­

**DEN1 TASK 1: Cybersecurity Management Plan**

David Garlisch

College of Information Technology, Western Governors University

9/16/2024

Cybersecurity Management Plan

**A. Summary of Gaps**

The Independent Security Report for SAGE books conducted by the Secure Tech Solutions team found many security gaps in the company’s current security posture.

1. **Not adequately aligned with security best practices:** The company’s security program is not aligned with the best practices and industry standards. The security program does not provide a fully integrated strategy for
   1. Safeguarding organizational assets (Inadequate asset protection measures, must use adequate policies)
   2. Compliance with PCI-DSS (Payment card data security needs to be implemented when dealing with users payment card data)
   3. Compliance with GDPR (EU customers need to comply with this privacy data law)
2. **Lack of appropriate expertise:** SAGE Book’s lacks the necessary expertise to implement security strategies and projects related to regulatory compliance effectively. The company must hire at least 3 additional staff to cover Governance, Risk, and Compliance (GRC) for the SAGE Book’s using the National Initiative for Cybersecurity Education (NICE) Cybersecurity Framework as a guide.
3. **Insufficient cybersecurity program:** The current program does not align with the best practices and industry standards. At the same time, only a quarter of the new hires had training, and only a 10th of the current employees have taken training at all. The company should use the National Institute of Standards and Technology (NIST) standards as a reference point as well as the PCI requirement 12.6, which says that the program should educate all employees on the importance of protecting cardholder data while maintaining security practices.
4. **The Incident Response Plan (IRP) lacks comprehensive coverage of the incident response process:** The key gaps are undefined roles and responsibilities for the incident response team and insufficient procedures for incident handling and analysis. This can be rectified by aligning the IRP with NIST SP 800-61 R2, which is recommended to enhance response capabilities and better protect information assets.
5. **Business Continuity Gaps (BCP) Gaps Identified:** SAGE Books' BCP does not adequately address natural disasters based on the location of the distribution centers. It lacks specific recovery plans for earthquakes, tornadoes, and flooding. Enhancements are needed in

* project scope and planning
* business impact analysis
* continuity planning
* plan approval and implementation efforts

, which will ensure efficient recovery and minimize potential revenue loss.

**B. Mitigation Strategies**

**1. Safeguarding the Organization's assets:** Implementing Acceptable Use Policies (AUP) will help us define the appropriate use of the company’s assets and each user's responsibility.This will work in tandem with utilizing the principle of least privilege by only allowing authorized users access to sensitive payment card data or PII. Mobile Device Management (MDM) should be implemented to ensure secure usage and remote encryption/wipe capabilities. Enforcing password policies by NIST can help the company enhance security and compliance with best practices. Lastly, we can add multi-factor authentication (MFA) to help prevent users from being compromised (NIST, 2020).

**Security of payment card data | Compliance with PCI-DSS:** To ensure the security of payment card data and maintain compliance with PCI-DSS, a detailed policy is being enforced that governs the secure collection, transmission, and storage of payment card data. This includes encrypting cardholder data in transit and at rest, implementing strict access control measures to limit data access to authorized personnel only, and conducting regular PCI-DSS audits to ensure compliance. These actions will protect sensitive payment information while reducing the risk of data breaches and safeguarding the organization's reputation.

**Privacy protection with EU customers | Compliance with GDPR:** This policy encompasses procedures designed to protect the rights of EU citizens. This includes the right to access, correct, and delete their personal data. It ensures that data collection, processing, and retention are limited strictly to what is necessary for legitimate business purposes. A breach notification process is in place to promptly report any data breaches within the 72-hour timeframe stipulated by GDPR.

2. **Expertise Gap:** We must hire 3 additional employees to oversee the GRC program. These roles will be identified and filled based on the National Initiative for Cybersecurity Education (NICE) Cybersecurity Framework, ensuring that each position is aligned with the necessary knowledge, skills, abilities, and tasks critical to the success of the GRC program (NIST, 2020).

