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	HIGH

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	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	HIGH
Separation of duties	Preventative; ensure no one has so much access that they can abuse the system for personal gain	X	MEDIUM

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
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	MEDIUM
Backups	Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan		N/A
Password management system	Corrective; password recovery, reset, lock out notifications		N/A
Antivirus (AV) software	Corrective; detect and quarantine known threats		N/A
Manual monitoring, maintenance, and intervention	Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities	X	LOW

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	HIGH
Adequate lighting	Deterrent; limit “hiding” places to deter threats	X	MEDIUM
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for investigation	X	HIGH
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	MEDIUM
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

CONSIDERATION

Potential Impact:

- The assessment of a medium impact from the loss of an asset suggests that while the specific assets at risk may not be known, the consequences of such losses could have a significant effect on the organization.

- Medium impact typically implies that the loss could result in financial losses, operational disruptions, or damage to the company's reputation, among other potential consequences.

Likelihood:

- The assessment of a high likelihood of asset loss or fines indicates that there is a strong probability that these events may occur.
- This high likelihood is attributed to the lack of necessary controls and non-compliance with regulations and standards related to data privacy.

Risk Mitigation:

- Given the high likelihood and potential medium impact, it becomes imperative for Botium Toys to take immediate action to mitigate these risks.
- Implementing controls such as access controls, encryption, and data protection measures can reduce the likelihood of asset loss and improve compliance with data privacy regulations.

Regulatory Compliance:

- Non-compliance with regulations and standards related to customer data privacy can result in severe financial penalties, legal consequences, and reputational damage.
- To address this, Botium Toys should prioritize compliance efforts, including GDPR, PCI DSS, or other relevant regulations, based on its business operations and customer data handling.

Data Inventory and Classification:

- To better understand the assets at risk, Botium Toys should conduct a thorough data inventory and classification process. This will help identify critical assets and prioritize their protection.

Continuous Improvement:

- Risk management and compliance are ongoing processes. Botium Toys should establish a culture of continuous improvement in security and compliance to adapt to evolving threats and regulations.

In conclusion, the provided information underscores the urgency of addressing the identified risks, enhancing controls, and ensuring compliance with data privacy regulations. Failure to do so could have significant consequences for the organization, its customers, and its reputation. Prioritizing security and compliance efforts is essential to protect Botium Toys' assets and maintain trust with stakeholders.