Stakeholder Memorandum

TO: IT Manager, Stakeholders

FROM: John Matthew Pasuelo

DATE: 24/05/23

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**: Botium Toys internal IT audit will assess the following:

* Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
* Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
* Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
* Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
* Ensure current technology is accounted for. Both hardware and system access.

**Goals**:

* To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
* Establish a better process for their systems to ensure they are compliant
* Fortify system controls
* Implement the concept of least permissions when it comes to user credential management
* Establish their policies and procedures, which includes their playbooks
* Ensure they are meeting compliance requirements

**Critical findings** (must be addressed immediately):

* Botium Toys needs to adhere to GDPR because they conduct business and collect personal information from people worldwide, including the E.U.
* Botium Toys needs to adhere to PCI DSS because they store, accept, process, and transmit credit card information in person and online.
* 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 Names that need to be implemented immediately:

* Least Privilege - reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs.
* 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.
* Password policies - establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques.
* Access control policies - increase confidentiality and integrity of data.
* Separation of duties - ensure no one has so much access that they can abuse the system for personal gain.
* Intrusion Detection System (IDS) - allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly
* Backups - supports ongoing productivity in the case of an event; aligns to the disaster recovery plan.
* Antivirus (AV) software - detect and quarantine known threats
* Manual monitoring, maintenance, and intervention - required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities
* Locks - physical and digital assets are more secure

**Findings** (should be addressed, but no immediate need):

Administrative Controls:

1. Account management policies: While it is important to have policies in place to reduce the attack surface and limit the overall impact from disgruntled or former employees, it may not be an immediate priority unless there is a high turnover rate or specific concerns related to employee access.

Technical Controls:

1. Encryption: Encryption is a valuable control for making confidential information more secure, but its implementation may be prioritized based on the specific data and systems that require encryption. The priority can be determined by conducting a risk assessment to identify the sensitivity of the data and potential threats.

Physical Controls:

1. Time-controlled safe: While having a time-controlled safe can reduce the attack surface and impact of physical threats, its implementation may be considered a lower priority unless there are specific concerns related to physical security or a high-value inventory.
2. Adequate lighting: Adequate lighting is important for limiting hiding places and deterring threats, but its implementation may depend on the specific security risks associated with the physical location of Botium Toys. It can be considered a medium to low priority compared to other controls.
3. Locking cabinets (for network gear): While locking cabinets for network gear can increase the integrity of the network infrastructure, the priority of implementation may vary based on the sensitivity of the network equipment and the physical security risks specific to the organization.
4. Signage indicating alarm service provider: While signage indicating the alarm service provider can act as a deterrent, its implementation may be considered a lower priority compared to other physical controls. It can be addressed once other more critical controls are in place.
5. Fire detection and prevention (fire alarm, sprinkler system, etc.): Fire detection and prevention measures are important for protecting inventory and servers, but their priority may depend on the specific risks associated with fire incidents and compliance requirements. It can be considered a medium to low priority compared to other controls.

Summary/Recommendations:

The internal IT audit at Botium Toys aimed to assess current user permissions, controls, procedures, and protocols in various systems to ensure compliance and fortify system controls. The audit had several critical findings that require immediate attention. Botium Toys must adhere to GDPR and PCI DSS due to their global business operations and handling of personal and credit card information. Implementing the concept of least privilege and establishing appropriate user access controls for both internal and external personnel is essential to mitigate risks and ensure data safety. The audit also identified the need for controls such as disaster recovery plans, password policies, access control policies, separation of duties, intrusion detection systems, backups, antivirus software, manual monitoring, maintenance, and locks. Addressing these critical findings promptly, while considering other important findings, will strengthen Botium Toys' compliance, data security, and overall IT infrastructure.