TO: IT Manager, Stakeholders

FROM: Jeff Reeder  
DATE: 9/5/2023  
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:**

* 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, firewalls, 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
* Impliment 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**

* Least Privilege- reduces risk by making sure vendors and non auuthorized staff only have access to the assets/data they need to do their jobs
* Disaster recovery plans- 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, stc.); 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.
* Account management policies- reduce attack surface and limit overall impact from disgruntled/former employees
* 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
* Encryption- makes confidential information/data more secure (e.g., website payment transactions)
* Backups- supports ongoing productivity in the case of an event; aligns to the disaster recovery plan
* Password management system- password recovery, reset, lock out notifications
* 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
* Closed-cercuit television (CCTV) surveillance- can reduce risk of certain events; can be used after event for investigation
* Locking cabinets (for network gear)- increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear
* Locks- physical and digital assets are more secure

**Findings**

* Adequate lighting- limit "hiding" places to deter threats
* Signage indicating alarm service provider- makes the likelihood of a successful attack seem low
* Fire detection and prevention (fire alarm, sprinkler system, etc.)
* Time controlled safe- reduce attack surface/impact of physical threats

**Summary/Recommendations:**

It is recommended that the critical findings be addressed immediately to be in compliance with PCI DSS and GDPR, since Botium Toys accepts online payments internationally, including the E.U. With respect to the other guidelines, SOC1 and SOC2, since one of the goals was the concept of least permissions, these two should be used to create the correct policies and procedures. Having disaster recovery plans and backups are critical because they support business continuity during an incident. Using Intrusion Detection Systems and Antivirus software with the current systems will help our ability to identify and mitigate potential risks. To protect Botium Toys' only brick and morter location, locks and CCTV should be used to secure assets and to monitor and investigate threats. Doing these in conjunction with using encryption and having a time controlled safe, better lighting, locking cabinets, fire detection and prevention systems, and correct signage about the alarm service provider will improve Botium's security posture.