DEN1 TASK 1: CYBERSECURITY MANAGEMENT PLAN

Skerdilaid Hoti

College of Information Technology, Western Governors University

February 10, 2024

A. Summary of Gaps in Security Framework

SAGE Brook’s security framework includes many identified gaps that were described in the report. The first is a lack of alignment with security best practices and industry standards. Based on policies and procedures present there is a lack of coverage for securing payment card data (PCI DSS) and the company lacks the proper controls for protecting privacy for EU customers in compliance with GDPR. There are also many present deficiencies in the cybersecurity program present, the incident response plan is missing many key features including specific roles and responsibilities, and the business continuity plan is missing key features.

B. Mitigation Strategies

In order to fix the gaps present in the framework mitigation strategies must be put in place. To first meet compliance standards the company must first create policy documents for securing organizational assets, protecting payment card data, and ensure privacy protection for EU customers. It is also important to regularly review and update these policies to stay updated on current threats and regulatory changes. To do all this SAGE could hire an expert on regulatory compliance and assign them in charge of fixing the company's current lack of present policies. Next the company needs to revamp its current cybersecurity awareness training program. NIST standards are a good place to start in learning what should be covered but more specifically it should recognize phishing, safeguarding sensitive information, email threats, and adhering to company security policy. It should become policy for the training to be mandary and put in place a metric and evaluation system to ensure the new policy is effective. Next it is important for the incident response plan to be updated. Clear defined roles and responsibilities need to be assigned due to the lack of. Then once those are defined a detailed list of procedures which should follow the outlines present in the NIST SP 800-61 which provides steps for identifying and categorizing incidents, coordinating response efforts, and documenting findings for post-incident review (NIST). Finally the last step would be to improve the BCP. The first step would be to conduct a risk assessment to identify potential disaster threats and their potential impact. Then define the steps of recovery for each identified risk. Finally test and review the BCP using tabletop exercise and simulations to ensure it will be effective.

C. Critical Security Staff Positions and Responsibilities

Three critical security staff that will need to be hired would be a compliance officer, risk analyst, and a governance specialist. The compliance officer will ensure the company is adhering to regulatory requirements such as PCI DSS and GDPR. Their job will be to monitor and assess the organization's compliance with applicable laws, regulations and standards. They will also be incharge of developing, implementing and maintaining these policies. Finally they will ensure audits are being completed to ensure compliance is being maintained throughout the organization. The next staff to be hired will be the risk analyst. They will be responsible for identifying, assessing, and prioritizing security risks to the organization. They will first begin by conducting a risk assessment and vulnerability scans to identify all the issues currently present. Following this they will begin to develop risk mitigation strategies and controls to reduce residual risk present in the organization and finally provide reports and updates to upper management to identify critical risk and recommend remediations for these risks. The last hire will be the governance specialist. His job will be to develop and maintain security policies, procedures and standards to help the company align with industry best practices. In order to accomplish this they will need to establish the governance frameworks to ensure effective oversight of security related activities. As with all the other roles they will need to ensure regular reviews of the controls are present in order to maintain compliance with company policy.

D. Physical and Logical Vulnerabilities

Three physical vulnerabilities present include vulnerable distribution centers, weak physical access controls, and weak security measures during transportation. Some of their distribution centers located in San Joaquin, Keene, Cape Coral are all vulnerable to natural disasters and especially with the current lack of a proper BCP plan this weakness becomes more apparent. Natural disasters disrupt operations, damage infrastructure and can compromise the safety of staff. The next weakness is physical access controls. The report mentions a weakness which can lead to access to unauthorized areas. Weak physical access controls can result in theft, vandalism or a compromise of sensitive information. The third physical vulnerability is weak security measures during transportation. Lack of security controls can result in theft, loss or tampering of merchandise. This can cause customer dissatisfaction and damage to brand image.

Next for the logical vulnerabilities, they include a weakness in the E-commerce website security, weak network security measures, and lack of data encryption policy. The report includes concerns regarding the security of the company website such as unpatched software, insufficient encryption protocols, and lack of proper access controls. This can lead to privilege escalation, data exfiltration or leave the site open to attacks such as injection or scripting attacks. Issues such as weak network access controls could lead to malware infections, phishing attempts or network access which can lead to data exfiltration. The final logical control would be the lack of encryption protocols. Without proper encryption protocols it becomes difficult to adhere to confidentiality promised to customers. Unencrypted data can lead to data leakes and compliance violations.

E. Cybersecurity Awareness Training Program

We can use NIST SP 800-50 This NIST publication provides guidance on developing, implementing, and maintaining an effective security awareness and training program within an organization (NIST). Also to better understand specific instructions based on job role we can use NIST SP 800-16 This NIST publication presents a role-based model for designing security training programs tailored to specific job functions and responsibilities within an organization (NIST).To limit the scope of attack a new cybersecurity awareness training program must be initiated. As part of the new system annual training requirements will be added. Staff will be required to complete annual training modules covering topics such as phishing awareness, password security, social engineering, data protection, and incident reporting procedures. Staff will be given interactive learning platforms, workshops, and quizzes to ensure they are engaged and taking the training seriously. In order to better cover each topic specialized roles will receive more training due to the higher risk they pose to the organization. In order to ensure the yearly training will be effective it is important to continuously remind employees of what was learned using ongoing newsletter, posters or awareness messages. Phishing simulations are also used at many companies to ensure employees are not being tricked by common email scams. To ensure the effectiveness of the program it will be essential to use key performance indicators (KPI) such as completion rates, quiz scores, number of people who clicked on the fake phishing emails.

