Botium Toys: Controls assessment

Administrative Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Least Privilege	Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs	X	High
Disaster recovery plans	Corrective; business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration	X	High
Password policies	Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques	X	High
Access control policies	Preventative; increase confidentiality and integrity of data	X	High
Account management policies	Preventative; reduce attack surface and limit overall impact from disgruntled/former employees	X	Medium
Separation of duties	Preventative; ensure no one has so much access that they can abuse the	X	High

Administrative Controls			
	system for personal gain		

Technical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Firewall	Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network	X	High
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly	X	High
Encryption	Deterrent; makes confidential information/data more secure (e.g., website payment transactions)	X	Medium
Backups	Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan	X	High
Password management system	Corrective; password recovery, reset, lock out notifications	X	Medium
Antivirus (AV) software	Corrective; detect and quarantine known threats	X	High
Manual monitoring, maintenance, and intervention	Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities	X	High

Physical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Time-controlled safe	Deterrent; reduce attack surface/impact of physical threats	X	Low
Adequate lighting	Deterrent; limit “hiding” places to deter threats	X	Low
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for investigation	X	Medium
Locking cabinets (for network gear)	Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	X	Medium
Signage indicating alarm service provider	Deterrent; makes the likelihood of a successful attack seem low	X	Low
Locks	Preventative; physical and digital assets are more secure	X	High
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc.	X	Medium

Botium Toys: Audit

Analyze the audit scope, goals, and risk assessment

What are the biggest risks to the organization?

The main risks are the uncertainty of which assets could be lost in a breach and the organization's non-compliance with data protection regulations.

Which controls are most essential to implement immediately versus in the future?

The controls necessary to comply with U.S. regulations should be implemented without delay. Immediate steps to take would include implementing additional controls for business continuity, such as establishing data backup systems and ensuring secure default states for internal applications. Enhancing network management will also be crucial to prioritize as a growing number of worldwide clients start utilizing the service. In general, it is important to prioritize the implementation of administrative and technological controls.

The speed at which Botium Toys will enter the E.U. markets will determine the future controls to be implemented. Delaying compliance with E.U. regulations is possible until the organization is prepared, or else these controls must be put into effect right away. Adequate physical security measures, like badge readers and surveillance cameras, are currently implemented based on the risk assessment, so there is potential for further enhancement in the future.

Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.?

- PCI DSS
- FISMA
- GDPR for E.U

Botium Toys: Compliance checklist

FERC-NERC

The FERC-NERC regulation pertains to entities involved in electricity or the U.S. and North American power grid. Organizations must be ready for, lessen, and disclose any possible security incident that could harm the power grid. Organizations must follow the Critical Infrastructure Protection Reliability Standards (CIP) set by the FERC according to the law.

- **General Data Protection Regulation (GDPR)**

GDPR is an E.U. regulation that safeguards the handling of data belonging to E.U. citizens and their privacy rights both within and outside E.U. borders. Moreover, in the event of a breach leading to the compromise of a E.U. citizen's data, they need to be notified within 72 hours of the occurrence.

Explanation: Botium Toys plans to expand their operations to E.U. countries in the future, and ensuring GDPR compliance is a key focus to avoid potential significant fines for the organization.

- **PCI DSS**

PCI DSS is a global security standard designed to guarantee that organizations which store, accept, process, and transmit credit card data do it in a safe setting..

Explanation: Botium Toys operates as both a physical store and an online store, processing payments as part of its regular activities.

- **HIPAA**

HIPAA, enacted in 1996, is a federal legislation aimed at safeguarding the health information of American patients. This regulation makes it illegal to disclose patient information without their permission. It is a legal requirement for organizations to notify patients of a breach.

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

The SOC1 and SOC2 reports examine an organization's user access policies across various levels within the organization. They are utilized to evaluate the financial adherence and risk levels of an organization. Confidentiality, privacy, integrity, availability, security, and overall data safety are also addressed. Fraud can result from lack of control in these areas.

Explanation: SOC2 focuses on fundamental security practices to protect customer data, and Botium Toys must comply with these practices since the organization will manage payment information and personally identifiable information for customers.

Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Ayush J Shukla
DATE: 07/06/2024
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Teams,
Please examine the Botium Toys internal audit scope, objectives, major discoveries, overview, and suggestions..

Scope:

In this audit, we will evaluate the current user permissions, controls, procedures, and protocols in place for Botium Toys across the specified systems.

• Bookkeeping
• Identifying the end of a point.
• Security barriers
• Systems for detecting intrusions (IDSs)

Tools for Security Information and Event Management (SIEM)

The audit will check if these elements meet all required regulations for Botium Toys. Moreover, the audit will cover all current technology used by Botium Toys, including hardware and system access.

Goals:

- Implement the National Institute of Standards and Technology Cybersecurity Framework
- Ensure that Botium Toys adheres to any required compliances and establish a better process for their systems to ensure compliance
- Identify assets and the current controls that are protecting them, as well as required controls to be implemented
- Establish policies playbooks
- Implement the principle of least privilege for user credential management

Critical findings (must be addressed immediately):

The following compliances will need to be implemented:

- System and Organizations Controls (SOC type 1, SOC type 2)
    - Required to protect PII of personnel and customers
- Payment Card Industry Data Security Standard (PCI DSS)

    - Required when handling payment data
- General Data Protection Regulation (GDPR)
    - This only applies to when Botium Toys begins to do business in E.U. countries

Numerous crucial security controls must be put in place to uphold strong security posture, business continuity, and safety. The majority of urgent controls to focus on are related to administration and technology, like enforcing the principle of least privilege, developing a disaster recovery plan, establishing firewalls, and utilizing Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) tools.

Please see the full controls assessment for individual priority scores of the controls.

Findings

Following the NIST CSF will assist in achieving numerous security objectives and meeting compliance requirements, therefore additional security frameworks may be considered as Botium Toys continues to expand.

Because Botium Toys is a rapidly growing small company, most security measures must be put into place right away. Nevertheless, certain physical measures like safes, lighting, and signage do not operate as quickly as the rest.

Summary/Recommendations:

This examination has brought to light several important security measures and regulations that Botium Toys must promptly put in place in order to achieve the organization's security objectives, especially with their fast expansion. Improving security posture involves aligning with necessary compliances (GDPR, PCI DSS, SOC type 1 and SOC type 2), categorizing all current assets, and implementing essential security controls.

Following the NIST CSF can simplify the completion of many tasks, as it is recognized as a security objective. As Botium Toys expands its business, it will be crucial to enhance disaster recovery plans and controls for business continuity. Kindly refer to the comprehensive controls evaluation and adherence checklist for specific measures to enhance security position. Please think about incorporating the NIST Risk Management Framework for more suggestions, as starting this process early in the business can greatly help in achieving security objectives.