Renaldo Schmidt

Google Cybersecurity Course Security Audit

Summary: Perform an audit of Botium Toys' cybersecurity program. The audit needs to align current business practices with industry standards and best practices. The audit is meant to provide mitigation recommendations for vulnerabilities found that are classified as "high risk," and present an overall strategy for improving the security posture of the organization. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

You receive the following email from your IT manager:

Hello!
I have completed the audit scope and goals, as well as a risk assessment. At a high level, the main goals and risks are as follows:

Goals:

- Improve Botium Toys' current security posture by aligning to industry best practices (e.g., adhere to the NIST CSF, implement concept of least permissions)
- Provide mitigation recommendations (i.e., controls, policies, documentation), based on current risks
- Identify compliance regulations Botium Toys must adhere to, primarily based on *where* we conduct business and *how* we accept payments
- To review the full report, read the Botium Toys: Audit scope and goals document

Risks:

- Inadequate management of assets
- Proper controls are not in place
- May not be compliant with U.S. and international regulations and guidelines
- Current risk score is 8/10 (high), due to a lack of controls and adherence to compliance regulations and standards
- To review the complete list of assets and risks, read the Botium Toys: Risk assessment document

Thank you, Botium Toys IT Manager

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, 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 includes their playbooks
- Ensure they are meeting compliance requirements

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, ecommerce, 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

Risk description

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have the proper controls in place and may not be compliant with U.S. and international regulations and standards.

Control best practices

The first of the five functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to managing assets. Additionally, they will need to determine the impact of the loss of existing assets, including systems, on business continuity.

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, ecommerce, 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	X	HIGH
Disaster recovery plans	Corrective; business continuity to ensure systems are able to run in the event of an	X	HIGH

Administrative Controls			
	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	Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques	X	HIGH
Access control policies	Preventative; increase confidentiality and integrity of data	X	HIGH
Account management policies	Preventative; reduce attack surface and limit overall impact from disgruntled/former employees	X	MED
Separation of duties	Preventative; ensure no one has so much access that they can abuse the system for personal gain	X	HIGH

Technical Controls

Control Name	Control type and explanation	Needs to be implemented (X)	Priority
Firewall	Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network	X	HIGH
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly	X	HIGH
Encryption	Deterrent; makes confidential information/data more secure (e.g., website payment transactions)	X	MED
Backups	Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan	X	HIGH
Password management system	Corrective; password recovery, reset, lock out notifications	X	LOW
Antivirus (AV) software	Corrective; detect and quarantine known threats	X	HIGH
Manual monitoring, maintenance, and intervention	Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities	X	HIGH

Physical Controls

Renaldo Schmidt

Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Time-controlled safe	Deterrent; reduce attack surface/impact of physical threats	X	LOW
Adequate lighting	Deterrent; limit “hiding” places to deter threats	X	LOW
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for investigation	X	LOW
Locking cabinets (for network gear)	Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	X	MED
Signage indicating alarm service provider	Deterrent; makes the likelihood of a successful attack seem low	X	MED
Locks	Preventative; physical and digital assets are more secure	X	HIGH
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.	X	MED

Renaldo Schmidt

Compliance Checklist

□ **The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)**

The FERC-NERC regulation applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. Organizations are legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

Explanation:

☑ **General Data Protection Regulation (GDPR)**

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens' data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and an E.U. citizen's data is compromised, they must be informed within 72 hours of the incident.

Explanation: Botium Toys needs to adhere to the GDPR because if they conduct business in the E.U. without following this regulation they are at the risk of serious fines and legal trouble if a breach were to occur.

☑ **Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

Explanation: Since Botium Toys sells toys online, they must adhere to the PCI DSS in order to keep credit card information safe. If hackers were to gain access to the credit card data, it would result in serious issues for the company including a blemished reputation.

☐ **The Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA is a federal law established in 1996 to protect U.S. patients' health information. This law prohibits patient information from being shared without their consent. Organizations have a legal obligation to inform patients of a breach.

Explanation:

☑ **System and Organizations Controls (SOC type 1, SOC type 2)**

The 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.