The expanded team will include roles specifically focused on:

* **Governance Analyst:** This position will focus on developing and enforcing security governance policies, ensuring that all security efforts align with the company’s strategic goals and regulatory obligations.
* **Risk Management Specialist:** This individual will identify, assess, and mitigate risks to the organization, ensuring that risk management processes are integrated across all security initiatives.
* **Compliance Specialist:** This role will oversee adherence to regulatory requirements and ensure all policies and procedures comply with relevant standards.

3. **Cybersecurity Awareness and Training:** A structured cybersecurity awareness training program will be conducted for all employees and new hires regularly, which will fully align with NIST standards and comply with PCI DSS Requirement 12.6, which mandates regular training to ensure that all personnel know the importance of protecting cardholder data (NIST, 2020). The training will be mandatory. It will cover essential topics such as recognizing phishing attacks, understanding the importance of strong passwords, and maintaining secure practices. Regular refresher courses will be implemented to ensure ongoing compliance and to adapt to emerging threats. This program ensures that all employees have the knowledge and skills to protect sensitive information and contribute to a secure working environment.

4. Enhancing IRP Roles and Procedures: Key enhancements to the IRP will include: NIST SP 800-61 R2 framework will help SAGE Books by significantly enhancing its incident response capabilities, ensuring that the organization is better prepared to protect its information assets and respond to security threats in a timely and effective manner (NIST, 2020). We can also define roles and have clear procedures for our employees in case of an incident.

* **Defining Roles and Responsibilities**: Establishing clear roles for each incident response team member, including specific responsibilities during each phase of an incident. This ensures everyone knows their duties and can act quickly and decisively when a security incident occurs.
* **Detailed Incident Handling Procedures**: Developing comprehensive procedures for each phase of incident response. These are preparation, detection and analysis, containment, eradication and recovery, and post-incident activities. These procedures will provide a step-by-step guidance to ensure that incidents are managed effectively and efficiently, which minimizes potential damage and ensures a swift recovery.

1. **Enhancing the Business Continuity Plan BCP:** To ensure that SAGE Books can maintain or quickly restore operations following these events, the BCP will be revised to include a comprehensive recovery strategy focusing on natural disasters at each location.

* **Project Scope and Planning**: Clearly define the scope of the continuity plan, identify critical business functions, and assign responsibilities to ensure that all aspects of disaster preparedness are covered. This phase will involve collaboration with key stakeholders across the organization to ensure that the plan addresses the needs of each distribution center.
* **Business Impact Analysis (BIA)**: Conducting a detailed analysis to assess the potential impact of various natural disasters on business operations. The BIA will identify critical business functions, dependencies, and disruptions' potential financial and operational impacts. This analysis will also help inform the prioritization of any recovery efforts and resource allocation during a disaster.
* **Continuity Planning**: Developing specific strategies and procedures to ensure continuity of operations during and after a natural disaster. This includes identifying alternative facilities, establishing communication plans, and ensuring that critical systems and data are backed up and can be quickly restored. It will also outline evacuation plans and emergency response procedures.
* **Plan Approval and Implementation**: Once the revised BCP is developed, it will undergo a formal review and approval process by senior management. Following approval, the plan will be implemented through training, drills, and regular updates to ensure that all employees know their roles and responsibilities during a disaster.

**C. Roles and Responsibilities**

As we discussed before, these 3 key roles below are recommended by the NICE framework. Each role is essential for ensuring that SAGE Book’s can bolster its security posture and adhere to industry standards with GRC.

* **Governance Analyst:** This position will focus on developing and enforcing security governance policies, ensuring that all security efforts align with the company’s strategic goals and regulatory obligations.
* **Risk Management Specialist:** This individual will identify, assess, and mitigate risks to the organization, ensuring that risk management processes are integrated across all security initiatives.
* **Compliance Specialist:** This role will oversee adherence to regulatory requirements and ensure all policies and procedures comply with relevant standards.

**D. Vulnerability and/or Threats**

**Physical Vulnerabilities/Threats**

**Natural Disasters at Distribution Centers:**

SAGE Books has strategically located distribution centers in CA, TX, and FL. However, they didn’t consider that these areas are prone to natural disasters such as earthquakes, tornadoes, and flooding.

