Barbara Garcia

5/15/2024

**D489 – Cybersecurity Management Plan**

**A.**

Sage Books’s security framework contains many gaps that leave it vulnerable to attack and out of compliance with regulatory standards. There is no comprehensive approach covering the plan to protect organizational assets, secure payment card data and ensure privacy of data for customers in the European Union. The security team does not have the expertise to implement the company’s compliance-related security strategies and projects. Current security staff does not reflect compliance and regulatory efforts. The security awareness program is not sufficiently aligned with security best practices and incident standards. Additionally, the incident response plan does not fully cover the incident response process and the business continuity plan does not address natural disasters.

**B.**

The gaps in the security framework at Sage Books cause the company to be noncompliant with key regulatory requirements such as PCI DSS and GDPR. Mitigations need to be put in place to resolve these gaps and bring the company into compliance with these standards.

**PCI DSS**

One of these is that Sage Books lacks a comprehensive approach that covers securing and protecting organizational assets and security of payment card data. PCI DSS, short for Payment Card Industry Data Security Standard, while not a law, is a requirement put in place by credit card companies that any company that processes, stores, or transmits credit card or debit card information. To mitigate the lack of a comprehensive security approach, PCI DSS requirements should be integrated into the company’s comprehensive security plan as it is crafted.

Another gap identified in the Independent Security Report is that the security team lacks expertise to implement the company’s security strategies and projects relating to regulatory compliance. This can be mitigated by hiring a Cyber Policy and Strategy Planner to guide regulatory policy and procedures at Sage Books.

Similarly, the company’s compliance and regulatory efforts are lacking when it comes to security team staffing. This can be mitigated by hiring additional staff to strategize and plan regulatory compliance efforts, provide cyber training company wide, and analyze the company’s cybersecurity efforts.

Also identified as a gap in the security report is that the security awareness program at Sage Books is not adequately aligned with security best practices and industry standards. To mitigate this, “employees handling credit card information should receive training on PCI DSS requirements.” (Chapple, 2022 p. 123)

Additionally, the Incident Response Plan does not comprehensively cover the incident response process and the Business Continuity Plan does not adequately address natural disasters. To address these respectively, Sage Books should develop a thorough incident response plan and a comprehensive business continuity plan that comply with PCI DSS.

**GDPR**

Many of the same gaps that leave the Sage Books noncompliant with PCI DSS also affect the company’s adherence to the GDPR (General Data Protection Regulation).

Additionally, currently SAGE Books does not have any measures in place to protect the collection, storage, or use of data. This can be mitigated by integrating compliance with GDPR into the company’s comprehensive security policies. The company should ensure compliance with data rights for European citizens, ensure data that contains personally identifiable information is stored, collected, and manipulated in accordance with the requirements of the law. This should be taken account not only when building policies and procedures but also when implementing technical infrastructure.

**C.**

While SAGE Books has a security team, they do not have the specialized staff necessary to ensure the success of security compliance and regulatory efforts. Hiring a Security Control Assessor, a Cyber Instructor, and a Cyber Policy and Strategy Planner will give the expertise it needs to implement comprehensive security strategies and projects that will ensure a strong security posture and compliance with all legal and contractual standards.

The NICE Framework by NIST gives thorough guidance on cybersecurity roles and identifies the tasks, knowledge, skills, and abilities each position requires. This framework was used to identify the responsibility for each of the newly hired positions at SAGE Books. (*Workforce Framework for Cybersecurity (NICE Framework) | NICCS*, 2023)

**C1.**

Under the category of risk management, a Security Control Assessor will be hired to conduct independent assessments of the management, operational, and technical security controls and enhancements used by SAGE Books’s IT system to determine the effectiveness of the controls. The assessor’s responsibilities will include: Manage and approve accreditation packages; plan and conduct security authorization reviews and assurance development for initial installation of systems and networks; review authorization and assurance documents to confirm that the risk level is within acceptable limits for each software application, system, and network; verify that technical system security postures are implemented according to plan, document deviations and recommend actions to correct the deviations; and perform risks analysis upon major changes, verify and update security documentation based on application and system security design features; and define and document how implementation of new systems or interfaces impact security posture of current environment.

