommendable protocol that the Zig systems should have in place. In an incident, all employees are expected to follow protocol:

- The safety crisis management team should be notified.
- The source of the incident should be established for ease of containing it.
- Disable or disconnect that affected network or devices to cut the connection.

- Depending on the severity of the attack, the incidence may be reported to the relevant authorities, such as the police, to mitigate the damage.
- An alert is made to all users and guides on how to navigate through the situation issued.
- Establish the needed improvement and modification of the system that can help overcome such attacks in the future.

As stated, besides the step-by-step address of an attack, the Zig systems must invest more in the system's security. This will be a strategic plan that can help it win the users' loyalty due to their trust in the system. Thus, the company should have real updates on the system's security features and threats to make the users aware of their role in the security system (Fahimnia et al., 2019). Nevertheless, to avoid attacks facilitated by the insiders, the administrators should have the power to suspend a suspected user’s account, close cloned accounts, and monitor transactions. Additionally, the users should first agree to meet the condition of avoiding any activity that risks other users. The violation should be countered with suspension or closure of the user’s account, depending on the severity of the violation.

Access Control Protocols

Control of the access is an effective way to minimize cyber-security issues. There are sensitive details that can be exposed if the system is not regulated and the users are not awarded different privileges (Pineiro-Chousa et al., 2017). For instance, if a user has the privilege of monitoring the transaction of other users, the chances of the misuse of the privilege are high due to personal interests. Thus, the administrators should ensure that all the users have been awarded limited privileges and powers per their platform use. Additionally, access to the user’s credentials, inventories, passwords, log-in certifications, and product descriptions should only be limited to the administrators. This will ensure that the authorized users will not have access to information that can be used to harm the system or other users. Among the measures to ensure that the system is secure and the user’s privileges are not misused will be to have strong passwords and two-factor authentication. Due to high privileges, biometric authentication is a big deal that the administrators should adopt to enhance the security and safety of systems.

References

Adil, M., Khan, R., and Ghani, M.A.N.U., 2020, February. Preventive techniques of phishing attacks in networks. In *2020 3rd International Conference on Advancements in Computational Sciences (I.C.A.C.S.)* (pp. 1-8). IEEE.

Aven, T., 2016. Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, *253*(1), pp.1-13.

Alhazmi, O.H. and Malaiya, Y.K., 2013, January. Evaluating disaster recovery plans using the cloud. In *2013 proceedings annual reliability and maintainability symposium (rams)* (pp. 1-6). IEEE.

Fahimnia, B., Pournader, M., Siemsen, E., Bendoly, E. and Wang, C., 2019. Behavioral operations and supply chain management–a review and literature mapping. *Decision Sciences*, *50*(6), pp.1127-1183.

Fraser, J.R. and Simkins, B.J., 2016. The challenges of and solutions for implementing enterprise risk management. *Business horizons*, *59*(6), pp.689-698.

Gupta, S. and Gugulothu, N., 2018. Secure NoSQL for the social networking and e-commerce based bigdata applications deployed in cloud. *International Journal of Cloud Applications and Computing (I.J.C.A.C.)*, *8*(2), pp.113-129.

Marks, L. 2019. The Optimal Risk Management Framework: Identifying the Requirements and Selecting the Framework.

Pineiro-Chousa, J., Vizcaíno-González, M., López-Cabarcos, M.Á. and Romero-Castro, N., 2017. Managing reputational risk through environmental management and reporting: An options theory approach. *Sustainability*, *9*(3), p.376.

Ridley, A., McCloskey, J. and Mountain, D. 2018. Machine Learning for Autonomous Cyber Defense. *The Next Wave22* (1): 7-14.

Sutton, D. 2021. *Information Risk Management*. 2nd ed. Swindon, U.K.: B.C.S. Learning & Development Limited.

Upadhyay, D. and Sampalli, S., 2020. SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, *89*, p.101666.

Varshney, K.R. and Alemzadeh, H., 2017. On the safety of machine learning: Cyber-physical systems, decision sciences, and data products. *Big data*, *5*(3), pp.246-255.

Veerasamy, N., 2020. Cyberterrorism–the spectre that is the convergence of the physical and virtual worlds. In *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 27-52). Academic Press.