Cybersecurity Management Plan

Jamal Rizki

Cybersecurity Management Plan

A1. Summary of Gaps

The Security Report performed by Secure Tech Solutions identified several significant issues within SAGE Books current security posture. The organization does not currently meet either the Payment Card Industry Data Security Standard or the General Data Protection Regulations. As it stands, there are currently no acceptable use, device management, or password management policies. This leaves personally identifiable information (PII) vulnerable, exposing the company to potential regulatory breaches.

SAGE Books cybersecurity team is currently understaffed and lacks expertise. Cybersecurity awareness training is conducted on an irregular schedule, with current statistics showing only a 10 percent completion rate among employees. These findings demonstrate a weak security culture and ultimately leave employees more susceptible to social engineering attacks.

The current Incident Response Plan (IRP) and Business Continuity Plan (BCP) both lack key information such as defined roles, recovery planning, recovery timeframes, and clear procedures for incident handling processes.

B. Mitigation Strategies

To address these gaps, SAGE books should implement the following:

PCI DSS Compliance – Develop and implement written policies for secure payment processing that align with PCI DSS requirements. Protect data confidentiality by encrypting data in transit and at rest to prevent unauthorized access. Enforce and monitor network segmentation between the retail system and both the corporate and public network to prevent the loss of sensitive cardholder data. Conduct annual PCI DSS assessments to assess compliance.

GDPR Compliance – Establish lawful collection of users data and delegate the monitoring and compliance to dedicated representatives. Protect the confidentiality of data by encrypting data in transit and data at rest to prevent unauthorized access.

General controls – Establish Acceptable Use, Password, and Mobile Device policies that align with NIST best practice standards. Implement mandatory security awareness trainings for all employees, as well as continuous social engineering simulations. Implement regular Incident Response Plan (IRP) and Business Continuity Plan (BCP) revisions and simulations to prepare for and test response readiness.

C. Roles and Responsibilities

To meet compliance, risk and governance requirements, SAGE book should hire extra staff. Three critical roles include:

1. Security Control Assessor (SP-RSK-002) - The Security Control Assessor will be responsible for evaluating the effectiveness of the company's security controls. This includes assessing compliance with PCI DSS and GDPR regulations. They will review policies and procedures to assess effectiveness and confirm that business objectives are being met.
2. Cyber Defense Incident Responder (PR-CIR-001) - The Cyber Defense Incident Responder will oversee all phases of the incident-handling process. They will investigate, analyze, and

respond to cyber incidents. They will develop documentation to ensure business readiness and will evaluate and plan incident-response processes to strengthen organizational response efforts.

3. Cyber Instructional Curriculum Developer (OV-TEA-002) - The Cyber Instructional Curriculum Developer will be responsible for designing, implementing, and maintaining cybersecurity-awareness and training programs for all employees. They will monitor employee participation and program effectiveness and ensure the material remains current. The training content will align with company policies and with third-party regulations and standards where applicable.

D. Vulnerability and/or Threats

Physical Threats and/or Vulnerabilities:

Natural Disasters – The company currently has distribution centers in California, Texas, and Florida. These are all high-risk areas where earthquakes, hurricanes, flooding, and tornadoes are potential threats.

Physical Access – A lack of physical access controls can lead to instances of unauthorized entry. This could include theft of physical

equipment, loss of data or intellectual property, or potential sabotage by a threat actor.

Power failure – Critical systems lack redundancy. Outages could lead to a loss of revenue for the business, potential in-store downtime, and outages across the e-commerce platform.

Logical Threats and/or Vulnerabilities:

Social Engineering – Employees are currently lacking proper training. Potential issues include the introduction of malware, phishing attempts, and PII data loss. Overall, this leads to a compromise of the confidentiality, integrity, and availability (CIA) of data.

Unencrypted data – Missing thorough encryption of data at rest and in transit can lead to the unintended exposure of cardholder data.

Weak Passwords – A lack of password policies undermines account security. Policies should include password-complexity requirements, rotation schedules, and reuse prevention.

E. Training

To strengthen SAGE books security culture, it is recommended to implement a cybersecurity awareness training program, this will include:

Annual Training – This session will cover the basics of cybersecurity and how it relates to the business. It will include information on social engineering, password security and policies, the legal requirements regarding personally identifiable information (PII), and the Acceptable Use Policy.