* **Impact**: The BCP does not sufficiently cover recovery strategies for these events. If a natural disaster were to occur, it could result in significant downtime, loss of inventory, or even severe disruptions in the supply chain. This would negatively affect customer satisfaction and lead to considerable revenue losses.

**Inadequate Physical Security Controls at Retail Locations:**

With 400 retail locations across the United States, there is a large potential for inconsistencies in physical security measures. This can include surveillance, access controls, and alarm systems.

* **Impact**: These vulnerabilities could lead to the theft of physical assets, unauthorized access to sensitive information stored on any stolen equipment or devices, and potential harm to employees or customers. This could compromise the safety of staff and customers, result in financial loss, and damage the company’s reputation.

**3. Insider Threats Due to Unsecured Facility Access:**

SAGE Books may lack comprehensive access control to its facilities, including corporate headquarters and distribution centers. This lack of control can lead to potential insider threats, where employees or other trusted individuals could exploit their access to harm the company.

* **Impact**: The theft of sensitive information, sabotage of systems, or unauthorized access to critical areas can all happen when enabling insider threats with a lack of these controls. This could lead to data breaches, operational disruptions, and significant financial and reputational damage. Addressing these vulnerabilities through stricter access controls, job rotation, mandatory vacation, least privilege, and monitoring could mitigate the risks associated with insider threats (NIST, 2020).

**Logical Vulnerabilities/Threats**

**Insufficient Security Training:**

The company’s cybersecurity awareness program is significantly lacking, with only 10 percent of employees receiving any form of security training. Also, the training content does not align with industry best practices or standards, such as those outlined by NIST and PCI DSS.

* **Impact**: Employees are less likely to recognize and respond appropriately to security threats like phishing or social engineering attacks without adequate training. This vulnerability increases the likelihood of successful attacks, which could compromise sensitive data, disrupt business operations, and lead to financial and reputational harm. Ensuring that all employees receive regular and comprehensive training is critical to mitigating these risks.

**Inadequate Incident Response Plan (IRP):**

The current IRP is insufficient, lacking detailed procedures and clearly defined roles and responsibilities for incident response team members. This misalignment with best practices, such as those outlined in NIST SP 800-61 Revision 2, limits the organization's ability to respond to security incidents (NIST,2020).

* **Impact**: An ineffective IRP can result in delayed responses to security incidents, allowing threats to escalate and causing even greater damage. This could lead to extended system outages, significant financial losses, and long-term damage to the company's reputation. Going over the company’s MTD, RTO, and RPO will help strengthen the IRP, and it can also be strengthened by aligning it with recognized best practices, which will enhance the organization’s ability to mitigate and recover from security incidents. Going over the

**Gaps in the Business Continuity Plan (BCP):**

The BCP currently being used is rudimentary at best and does not adequately address recovery strategies for various potential disruptions, particularly those caused by natural disasters. The plan lacks comprehensive sections on project scope and planning, BIA, and continuity planning.

* **Impact**: Without a robust BCP, the company is vulnerable to prolonged downtime and significant operational disruptions in the event of a disaster or other critical incidents. This can lead to substantial financial losses and damage to customer trust. Updating the BCP to include detailed recovery strategies and regularly testing the plan will be essential to maintaining operational continuity and protecting the company's interests during emergencies.

**E. Training**

For our cybersecurity security and awareness program, we will use the standards set by NIST by using the NIST SP 800-50 Rev. 1 (NIST, 2024). The importance of this training program will make sure that each employee and new hire has adequate training to help them understand the importance of protecting data and utilizing best practices in the workplace.

**Annual Training Requirements:** Annual training will take place at SAGE Books to make sure each employee is up-to-date on phishing attacks and how to deal with them, how to protect PII, password security best practices, the company’s AUPs, and the importance of GDPR and PCI-DSS compliance is and what that entails. Training will be done through an online platform where each person can meet and interact with others, and there can be a quiz to ensure each employee understands the content and its importance. There will also be a mandatory assessment to ensure that each employee/new hire receiving the training understands the material.

**Specialized Training Requirements:** Specialized training will include everything from secure coding best practices and compliance procedures/protocols on handling EU users' Data for GDPR, being compliant with PCI-DSS, and receiving audits to stay up-to-date and in good standing. The specialized training will be conducted semi-annually because of the importance of these topics and because we will meet regulatory compliance continuously. Each role can be tailored to receiving specific training targeted at the users’ current role to help ensure the best training practices for them.  
  
