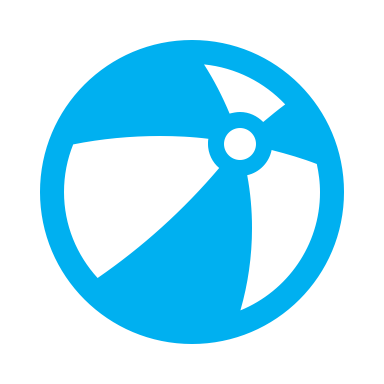
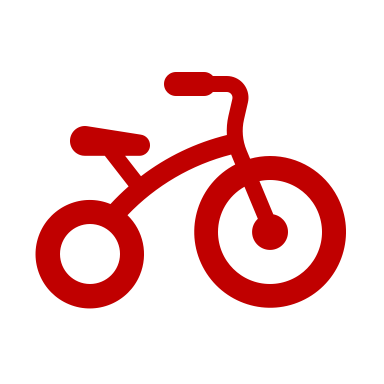
(Mock) Internal Security Assessment Analysis & Recommendations for Botium Toys

****

Material & instructions developed by: Google Cybersecurity Professional Certificate Course

Completed by: Alexander Herman on 01/08/24

**Table of Contents:**

Scenario Instructions (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Botium Toys: Scope, Goals, and Risk Assessment Report (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2-4**

Alex’s Quick Notes on Provided Material (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**4**

Controls and Compliance Checklist (Provided/My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**5-6**

Analysis of Controls Checklist (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**6-7**

Recommendations (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**7-9**

**Scenario Instructions**

This scenario is based on a fictional company:

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location, which serves as their main office, a storefront, and warehouse for their products. However, Botium Toy’s online presence has grown, attracting customers in the U.S. and abroad. As a result, their information technology (IT) department is under increasing pressure to support their online market worldwide.

The manager of the IT department has decided that an internal IT audit needs to be conducted. She expresses concerns about not having a solidified plan of action to ensure business continuity and compliance, as the business grows. She believes an internal audit can help better secure the company’s infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. The manager is also interested in ensuring that they comply with regulations related to internally processing and accepting online payments and conducting business in the European Union (E.U.).

The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, listing assets currently managed by the IT department, and completing a risk assessment. The goal of the audit is to provide an overview of the risks and/or fines that the company might experience due to the current state of their security posture.

**Botium Toys: Scope, goals, and risk assessment report**

**Scope and goals of the audit**

**Scope:** The scope is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures related to the implementation of controls and compliance best practices.

**Goals:** Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve Botium Toys’ security posture.

*Current assets*

Assets managed by the IT Department include:

* On-premises equipment for in-office business needs
* Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
* Storefront products available for retail sale on site and online; stored in the company’s adjoining warehouse
* Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
* Internet access
* Internal network
* Data retention and storage
* Legacy system maintenance: end-of-life systems that require human monitoring

**Risk assessment**

*Risk description*

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all the proper controls in place and may not be fully compliant with U.S. and international regulations and standards.

*Control best practices*

The first of the five functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to identify assets so they can appropriately manage them. Additionally, they will need to classify existing assets and determine the impact of the loss of existing assets, including systems, on business continuity.

*Risk score*

On a scale of 1 to 10, the risk score is 8, which is high. This is due to a lack of controls and adherence to compliance best practices.

*Additional comments*

The potential impact from the loss of an asset is rated as medium because the IT department does not know which assets would be at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure. Review the following bullet points for specific details:

* Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers’ PII/SPII.
* Encryption is not currently used to ensure confidentiality of customers’ credit card information that is accepted, processed, transmitted, and stored locally in the company’s internal database.
* Access controls pertaining to least privilege and separation of duties have not been implemented.
* The IT department has ensured availability and integrated controls to ensure data integrity.
* The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
* Antivirus software is installed and monitored regularly by the IT department.
* The IT department has not installed an intrusion detection system (IDS).
* There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
* The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.
* Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).
* There is no centralized password management system that enforces the password policy’s minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
* While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
* The store’s physical location, which includes Botium Toys’ main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