**C2.**

It is essential that the company have a strong training, education, and awareness program. Both the company’s security posture and compliance requirements necessitate having a Cyber Instructor on staff to continually provide both general and specialized cybersecurity training to staff. The Cyber Instructor will be responsible to develop and conduct training or education of personnel with the cyber domain. Some of their tasks will include conducting training exercises, develop, and improve awareness and training materials appropriate for the intended audiences, review training documentation, support the design and execution of exercise scenarios, develop course assignments and evaluations, and conduct learning needs assessments and identify requirements.

**C3.**

To shore up the company’s strategic planning and policy posture, a Cyber Policy and Strategy Planner will be hired. This strategy specialist will develop and maintain cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance. (*Workforce Framework for Cybersecurity (NICE Framework) | NICCS*, 2023)

He or she will develop policy, programs, and guidelines for implementation; establish and maintain communication channels with stakeholders; advocate for adequate funding for cyber training resources; promote awareness of cyber policy and strategy; assess cyber workforce effectiveness to adjust skill standards; and analyze organizational cyber policy.

**D.**

**Physical Vulnerabilities/Threats**

One physical threat to SAGE Books is the threat of natural disasters. The locations where SAGE Books operates are susceptible to hurricanes, tornadoes, floods, and earthquakes. The impacts of this threat to the business are business disruption, loss/theft of assets immediately following property damage, and loss of data.

Another physical threat to SAGE Books is mobile device theft. Theft of an employee’s company owned or enabled mobile device can impact the company’s security posture by way of data disclosure, smishing attacks performed by a bad actor who has possession of the device post theft, and exposure of sensitive data to unauthorized parties.

A third threat that impacts the physical realm is a lack social engineering awareness programs. Employees not trained in social engineering will be open to physical social engineering attacks such as impersonation and USB drops.

**Logical Vulnerabilities/Threats**

One logical vulnerability at SAGE Books is the lack of data privacy controls. The impact of not having proper privacy controls such as encryption, network segmentation, and screen subnets is the disclosure of personally identifiable information which will impact the company financially, legally, and reputationally.

Another logical vulnerability is the lack of payment card encryption. The impact of payment card data not being encrypted in storage and in transit can result in card data disclosure.

A third logical vulnerability is a lack of appropriate identity and access management (IAM). Not having proper controls such as enforced password requirements, multifactor authentication and effective authorization methods can result in impacts such as account takeover and unauthorized access to sensitive information.

**E.**

Sage Books will develop a cybersecurity awareness training program with annual training requirements, specialized training requirements and continued awareness.

To have a strong security posture and comply with regulatory standards, SAGE Books should ensure that the entire workforce is exposed to cybersecurity training annually, at minimum. This annual training needs to be engaging and targeted to the audience.

Specialized training requirements should be in place. Cybersecurity training should be customized to fit the role of the person participating in the training so that each person is appropriately equipped to provide sufficient security. Employees should also be trained before using new systems and tools. “When using cybersecurity systems and applications, employees must receive sufficient training before accessing and using the tools.” (Wilson & Hash, 2003)

Given that one session of cybersecurity training is not enough to equip employees, continued awareness efforts are necessary. Employees should have regular access to learning opportunities in person, online, and via exercise in order to ensure continued growth in cybersecurity preparation and knowledge. Training must also be regularly updated to remain relevant. “Specific security control options and tools are rapidly changing and evolving. Continued training enforces the availability of necessary security information.” (Wilson & Hash, 2003)

**F.**

Most standards have requirements for securing organizational assets. These standards should be used by SAGE Books to guide organizational security policies as they craft their security infrastructure, internal policy, and technical implementation. Acceptable use, mobile devices, passwords, and personally identifiable information are areas that are important to the organization’s security and will be examined by assessors who are rating the company’s compliance with external standards and regulations and as such, should be well defined, communicated clearly to employees, and enforce via administrative and technical means.

