Security Audit Inc.

456 Harold St

Winterville NC, 28590

1/19/24

Joseph Johnson

Head of Cybersecurity Operations

Toy World Retailers

123 Manhattan Ave

New York NY, 1008

Subject: Network Security Audit and Recommendations

Dear Mr. Johnson,

We hope our message finds you well. Security Audit Inc has concluded our recently requested security audit of your company and its systems and are pleased to provide you with an update on our findings.

Our research within your company’s systems aimed to assess the effectiveness, safety, and security of these networks which you use for day-to-day operations, as well as transfer and storage of sensitive information. This survey covered several aspects regarding cybersecurity ranging from personnel access control, data protection and storage, incident or breach response, and of course actual network security.

Below you will find the key areas tested, as well as some specific weaknesses that we uncovered in regard to the protection of your network. Please review the listed recommendations and weaknesses and apply changes as you and your colleagues see fit.

**Scope of Survey:**

*General Network Security:*

Upon conclusion of the review of your active cyber security systems, it is apparent that your firewalls, detection systems and the like are up to date and very capable of defending and detecting against high level threats. There are likely no changes that are necessary to the software responsible for defense.

*User Access Control:*

The review of access pertaining to more sensitive data as it relates to who may be able to view boasted more concerning results. Most importantly, access privileges are not well defined as employees at the lowest level have access to information which is completely unnecessary to the performance of their duties such as sensitive customer data, supplier information, and company financial records. Additionally, the company has no multi factor authentication systems connected to any of the software used by employees, which would be incredibly troublesome should an account be breached. Finally, the employee database contains several accounts which are completely inactive. Whatever the reason for these dormant accounts, keeping them within the system is simply leaving another way for adversaries to access company data.

*Data and Threat Protection:*

Regarding data protection, this audit highlighted a few weaknesses related to the applied data classification system. This has caused employees to carry uncertainties in handling sensitive information. Employees are also poorly trained in the importance of protecting user data and techniques to ensure this is the case. The technology department of the company also lacks real time monitoring of user activities, which would prove to make the response to unauthorized access significantly more difficult. We also identified weaknesses in the encryption of company financial data.

*Incident Response:*

Our assessment determined that while the company incident response plan is strong, the department responsible for handling such a response is not well briefed on the plan in place to defend and manage such an event. Ultimately, your roles, communication protocol, and structure are well outlined in the plan.

Concluding this assessment, recommendations will be listed below sorted by priority.

**High Priority Recommendations:**

* Review permissions protocol for user access to data not related to performance of duties.
* Define what constitutes the need of privileges for different levels of access to different databases.
* Brief employees on procedure for incident response of breach of company information
* Develop policy to meet organization requirements for real time monitoring of employee activity within the scope of stored data.
* Implement a multi factor authentication system for all data related to company operation and records.
* Improve encryption for company financial transactions and data.

**Intermediate Priority Recommendations:**

* Provide training to non-technical employees on the importance of and methods pertaining to the protection of data used during their performance of duties.
* Develop and undergo a practice scenario for a data breach or other form of incident response.
* Test software defense systems such as firewalls against newer threats to ensure this protection is up to date.
* Inform employees about pier to pier initiated cyber-attacks such as phishing, inform employees on methods to spot these tactics and develop a plan for reporting and handling these threats.

**Low Priority Recommendations**

* Implement regular security awareness updates and reminders.
* Phase in the implementation of DLP solutions beginning with higher risk areas.
* Improve documentation of incidents, include future avoidance techniques and procedures to rectify similar incidents.
* Implement third party security reviews.
* Remove and/or delete old, inactive, or low usage user accounts to eliminate excess lanes for data breaches.

Summary of Recommendations:

Critical recommendations are advised to be promptly addressed, as these findings result in a very high risk for incidents which would result in a much higher cost than implementation of measures against them. Additionally, many of the risks found associated with company systems come from user incompetence, it is highly recommended that you reference user guides, such as the SANS Sec Awareness resource and develop training plans as soon as possible. While not urgent due to existing software, it is also recommended that improved encryption software is implemented such as Veritas, Ax Crypt, Symantec or any other software of your choosing.