Security Audit

Botium Toys: Scope, Goals, and Risk Assessment Report

Scope and goals of the audit

Scope: The scope of this audit is defined as the entire security program at Botium Toys. This includes their assets like employee equipment and devices, their internal network, and their systems. You will need to review the assets Botium Toys has and the controls and compliance practices they have in place.

Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices that need to be implemented to improve Botium Toys' security posture.

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.
- Storefront products available for retail sale on site and online; stored in the company's adjoining warehouse
- Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
- Internet access
- Internal network
- Data retention and storage
- Legacy system maintenance: end-of-life systems that require human monitoring

Risk assessment

Risk description

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of the proper controls in place and may not be fully 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 identify assets so they can appropriately manage them. Additionally, they will need to classify existing assets and 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 compliance best practices.

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 at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure. Review the following bullet points for specific details:

- Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
- Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
- Access controls pertaining to least privilege and separation of duties have not been implemented.
- The IT department has ensured availability and integrated controls to ensure data integrity.
- The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
- Antivirus software is installed and monitored regularly by the IT department.

- The IT department has not installed an intrusion detection system (IDS).
- There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
- The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.
- Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).
- There is no centralized password management system that enforces the password policy's minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
- While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
- The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

Controls and Compliance Checklist

Select "yes" or "no" to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	**No**	**Control**
□	☑	Least Privilege
□	☑	Disaster recovery plans
□	☑	Password policies
□	☑	Separation of duties
☑	□	Firewall

□	☑	Intrusion detection system (IDS)
□	☑	Backups
☑	□	Antivirus software
□	☑	Manual monitoring, maintenance, and intervention for legacy systems
□	☑	Encryption
□	☑	Password management system
☑	□	Locks (offices, storefront, warehouse)
☑	□	Closed-circuit television (CCTV) surveillance
☑	□	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Compliance checklist

<u>Payment Card Industry Data Security Standard (PCI DSS)</u>

Yes	**No**	**Best practice**
□	☑	Only authorized users have access to customers’ credit card information.
□	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
□	☑	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☐	☑	E.U. customers' data is kept private/secured.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☐	☑	Ensure data is properly classified and inventoried.
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.

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

Yes	No	Best practice
☐	☑	User access policies are established.
☐	☑	Sensitive data (PII/SPII) is confidential/private.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☐	☑	Data is available to individuals authorized to access it.

Recommendations: While understanding the implementation and adjustment for security safeguards may be time-consuming and expensive, it is recommended that Botium Toys implement many changes to their security procedures and protocols to address potentially costly high-risk situations.

Recommended adjustments include addressing security controls and compliance issues. The highest and first recommendation would be to address issues securing SPII access, authorization, and potential recovery methods as this could be most costly for

Botium Toys in case of a breach. Next would be to focus on compliance issues with GDPR and PCI DSS as fines may result due to being out of compliance, posing an even costlier risk.

All further recommendations would be to refer to the checklists above and adjust any other remaining areas in checked as “no”.

Included below are administrative, technical, and physical controls that may be implemented for Botium Toys, some of which were identified as areas of change from the checklist:

Administrative/Managerial Controls		
Control Name	**Control Type**	**Control Purpose**
Least Privilege	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts
Disaster recovery plans	Corrective	Provide business continuity
Password policies	Preventative	Reduce likelihood of account compromise through brute force or dictionary attack techniques
Access control policies	Preventative	Bolster confidentiality and integrity by defining which groups can access or modify data
Account management policies	Preventative	Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage

Administrative/Managerial Controls		
Separation of duties	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts

Technical Controls		
Control Name	**Control Type**	**Control Purpose**
Firewall	Preventative	To filter unwanted or malicious traffic from entering the network
IDS/IPS	Detective	To detect and prevent anomalous traffic that matches a signature or rule
Encryption	Deterrent	Provide confidentiality to sensitive information
Backups	Corrective	Restore/recover from an event
Password management	Preventative	Reduce password fatigue
Antivirus (AV) software	Preventative	Scans to detect and quarantine known threats
Manual monitoring, maintenance, and intervention	Preventative	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems

Physical/Operational Controls

Control Name	**Control Type**	**Control Purpose**
Time-controlled safe	Deterrent	Reduce attack surface and overall impact from physical threats
Adequate lighting	Deterrent	Deter threats by limiting “hiding” places
Closed-circuit television (CCTV)	Preventative/Detective	Closed circuit television is both a preventative and detective control because it’s presence can reduce risk of certain types of events from occurring, and can be used after an event to inform on event conditions
Locking cabinets (for network gear)	Preventative	Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear
Signage indicating alarm service provider	Deterrent	Deter certain types of threats by making the likelihood of a successful attack seem low
Locks	Deterrent/Preventative	Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative	Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc.