An effective acceptable use policy is essential to an organization’s security posture. It will also be examined by third parties who are auditing the company for compliance with regulatory requirements. Acceptable use policies define and communicate with employees how they may and may not use company-owned technology, including workstations and the network. While drafting this policy, company leadership should consider the needs of the company, what standards must be adhered to, and the sensitivity of the data and other assets the company has. The PCI DSS is clear that acceptable use policies will be open to critique: “To test compliance with PCI Requirement 12.3.5, an assessor will need to examine your usage policies to ensure that they define acceptable uses for the technology at your organization.” (Bartels, 2018)

Mobile devices are a component of a company’s security exposure that is often overlooked. To be secure and compliant with industry standards, SAGE Books must address mobile device security. According to the GDPR, the main data protection issues when it comes to mobile devices are accountability, right of information, and data security. (*Mobile Devices | European Data Protection Supervisor*, 2024) Companies need to be aware of what data is stored and accessed using mobile devices so that it can be appropriately categorized and secured in compliance with regulations. In addition to properly securing data, under PCI DSS standards, mobile devices that process payment card transactions must comply with data transmission guidelines.

Password security is extremely important in every context. If a password for just one user is compromised, the results can be devastating to the entire organization as well as its customers. PCI DSS has the following requirements for passwords: Do not use vendor-supplied defaults for system passwords, use strong authentication and encrypt all passwords, and use multi-factor authentication, not passwords alone.

An immutable component of a company’s cybersecurity stance is the protection of personally identifiable information, or PII. Personal information, especially containing financial and/or health details must remain confidentiality, integrity, and availability. SAGE Books needs to ensure all personally identifiable information is handled in accordance with standard practice and compliance requirements. For example, PCI DSS requires some of the following when handling cardholder data: PIN encryption, encryption of all cardholder data while in storage and in transit, and strong access control. (Chapple, 2022)

**G.**

SAGE Books needs to establish a comprehensive incident response plan that will prevent security incidents and facilitate quick action in the event one does take place. As the incident response plan is being crafted, it is important that the following elements are included: Statement of purpose, strategies and goals for incident response, approach to incident response, communication channels with other groups, and senior leadership approval.

The company’s incident response team should be established ahead of time and each one aware of their responsibilities during an incident. These members include: The CEO who will be responsible for making high level final decisions on things such as costs and logistics. The Cyber Policy and Strategy Planner will be responsible for developing the incident response plan with the input of the IT Manager. The Security Assessor will analyze the incident response plan on an ongoing basis and lead lessons learned meetings. The IT Manager will help develop and implement the incident response plan and will oversee analysis and monitoring efforts of security incidents. He or she will also oversee recovery efforts. The Security Engineer will be responsible for configuring detection and response plans and ensuring tools such as security incident and event monitoring (SIEM) system are properly provisioned. The Cybersecurity Analyst will participate in detection and analysis by monitoring security information systems for indicators of compromise and will be responsible for implementing containment, eradication, and recovery efforts.

**Prevention**

While it can be natural to respond to incidents as they come, it is essential that the incident response team prepare in advance of an incident. This will not only help to prevent incidents but will leave the team equipped to respond quickly and effectively when an event does occur. One thing done in this phase is to establish incident handler communication channels and facilities needed to implement it. Incident analysis hardware, software and other resources need to be provisioned and put into place, along with incident mitigation tools and software. A risk assessment needs to be conducted and host security, network security, malware prevention and user awareness and training put in place to mitigate the risks identified.

**Detection and Analysis**

Next up comes the detection and analysis phase. During the detection phase, the monitoring team should focus on attack vectors such as removable media, brute force, web email, impersonation, improper usage, and equipment theft. To quickly detect an attack, the team must monitor for indicators of compromise by analyzing alerts from tools like intrusion detection and prevention systems, security incident and event monitors, antivirus software, and file integrity software as well as logs from company assets such as operating systems, applications, network devices, and network flows. Indicators of compromise can also come from publicly available information and people within or outside the organization.

