Case Study:
Retail Manufacturer and Distributor

Through an in-depth Cybersecurity Assessment and implementation of resulting recommendations, NexusTek assisted a retail manufacturer and distributor to address multiple existing security vulnerabilities, greatly reducing their exposure to cybersecurity risk.

Overview

Location: Colorado

Company Size: 350+ employees

Type: Privately held

Industry: Retail Manufacturing and Distribution

Customer Profile:

Provides consumer goods programs and category solutions to their retail and wholesale partners, simplifying supply chain processes while elevating product quality.

Solution Benefits:

- Instituted policies and procedures that reduce risk of security incidents.
- Employee security awareness training to improve adherence to best practices.
- Revamped password practices to better control user access while promoting ease of use.
- Implemented 24x7x365 monitoring to immediately spot threats and issue alerts.
- Provide ongoing IT leadership for proactive security policy and procedure management.

Business Need

Over its 40 years of business, the company has expanded its offerings to meet the demands of its retailers and wholesalers, offering a diverse range of health, beauty, and wellness products, as well as eye wear, electronics, and general merchandise. Continuing their trajectory of expansion, the company made two acquisitions in 2018, has over 350 employees, four distribution centers, thousands of products, and works with numerous wholesalers and retailers across the United States.

Although their business success was vibrant, the company had experienced two security incidents that caused them to question the sufficiency of their cybersecurity program. They had implemented cybersecurity solutions in recognition of the importance of protecting their business from cyber threats, but in spite of their efforts, they suffered two separate data breaches that stemmed from two different root causes. This led the company to request NexusTek's assistance to strengthen their security posture.

Solution

To gain an in-depth understanding of their current cybersecurity posture, NexusTek's Virtual CIO (vCIO) completed a Cybersecurity Assessment using both on-site and remote observation of the company's infrastructure and processes. The assessment—based on the NIST framework—used a comprehensive, multi-method approach that combined information from diverse sources, including:

- Interviews of key personnel to understand the people, processes, and technologies that support their needs
- Documentation review to evaluate current IT policies and practices
- Automated scanning to identify existing vulnerabilities
- On-site assessments via walk-through of the company's IT environments
- Use of network discovery tools to identify any security and patch issues, sensitive data, etc.

After completing this in-depth assessment, NexusTek's vCIO created a thorough report to summarize the findings of the evaluation and to present recommendations for cybersecurity solutions to address each identified area of risk. This allowed the company to understand the collection of vulnerabilities that together impacted their security risk.

In a cumulative sense, the findings of the cybersecurity assessment indicated that the company experienced a substantially high level of cybersecurity risk. Although they had made efforts to implement a security program independently, they had focused exclusively on technology-based cybersecurity solutions, leaving key nontechnical security fundamentals unaddressed.

Results

Using the vCIO's Cybersecurity Assessment report as a guide, the company began implementing technical and nontechnical security practices and solutions to strengthen their cybersecurity posture:

- **Technology Leadership:** Recognizing the need for an executive-level technology leader as a consistent member of their team, the company added a NexusTek vCIO for 16 hours each month. This provides them with expert IT leadership that allows them to implement IT best practices and address any potential security issues proactively rather than reactively.
- **Formal Cybersecurity Program:** One of the most critical findings of the assessment was the lack of a formal cybersecurity program, which left the company in a vulnerable position. To address this gap in their security, they worked with the vCIO to develop formal policies and procedures related to IT security, to provide regular training to employees regarding security practices, and to put in place routine processes to assess IT health and security risk. The importance of routine security awareness training was underscored by the vCIO's finding that their employees' credentials were on the dark web. This was most likely the result of those employees falling for phishing scams, an ever-present cyber threat that security awareness training addresses.
- **24x7x365 Monitoring & Alerting:** At the time of the assessment, the company had various security solutions (e.g., antivirus, network monitoring), but they had siloed views into each of them. With limited visibility and no event data aggregation, emerging threat activity would be difficult to identify using their existing solutions as configured. Recognizing the difficulty of managing 24x7x365 monitoring and alerting in-house, they chose to partner with NexusTek for managed cybersecurity. This gives them the assurance that their full network, from endpoint to endpoint, is being monitored constantly, and that they will be alerted immediately if threat activity is detected.
- **Password Practices:** They had taken steps to implement password practices that align with zero trust, adopting a password-less approach. The unexpected outcome, however, was that they had overlooked the implementation of password best practices in Active Directory. Complicating the situation further, some employees struggled to access their accounts. At the vCIO's recommendation, they replaced the challenging password-less system with multifactor authentication (MFA), also instituting best password practices such as requiring passwords change every 90 days, enabling screen lockout time instructions, and enabling account lockout after a designated number of attempted logins.

- **Software Development Life Cycle (SDLC) Practices:** The company's in-house IT staff develop custom coding, but the security assessment revealed that the company did not have formal secure coding practices in place. Their developers were not receiving training on top vulnerabilities, nor did they complete vulnerability scanning to check their custom code. Because this could potentially result in vulnerabilities in their code that threat actors could exploit, the company accepted the recommendation to adopt a formal SDLC security process, which NexusTek's vCIO developed on their behalf.
- **Systems Hardening:** NexusTek's vCIO also found that they did not have hardening standards for technology assets, which could lead to misconfigurations and unaddressed vulnerabilities. To address this gap in their security program, the company implemented a formal system hardening standard to ensure all devices are properly secured before use, which was developed on their behalf by NexusTek's vCIO.
- **IT Security Policy:** Another finding of the assessment was that the company had scant IT policy. As a nontechnical security practice that guides and limits employee behavior related to technology, thorough IT and IT security policies are a crucial piece of a comprehensive cybersecurity program. At the company's request, NexusTek's vCIO wrote policies for both acceptable use of technology and change management. With an acceptable use policy, employees are given clear instructions on allowed uses of technology along with prohibited uses. A change management policy now guides the company's IT practices, ensuring that any changes that are made to any of the IT systems are communicated to all parties with a need to know. This not only creates a more orderly and coordinated approach to IT changes, but also ensures that any IT changes that may inadvertently impact security are identified and addressed quickly.

By augmenting their cybersecurity program with these technology-based solutions and nontechnical practices, the company has moved from a high level of risk to a drastically lower level of risk. With the recognition that cybersecurity is dynamic, this retail manufacturer and distributor is now equipped with both the solutions and the ongoing technology leadership to manage their cybersecurity risk capably into the future.