Internal Security Audit for Botium Toys

Scope and Goals of the Audit

Scope: The audit covers the entire security program at Botium Toys, including all assets, internal processes, and procedures related to controls and compliance best practices.

Goals:

- Assess existing assets.
- Complete the controls and compliance checklist.
- Determine which controls and compliance best practices need to be implemented to improve Botium Toys' security posture.

Current Assets Managed by the IT Department

1. On-premises equipment for in-office business needs.
2. Employee equipment: desktops/laptops, smartphones, remote workstations, peripherals.
3. Storefront products available for retail sale on-site and online; stored in the company's adjoining warehouse.
4. Management systems, software, and services: accounting, telecommunication, database, security, ecommerce, inventory management.
5. Internet access.
6. Internal network.
7. Data retention and storage.
8. Legacy system maintenance: end-of-life systems that require human monitoring.

Risk Assessment Summary

Risk Description:

- Inadequate management of assets.
- Lack of proper controls.
- Potential non-compliance with U.S. and international regulations.

Control Best Practices:

- Dedicate resources to identify and manage assets.
- Classify assets and determine their impact on business continuity.

Risk Score: 8 out of 10 (high risk).

Potential Impact:

- Medium impact from asset loss.
- High risk of fines due to lack of controls and compliance.

Specific Issues Identified:

- All employees have access to internally stored data.
- No encryption for customer credit card information.
- Missing access controls and separation of duties.
- No intrusion detection system (IDS) or disaster recovery plans.
- No regular backups of critical data.
- Plan to notify E.U. customers of security breaches within 72 hours.
- Nominal password policies lacking complexity requirements.
- No centralized password management system.
- Unclear and irregular legacy system maintenance.
- Physical security measures in place: locks, CCTV, fire detection.

Controls and Compliance Checklist

Control Category	Control Name	Control Type	Control Purpose	Implemented? (Yes/No)
Administrative/Managerial	Least Privilege	Preventative	Reduce risk of malicious insider or compromised accounts	No
Administrative/Managerial	Disaster Recovery Plan	Corrective	Provide business continuity	No
Administrative/Managerial	Password Policies	Preventative	Reduce likelihood of account compromise	No
Administrative/Managerial	Access Control Policies	Preventative	Define which groups can access or modify data	No
Administrative/Managerial	Account Management	Preventative	Manage account lifecycle, reduce attack surface	No
Administrative/Managerial	Separation of Duties	Preventative	Reduce risk of malicious insider or compromised accounts	No
Technical	Firewall	Preventative	Filter unwanted or malicious traffic	Yes
Technical	IDS/IPS	Detective	Detect and prevent anomalous traffic	No
Technical	Encryption	Deterrent	Provide confidentiality to sensitive information	No
Technical	Backups	Corrective	Restore/recover from an event	No

Technical	Password Management	Preventative	Reduce password fatigue	No
Technical	Antivirus (AV) Software	Corrective	Detect and quarantine known threats	Yes
Technical	Manual Monitoring	Preventative	Identify and manage threats to out-of-date systems	Yes
Physical/Operational	Time-Controlled Safe	Deterrent	Reduce attack surface and impact from physical threats	No
Physical/Operational	Adequate Lighting	Deterrent	Deter threats by limiting “hiding” places	Yes
Physical/Operational	CCTV	Preventative/Detective	Reduce risk and inform on event conditions	Yes
Physical/Operational	Locking Cabinets	Preventative	Prevent unauthorized access to network gear	No
Physical/Operational	Signage	Deterrent	Deter threats by indicating alarm service provider	No
Physical/Operational	Locks	Deterrent/Preventative	Bolster integrity by preventing unauthorized access	Yes
Physical/Operational	Fire Detection/Prevention	Detective/Preventative	Detect fire and prevent damage to physical assets	Yes

Recommendations for Improvement

1. **Implement Least Privilege and Access Control Policies**:

   - Restrict access to sensitive data based on employee roles.
   - Implement separation of duties to minimize risk from compromised accounts.

2. **Enhance Password Policies:**

   - Introduce more stringent password complexity requirements.
   - Implement a centralized password management system.

3. **Introduce Encryption for Sensitive Data:**

   - Encrypt customer credit card information and other sensitive data.

4. **Establish Disaster Recovery and Backup Plans:**

   - Develop and regularly test disaster recovery plans.
   - Regularly back up critical data and store backups securely.

5. **Deploy Intrusion Detection Systems (IDS):**

   - Implement IDS to detect and respond to suspicious activity.

6. **Regularly Maintain Legacy Systems:**

   - Establish a regular maintenance schedule for legacy systems.
   - Clearly define intervention methods for these systems.

Self-Assessment

1. **Reviewed the scope, goals, and risk assessment report**: Yes
2. **Considered risks to customers, employees, and assets**: Yes
3. **Reviewed the control categories document**: Yes
4. **Selected "yes" or "no" for each control listed**: Yes
5. **Selected "yes" or "no" for each compliance best practice**: Yes