Botium Toys:
Audit scope and goals

Summary:

Perform an audit of Botium Toys' cybersecurity program. The audit needs to align current business practices with industry standards and best practices. The audit is meant to provide mitigation recommendations for vulnerabilities found that are classified as "high risk," and present an overall strategy for improving the security posture of the organization. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

Scope:

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.

Goals:

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

Risk Assessment

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.
- Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
- Internet access
- Internal network
- Vendor access management
- Data center hosting services
- Data retention and storage
- Badge readers
- 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 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 necessary compliance regulations and standards.

Loss of Assets

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.

Controls Assessment

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.
- Management of systems, software, and services: accounting, telecommunication, database, security, e-commerce and inventory management
-
- Internet access
- Internal network
- Vendor access management
- Data center hosting services

- Data retention and storage

- Badge readers

- Legacy system maintenance: end-of-life systems that require human monitoring

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	Medium
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 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	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	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	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	Medium

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	Low
Signage indicating alarm service provider	Deterrent; makes the likelihood of a successful attack seem low	X	Medium
Locks	Preventative; physical and digital assets are more secure	X	Medium

Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative; detect fire in the toy stores physical location to prevent damage to inventory, servers, etc.	X	Low

Compliance checklist

Below are the standards and compliance regulations Botium Toys must adhere to for business continuity and protection of assets:

- **The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)**

  As Botium Toys has increasingly high demand for online sales, it's critical that the company keeps up with their security in North America. This includes protecting customer PII and SPII, as well as company assets in the event of an attack on the power grid. It is recommended that employees change their passwords every 90 days with stringent requirements, such as the use of special characters and numbers included in password criteria.

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

  Since the company would like to expand and conduct business in the E.U, it's crucial they adhere to the GDPR regulations in place to protect their company and overseas customers. Botium toys would be required to alert customers within 72 hours if their data has been compromised, which is extremely important considering there is a growing interest in their products in multiple new European markets.

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

  As Botium toys sees an extremely quick increase in online sales, they must ensure that their customer's credit card transaction data is properly processed, transmitted and stored in a secure environment. It is recommended Botium Toys does an audit report on credit card transactions quarterly in tandem with their quarterly financial reports.

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

  Botium toys should use controls such as least privilege and separation of duties to ensure everyone in the company has the proper level of access when conducting business. Giving too much access or too little can impact confidentiality, privacy, integrity and overall data security within the company's security posture.