Internal Security Audit – Botium Toys

Controls Assessment

Current Assets Managed by the IT Department:

- 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.

Administrative Controls			
Control Name	**Control Type and Explanation**	**Needs To Be Implemented**	**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.	Yes	High
Disaster Recovery Plans	Corrective: Business continuity to ensure systems can 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.	Yes	High
Password Policies	Preventative: Establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques.	Yes	High

Access Control Policies	Preventative: Increase confidentiality and integrity of data.	Yes	High
Account Management Policies	Preventative: Reduce attack surface and limit overall impact from disgruntled/former employees.	Yes	High/ Medium
Separation of Duties	Preventative: Ensure no one has so much access that they can abuse the system for personal gain.	Yes	High

Technical Controls			
Control Name	**Control Type and Explanation**	**Needs To Be Implemented**	**Priority**
Firewall	Preventative: Firewalls are already in place to filter unwanted/malicious traffic from entering internal network.	No	
Intrusion Detection System (IDS)	Detective: Allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly.	Yes	High
Encryption	Deterrent: Makes confidential information/data more secure (e.g., website payment transactions).	Yes	High/ Medium
Backups	Corrective: Supports ongoing productivity in the case of an event; aligns to the disaster recovery plan.	Yes	High
Password Management System	Corrective: Password recovery, reset, lock out notifications.	Yes	High/ Medium
Antivirus (AV) Software	Corrective: Detect and quarantine known threats.	Yes	High
Manual Monitoring, Maintenance, & Intervention	Preventative/Corrective: Required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities.	Yes	High

Physical Controls			
Control Name	**Control Type and Explanation**	**Needs To Be Implemented**	**Priority**
Time-Controlled Safe	Deterrent: Reduce attack surface/impact of physical threats.	Yes	Medium/ Low
Adequate Lighting	Deterrent: Limit “hiding” places to deter threats.	Yes	Medium/ Low
Closed-Circuit Television (CCTV) Surveillance	Preventative/Detective: Can reduce risk of certain events; can be used after event for investigation.	Yes	High/ Medium
Locking Cabinets (For Network Gear)	Preventative: Increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear.	Yes	Medium
Signage Indicating Alarm Service Provider	Deterrent: Makes the likelihood of a successful attack seem low.	Yes	Low
Locks	Preventative: Physical and digital assets are more secure.	Yes	High
Fire Detection & Prevention (Fire Alarm, Sprinkler System, etc.)	Detective/Preventative: Detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc.	Yes	Medium/ Low

Compliance Checklist

- General Data Protection Regulation (GDPR)
  Why: If Botium Toys is conducting business within the European Union, GDPR is a mandatory regulation to protect the personal data of EU citizens.
- Payment Card Industry Data Security Standard (PCI DSS)
  Why: As Botium Toys accepts online and in person payments, they must ensure the secure handling of cardholder data.
- California Consumer Privacy Act (CCPA)
  Why: If selling to customers in California, CCPA provides rights to consumers about how their personal data is used.
- Children's Online Privacy Protection Act (COPPA)
  Why: If Botium Toys' products are targeted towards children under 13, they need to ensure they meet COPPA requirements regarding children's data.
- International Traffic in Arms Regulations (ITAR)
  Why: If any toys or components are considered defense articles or services, Botium Toys needs to comply with ITAR when exporting.
- System and Organizations Controls (SOC type 1, SOC type 2)
  Why: Botium Toys needs to establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety.

Stakeholder Memorandum

TO: IT Manager, Stakeholders
FROM: Cailyn Couchman
DATE: September 12, 2023
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the internal IT audit for Botium Toys. Below are the findings and recommendations derived from our in-depth analysis.

Scope:

- Current user permissions across key systems, including accounting, end-point detection, firewalls, intrusion detection systems, and the SIEM tool.
- The existing controls implemented in the same systems.
- Current procedures and protocols set for each of these systems.
- Ensuring that the current user permissions, controls, procedures, and protocols adhere to necessary compliance requirements.
- A comprehensive review to ensure all technology assets, both hardware and system access, are accounted for.

Goals:

- Improve Botium Toys' security posture by identifying vulnerabilities and strengthening system controls.
- Ensure adherence to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).
- Establish compliance-focused processes.
- Implement the concept of 'least permissions' in user management.
- Establish concrete policies, procedures, and playbooks.
- Meet all relevant compliance requirements especially as we expand our digital and international footprint.

Critical Findings:

- Control of Least Privilege and Separation of Duties: Essential for minimizing risk associated with user access.
- Disaster Recovery Plans: Required to minimize business disruptions.
- Policies: Password, access control, and account management policies must be developed. This includes the integration of a password management system.
- Encryption: Especially crucial for securing website transactions.
- Intrusion Detection System (IDS): To detect potential security breaches.
- Backups: To secure data and ensure business continuity.

- Antivirus (AV) Software: For ongoing threat detection and mitigation.
- CCTV: To deter and detect physical security threats.
- Locks: Physical and digital assets need strengthened security.
- Legacy Systems: Manual monitoring, maintenance, and intervention to ensure these systems remain secure.
- Fire Detection and Prevention Systems: To protect physical assets from potential fire hazards.
- Compliance: Develop and implement policies for PCI DSS and GDPR.
- User Access and Data Safety: Align with SOC1 and SOC2 guidance.

Secondary Findings:
- Time-Controlled Safe: An added layer of physical security.
- Adequate Lighting: Deters potential threats and improves surveillance.
- Locking Cabinets: For added security of physical documents and network gear.
- Signage: Indicating the presence of an alarm service provider can act as a deterrent.

Summary/Recommendations:
Given the critical insights, it is imperative that Botium Toys expediently addresses these areas, particularly those concerning user access, data security, and threat mitigation. As we venture further into the digital realm and expand globally, compliance with international standards and regulations is paramount.

Regarding the secondary findings, while not urgently pressing, they add significant value to our overall security infrastructure and are recommended for phased implementation.

As Botium Toys continues its growth trajectory, these steps are not only recommended but essential to protect our assets, data, and reputation. I look forward to our collaborative efforts in enhancing Botium Toys' security posture.

Best regards,

Cailyn Couchman
Cybersecurity Analyst