Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Aidan Gale
DATE: 7/28/2023
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:

- Systems included in the scope: Firewalls, intrusion detection systems, and Security Information and Event Management (SIEM) tools. These systems will be evaluated by looking at:
    - Current user permissions
    - Current implemented controls
    - Current procedures and protocols

Goals:

- Adhere to the (NIST CSF) framework
- 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):

- Least Privilege Principles
- Disaster recovery plans

- Password policies
- Access control policies
- Account management policies
- Separation of duties
- Intrusion Detection System
- Encryption
- Backups
- Password management system
- Antivirus (AV) software
- Manual monitoring, maintenance, and intervention
- Locking cabinets (for network gear)
- Locks

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

- Time-controlled safe
- Closed-circuit television (CCTV) surveillance
- Signage indicating alarm service provider
- Fire detection and prevention
- Adequate lighting

Summary/Recommendations:

In order to be in compliance with laws and regulations, Botium Toys needs to follow the above recommendations. As a first step it is important to make sure that the controls in the critical findings area are addressed first, relating to the PCI DSS and GDPR compliances. These are important to address because Botium Toys will be accepting credit card payments and expanding their customer base which includes the European Union. Expanding their customer base also means they will be handling a larger amount of user data. In addition, they must follow SOC type 1 and SOC type 2 compliance which will ensure the organization's financial compliance and levels of risk. It will also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

To keep business continuity, establishing a disaster plan and backups will keep data safe from things like fires and floods. To help prevent disasters like this, considering integrating fire detection will prevent fires from spreading rampantly and destroying large amounts of data. In addition, having antivirus software is important to defend against cyber attacks that could be detrimental to the organization.

To also help defend against cyber attacks, it is recommended to incorporate an Intrusion Detection System to mitigate the risks with any legacy systems that might have to be manually monitored.

Finally, the physical location and its assets need to be secured. In order to do so, installing the proper controls is necessary. A time-controlled safe, adequate lighting, closed-circuit television (CCTV) surveillance, locking cabinets (for network gear), and signage indicating alarm service providers will all help improve security posture.

Conclusion

Overall, I think this practice case study helped me understand how to classify the importance of a control given the scope and goals of the audit. Being able to determine the organization’s needs given the scope and goals is an important skill when conducting an audit. Learning what controls corresponded to each compliance guideline was an important step in completing the stakeholder memorandum.