**Continued Awareness:** To help maintain a continuous awareness program throughout the year, we will send out newsletters via email with current information and simulate phishing attacks through email, where we can see who is clicking on links or not dealing with these social engineering attacks effectively. We can then make sure they are properly educated and trained. We can also offer refresher courses for all employees. The goal is to help the company’s users stay proactive and educated on these best practices because the threat landscape is ever-changing.

**F. Policies**

NIST will aid SAGE Book’s in implementing a comprehensive policy for AUPs, mobile devices, passwords, and PII to help protect the organization most effectively.

**Acceptable Use Policy:** To ensure that all employees at SAGE Books understand their responsibilities when using company assets, we will implement policies guided by NIST SP 800-53 Rev. 5. This standard provides a robust framework for system and communications protection, particularly through Control SC-12, which outlines the necessary controls for enforcing acceptable use requirements. These controls will help ensure that employees are fully aware of the appropriate use of organizational resources and the potential consequences of failing to adhere to these guidelines. This will help reduce the overall risk of security incidents caused by improper use by the employees at SAGE Book’s.

**Mobile Devices:** Mobile Device Management will now come into play and be utilized by the company, a policy covering both company-owned and any BYOD devices, which will help safeguard corporate data. NIST SP 800-124r2 will aid SAGE Book’s in the best practices for the security of mobile devices. Some key elements are remote wipe capabilities, encryption, and strong authentication methods, which will, in turn, help safeguard sensitive information and reduce the risk of data breaches.

**Password Policy:** A robust password policy is paramount for a secure environment. NIST SP 800-63B will aid the company with a strong password policy to protect against unauthorized access and sensitive data. NIST offers password security recommendations on complexity, password rotation, and recovery while stating the importance of using multi-factor authentication (MFA). MFA can help greatly reduce the chance of a user's account being compromised and is a relatively easy implementation. Following NIST SP 800-63-B on the best password policies will greatly minimize the risk of any authorization/password-related attack.

**PII Protection:** Protecting any PII when dealing with customer data is of the utmost importance because it can cause legal problems and damage to the company's reputation. We must ensure that any PII is handled properly and securely throughout its lifecycle of storage, processing, and disposal of data. NIST SP 800-122 will guide SAGE Book’s on the importance of this data and how we should encrypt the data as well as the access controls around it protecting the PII and how to properly have an incident response plan in place in case any issues arise. The company also has EU customers' data, which is why we need to keep up-to-date on complying with the General Data Protection Regulation, which is a guide on how to handle EU citizens' data properly by only collecting data for legitimate purposes, making sure it's stored securely, and only processed with the necessary consent from the user.

**G. Incident Response Plan**

NIST SP 800-61 Rev. 2 will aid us in developing a proper IRP utilizing the 4 phases of an incident response plan: Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity.

* **Preparation:** In this initial phase, we will establish a dedicated incident response team(IRT) with defined roles and responsibilities. They will have to undergo regular training to stay up-to-date and properly handle and deal with any potential incidents. We must ensure that our team has the necessary tools to monitor and analyze data. Policies and procedures will be developed using NIST SP 800-61 Rev. 2 and cover the lifecycle of the incident from beginning to end. We will regularly update and review these policies to align with the industry's best practices.
* **Detection and Analysis:** The second phase will identify potential security incidents. Monitoring and detection will be used to detect any unusual traffic across networks and systems. Automated alerts can be set in place with a SEIM or other means to alert of any suspicious behavior that may indicate a security incident or breach has occurred. When the team detects incidents, we will use incident classification and rate the severity, impact, and urgency. This will allow the team to respond appropriately and effectively. At the end of the incident, we will use documentation in a tracking system to help with future incidents and document what was done.
* **Containment, Eradication, and Recovery:** In this phase will focus on containing the incident, then eradicating the threat, and finally recovering from the incident as a whole back to normal. The team will contain the incident by isolating affected systems and getting them off the internet to prevent any further damage. After isolating and containing the system, we can focus on eradicating the root cause of the issue by removing the threat or malware, for example. We then can move on to recovery, restoring the company to normal operation. If needed, we can use backups or rebuild affected systems.
* **Post-Incident Recovery:** In this final phase, we will learn from the event and see what we can improve on in the future. We will do an incident review, including the timeline of the incident and the actions taken by the IRT. Then, we can document lessons learned and provide any training needed to the IRT. Lastly, we will want to provide a detailed report to management and stakeholders to concisely say what the incident was, how it was handled, and how the IRT will improve on this going forward.

