ToyNest LTD: Scope, goals, and risk assessment report

Scope and goals of the audit

Scope

This audit covers the entire **security framework** of **ToyNest LTD**, including all company assets, internal networks, and IT systems. The review focuses on evaluating the company's assets, as well as the effectiveness of their current controls and compliance practices.

Goals

- Review and assess all company assets
- Complete a controls and compliance evaluation to identify areas for improving **ToyNest LTD**'s security posture.

Current Assets

The IT department manages the following resources:

- **On-site equipment** supporting office operations.
- **Employee devices:** desktops, laptops, smartphones, remote workstations, headsets, keyboards, mice, docking stations, surveillance cameras, and other peripherals.
- **Inventory for retail:** products available both in-store and online, stored in the adjacent warehouse.
- **Software and systems:** accounting, telecom, database management, cybersecurity tools, e-commerce platforms, and inventory systems.
- Internet connectivity and internal networking infrastructure.
- Data storage and retention solutions.
- **Legacy systems:** older technology requiring manual supervision and maintenance.

Risk Assessment

Overview of Risks

Asset management is currently insufficient, and **ToyNest LTD** lacks several key security controls. The company may not be fully compliant with relevant U.S. and international standards.

Control Recommendations

According to the **Identify** function of the NIST Cybersecurity Framework (CSF), the company should allocate resources to catalog and classify all assets. This enables proper risk management and helps determine the consequences of potential asset loss on business continuity.

Risk Score

The overall risk is rated **8 out of 10**, reflecting the absence of several essential controls and limited compliance with security best practices.

Additional Observations

The potential impact of asset loss is considered **moderate**, while regulatory and compliance risks are **high** due to insufficient controls. Key findings include:

- All employees currently have broad access to internal data, including potentially sensitive customer information.
- Customer credit card data is not encrypted during storage, processing, or transmission.
- Access control policies like least privilege and segregation of duties are not enforced.
- Measures are in place to maintain data integrity and availability.
- A firewall is operational with rule-based traffic filtering.
- Antivirus solutions are deployed and monitored regularly.
- No intrusion detection system (IDS) is currently in use.
- Disaster recovery plans are absent, and critical data lacks proper backups.
- Procedures exist for notifying EU customers within 72 hours of a data breach. Privacy policies and documentation standards are followed for data handling.
- Existing password policies are minimal and do not meet modern complexity standards (e.g., minimum 8 characters with letters, numbers, and special symbols).
- There is no centralized system enforcing password policies, occasionally impacting productivity during reset requests.

- Legacy systems are monitored, but maintenance schedules are irregular and procedures unclear.

- The physical premises, including the main office, retail store, and warehouse, are secured with locks, modern CCTV surveillance, and functional fire detection/prevention systems.