Network protocols

Communication protocols

Communication protocols govern the exchange of information in network transmission. They dictate how the data is transmitted between devices and the timing of the communication. They also include methods to recover data lost in transit. Here are a few of them.

- Transmission Control Protocol (TCP) is an internet communication protocol that allows two devices to form a connection and stream data. TCP uses a three-way handshake process. First, the device sends a synchronize (SYN) request to a server. Then the server responds with a SYN/ACK packet to acknowledge receipt of the device's request. Once the server receives the final ACK packet from the device, a TCP connection is established. In the TCP/IP model, TCP occurs at the transport layer.
- User Datagram Protocol (UDP) is a connectionless protocol that does not establish a connection between devices before a transmission. This makes it less reliable than TCP. But it also means that it works well for transmissions that need to get to their destination quickly. For example, one use of UDP is for sending DNS requests to local DNS servers. In the TCP/IP model, UDP occurs at the transport layer.
- Hypertext Transfer Protocol (HTTP) is an application layer protocol that provides a method of communication between clients and website servers. HTTP uses port 80. HTTP is considered insecure, so it is being replaced on most websites by a secure version, called HTTPS that uses encryption from SSL/TLS for communication. However, there are still many websites that use the insecure HTTP protocol. In the TCP/IP model, HTTP occurs at the application layer.
- Domain Name System (DNS) is a protocol that translates internet domain names into IP addresses. When a client computer wishes to access a website domain

using their internet browser, a query is sent to a dedicated DNS server. The DNS server then looks up the IP address that corresponds to the website domain. DNS normally uses UDP on port 53. However, if the DNS reply to a request is large, it will switch to using the TCP protocol. In the TCP/IP model, DNS occurs at the application layer.

Management Protocols

The next category of network protocols is management protocols. Management protocols are used for monitoring and managing activity on a network. They include protocols for error reporting and optimizing performance on the network.

- Simple Network Management Protocol (SNMP) is a network protocol used for monitoring and managing devices on a network. SNMP can reset a password on a network device or change its baseline configuration. It can also send requests to network devices for a report on how much of the network's bandwidth is being used up. In the TCP/IP model, SNMP occurs at the application layer.
- Internet Control Message Protocol (ICMP) is an internet protocol used by devices to tell each other about data transmission errors across the network. ICMP is used by a receiving device to send a report to the sending device about the data transmission. ICMP is commonly used as a quick way to troubleshoot network connectivity and latency by issuing the "ping" command on a Linux operating system. In the TCP/IP model, ICMP occurs at the internet layer.

Security Protocols

Security protocols are network protocols that ensure that data is sent and received securely across a network. Security protocols use encryption algorithms to protect data in transit. Below are some common security protocols.

- Hypertext Transfer Protocol Secure (HTTPS) is a network protocol that provides a secure method of communication between clients and website servers. HTTPS is a secure version of HTTP that uses secure sockets layer/transport layer security (SSL/TLS) encryption on all transmissions so that malicious actors cannot read the information contained. HTTPS uses port 443. In the TCP/IP model, HTTPS occurs at the application layer.

- Secure File Transfer Protocol (SFTP) is a secure protocol used to transfer files from one device to another over a network. SFTP uses secure shell (SSH), typically through TCP port 22. SSH uses Advanced Encryption Standard (AES) and other types of encryption to ensure that unintended recipients cannot intercept the transmissions. In the TCP/IP model, SFTP occurs at the application layer. SFTP is used often with cloud storage. Every time a user uploads or downloads a file from cloud storage, the file is transferred using the SFTP protocol.

Additional Network protocols:

Protocol	Port
DHCP	UDP port 67 (servers) UDP port 68 (clients)
ARP	none
Telnet	TCP port 23
SSH	TCP port 22

POP3	TCP/UDP port 110 (unencrypted) TCP/UDP port 995 (encrypted, SSL/TLS)
IMAP	TCP port 143 (unencrypted) TCP port 993 (encrypted, SSL/TLS)
SMTP	TCP/UDP Port 25 (unencrypted)
SMTPS	TCP/UDP port 587 (encrypted, TLS)