Once detected by the SAGE Books incident response team, an incident should be analyzed, documented, and prioritized. During analysis, the team will profile networks and systems, understand normal behaviors, follow a log retention policy, perform event correlation, use packet sniffers to collect data, and filter the data being analyzed. The team should also maintain documentation that includes a summary, the indicators of compromise that alerted them to it, actions taken by handlers, chain of custody, impact assessments, and an evidence list. Incidents should be prioritized by functional impact, informational impact, and recoverability. During this phase, the appropriate people need to be notified. In addition to the incident response team members, other departments such as the system administrator as well as the human resources, public affairs, and legal departments, should be notified.

**Containment, Eradication and Recovery**

Once an incident has been detected and analyzed, SAGE Books should start the containment, eradication, and recovery process. This is when the team chooses and implements a containment strategy and gathers evidence that is kept in a log. To identify the attacking hosts, the team should validate IP addresses, research the attacking hosts, use incident databases, and monitor attacker communication channels. Infected hosts and systems should be isolated to contain the damage. The team then needs to delete malware and other artifacts left by the attacker, restore systems to normal operation, and confirm functionality.

**Post-Incident Activity**

Actions taken after an incident occurs at SAGE Books will be equally as important as the previous steps. It is important to have a lessons-learned meeting that looks at the timeline of the incident, staff performance, actions that inhibited recovery, what to do different next time, how to improve sharing, indicators of compromise to look for, corrective actions to prevent recurrence, and identifies additional tools and resources that may be needed to detect, analyze, and mitigate future incidents.

Data that was collected during the incident should be used to identify things such as numbers of incidents handles, times each incident type occurred, and an objective and subjective assessment of each incident. Evidence should be retained in case it is needed for legal proceedings.

**H.**

As they expanded, SAGE Books purchased locations in San Joaquin, California, Keene, Texas, and Cape Coral, Florida. San Joaquin, like elsewhere in California, is susceptible to earthquakes. The location in Keene, Texas is at great risk for tornadoes, as it is within the famous ‘tornado alley’ area of the United States. Cape Coral, Florida is at significant risk of hurricanes and the floods that can accompany hurricanes. They chose these places for their strategic location. However, each of these geographical areas has significant risk of natural disasters occurring. To prevent one of these disasters from putting them out of business, it is necessary for the company to develop a Business Continuity Plan (BCP) that addresses how the business will continue in the face of one of these natural disasters.

“The overall goal of BCP is to provide a quick, calm, and efficient response in the event of an emergency and to enhance a company’s ability to recover from a disruptive event promptly.” (Chapple, 2022 p.199) A comprehensive business continuity plan includes the four phases of project scoping and planning, business impact analysis, continuity planning, and plan approval and implementation.

**Project Scope and Planning**

The project scoping and planning phase is the foundation of the business continuity plan process and consists of a structured review of the business from a crisis planning point of view. While identifying the scope of the plan, the team should consider operational departments that provide core services, critical support services, physical security teams to safeguard facilities, and senior executives and other staff that essential to ongoing business functionality.

During this phase the team is identified. The Business Continuity Plan Team should be created with senior management approval and include people from all over the company who can take ownership of the tasks necessary for business continuation. The BCP team from SAGE books should include a representative from each department that provides key services, a team member from each business unit that represents a functional area identified during the analysis of the organization, IT subject matter experts, cybersecurity staff, physical security and facility staff, attorneys to guide corporate legal responsibilities, human resource members to address employee impact, public resources personnel who will communicate externally during a disaster and a member of senior management who has authority to authorize vision, define priorities and approve resources.

For effective planning, the team needs to assess resources available to them for use in business continuity activities. During the development stage, effort from the team and the use of additional support staff will be necessary. As the team conducts testing, training , and maintenance, specialized hardware and software, as well as employee effort will be needed. When the plan is implemented, a large time and effort requirement will be placed on the team and the company will have significant financial expenditures in the form of recovery, alternate locations, and other efforts.

