Justin Goncalves

7/13/24

Botium Toys Security Audit Scenario

Review the following scenario, then complete the Controls and Compliance Checklist Activity.

T*his 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'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.

IT Managers Risk Assessment Report: Botium Toys: Risk Assessment Report

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.

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

Recommendations (optional): In this section, provide 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.

Recommendations for Botium Toys' Risk Assessment Report

1. Asset Management and Identification:

Recommendation**:**

- **Asset Inventory:** Implement a comprehensive asset inventory system to track and classify all assets, including on-premises equipment, employee devices, and systems. Use automated tools to regularly update the inventory and ensure all assets are accounted for.
- **Asset Classification:** Classify assets based on their criticality to business operations and data sensitivity. This will help prioritize security measures and allocate resources effectively.

2. Access Control and Data Privacy:

Recommendation**:**

- **Least Privilege and Separation of Duties:** Implement access controls based on the principle of least privilege. Ensure that employees have access only to the data and systems necessary for their roles. Separate duties to prevent conflicts of interest and reduce the risk of unauthorized access.
- **Encryption:** Encrypt sensitive data, including customers' credit card information and PII/SPII, both at rest and in transit. Use strong encryption standards to protect data confidentiality.
- **Access Logging and Monitoring:** Implement logging and monitoring of access to sensitive data to detect and respond to unauthorized access attempts.

3. Compliance with Regulations:

Recommendation**:**

- **Compliance Audit:** Conduct regular audits to ensure compliance with U.S. and international regulations such as GDPR, PCI-DSS, and CCPA. Address any gaps identified during these audits promptly.
- **Policy Updates:** Update privacy policies, procedures, and processes to reflect current regulatory requirements and best practices. Ensure all employees are trained on these policies.

4. Technical Controls and Security Measures:

Recommendation**:**

- **Intrusion Detection System (IDS):** Install and configure an IDS to monitor network traffic for suspicious activities and potential security breaches.
- **Firewall Rules:** Regularly review and update firewall rules to ensure they effectively block unauthorized traffic while allowing legitimate business operations.

- **Antivirus and Anti-Malware:** Ensure antivirus software is updated regularly and conduct periodic scans to detect and mitigate malware threats.

5. Disaster Recovery and Data Backup:

Recommendation**:**

- **Disaster Recovery Plan:** Develop and implement a comprehensive disaster recovery plan. This plan should include procedures for data backup, restoration, and recovery in the event of a disaster.
- **Regular Backups:** Perform regular backups of critical data and store these backups in a secure, off-site location. Test backup and recovery procedures periodically to ensure data can be restored successfully.

6. Password Policies and Management:

Recommendation**:**

- **Password Policy:** Strengthen the password policy to meet current best practices, such as requiring at least 12 characters, including a mix of letters, numbers, and special characters. Implement multi-factor authentication (MFA) where possible.
- **Password Management System:** Implement a centralized password management system to enforce password policies and simplify password recovery and reset processes for employees and vendors.

7. Legacy Systems Management:

Recommendation**:**

- **Regular Maintenance Schedule:** Establish a regular maintenance schedule for legacy systems to ensure they are monitored and updated appropriately. Document intervention methods clearly and train staff on these procedures.
- **Upgrade and Replacement:** Develop a plan to gradually replace or upgrade end-of-life systems with more secure and supported alternatives.

8. Physical Security:

Recommendation**:**

- **Access Controls:** Enhance physical access controls to sensitive areas within the store and offices. Implement measures such as keycard access and biometric authentication where appropriate.
- **Surveillance and Monitoring:** Regularly review CCTV footage and ensure that surveillance systems are operational and cover all critical areas.

Communicating to Stakeholders:

To communicate these recommendations to stakeholders, the IT Manager should prepare a detailed report outlining the identified risks, proposed controls, and the benefits of implementing these measures. The report should include a timeline for implementation, estimated costs, and the expected improvement in Botium Toys' security posture.