Jasper Davis

Compliance Checklist

☑ **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 a E.U. citizen's data is compromised, they must be informed within 72 hours of the incident.

Explanation: As Botium's online presence has grown, they are starting to conduct business abroad including in the European Union and are thus subject to the requirements of GDPR.

☑ **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: As an online retailer that accepts digital payments, Botium is required to adhere to the PCI DSS.

☐ **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: These reports do not appear to be mandatory for Botium.

☐ **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: Not applicable as Botium does not deal with health information.

☐ **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: Not applicable as Botium doesn't oversee or interact with the power grid.

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 incident/there is limited to no loss of productivity	**X**	**Medium**

Administrative Controls			
	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**	**Medium**
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**	**Medium**
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**	**Priority**

		(X)	
Firewall	Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network	**N/A**	**N/A**
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly	**X**	**Medium**
Encryption	Deterrent; makes confidential information/data more secure (e.g., website payment transactions)	**X**	**High**
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**	**Medium**
Antivirus (AV) software	Corrective; detect and quarantine known threats	**X**	**Medium**
Manual monitoring, maintenance, and intervention	Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities	**X**	**Medium**

Physical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented**	**Priority**

		(X)	
Time-controlled safe	Deterrent; reduce attack surface/impact of physical threats	**X**	**Medium**
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**	**Medium**
Locking cabinets (for network gear)	Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	**X**	**High**
Signage indicating alarm service provider	Deterrent; makes the likelihood of a successful attack seem low	**X**	**Low**
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**	**High**

Stakeholder Memorandum

TO: IT Manager, Stakeholders
FROM: Jasper Davis
DATE: 2023-06-17
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: This audit evaluated the entire security program at Botium Toys. This included the review of internal processes and procedures and an examination of all security-related assets. Asset examples include all employee equipment, company systems, software, internet and internal network access, vendor access, physical security items (e.g. badge readers), data hosting, retention, & storage, and legacy systems.

Goals:

- Ensure compliance with all mandatory legal requirements.
- Improve credential management through implementation of least permissions.
- Develop security playbooks through establishment of standard policies and procedures.
- Fortify all system controls.

Critical findings (must be addressed immediately):

- Certain practices that impact how data is handled must be prioritized to ensure legal compliance with GDPR and PCI DSS. Examples include:
    - Access Control Policies
    - Least Privilege
    - Encryption
    - Separation of Duties
- Regular backups should also be implemented to ensure that data is protected in the event of a security incident.

- Physical security should also be prioritized, including installation of locks and fire detection & prevention systems.

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

- Botium needs to develop and implement disaster recovery plans.
- Implementation of password and account management policies would further reduce attack surface and lower the risk of system compromise.
- Additional physical deterrents like a time-controlled safe, CCTV surveillance system, alarm service provider signace would increase the security of the physical premises.

Summary/Recommendations: Overall, Botium has identified a number of important areas for improvement as the business continues to grow and especially as online sales expand internationally. The top priority for Botium should be implementation of data-management related safeguards to ensure regulatory compliance with international standards like GDPR and PCI DSS. In particular, this would involve implementation of least privilege and other access control policies. While not considered absolutely critical, Botium would benefit significantly from the creation of disaster recovery plans, including the development of a business continuity plan. Various other measures could be implemented to increase the physical security of Botium's premises.