**Alex’s Quick Notes on Provided Material:**

* No least privilege or separation of duties
* $$ transactions not protected online; compliance not met
* I and A of CIA triad supposedly met (not)
* No separation of duties in IT department so that brings data integrity into question for me
* Because all employees have access to internally stored data that tells me the privacy policy is useless or not being enforced
* Antivirus software and firewall used but no IDS
* No DRP/BCP or data backups/backup procedure
* There are some documented processes and procedures for maintaining integrity
* Weak password policy
* No IAM admin = weak user security
* No procedure/guidelines for monitoring legacy systems
* Physical security is okay but no alarm system
* Mentioned that information is internally stored but didn’t read about on-prem servers or a secure sever room
* Mentioned remote workstations in the assets report but no mention of a VPN being used for remote devices connecting to company network

**Controls and Compliance Checklist**

Type an X in the “yes” or “no” column to answer the question: *Does Botium Toys currently have this control in place?*

**Controls assessment checklist**

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Control** |
|  | x | Least Privilege |
|  | x | Disaster recovery plans |
|  | x | Password policies |
|  | x | Separation of duties |
| x |  | Firewall |
|  | x | Intrusion detection system (IDS) |
|  | x | Backups |
| x |  | Antivirus software |
|  | x | Manual monitoring, maintenance, and intervention for legacy systems |
|  | x | Encryption |
|  | x | Password management system |
| x |  | Locks (offices, storefront, warehouse) |
| x |  | Closed-circuit television (CCTV) surveillance |
| x |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) |

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  | x | Only authorized users have access to customers’ credit card information. |
|  | x | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. |
|  | x | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |
|  | x | Adopt secure password management policies. |

General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  | x | E.U. customers’ data is kept private/secured. |
| x |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. |
|  | x | Ensure data is properly classified and inventoried. |
|  | x | Enforce privacy policies, procedures, and processes to properly document and maintain data. |

System and Organizations Controls (SOC type 1, SOC type 2)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  | x | User access policies are established. |
|  | x | Sensitive data (PII/SPII) is confidential/private. |
|  | x | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
|  | x | Data is available to individuals authorized to access it. |

**Analysis & Recommendations:** In this section, provide an analysis of the current security controls and then your recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys’ security posture.

**Analysis of Controls Checklist:**

**Physical Security Measures:**

Based on the risk assessment and the list of current assets provided by Botium Toys, it's evident that the organization is exposed to high risks in various sections of the controls checklist. While the company has invested in physical security measures such as CCTV cameras, “sufficient” locks, and a fire detection/prevention system, notable omissions include the absence of a security alarm system and a secure server room to safeguard business-critical data, which is supposedly managed internally. The lack of these security measures could potentially impact the overall physical security of sensitive information.

**Identity and Access Management (IAM):**

Moving on to the digital security aspect, a significant concern is the absence of a robust Identity and Access Management (IAM) strategy. The report indicates that all Botium Toys employees currently have unrestricted access to internally stored data, including potential access to cardholder data and customers’ Personally Identifiable Information (PII)/Sensitive Personally Identifiable Information (SPII). This lack of access control violates the principles of least privilege and separation of duties, undermining the confidentiality and integrity of the company's data. Additionally, the weak password policy and the absence of Multi-Factor Authentication (MFA) present substantial vulnerabilities that could be exploited by threat actors.

**Security of Customer Transactions:**

A critical issue that demands immediate attention is the absence of security measures for customer transactions. The failure to implement encrypted transactions poses a significant risk, not only resulting in potential revenue loss from security-conscious customers but also exposing the entire eCommerce business to severe risks. Government agencies, upon discovering such lapses, could impose heavy fines, and the company might face the suspension of online operations until compliance standards are met, potentially dealing a devastating blow to this small business.

