Botium Toys Security Audit Recommendations

Key Observations and Recommendations

Based on the comprehensive review of Botium Toys' security posture, the following high-priority recommendations have been identified to address critical gaps and enhance compliance:

1. Access Controls

- **Observation**: All employees currently have access to customer data, increasing the risk of a data breach.
- **Recommendation**: Implement the principle of Least Privilege to limit access to sensitive information based on job responsibilities.

2. Disaster Recovery Plans

- **Observation**: No disaster recovery plans are in place.
- **Recommendation**: Develop and implement comprehensive disaster recovery plans to ensure business continuity in the event of an incident.

3. Password Policies

- **Observation**: Password requirements are minimal, increasing the risk of unauthorized access.
- **Recommendation**: Enforce strong password policies and implement a password management system to enhance security and productivity.

4. Separation of Duties

- **Observation**: The company lacks separation of duties, with critical responsibilities centralized under the CEO.
- **Recommendation**: Distribute responsibilities to reduce the risk of fraud and improve oversight of critical data and processes.

5. Firewall

- **Observation**: The existing firewall effectively blocks traffic based on an appropriately defined set of security rules.
- **Recommendation**: Continue to monitor and review firewall configurations regularly to ensure ongoing effectiveness.

Botium Toys Security Audit Recommendations

Key Observations and Recommendations

Based on the comprehensive review of Botium Toys' security posture, the following high-priority recommendations have been identified to address critical gaps and enhance compliance:

6. Intrusion Detection System (IDS)

- **Observation**: No IDS is currently in place to monitor for potential intrusions.
- **Recommendation**: Deploy an IDS to identify and respond to potential security breaches.

7. Backups

- **Observation**: The IT department lacks a reliable backup solution for critical data.
- **Recommendation**: Establish a regular backup process to ensure data can be restored quickly in case of a breach or loss.

8. Antivirus Software

- **Observation**: Antivirus software is installed and monitored regularly by the IT department.
- **Recommendation**: Maintain current antivirus practices and ensure the software remains up to date.

9. Legacy Systems Monitoring

- **Observation**: Legacy systems are monitored and maintained irregularly, with unclear procedures.
- **Recommendation**: Develop a regular schedule for monitoring and maintenance, including clear intervention policies, to reduce vulnerabilities.

10. Encryption

- **Observation**: Sensitive information, including credit card data and PII, is not encrypted.
- **Recommendation**: Implement encryption to secure sensitive data both in transit and at rest.

Botium Toys Security Audit Recommendations

Key Observations and Recommendations

Based on the comprehensive review of Botium Toys' security posture, the following high-priority recommendations have been identified to address critical gaps and enhance compliance:

11. Compliance with PCI DSS and GDPR

- **PCI DSS**:
  - Ensure only authorized users have access to customers' credit card information.
  - Encrypt all credit card data and implement secure processing and storage methods.
- **GDPR**:
  - Encrypt E.U. customers' data to maintain confidentiality.
  - Classify and inventory data assets to enhance management and security.
  - Maintain and enforce privacy policies, ensuring compliance with regulatory requirements.

12. System and Organization Controls (SOC)

- **Observation**: Lack of user access policies and encryption for PII/SPII.
- **Recommendation**:
  - Establish user access policies and enforce encryption for sensitive data.
  - Continue maintaining data integrity while improving access controls to limit data availability to authorized individuals only.

13. Physical Security

- **Observation**: Physical security measures such as locks, CCTV, and fire detection systems are sufficient.
- **Recommendation**: Maintain current physical security systems and review periodically for continued effectiveness.

Conclusion

These steps will help Botium Toys reduce risks and improve its overall security. Taking action now will not only protect the company’s operations but also build trust with customers, which is critical for a growing online business.