TO: IT Manager, stakeholders
FROM: Eric
DATE: 2023.06.12
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

I am writing to present the findings and recommendations of the internal audit conducted at Botium Toys. The purpose of this audit was to assess the company's assets, controls, and compliance with regulations. Based on the audit results, the following information summarizes the scope, goals, critical findings, other findings, and recommendations.

Scope:
- The audit focused on the following systems: accounting, end point detection, firewalls, intrusion detection system, and SIEM tool.
- The evaluation included an assessment of current user permissions, implemented controls, procedures, and protocols.
- The objective was to ensure that the existing user permissions, controls, procedures, and protocols align with PCI DSS and GDPR compliance requirements.
- The audit also accounted for the technology infrastructure, encompassing both hardware and system access.

Goals:
- Adhere to the NIST CSF framework for cybersecurity.
- Establish an improved process to ensure compliance with regulatory standards.
- Strengthen system controls to mitigate risks effectively.
- Implement the concept of least privileges for user credential management.
- Develop comprehensive policies and procedures, including playbooks.
- Ensure compliance with relevant industry standards and regulations.

Critical Findings (must be addressed immediately):
1. Control of Least Privilege and Separation of Duties: Develop and implement controls to limit user access privileges and prevent unauthorized actions.
2. Disaster Recovery Plans: Establish comprehensive plans to ensure business continuity in the event of incidents or disruptions.
3. Password, Access Control, and Account Management Policies: Develop and enforce robust policies to ensure strong passwords, secure access control, and effective account management. Consider implementing a password management system.
4. Encryption (for secure website transactions): Deploy encryption mechanisms to enhance the security of customer data during online transactions.
5. Intrusion Detection System (IDS): Integrate an IDS to detect and respond promptly to potential intrusions or suspicious activities.
6. Backups: Implement regular backups of critical data to facilitate data recovery and minimize downtime.

7. Antivirus (AV) Software: Deploy reliable AV software to detect and quarantine known threats, enhancing the overall security posture.
8. Closed-Circuit Television (CCTV): Install CCTV systems to monitor and deter unauthorized access or suspicious activities.
9. Locks: Enhance physical security by implementing robust locking mechanisms for physical assets and facilities.
10. Manual Monitoring, Maintenance, and Intervention for Legacy Systems: Implement manual monitoring processes to mitigate potential threats and vulnerabilities associated with legacy systems.
11. Fire Detection and Prevention Systems: Install fire detection and prevention systems to minimize the risk of fire-related incidents and damages.

Other Findings (should be addressed in the future):
- Time-controlled safe: Consider implementing time-controlled safes to restrict access during specific periods.
- Adequate lighting: Ensure sufficient lighting to minimize potential hiding places and enhance overall security.
- Locking cabinets: Implement locking cabinets for network gear to prevent unauthorized access.
- Signage indicating alarm service provider: Install signage to create the perception of low attack success likelihood.

Summary/Recommendations:
Based on the critical findings, it is crucial that immediate actions be taken to address compliance with PCI DSS and GDPR. Given that Botium Toys accepts online payments globally, including the EU, meeting these requirements is paramount. Additionally, adopting the concept of least privileges and referring to SOC1 and SOC2 guidance for user access policies and overall data safety will contribute to a robust security framework. Establishing disaster recovery plans and regular backups will ensure business continuity and quick recovery in the event of incidents. Integrating an IDS and AV software will bolster threat detection capabilities, especially considering the manual monitoring required for legacy systems. Strengthening physical security through the installation