**H. Continuity Plan**

To safeguard SAGE Books against natural disasters such as earthquakes, tornadoes, and floods, a comprehensive Business Continuity Plan (BCP) should be implemented. We will use the guidelines provided in NIST SP 800-34 Rev. 1, SAGE Books will adopt industry best practices to ensure the continuity of critical operations during and after such events.  
  
**Project Scope and Planning:** In this initial phase of the BCP, we will define the project scope and identify critical assets the business must maintain during a disaster. We will also assign users with key roles and responsibilities to ensure critical functions are restored as soon as possible in case of a disaster. We will also look at our locations in CA, TX, and FL, which are at higher risk for earthquakes, tornados, and floods, and plan accordingly. The team can look at how we will back up data and maintain operations during a disaster as well.  
  
**Business Impact Assessment (BIA):** This phase will help us understand the financial and operational impact of the disaster disruptions on our distribution centers. The team will prioritize and identify the most important and critical business functions that must be restored as quickly as possible. We will want to minimize the downtime as best we can on things that can greatly impact the organization. An impact assessment of the BIA will help quantify the potential losses associated with different disaster scenarios at each location and help with our decision-making in our resource allocation and recovery priorities. In this phase, we will also establish our Recovery Time Objectives (RTO) to help restore operations and our Recovery Point Objectives (RPO) to help restore our data quickly and efficiently.

To safeguard SAGE Books against natural disasters such as earthquakes, tornadoes, and floods, a comprehensive Business Continuity Plan (BCP) should be implemented. Leveraging the guidelines provided in NIST SP 800-34 Rev. 1, SAGE Books will adopt industry best practices to ensure the continuity of critical operations during and after such events.In this phase, we will use strategies and procedures to help our business continue operating during and after a disaster. Disaster recovery strategies will be utilized here to ensure the business remains running. We can do so by using an alternate warm or cold site based on RTO, RPO, and MTD, or we can use different backup or cloud strategies for some redundancy. We also will create a communication plan that outlines different communication channels for employees, customers, and stakeholders. After that, performing drills with our users can help prove the effectiveness of our created plan and help identify any areas for improvement.

**Plan Approval and Implementation:** In this last phase, we will need approval from management to implement the created plan across the organization. Management will need to ensure the plan aligns with the company's goals and effectively identifies the critical assets based on the company's risk tolerance. Any feedback for revisions will given at this stage. When approval is given, it will be implemented across all locations, and the training of employees on proper resource allocation of the BCP will commence. Lastly, the BCP should regularly be reviewed and updated to ensure its effectiveness in any disaster. We can also review and update after a disaster based on lessons learned or any new emerging threats.

**References**

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

National Institute of Standards and Technology (NIST). (2020). NICE Cybersecurity Workforce Framework (NIST Special Publication 800-181 Rev. 1). <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

National Institute of Standards and Technology. (2024). Building an information technology security awareness and training program (NIST Special Publication 800-50 Rev. 1). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf>

National Institute of Standards and Technology. (2021). Guidelines for managing the security of mobile *devices in the enterprise* (NIST Special Publication 800-124 Rev. 2). U.S. Department of Commerce. <https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/final>

National Institute of Standards and Technology. (2021). Digital identity guidelines (NIST Special Publication 800-63B). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>

National Institute of Standards and Technology. (2010). Guide to protecting the confidentiality of personally identifiable information (PII) (NIST Special Publication 800-122). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>

**National Institute of Standards and Technology.** (2012). Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

**National Institute of Standards and Technology.** (2010). Contingency planning guide for federal information systems (NIST Special Publication 800-34 Rev. 1). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>