Explanation: Botium Toys must adhere to SOC types 1 and 2 as it will help implement proper user access in order to prevent fraud and keep the company from having to stop in its tracks if a threat actor were to abuse a vulnerability.

Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Renaldo Schmidt
DATE: 8/28/23
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: Since we are a rapidly growing e-commerce company, we had to look at our entire security program for vulnerabilities. All of our assets were assessed alongside our internal processes and procedures. We examined current user permissions, controls, procedures, and protocols in the following systems: accounting, endpoint detection, firewalls, IDS, and SIEM tools. We also ensured that all of these align with necessary compliance requirements such as PCI DSS and GDPR.

Goals: The overall goal of the audit was to improve the security posture of our organization so that we do not encounter unnecessary turmoil in the future. Specifically, we looked to adhere to the NIST CSF, establish better processes for our systems, fortify system controls, implement the concept of least permission, establish policy and procedures, and ensure that we meet compliance requirements. All of these measures will ensure that business operations go smoothly and continuously.

Critical findings (must be addressed immediately):

These controls need to be implemented first to meet the audit goals

Least Privilege - We must implement the principle of least privilege soon because it reduces risk by ensuring that people only have access to what they need to complete their jobs. This will help keep our data safe from internal threats, and if an event were to occur, we can narrow down who it could have been easier.

Disaster Recovery Plans - We need a plan in place to ensure continuity if a disaster were to occur in our network, physical location, or other assets. If we had a recovery plan, we could return to normal procedures quicker to stay profitable.

Password Policies - Our employees should have hard-to-hack complex passwords so they don't get their accounts compromised.

Access Control Policies - We should ensure the employees can only access what they need.

Separation of Duties - We should make sure that no one employee has access to so much data and information that they could abuse the company for personal gain.

Firewall - We need to make sure our firewall is strong and effectively filters out malicious traffic from entering our internal network.

Intrusion Detection System - We need to have an IDS to aid in the monitoring of the network to help prevent any breaches.

Backups - We need backups in case a disaster were to occur.

Antivirus Software - Antivirus software is a must for our company. We should soon implement it on all our devices to strengthen our security.

Manual Monitoring, Maintenance, and Intervention - We need more Cybersecurity personnel to manually monitor our network and assets to ensure security.

Locks - We need to lock our facility and high-value rooms and ensure that only accredited people have access.

Policies need to be developed and implemented to meet PCI DSS, GDPR, and SOC Type 1 and 2 compliance requirements and guidance.

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

Account Management Policies - We must make sure that our accounts have a time limit on them and must be renewed. This is important because an old employee should not have access to the company data after termination.

Encryption - Eventually we must keep data encrypted as another means to keep data safe.

Password Management System - Soon we must implement a password management system so that employees can carry on their usual business quickly if they forget their passwords, while at the same time ensuring that everything is confidential and secured.

Time-Controlled Safe - Keep our valuable physical assets locked behind a time-controlled safe with access only to those who need it.

Adequate Lighting - We must eventually contract someone to install better lighting in our facility so that our cameras can see everything and also it will limit hiding spots.

CCTV - A camera system is a must for our organization so that it can deter illegal activity and give us a record if anything were to happen.

Locking Cabinets - Lock up our network gear so that unauthorized individuals cannot modify or hack our system.

Signage Indication Alarm Service Provider - Scare away intruders by putting alarm system signs.

Fire Detection and Prevention - Ensure we have a sprinkler and fire detection system to keep our employees and physical assets safe.

Summary/Recommendations:

The security team concluded that the business currently has a poor security posture as a result of this security audit. We recommend that we swiftly implement the controls from our critical findings in order to boost our security posture as an organization. This will aid in business continuity if a disaster were to occur and keep the business profitable. Eventually, once the critical findings are all implemented at a high level, we must add the controls from our other findings to maximize our security and keep us from receiving fines and encountering legal trouble. This needs to be done to adhere to the GDPR, PCI DSS, SOC Type 1 and 2, and the NIST CSF since we accept online payments from customers worldwide. If all these things are implemented and enforced, then we are highly unlikely to face adversity as an organization from hackers, regulators, and internal threats.