**Scenario:**

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location. However, its online presence has grown, attracting customers in the U.S. and abroad. 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 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, and completing a risk assessment.**

**The goal of the audit is to provide an overview of the risks the company might experience due to the current state of their security posture. The IT manager wants to use the audit findings as evidence to obtain approval to expand his department.**

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

Steps of Performing A Security Audit

1. Identify Scope and Goals of Audit
2. Complete a Risk Assessment
3. Completing a Controls Assessment
4. Assessing Compliance
5. Communicating Results

**Step 1 - Botium Toys: Audit Scope & Goals**

Botium Toys internal IT audit will assess the following:

* Current user permissions set in the following systems: accounting, end point
* detection, firewalls, intrusion detection system, security information and event
* management (SIEM) tool.
* Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event

Management (SIEM) tool.

* Current procedures and protocols set for the following systems: accounting,end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
* Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
* Ensure current technology is accounted for. Both hardware and system access.

The goals for Botium Toys’ Internal IT audit are:

* To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
* Establish a better process for their systems to ensure they are compliant
* Fortify system controls
* Implement the concept of least permissions when it comes to user credential management
* Establish their policies and procedures, which includes their playbooks
* Ensure they are meeting compliance requirements

**Current Assets:**

Assets managed by the IT Department include:

1. On-premises equipment for in-office business needs
2. Employee Equipment - End-user devices (desktops/laptops, smartphones, remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc).
3. Management of systems, software and services: accounting, telecommunications, database, security, ecommerce and inventory management…
4. Internet Access
5. Internal Network
6. Vendor Access Management
7. Data Center Hosting Services
8. Data Retention and Storage
9. Badge Renders
10. Legacy System Maintenance: End-of-life systems that require human monitoring…

**Risk Description**

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have the proper controls in place and may not be 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 managing assets. Additionally, they will need to determine the impact of loss of existing assets, including systems, on business continuity.

**Risk Score:**

On a scale of 1 to 10, the risk score is 8 - fairly high… Due to a lack of controls and adherence to necessary compliance regulations and standards…

**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 lost. The likelihood of a lost asset or

fines from governing bodies is high because Botium Toys does not have all of the

necessary controls in place and is not adhering to required regulations and standards

related to keeping customer data private.

**What are the biggest risks to the organization?**

The biggest risk to the organizations include:

1. Data Breach - As Botium Toys does not have all the necessary controls in place to protect the organizations’ data generated and stored in its systems, software, and services, malicious actors could potentially exploit this vulnerability to access confidential information.
2. Financial Fraud - As indicated in the information provided about Botium Toys’ security posture, the accounting system also does not seem to have any controls in place to protect consumer and organization-related data. In the case of a data breach, the company’s finances along with customer deposits are likely to be compromised.
3. Reputational Risk - If an organization fails to adhere to regulations and standards related to keeping customer data private and the general public becomes aware of this, it is likely to affect the company’s long-term prospects, including its operations in the short-term.
4. **Legal Implications** - The chances of costly legal fines & penalties along with the legal implications of not adhering to required regulations and standards will further impede the company’s positive brand image.
5. **Disruption of Service** - As the business does not have a structured plan in place to ensure business continuity in the face of a data breach or an attack, the disruption of services including its online website and applications are likely to place a strain on its operating cash flow, revenues, and also anger customers.

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

| **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 | High |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain | X | High |

| **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 | NA (already in place) | NA |
| 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 | High |
| 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 | High |
| 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 | Medium |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats | X | Medium |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | X | High |
| 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 | Low |

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

Although the business’s headquarters is situated in the United States, we are aware of the fact that Botium Toys’ operations span globally and that they also operate and deal with customers in the European Union as well.

**GDPR** - E.U general data regulation that protects the processing of E.U. citizens’ data and their right to privacy in and out of European Union territory.

To ensure that the company keeps customer and vendor data safe and to avoid fines, it will have to comply with the GDPR. If a breach occurs and a E.U. citizen’s data is compromised, they must be informed within 72 hours of the incident..

**Payment Card Industry Data Security Standard (PCI DSS)**

An international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure information environment.

Botium Toys must ensure that the organization is storing, accepting, processing and transmitting credit card information securely or in a secure, encrypted environment.

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

A series of reports that focus on an organization’s user access policies at different organizational levels. Used to assess an organization’s financial compliance and levels of risk. Also cover organization’s financial compliance and levels of risk.

Botium Toys needs to establish and enforce appropriate user access policies for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety…

**Audit Report**

**To: IT Manager, Stakeholders**

**From: Birawin Jeevothayan, Cybersecurity Analyst - CyberVerse**

**DATE: Monday, July 17th, 2023**

**Subject: Internal IT Audit Findings And Recommendations**

**Scope:**

The scope of the internal IT audit conducted for Botium Toys encompassed an assessment of various key areas within the organization's information technology infrastructure. The audit focused on evaluating the current user permissions set in systems such as accounting, endpoint detection, firewalls, intrusion detection system, and security information and event management (SIEM) tool.

