Case Study: A National Construction Company

NexusTek helped this customer to strengthen their cyber defenses against an escalating threat landscape in the construction industry, while keeping their IT infrastructure running smoothly and reliably.

Overview

Location: U.S. Mountain West Region

Company Size: 220+ employees

Type: Privately Held

Industry: Construction

Customer Profile:

This customer is recognized as a leading producer of high-quality architectural and structural precast concrete structures in the U.S., with an in-house design group and multiple production facilities that allow them to serve construction customers several states.

Solution Benefits:

- Protects network against unauthorized user access
- Safeguards data backups from ransomware attacks and disasters
- Improves security posture to better satisfy cyber insurance criteria
- Keeps IT infrastructure running reliably
- Provides a single partner for cybersecurity and managed IT services

Business Need

As a producer of precast concrete building components, the customer maintains a repository of sensitive data, such as intellectual property, architectural designs, and other customer data. As ransomware attacks surged in frequency in the construction industry, the customer recognized the urgent need to strengthen their cybersecurity defenses and protect their data. The customer was also interested in reducing their cyber insurance premiums, and they understood that improving their cybersecurity program could make this possible.

Without cybersecurity expertise internally, the company could not identify where their cybersecurity vulnerabilities lay, and without this understanding, they could not choose cybersecurity solutions that would resolve those vulnerabilities. The customer needed an expert assessment of their security posture to identify gaps in their cybersecurity, and they needed recommendations for appropriate solutions to close those gaps.

Solution

Having partnered with NexusTek for managed IT services for over 15 years, the customer turned to NexusTek for an assessment of their cybersecurity posture. NexusTek's cybersecurity expert conducted a thorough assessment of the customer's proactive and reactive strategies, providing a report with recommendations for solutions to strengthen their defenses. The assessment revealed a need for stronger defenses around user sign-in, as their existing single-factor authentication system left them vulnerable to bad actors who might attempt to hack an employee's account. To address this weakness, The customer chose to implement multi-factor authentication (MFA), which NexusTek deployed for all users.

In terms of data protection, the customer's existing backup solution needed strengthening, as they were only maintaining backups onsite, and lacked offsite backups. To resolve this vulnerability, NexusTek deployed a Datto backup solution that included offsite backups that are not accessible via the company's primary network. Furthermore, two standalone systems were discovered at one of the customer's locations that had not been included in their backups; NexusTek incorporated these systems' data into the customer's new backup system.

Results

By adopting MFA, the customer has drastically reduced the likelihood of unauthorized sign-ins on employee accounts. In addition to their usual credentials, the customer's users now also need to supply a third source of verification, such as a numerical code sent to their cell phone. This third form of verification blocks hackers who try to log in using stolen credentials or password spraying.

MFA strengthens the customer's defenses against ransomware attacks and other forms of cybercrime that start with compromise of an employee's account. By keeping threat actors out of their own network, they also protect against hackers who may try to leverage a compromised employee account to launch an attack on one of the customer's customers or vendors. And with customers in heavily targeted industries like healthcare, government, and education, the customer's adoption of MFA creates an important layer of protection against unauthorized login.

By implementing the Datto backup solution, the customer has greatly reduced their risk of losing data such as production specifications, engineering and design documents, and customer information. While their previous backup system maintained all backups on the customer premises, their new backup system stores a set of backups at an offsite location that is unconnected to their primary network. These "air-gapped" backups are an important safeguard against ransomware attacks, because threat actors often locate and encrypt backups before unveiling their attack to their victim.

Storing a set of backups offsite prevents threat actors from encrypting or destroying them, and it also provides an extra layer of protection in the event of disaster. Disasters may destroy data or make it temporarily inaccessible, but even temporary loss of access to design or product data could result in significant financial loss due to production downtime. Having reliable access to their data, even during crisis events, allows the customer to produce concrete structures as contracted, and provide reliable service to construction customers in the worst of circumstances.

Because MFA and offsite backups are regarded as essential safeguards by most cyber insurance companies, The customer's newly strengthened cyber posture demonstrated a higher level of compliance with cyber insurance criteria. By strengthening their cybersecurity and cyber resilience, they were able to secure lower premiums for their cyber insurance policy. This means that the customer now has a thorough cybersecurity program, including proactive safeguards to reduce risk, reactive measures to mitigate risk, and liability coverage as a final safeguard should they fall victim to an attack.

NexusTek continues to provide the customer with Complete Managed IT Services, providing the company with a single partner for managing its IT infrastructure and cybersecurity. The customer has relied on NexusTek for over 15 years to handle proactive IT tasks such as network monitoring and patch management, as well as for urgent issues that require help desk or dedicated engineer support. As their IT needs changed in relation to an escalating threat landscape, The customer was able to turn to a familiar source of support to strengthen their cybersecurity. With their cyber solutions integrated seamlessly into their existing service package, the customer is prepared to move forward confidently as a top producer of precast concrete structures.

This case study was prepared with the customer's full knowledge and involvement. To respect the customer's privacy, we have omitted their name, logo, and any other identifying information.