CYBERSECURITY: JOB ONE FOR DISTRIBUTORS

As data security risks continue to multiply, distributors need to reconsider the role security plays in their organizations.

November 20th, 2019 • Industry Today • Todd Endsley

There's growing evidence that distributors need to make cybersecurity a top priority in 2020. In 2018, 1,244 data breaches exposed more than 446 million records in the U.S. And in 2019, the number of data breaches affecting U.S. businesses increased 50% over the previous four years.

As we get ready to enter a new calendar year, decision-makers across the distribution industry are focused on strategies designed to achieve operational improvement. But distributors that ignore the security of data and systems do so at their own peril — a single data breach can cripple your operation and jeopardize your relationship with partners across the supply chain and also have legal implications.

More than ever before, it's critical to not only understand the cybersecurity risks that threaten your operation, but to develop an achievable strategy that protects your data ecosystem from intrusion and theft.

No business is immune from cyber threats

The recent data breach at Network Solutions, one of the biggest domain registrars in the business, shows that not even internet-savvy companies are immune from the risk of cyberattacks. With major cyber security incidents making headlines on a near-weekly basis, it's clear that no industry or business is safe — including distributors.

But it's important to recognize that data breaches can occur in a variety of ways. In addition to brute force attacks, smaller threats like malware or phishing can jeopardize data and systems. With a single click, an employee can unleash a cyberattack on your organization.

In the 1990s, most companies prioritized the features and functions of their offerings first, followed by operational concerns like stability and scalability. Security considerations entered into the equation much farther down the line.

However, IBM and other large technology enterprises bucked the trend and moved security to the top of the list. Their rationale was that without security, you can't achieve stability or scalability. Essentially, they flipped the order of priorities because they recognized that security is table stakes for business success.

By recognizing the urgency of security concerns, IBM and others developed a "security-by-design" approach — a strategy that can pay big dividends for distributors in today’s industry environment.

“Security by design” for distributors

A security-by-design approach recognizes that cybersecurity is a primary operational requirement for distributors. Rather than considering security after function, scalability, or other concerns, forward-thinking distributors are adapting to the current technology climate by making security a top priority.

Although security by design can involve a complex range of security elements, several basic considerations lay the groundwork for a robust strategy to mitigate the risks posed by the threat of data breaches and cyberattacks.

1. Identify and target areas of exposure. The cloud provides a cost-effective path to security by design. But your cloud partner should help identify and address specific areas of exposure. For example, does your website accept credit card payments? If so, you need to protect customer data by making a secure mandated system a first-level priority when receiving payments online. It’s not reasonable for most distributors to staff these capabilities in-house, so look to your cloud partner to provide intrusion and detection features as well as other capabilities that deliver an extra layer of security.

2. Implement industry-specific data storage practices. Industry-specific requirements present additional data security hurdles for distributors. For example, data storage regulations for medical supplies are very different from the data storage regulations in food distribution. Cloud technology can streamline compliance with data storage regulations, but you need to make sure your cloud-based solution meets the baseline security requirements for the verticals in which you operate.

3. Maintain multiple data back-ups. Back-ups protect data in the event of a breach. Multiple data back-ups located in multiple geographies ensure the continued integrity of customer data and enable recovery from security events. Given the value of data to your company and customers, it’s essential to prioritize redundancy in data storage as part of your operation’s security-by-design strategy.

Robust security standards and a security-by-design approach allow distributors to maintain operational continuity in the face of growing security risks. By remedying the vulnerabilities of on-premise technology and single data back-ups, cloud technology eliminates single points of failure and provides an assurance of seamless operations.

But more importantly, security by design equips your operation with the tools and resources to prevent cyberattacks and data breaches from occurring in the first place. With the help of the cloud and the reprioritization of security considerations, you can flip the narrative and reap the benefits of a more secure, more stable operating environment.