**Botium Toys: Scope, goals, and risk assessment report**

**Scope**

Th scope of this risk assessment is to solidify business continuity and to ensure that the organisation follows current compliance avoiding risks threats and vulnerabilities to company assets, whether it physical or digital that poses a thrat to the organisation and individuals.

**Goals**

* Following the guidelines as outlined from the framework NIST CSF
* Comply with EU rgulations specified in GDPR

**Assets**

* Computers including servers and workstations.
* Headsets, keyboards. Mices, printers, projectors
* PII / SPII data
* Internet / Intranet
* Network devices
* SQL Databases
* CCTV
* stocks inventory

**Assessment**

Description

Currently the business does not have an effective disaster recovery plan in place, the company would have an impact with business continuity if a cyberattack was ever to occur. Inadequate security controls enabling some employees to have more access than they should for their job functions. The latter could place the company at risk of paying penalties.

Recommendation

Step 4 of NIST is respond the company should considered a contingency plan in having a 2nd distribution center replication their network. infrastructure within a separate location. Although this is a costly option in the event that data has been compromised the 2nd distribution can be launched avoiding impact to business continuity.

Additional Considerations:

* Consider segregation of duties to minimize risk.
* Use the concept of least priviledged possibly by implementing role base access control.
* Consider complex password and implementation of 2FA (depth of defense)
* For better security implement regular change of passwords every 30 days.
* Impove on the accout management process once an employee has been terminated accesses should be rvokd imppediately otherwise there could be risk of data leakage and sabotage.
* There is no activity logs consider implemnting a SIEM such as splunk.
* There is outdated software which should be updated immediately.
* Wihin company firewall limit ports that are not used this will minimize the attack surface.
* IDS is implemented and functioning as required.
* There is no backups implemented causing impact if data is compromised the company would not be able to restore to a working state.
* Antivirus software is implemented and updated regularly.
* CCTV functioning as expected
* servers, switches, router and appliances are secured within its cabinets.
* Locks are in place on cabinets and entry to DC preventing unauthroized access. However consider using a badging system.
* Fire detection system implemented on all floors of the building.