Denzel Frimpong

D489 Cybersecurity Management

Professor: Jenny Heiner

Student ID: 0114840496

A. Summary of Security Gaps

The independent Security Report for SAGE Books identifies several key weaknesses in the company's existing security framework. First, there is a lack of comprehensive security policies and procedures, leading to inconsistent practices across departments. Additionally, the report identifies inadequate employee training on cybersecurity threats, resulting in a workforce ill-equipped to recognize and respond to potential breaches. The absence of robust access controls poses further risks, as sensitive data is not sufficiently protected from unauthorized access. Finally, the report notes insufficient incident response protocols, leaving the organization vulnerable in the event of a security breach.

B. Mitigation Strategies

To address the identified gaps, SAGE Books will implement several mitigation strategies. First, we will develop and standardize comprehensive security policies that comply with PCI DSS and GDPR, ensuring data protection and privacy. Employee training programs will regular assessments to gauge effectiveness. We will also strengthen access controls

through role-based access management, ensuring that employees only have access to the information necessary for their roles. Lastly, we will establish clear incident response protocols to streamline actions taken during a breach, thereby reducing response time and potential damage.

C. Critical Security Staff Positions

To bolster our cybersecurity framework, three critical positions will be created:

1. **Security Analyst:** Responsible for monitoring and analyzing security threats, the Security Analyst will conduct regular vulnerability assessments and manage incident reports, ensuring timely responses to potential breaches.
2. **Compliance Officer:** This position will oversee adherence to regulatory standards such as PCI DSS and GDPR, ensuring that all processes and systems meet compliance requirements while conducting regular audits and assessments.
3. **Security Awareness Trainer:** Responsible for creating and executing the cybersecurity training program, the Security Awareness Trainer will concentrate on informing staff about new threats and effective strategies for safeguarding data security.

D. Vulnerabilities and Threats

The assessment identifies various physical and logical weaknesses that impact the security posture of SAGE Books. Physically, inadequate surveillance and access controls at retail locations expose the company to theft and unauthorized access, potentially

leading to data breaches. Environmental risks, such as flooding or fire, could also compromise critical infrastructure. Logically, outdated software and systems create entry points for cybercriminals, while insufficient encryption of sensitive data heightens the risk of unauthorized access and data leaks. Each of these vulnerabilities threatens the integrity and confidentiality of the company's information systems.

E. Cybersecurity Awareness Training

To foster a security-conscious culture, SAGE Books will develop a comprehensive cybersecurity awareness training program in alignment with NIST standards. Annual training will cover fundamental cybersecurity principles, emerging threats, and incident reporting procedures. Specialized training sessions will be offered for employees in high-risk roles, focusing on specific threats relevant to their functions. Ongoing awareness will be fostered through regular newsletters, phishing simulations, and quarterly refresher courses, keeping employees alert and knowledgeable about changing cybersecurity threats.

F. Standards for Securing Organizational Assets

SAGE Books will follow various standards to protect its organizational assets, highlighting the significance of policies related to acceptable use, mobile devices, passwords, and personal identifiable information (PII). The Acceptable Use Policy will define permissible actions for employees using company resources, while the Mobile Device Policy will establish guidelines for securing devices that access sensitive information. Robust password policies will mandate the use of complex passwords and regular updates to reduce the likelihood of unauthorized access. Additionally, compliance

with regulations such as GDPR will guide our handling of PII, ensuring data is collected, stored, and processed in accordance with legal requirements.

G. Incident Response Plan

In accordance with the Independent Security Report, SAGE Books will create a comprehensive incident response plan based on the NIST framework. The four phases include:

1. Preparation: Establishing incident response teams and protocols to ensure readiness.
2. Detection and Analysis: Utilizing monitoring tools to quickly identify potential incidents.
3. Containment, Eradication, Recovery: Rapidly isolating impacted systems, eliminating threats, and restoring operations while reducing overall impact.
4. Post-Incident Activity: Carrying out comprehensive evaluations of the incident to extract lessons learned and enhance future response strategies.

H. Business Continuity Plan (BCP)

SAGE Books will develop a comprehensive business continuity plan (BCP) to address potential natural disasters. The project scope and planning phase will define objectives and the roles of key personnel. A business impact analysis will identify critical functions and assess the potential impact of disruptions. Continuity planning will establish strategies to maintain operations during and after a disaster, ensuring essential services remain available. Finally, the plan approval and implementation phase will involve senior management to ensure commitment and resources for effective execution. Regular testing and updates to the BCP will ensure its effectiveness in the face of evolving threats.