**Disaster Recovery and Business Continuity:**

Equally concerning is the lack of a Disaster Recovery Plan (DRP) and a Business Continuity Plan (BCP). For a small business like Botium Toys, where all assets are concentrated in one location, the absence of these plans raises serious concerns about the availability of business-critical data in case of emergencies such as floods, fires, or tornadoes. Without a clear plan for data recovery, there is a risk of temporary or permanent loss of critical information.

**Other Considerations:**

In addition to these major issues, there are smaller but noteworthy problems such as improper monitoring of legacy systems and the absence of a Virtual Private Network (VPN) for remote workers connecting to the company network. These issues, while smaller in scale, contribute to the overall security vulnerabilities that need to be addressed promptly.

**Personal Recommendations:**

**Restructure IT Environment:**

* Evaluate the advantages of migrating databases to a 3rd-party cloud storage platform, emphasizing scalability, redundancy, and enhanced security features.
* Reconfigure the network infrastructure to align with the defense-in-depth principle, segmenting business-critical systems for heightened security.
* Implement a 3rd-party IAM solution to facilitate user identity management, ensuring capabilities for creating, provisioning/de-provisioning, verifying, monitoring, and deleting digital users.
* Employ dedicated IAM admins to handle user identity concerns.
* Recruit a digital security leader to oversee comprehensive security measures.
* Purchase a VPN for remote workers, coupled with anti-virus software, to ensure secure connections to the company network.
* Acquire SIEM tools, like an IDS, for analyzing filtered events, patterns, and proactive threat detection.
* Consider a hybrid storage model for secure on-premises data backups.
* If legacy systems persist, segment them from critical systems and implement increased security measures around them.
* If the company relies on third-party vendors or partners, conduct thorough security assessments to ensure that their cybersecurity practices align with your organization's standards.

**Update Company IT Procedures, Policies, and Plans:**

* Rewrite the password policy to align with current compliance standards and enforce it through IAM admins.
* Revise all existing policies and procedures, emphasizing principles like least privilege, separation of duties, defense in depth, secure defaults, minimized attack surfaces, and asset classification.
* Introduce new security policies, including Data Handling Policy, Acceptable Use Policy, Bring-Your-Own-Device Policy, and Change Management Policy.
* Add Business Continuity Plan and Disaster Recovery Plan to safeguard the availability of business-critical data and regularly test the plans and ensure the availability of recent backups in case of data loss or system failure.
* Implement logging software and procedures for network traffic analysis and monitoring IT environment changes.
* Introduce internal and external auditing procedures to proactively search for vulnerabilities, compliance issues, and suspicious activity.
* Establish an incident response plan detailing procedures to follow in case of a cybersecurity incident. This should include roles and responsibilities, communication plans, and steps for mitigating and recovering from security breaches.
* Develop and implement a comprehensive cybersecurity training program for all employees to increase awareness of security best practices, social engineering threats, and the importance of data protection.
* Implement a robust patch management process to regularly update and patch software, operating systems, and applications to address known vulnerabilities promptly.
* If the company develops its software, implement secure coding practices, and conduct regular code reviews to identify and remediate security vulnerabilities in applications.

**Secure and Revamp eCommerce Business:**

* Explore the possibility of outsourcing customer identity management to trusted entities like Facebook, Google, or Amazon for enhanced security and user experience.
* Invest in eCommerce transaction software and consider outsourcing the secure transaction process to a reputable 3rd party.
* Store only essential user information and enforce the use of encryption for data both in transit and at rest to protect sensitive information from unauthorized access.
* Classify customer data into PII & SPII categories, storing them separately with stronger access requirements for SPII.
* Enable Multi-Factor Authentication (MFA) for customers or ensure the outsourced customer identity manager implements it.
* Ensure seamless integration of in-store and online customer accounts.

**Physical Security Additions:**

* Evaluate the inclusion of a security alarm system, specifying the type of alarms and the monitoring/response mechanisms.
* Consider establishing a secure room with restricted access for storing hardware, backup servers, CCTV recordings, physical currency, and other critical assets.