F. Standards for Securing Organizational Assets

To secure organizational assets we must implement standards such as AUP, mobile device management, password policy, and PII protection policy. The first policy or acceptable use policy is used to define acceptable activities in using organization resources which can include computers, networks, the internet, and data. The AUP should follow regulatory frameworks such as GDPR and PCI DSS in this case. A mobile device policy such as BYOD should also be present. In using BYOD it is essential that employees adhere to the AUP to maintain company policies and compliances in check. Password policy is also important in order to maintain security posture. PCI DSS and NIST both include guidelines and mandates to implement strong passwords to protect sensitive information. If we look at NIST SP 800-63 it recommends the use of longer passwords or passphrases over traditional complexity requirements, recommending a minimum length of 8 characters with allowances for longer passphrases. Additionally, they discourage frequent password changes except in cases of suspected compromise, promote secure storage practices such as salted hashing, and emphasize user education to foster better password hygiene and mitigate risks associated with password-based authentication (NIST). The last policy is to protect PII and to do this it is important to outline procedures and safeguards for collecting, storing, processing, and sharing this data. It is important this data is always encrypted at all stages of transportation and rest. PII protection is required for compliance with GDPR. If we look at GDPR policies we can explain it as GDPR mandates that personal data must be processed lawfully, transparently, and for specified purposes, with organizations minimizing data collection and ensuring its accuracy and security. Individuals have rights over their data, including access, rectification, and erasure, while organizations must promptly report data breaches and obtain explicit consent for data processing. International data transfers are subject to stringent requirements to maintain data protection standards equivalent to those within the EU (GDPR).

G. Incident Response Plan (IRP)

Preparation-

First establish an incident response team which includes members representing relevant departments such as IT, security, legal, and communications. Next it's important to define the roles and responsibilities of each team member including coordinators, investigators, and ensure proper communication. Next establish the proper communication channels and contract information for key stakeholders, including internal personnel, external partners, and regulatory authorities.

Detection and Analysis-

Implement monitoring tools to detect incidents such as IDS, SIEM and EDR solutions. Next it's important that staff is properly trained to recognize the signs of a security incident and report any suspicious activities. Ensure that this is an established procedure for assessing the scope and impact of security incidents including gathering evidence, analyzing log files, and conducting forensic investigations. Incidents should be classified based on severity defined in the risk assessment as a guideline.

Containment, Eradication, Recovery-

The first step is to Activate the incident response team and initiate the containment measures to prevent further damage. If the issue is within the network then Isolate affected systems or networks to limit the spread of malware or unauthorized access. Implement a recovery procedure to restore the affected systems to a known good state. Finally communicate with stakeholders and partners to keep them updated and notify them of potential impact to business operations.

Post-Incident Activity Phase:

Conduct a post-incident review to evaluate the effectiveness of the incident response process, identity lessons learned, and make recommendations for improvement. Update the incident response plan to improve it based on what was learned.

H. Business Continuity Plan (BCP)

Project Scope and Planning:

Establish a BCP team which includes members from key departments such as IT, operations, finance, human resources. Identify critical business functions, processes, and resources necessary for maintaining operations during and after a disaster. Conduct a risk assessment to identify potential threats and vulnerabilities that could disrupt operations. Define the scope and objectives of the BCP.

Business Impact Analysis (BIA):

Perform comprehensive BIA to assess the potential impact of the natural disasters such as earthquakes, tornadoes, and flooding on SAGE books operations and revenue. Identify critical dependencies, including key personnel, IT systems, infrastructure, and suppliers, and evaluate their status. Quantify financial and operations consequences of downtime or disruption to prioritize recovery efforts and allocate proper resources.

Continuity Planning:

Develop strategies and procedures for maintaining essential business functions and services during and after disaster. Establish redundant systems such as a hot site, remote capability to ensure continuity of operations. Implement protective measures for critical assets and infrastructure. Define escalation procedures and roles for decision making when activating the BCP in response to disaster in order to ensure clear communication and coordination among stakeholders.

Plan Approval and Implementation:

Present BCP to stakeholders such as senior management for review and approval. Obtain proper funding from stakeholders to ensure resources are allocated appropriately to maintain the BCP. Develop a detailed implementation plan outlining tasks timelines and parties responsible for executing the BCP. Conduct tabletop exercise and simulations to validate effectiveness of BCP. Monitor and evaluate BCP performance and make adjustments.

References

National Institute of Standards and Technology. (n.d.). NIST *cybersecurity framework (CSF)*. https://www.nist.gov/cyberframework

Chapple, M., & Seidl, M. (2023). (ISC)2 *CCSP certified cloud security professional official study guide.* Sybex. (3rd ed.) https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3375845&site=eds-live&scope=site

Copeland, M., Soh, J., Puca, A., & Harris, M. (2020). *Microsoft Azure: Planning, Deploying, and Managing the Cloud*. (2nd Edition). Springer. https://wgu.percipio.com/books/3066d572-95c9-49c4-ac7d-9a3c35458b25#epubcfi(/6/4!/4/2[epubmain]/2[g4b3ab31c-3312-43db-ab7d-aa8b2115ff18]/2/2/1:0)

Estrin, E. (2022). *Cloud security handbook: Find out how to effectively secure cloud environments using AWS, Azure, and GCP.* Packt Publishing. https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3198558&site=eds-live&scope=site