Specialized Training – This training will be specific to each team member's role and responsibilities. There will be different areas of focus for C-suite staff, privileged-access employees, and point-of-sale staff. This training will occur more regularly and be job specific.

Continued Awareness – This will be achieved through regular simulated phishing campaigns, videos, short courses, emails, and posters located in staff areas. Varying resources helps to keep the material interesting and increases employee enjoyment and engagement.

F. Policies

Acceptable Use Policy – This policy defines the appropriate use of company systems and devices. It also outlines which activities are considered acceptable and which are prohibited. This aligns with PCI DSS Requirement 12 which requires organizations to implement and maintain acceptable-use policies to remain compliant. (PCI Security Standards Council [PCI SSC], 2022, Requirement 12).

Mobile Device Policy – Mobile devices used to access and/or process company data need to be properly secured. This includes robust encryption, remote management and correct authentication methods. PCI DSS Requirement 3 focuses on security controls to protect cardholder data (PCI SSC, 2022, Requirement 3).

Password Policy – Passwords must be adequately complex, rotated regularly and kept secure. A combination of Strong passwords policies and multi factor authentication defend against unauthorized access. PCI DSS Requirement 8 provides guidelines on authenticating users who access company systems. (PCI SSC, 2022, Requirement 8).

Personally Identifiable Information – To remain in compliance with European law, SAGE Books must comply with the General Data Protection Regulation (GDPR). This regulation requires that the data of subjects that

reside within the European Union be processed lawfully, fairly, and securely (European Union, 2016)

G. Incident Response Plan

SAGE Nooks will implement an Incident Response Plan structured around the four phases found in NIST SP 800-61:

Preparation – SAGE books will create an incident response team and delegate responsibilities accordingly. The organization will define policies, procedures and relevant points of contact for handling incidents. It will ensure that the appropriate tools are available, including digital forensic tools, system logging tools and backup procedures.

Detection and Analysis – The incident response team will monitor logs and intrusion detection systems to identify potential threats. Alerts will be reviewed, and appropriate action taken where deemed necessary. Incidents will be documented in a central repository to aggregate and analyze data.

Containment, Eradication, and Recovery – Should an incident occur, affected systems will be isolated, malicious files will be removed, and systems will be restored from clean backups.

Post-Incident Activity – After the occurrence and remediation of an incident, the incident response team will conduct a lessons-learned review. The findings of this review will be reported to executive leadership and to any relevant third parties. The information found in the review will be used to improve existing policies, system configurations, and to guide employee training programs moving forward.

The process above has been derived from the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide (NIST, 2012)

H. Continuity Plan

Project Scope and Planning – SAGE Books will identify all critical business processes, and all key personnel will be designated according to their roles in recovery operations. The scope will include all relevant

business areas, including shipping, on-premise systems, e-commerce, and warehousing. Recovery objectives will be defined to ensure minimal disruption to business operations should an incident occur.

Business Impact Analysis – The organization will establish maximum tolerable downtimes for business processes and define recovery point objectives. By defining these metrics, SAGE Books can prioritize efforts and allocate resources effectively. The impact analysis will also evaluate potential financial and reputational impacts should the business be disrupted.

Continuity Planning – To ensure minimal downtime, SAGE Books will implement redundant cloud infrastructure to maintain system availability during service interruptions. Data will be backed up across geographically dispersed regions to reduce the risk of data loss in the event of a disaster. Logistically, the company will develop alternate shipping routes and suppliers to maintain operations should disruptions occur.

Plan Approval and Implementation – Plan approval will be obtained by executive leadership formally signing off on the plan. Regular tabletop exercises will be performed, and incident simulations will be conducted to test the efficiency and effectiveness of the current plan. Lessons learned from these events will be incorporated into future revisions. The plan will be

reviewed and updated frequently to ensure it remains current, and any weaknesses that are found will be corrected and implement immediately.

References

PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard: Requirements and testing procedures, version 4.0.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.* https://eur-lex.europa.eu/eli/reg/2016/679/oj

National Institute of Standards and Technology. (2012). *Computer security incident handling guide (NIST Special Publication 800-61 Revision 2).* https://csrc.nist.gov/pubs/sp/800/61/r2/final