Security Audit

Performing Internal Audit

Wendy Alayon
15/05/2024 **@syszern**

Table of Contents

Security audit

Scenario

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's worried about maintaining compliance and business operations as the company grows without a clear plan. 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.

Your task is to review the IT manager's scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist.

Botium Toys: Scope, goals, and risk assessment report

Scope and goals of the audit

Scope: The scope of this audit is defined as the entire security program at Botium Toys. This includes their assets like employee equipment and devices, their internal network, and their systems. You will need to review the assets Botium Toys has and the controls and compliance practices they have in place.

Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices that 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 of 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 fairly 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 of 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, storefront, and warehouse of products, has sufficient locks, up-to-dateclosed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

Controls and Compliance Checklist

Controls assessment checklist

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

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

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

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☐	☑	E.U. customers' data is kept private/secured.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☐	☑	Ensure data is properly classified and inventoried.
☑	☐	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
☐	☑	User access policies are established.
☐	☑	Sensitive data (PII/SPII) is confidential/private.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☐	☑	Data is available to individuals authorized to access it.

Recommendations

Botium Toys has been assessed with a high-risk score based on the risk assessment report. The report findings and checklist results highlight several critical recommendations. Firstly, the insecure handling of E.U. customer data (including cardholder data and personally identifiable information) presents a significant risk of compromise, given its unrestricted access to all employees. To mitigate this risk, the organization should prioritize implementing security controls such as least privilege and separation of duties. These measures would restrict access to only essential data necessary for employees to perform their tasks, thus minimizing exposure. Additionally, encrypting customer credit card information would enhance confidentiality.

Moreover, stricter password policies and centralized password management systems are advised to strengthen access security. Implementing an Intrusion Detection System (IDS) is also recommended to promptly identify and respond to potential security incidents. As a precautionary step, maintaining backups ensures easier data recovery in the event of a breach, while developing disaster recovery plans enhances overall resilience.

Addressing these vulnerabilities not only mitigates risks but also safeguards against potential compliance penalties under regulations like PCI DSS and GDPR.