**Step 2:**

* **What are the biggest risks to the organization?**

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.

* **Which controls are most essential to implement immediately versus in the future?**

The controls most enssential is to adopt a system to keep track of current assets as soon as possible to avoid or mitigate losses. In addition, it woul dbe good to have a back up system possibly by migrating on premise data to the cloud specially from legacy systems.

In there future, it would be a good idea to install, update and configure proper permissions and controls with a good anti-virus, IDS, IPS and SIEM and update or replace legacy systems with modern ones. Also to implement a NIST CSF compliant ISMS tailored to the company needs following industry regulations and best practices with correct standars, controls, procedures and protocols. For example a good containment and recovery strategy is key for ensuring bussiness continuity.

* **Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.?**

First and foremost the NIST Cybersecurity Framework is important to start with a good base to manage and reduce risk in addition to adhering the regulations to avoid fines and best industry practices for better security posture.

**Step3:**

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

**Control Types:**

|  |  |  |  |
| --- | --- | --- | --- |
| **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  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 | X | High |
| Password policies | Preventative; establish  password strength rules to  improve security/reduce  likelihood of account  compromise through brute  force or dictionary attack  techniques | X | High |

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical Controls** | | | |
| **Control Name** |  | **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 | 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 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Physical Controls** | | | |
| **Control Name** | **Control type and explanation** | **Needs to be**  **implemented**  **(X)** | **Priority** |
| Time-controlled  safe | Deterrent; reduce attack  surface/impact of physical  threats | X | High |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats | X | Medium/  Low |
| 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 |
| Locks | Preventative; physical and  digital assets are more secure | X | Medium/  Low |

**Step 4:**

1. **Consider where** the company conducts business and **how** they receive payments from customers.

According to the description of the scenario the business has a single physical location in the US with an online presence in the US and abroad expanding rapidly. It is assume that the company likes to adhere to the payment rules of the countries or regions in which does business, and perhaps because usually european law is ahead of the rest including laws, the manager wants to make sure that the company is acepting online payments in line with EU law so to demostrate that if it can comply with the highest standards possible its easily understood that the company will not have problemas in other countries or regions.

1. **Click the boxes** to select the compliance regulations and standards that Botium Toys needs to adhere to.\*
2. **Explain** why the company needs to adhere to the selected compliance regulations and standards.

Because rules and regulations were created to protect business and customers alike and therefore must be follow otherwise lack of compliance can incurr fines, sanctions and in the worst case closure of a bussiness in the host country.