The legal and regulatory items that govern SAGE Books need to be analyzed during this stage as well, so compliance does not suffer in the event of a disaster. Some of these include laws and regulations, banking and security regulations, and contractual obligations to customers and other stakeholders.

**Business Impact Analysis**

The portion of this process in which the team conducts the business impact analysis is pivotal, as it identifies how a disaster would impact a business and allows the team to identify risk and prioritize resources. “The BIA identifies the business processes and taks that are critical to an organization’s ongoing viability and the threats posed to those resources. It also assesses the likelihood that each threat will occur and the impact those occurrences will have on the business.” (Chappel, 2022 p. 304)

Impact Assessments can be approached from a quantitative view that uses numbers and formulas to reach a decision and puts the options in the form of dollar value or a qualitative view that looks at non-numerical factors such as reputation, customer confidence and workforce stability and prioritizes them as high, medium, or low. These assessments are used to identify priorities by stating essential business activities and ranking critical functions in order of importance.

**Continuity Planning**

Once priorities for continued operation are identified, the team will develop a strategy that bridges the gap between the business impact analysis and planning business continuity. The provisions and processes that are the bulk of the plan are then put in place as the team designs procedures and mechanisms designed to mitigate the unacceptable risks identified in the strategy development phase.

As ongoing business operations are strategized, the safety of the people within the organization must be prioritized before, during, and after an emergency. The team must then identify buildings and facilities that are critical to the organization’s post-disaster viability and harden those sites as well as plan alternate sites the business can be run out of if a disaster damages the primary location so much that it cannot be used to run critical business operations. Technology infrastructure must also be hardened by using methods such as computer-safe fire suppression and uninterruptible power supplies. Alternative systems should also be planned, including having backups of essential data available offsite in the event physical infrastructure is damaged. There should be redundancy in both systems and communication channels.

**Plan Approval and Implementation**

Once the team has developed an effective business continuity plan, it should be approved by the top executive of the company and implementation should begin. It is best to have executive buy in throughout the process to streamline this step and avoid a disjointed policy.

The BCP team at SAGE Books should create an implementation schedule that is both thorough and put in place as promptly as possible. Included in the schedule should be a maintenance program that can respond to changing business needs.

A plan is useless if nobody knows how to follow it. That considered, all employees should be made aware of the plan. All personnel involved in implementing the plan should undergo training for the plan, as well as their individual responsibilities. Staff who has direct essential duties need to be trained on specific tasks and evaluated to ensure they are prepared to execute them.

Throughout the planning process and moving forward, documentation is very important. Things that need to be documented include goals established during planning, statement of importance, statement of priorities, the risk assessment, risk assessment and mitigation, vital business records, emergency-response guidelines, plan maintenance and testing and exercise.

**References**

Bartels, R. (2018, July 3). *PCI Requirement 12.3.5 – Acceptable Uses of the Technology*. KirkpatrickPrice. https://kirkpatrickprice.com/video/pci-requirement-12-3-5-acceptable-uses-technology/

Chapple, M. (2022). *CISM certified information security manager study guide*. Sybex.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2

*Mobile devices | European Data Protection Supervisor*. (2024, May 13). Www.edps.europa.eu. https://www.edps.europa.eu/data-protection/data-protection/reference-library/mobile-devices\_en

NIST. (2020). Security and Privacy Controls for Information Systems and Organizations. *Security and Privacy Controlsfor Information Systems and Organizations*, *5*(5). https://doi.org/10.6028/nist.sp.800-53r5

PCI Security Standards Council. (2018). *PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.2.1 For merchants and other entities involved in payment card processing*. https://listings.pcisecuritystandards.org/documents/PCI\_DSS-QRG-v3\_2\_1.pdf

Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program Technology Administration*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

*Workforce Framework for Cybersecurity (NICE Framework) | NICCS*. (2023, August 28). Niccs.cisa.gov. https://niccs.cisa.gov/workforce-development/nice-framework