Additionally, the audit examined the implemented controls in these systems to ensure their effectiveness in safeguarding the organization's assets. The assessment also encompassed a review of the existing procedures and protocols associated with the aforementioned systems to identify any gaps or areas for improvement.

Furthermore, the audit aimed to ensure that the current user permissions, controls, procedures, and protocols were aligned with the necessary compliance requirements. The scope also extended to account for the organization's current technology landscape, including both hardware and system access.

**Goals:**

The internal IT audit conducted for Botium Toys aimed to achieve several important goals. The audit aimed to adhere to the guidelines outlined in the National Institute of Standards and Technology Cybersecurity Framework **(NIST CSF)**, which provides a comprehensive framework for managing and improving the security of information systems within an organization.

Furthermore, the audit sought to establish a more robust and efficient process for ensuring compliance of the organization's systems. This involved assessing the current user permissions, controls, procedures, and protocols to identify any gaps or areas of non-compliance.

The audit also aimed to fortify system controls to enhance the overall security posture of the organization's IT infrastructure. The concept of least privileges was also to be implemented to ensure proper user credential management and minimize potential risks.

Furthermore, the audit aimed to establish comprehensive policies and procedures, including playbooks, to guide the organization's cybersecurity practices effectively. The audit sought to ensure that the organization was meeting the applicable compliance requirements, taking into account the industry standards and regulations as well.

**Critical Findings:**

The audit revealed several critical findings that require immediate attention and the implementation of controls and policies.

Botium Toys lacks the proper management of critical organizational assets. This poses a significant risk as the organization might not have a clear understanding of its assets, including systems, and their impact on business continuity along with a robust mechanism to ensure that they are protected. Without understanding the assets’ impact on the business’s continuity, the chances of service disruptions prolonging are high.

The audit also identified a lack of proper controls within the organization. This raises the risk of data breaches, unauthorized access, financial losses and legal implications as a result of non-compliance with regulatory and international standards. The organization is also not fully compliant with U.S and international regulations and standards. This exposes them to more potential fines and penalties.

**Other Findings:**

The following controls should be implemented when possible:

1. Time Controlled Safe
2. Adequate Lighting
3. Locking Cabinets
4. Signage Indicating Alarm Service Provider

**Summary & Recommendations:**

**Controls**

Administrative Controls: The Principle of least privilege must be enforced to restrict access for vendors and non-authorized staff, reducing the risk of unauthorized access and potential data breaches. Botium must also develop and implement comprehensive disaster recovery plans to ensure business continuity by addressing system components and minimize downtime. Password policies should also be established to promote password strength, thereby lowering the likelihood of compromised accounts through brute force attacks. Access Control Policies must be implemented along with account management policies to enhance the confidentiality and integrity of data and to also limit the attack surface and mitigate the risks of insider threats. Considering the risk levels of the organization, the priority for implementation is high in order to enhance Botium’s security posture.

Technical Controls: An intrusion detection system must be implemented to detect possible intrusions quickly along with encryption of confidential information to enhance the security of data. Regular backups must be conducted on an ongoing basis and in alignment with the disaster recovery plan. A password management system should also be in place to ensure effective password recovery, reset and lockout notifications along with anti-virus software to detect and take action against any known threats. The legacy systems which are also under the purview of the IT department’s management should also be manually monitored & maintained on a regular basis. All these controls are of high priority and should be implemented immediately.

Physical Controls**:** A time-controlled safe acts as a deterrent to reduce the attack

Immediate action is required to implement the following technical controls: Intrusion Detection System (IDS) for quick identification of possible intrusions, encryption to enhance the security of confidential information and data, regular backups to support ongoing productivity and align with the disaster recovery plan, a password management system for effective password recovery, reset, and lockout notifications, antivirus (AV) software to detect and quarantine known threats, and manual monitoring, maintenance, and intervention for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities. These controls are of high priority and will significantly enhance the organization's security posture.

**Compliance**

To ensure the company keeps customer and vendor data safe, avoids fines, and maintains compliance, Botium Toys needs to adhere to the following compliance regulations:

General Data Protection Regulation (GDPR): As Botium Toys operates and deals with customers in the European Union (EU), they must comply with GDPR, which protects the processing of EU citizens’ data and their right to privacy. Compliance involves implementing measures to safeguard personal data, promptly notifying affected individuals in case of a data breach, and adhering to GDPR requirements in European Union territory.

Payment Card Industry Data Security Standard (PCI DSS): To securely handle credit card information, Botium Toys needs to comply with PCI DSS. This international security standard ensures that organizations storing, accepting, processing, and transmitting credit card data maintain a secure environment. Compliance involves implementing security measures, encryption, and maintaining a robust information security program.

System and Organizations Controls (SOC Type 1, SOC Type 2): Botium Toys should consider obtaining SOC reports, specifically SOC Type 1 and SOC Type 2. These reports focus on an organization's user access policies, financial compliance, and risk levels. By establishing and enforcing appropriate user access policies for internal and external personnel, Botium Toys can mitigate risks and ensure data safety.

Adhering to these compliance regulations will help Botium Toys protect customer and vendor data, avoid regulatory penalties, and maintain the trust of their stakeholders.