Botium Toys Internal Security Audit

Introduction

This is an internal security audit of Botium Toys. This fictitious company is part of Google's Cybersecurity Course as an exam, and I will add it to my personal and professional portfolio.

I will demonstrate ownership of what I've learned so far in this course, using business practices with industry standards and best practices.

Scenario

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location. However, its online presence has grown, attracting customers in the U.S. and abroad. Their information technology (IT) department is under increasing pressure to support their online market worldwide.

The manager of the IT department has decided that an internal IT audit needs to be conducted. She expresses concerns about not having a solidified plan of action to ensure business continuity and compliance, as the business grows. She believes an internal audit can help better secure the company's infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. The manager is also interested in ensuring that they comply with regulations related to accepting online payments and conducting business in the European Union (E.U.).

The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, and completing a risk assessment. The goal of the audit is to provide an overview of the risks the company might experience due to the current state of their security posture. The IT manager wants to use the audit findings as evidence to obtain approval to expand his department.

Botium Toys internal IT audit will assess the following:

● Current user permissions set in the following systems: accounting, endpoint detection, firewalls, intrusion detection systems, security information, and event management (SIEM) tool.

● Current implemented controls in the following systems: accounting, endpoint detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.

● Current procedures and protocols set for the following systems: accounting, endpoint 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.

The goals for Botium Toys' internal IT audit are:

● 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 include their playbooks

● Ensure they are meeting compliance requirements

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, e-commerce, 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	Absolutely	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 the 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	Absolutely	High
Password policies	Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques	Absolutely	High

Control name	Control Type and explanation	Needs to be implemented (x)	Priority
Access control policies	Preventative; increase confidentiality and integrity of data	Absolutely	High
Account management policies	Preventative; reduce attack surface and limit overall impact from disgruntled/former employees	Absolutely	High
Separation of duties	Preventative; ensure no one has so much access that they can abuse the system for personal gain	Absolutely	High

TECHNICAL CONTROLS

Control name	Control Type and explanation	Needs to be implemented	Priority
Firewall	Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network	No necessa…	Mid/High
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly	Absolutely	High
Encryption	Deterrent; makes confidential information/data more secure (e.g., website payment transactions)	Absolutely	High
Backups	Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan	Absolutely	High
Password management system	Corrective; password recovery, reset, lockout notifications	Absolutely	High
Antivirus (AV) software	Corrective; detect and quarantine known threats	Absolutely	High

Control name	Control Type and explanation	Needs to be implemented	Priority
Manual monitoring, maintenance, and intervention	Preventative/corrective; required for legacy systems to identify and mitigate	Absolutely	High

PHYSICAL CONTROLS

Control name	Control Type and explanation	Needs to be implemented	Priority
Time-controlled safe	Deterrent; reduce attack surface/impact of physical threats	No necessa…	Mid/High

Control name	Control Type and explanation	Needs to be implemented	Priority
Adequate lighting	Deterrent; limit “hiding” places to deter threats	Absolutely	Mid/High
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for investigation	Absolutely	High
Locking cabinets (for network gear)	Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	Absolutely	Mid/High
Signage indicating alarm service provider	Deterrent; makes the likelihood of a successful attack seem low	No necessa…	Mid/High
Locks	Preventative; physical and digital assets are more secure	Absolutely	High

Control name	Control Type and explanation	Needs to be implemented	Priority
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.	Absolutely	Mid/Low

Conclusion

Botium Toys needs to adhere National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the standards of:

> The General Data Protection Regulation (GDPR) The UE regulation is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. This would allow Botium Toys to use personal information on European customers.
>
> Payment Card Industry Data Security Standard (PCI DSS), The PCI DSS (Payment Card Industry Data Security Standard) is an information security standard designed to reduce payment card fraud by increasing security controls around cardholder data. This one is important since they would accept payments online and in person, and there would be international transactions, for this reason, compliance with this standard is absolutely important.

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. 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.

Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: (Jose Daniel Solis)
DATE: (09/26/2023)
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, security information, and event management (SIEM) tool. The systems will be evaluated for

Current user permissions

Current implemented controls

Current procedures and protocols

Ensuring current user permissions, controls, procedures, and protocols in place align with GDPR, PCI DSS, compliance requirements

Ensure current technology and assets are accounted for both hardware and system access.

Goals:

Adhere to the 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 include their playbooks

High-Risk Findings (must be addressed immediately): Multiple controls need to be developed and implemented to meet the audit goals, including

Principle of Least Privilege and Separation of duties

Disaster recovery plans

Password, Access control, and Account management policies

Intrusion Detection System (IDS)

Encryption (secure website transactions wand disk drive(s) containing sensitive information)

Backups

Implementation of a Password management system

Antivirus (AV) software

Manual monitoring, maintenance, and intervention for legacy systems

Closed-circuit television (CCTV) surveillance

Locks

Fire detection and prevention (fire alarm, sprinkler system, etc.)

Policies need to be developed and implemented for the following:

To meet PCI DSS and GDPR compliance requirements.

To meet SOC1 and SOC2 guidance related to user access policies and overall data safety.

Mid/High - Mid/Low Findings (should be addressed, but no immediate need):

Time-controlled safe

Adequate lighting

Signage indicating alarm service provider for restricted areas

Locking cabinets (for network gear)

Summary/Recommendations:

It is necessary to implement each of the security standards and frameworks mentioned in the security audit. We recommend implementing them as soon as possible to avoid any fines or issues in upcoming audits with the law, security, and every enforcing agent of the security regimen. Best regards in advance."