Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Bryan Fury
DATE: 7/5/2023
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings, summary and recommendations.

Scope:

- The following systems are in scope:, accounting, endpoint, detection, firewalls, intrusion detection systems, and security information and event management (SIEM) Tools. The systems will be evaluated for:
    - Current user permissions
    - Current implemented controls
    - Current procedures and protocols
- Ensure current user permissions, implemented controls, and procedures of these systems.
- Ensure the compliance of Botium Toys with necessary regulatory requirements, such as payment card industry standards and data protection regulations.
- Ensure current technology is accounted for both hardware and software access.

Goals:

- Adherence to the National Institute of Standards and technology (NIST) Cybersecurity Framework (CSF) to establish a strong security foundation.
- Establish a better process for ensuring compliance and fortifying systems controls
- Implementation of the concept of least privileges for user credentials management to minimize risks.
- Establish policies, procedures, and playbooks to guide secure operations and response.

- Ensure they are meeting compliance requirement**s.**

Critical findings (must be addressed immediately): Multiple controls need to be developed and implemented to meet the audit goals, including:

- Control Of Least Privilege and Separation Of Duties
- Disaster Recovery Plans
- Password, access control, and account management policies, and implementation of password management system
- Encryption
- Backups
- IDS
- AV
- Manual monitoring, maintenance, and intervention for legacy systems
- Fire detection and prevention systems

- Policies need to be developed and implemented to meet compliance requirements, including payment card industry standards (PCI DSS) and data regulations (GDPR).
- Policies need to be developed and implemented to align to SOC1 and SOC2 guidelines related to user access policies and overall data safety.

Findings (should be addressed, but no immediate need): Justification for the expansion of the IT department and the hiring of additional cybersecurity personnel to strengthen our security posture and capabilities.

- Time-controlled safe
- Adequate lighting
- Locking Cabinets
- Signage indicating alarm service provider

Summary/Recommendations: It is recommended that critical findings be addressed promptly relating to compliance with PCI DSS and GDPR since Botium Toys accepts online payments worldwide including the European Union (EU). Additionally, since one of the goals of the audit is to adapt the concept of least permissions, SOC1 and SOC2 guidance relating to user access policies and overall data safety should be used to develop policies and procedures. Having disaster recovery plans and backups is also critical because they support business continuity in the event of an incident.

Integrating an IDS and AV software into the current systems will support our ability to identify and mitigate potential risks, and could help with intrusion detection, since existing legacy systems require manual monitoring and intervention. To help further secure assets housed at Botium Toys locks and CCTV should be used to secure physical assets. While not necessarily immediately, time-controlled safe , adequate lighting, locking cabinets, fire detection and prevention systems, signage indicating alarm service provider, will help improve Botium Toys Security posture. By aligning with our best practices and regulatory practices, our aim is to enhance the overall security of Botium Toys and maintain the trust of our customers and partners.

Compliance checklist

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

The FERC-NERC regulation applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. Organizations are legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

Explanation: NA

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

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens' data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and a E.U. citizen's data is compromised, they must be informed within 72 hours of the incident.

Explanation: Yes, Botium Toys needs to adhere to GDPR because they conduct business and collects personal information from people worldwide including the European Union (EU)

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

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

Explanation: Botium Toys needs to adhere to PCI DSS because they store, accept, process, and transmit credit card information in person and online.

☐ **The Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA is a federal law established in 1996 to protect U.S. patients' health information. This law prohibits patient information from being shared without their consent. Organizations have a legal obligation to inform patients of a breach.

Explanation: NA

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

The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels. They are used to assess an organization’s financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Explanation: 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.

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, 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 (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	High
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	High/ 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	NA	NA
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/Medium
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	High/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	High

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	Medium/ Low
Adequate lighting	**Deterrent**; limit “hiding” places to deter threats	X	Medium/ Low
Closed-circuit television (CCTV) surveillance	**Preventative/detective**; can reduce risk of certain events; can be used after event for investigation	X	High/ Medium
Locking cabinets (for network gear)	**Preventative**; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	X	Medium
Signage indicating alarm service provider	**Deterrent**; makes the likelihood of a successful attack seem low	X	Low
Locks	**Preventative**; physical and digital assets are more secure	X	High
Fire detection and prevention (fire alarm, sprinkler system, etc.)	**Detective/Preventative**; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc.	X	Medium/ Low