Controls Assessment Botium Toys (Fictional)

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

<u>Administrative Controls:</u>

Least Privilege:
Control Type: Preventative
Explanation: Limit access privileges to vendors and non-authorized staff based on their job requirements.
Needs to be implemented (X): Yes
Priority: High

Disaster Recovery Plans:
Control Type: Corrective
Explanation: Establish plans for business continuity and system recovery in the event of an incident.

Needs to be implemented (X): Yes
Priority: Medium

Password Policies:
Control Type: Preventative
Explanation: Implement rules for password strength to enhance security and reduce the likelihood of account compromise.
Needs to be implemented (X): Yes
Priority: High

Access Control Policies:
Control Type: Preventative
Explanation: Define policies to increase the confidentiality and integrity of data.
Needs to be implemented (X): Yes
Priority: Medium

Account Management Policies:
Control Type: Preventative
Explanation: Establish policies to manage user accounts, reducing the attack surface and limiting potential impact from disgruntled or former employees.
Needs to be implemented (X): Yes
Priority: Medium

Separation of Duties:
Control Type: Preventative
Explanation: Implement measures to ensure that no single individual has excessive access privileges that could be exploited for personal gain.
Needs to be implemented (X): Yes
Priority: Medium

Technical Controls:

Firewall:
Control Type: Preventative
Explanation: Firewalls are already in place to filter unwanted and malicious traffic from entering the internal network.
Needs to be implemented (X): No
Priority: Not applicable

Intrusion Detection System (IDS):
Control Type: Detective
Explanation: Implement an IDS to quickly identify possible intrusions and anomalous traffic.
Needs to be implemented (X): Yes
Priority: High

Encryption:
Control Type: Deterrent
Explanation: Apply encryption measures to enhance the security of confidential information and data.
Needs to be implemented (X): Yes
Priority: Medium

Backups:
Control Type: Corrective
Explanation: Establish regular backup procedures to support ongoing productivity and align with the disaster recovery plan.
Needs to be implemented (X): Yes
Priority: Medium

Password Management System:
Control Type: Corrective
Explanation: Implement a password management system to assist with password recovery, resets, and lockout notifications.
Needs to be implemented (X): Yes
Priority: Low

Antivirus (AV) Software:
Control Type: Corrective
Explanation: Deploy AV software to detect and quarantine known threats.

Needs to be implemented (X): Yes
Priority: High

Manual Monitoring, Maintenance, and Intervention:
Control Type: Preventative/Corrective
Explanation: Continuously monitor and maintain legacy systems to identify and mitigate potential threats, risks, and vulnerabilities.
Needs to be implemented (X): Yes
Priority: Medium

Physical Controls:

Time-Controlled Safe:
Control Type: Deterrent
Explanation: Use time-controlled safes to limit the attack surface and minimize the impact of physical threats.
Needs to be implemented (X): Yes
Priority: Medium

Adequate Lighting:
Control Type: Deterrent
Explanation: Ensure proper lighting to deter threats by minimizing potential hiding places.
Needs to be implemented (X): Yes
Priority: Low

Closed-Circuit Television (CCTV) Surveillance:
Control Type: Preventative/Detective
Explanation: Install CCTV surveillance to reduce certain risks and assist with post-event investigations.
Needs to be implemented (X): Yes
Priority: Medium

Locking Cabinets (for Network Gear):
Control Type: Preventative
Explanation: Secure network infrastructure gear in locking cabinets to prevent unauthorized access or modifications.
Needs to be implemented (X): Yes
Priority: High
Signage Indicating Alarm Service Provider:
Control Type: Deterrent
Explanation: Display signage indicating the presence of an alarm service provider to discourage potential attackers.
Needs to be implemented (X): Yes
Priority: Low

Locks:
Control Type: Preventative
Explanation: Use locks to enhance the physical and digital security of assets.
Needs to be implemented (X): Yes
Priority: Medium

Fire Detection and Prevention (Fire Alarm, Sprinkler System, etc.):
Control Type: Detective/Preventative
Explanation: Implement fire detection and prevention measures to detect and mitigate fire incidents.
Needs to be implemented (X): Yes
Priority: Medium

Note: The "Needs to be implemented" and "Priority" ratings are subjective and may vary based on the specific context and risk appetite of Botium Toys. It is important to assess and prioritize controls based on the organization's unique requirements and risk assessment.