It's cybersecurity awareness month—is your retail business safe?

Cybersecurity Awareness Month is the perfect time to audit your current cybersecurity tech stack and processes, especially for retail businesses and startups.

It's Cybersecurity Awareness Month, which means there's no better time than now to audit your cybersecurity practices within your retail business. Retail cybersecurity is more important than ever, considering that credit card data has made the retail industry a prime target for cybercriminals. The attack playing ground of the sector is growing as merchants of all sizes attempt to increase sales and raise productivity by utilizing cutting-edge data-driven solutions. The utilization of big data and complex data warehouse models is expanding quickly.

Additionally, a lot of merchants are entering the pharmaceutical and healthcare industries, and as a result, they are storing more sensitive data than ever. In the meanwhile, emerging nations are steadily moving away from cash payments in favor of electronic card payments. As a result, retail cybersecurity must be at the forefront of business owners' focus.

In this article, we'll break down the state of cybersecurity in the retail world, as well as some cybersecurity trends and recommendations that are relevant and helpful.

cognizant®

Stats you need to know about retail cybersecurity

With a 264% yearly increase in ransomware assaults on e-commerce and online retail enterprises, cybercriminals have targeted the retail industry in 2021– and that number is only growing in 2022. According to data from SonicWall's biannual study, there will be more than 625 million digital assaults in 2021, more than twice as many as there were in the previous year, signaling an increase in cyberattacks and IT security risks over the previous year. In 2021, there were a record 97.1 million crypto-jacking assaults, a 33% rise in the retail industry. Ransomware, encrypted attacks, and IoT malware are just a few examples of destructive digital assaults that have been steadily rising.

According to the SonicWall analysis, supply chains are frequently targeted by ransomware attacks, which result in extensive system outages, financial loss, and reputational harm. UK-based ransomware assaultsoverall climbed by 227%, with one out of every five assaults being directed at an online retail company.

What is the state of retail today?

The pandemic's increase in e-commerce investments and online customers has made online shopping a more alluring target for would-be hackers. In recent years, malicious insiders, careless employees, and improperly installed or susceptible software across networks, endpoints, and POS devices have increased the corporate attack surface. The epidemic has aided in the transition of retail companies' back offices from POS terminals. It has, however, also exposed retail operations to new cybersecurity concerns, which might have a significant negative effect on specific businesses and the retail industry as a whole.

POS has always been the main target for data-hungry hackers. More criminal behavior is occurring online as a result of the widespread use of EMV cards, which can't be duplicated as readily as stolen POS data can, and new payment methods like Apple Pay.

What is the solution to the growing retail cybersecurity threat?

With an additional layer of protection provided by edge computing, assaults are less likely to occur and cause as much harm. Its zero-trust security paradigm enables consumers' quick and agile activities.

There are even more excellent recommendations out there for amping up your retail cybersecurity processes. Start by making sure staff members are aware of recommended practices for online safety. Staff members may either be a company's weakest link or its first line of defense when it comes to online safety. Employees who lack training and preparation are unable to consistently recognize and prevent cyber dangers. Retail companies may encourage staff to adopt a cyber-secure mentality and advance information security efforts rather than stifling them by implementing risk-based security awareness training programs.

Additionally, you have to use multi-factor authentication. The EMV payment system, which utilizes credit and debit cards with integrated chips and requires a PIN or signature to complete the transaction, has been adopted by the majority of US shops. However, online shops are unable to make use of the extra security measures offered by those kinds of cards. It's imperative that they utilize solutions for multi-factor authentication (a.k.a. MFA).

Last but not least, it's critical to audit and regularly monitor your systems. Fraudsters are adopting new strategies to get personal information during online card-not-present purchases as chip cards and MFA considerations aid to reduce data breaches at a point of sale. Look for harmful codes on your website. Check your POS terminals and networks as well. Key cyber security best practices include frequently evaluating self-checkout payment terminals with low staffing levels. This procedure assists in preventing the attachment of skimmers intended to collect private customer data, such as PIN numbers or account information.

About Cognizant Cybersecurity

Eliminate security blind spots and accelerate innovation, transformation and growth.

Outdated security solutions. Sophisticated cyberthreats. Increasing compliance requirements. Faced with these and other security challenges, today's companies need a proactive partner who can anticipate and neutralize threats before they materialize.

At Cognizant, we approach security as the starting point for delivering the outcomes that leading global organizations demand. Our end-to-end security solutions combine deep domain and industry expertise with a future-focused approach that encompasses advisory, transformation and managed services. We offer the foresight and expertise to solve your most complex challenges.

By providing a 360-degree view of your organization's security ecosystem, Cognizant can identify and eliminate today's blind spots—while also seeing and solving for the threats ahead—so you can accelerate business innovation, transformation and growth.

Have questions about today's most daunting security challenges? Cognizant is here to help. Reach out to our experts today.

cognizant®

World Headquarters
300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters
1 Kingdom Street
Paddington Central
London W2 6BD England
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102

India Operations Headquarters
#5/535 Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060

APAC Headquarters
1 Changi Business Park Crescent
Plaza 8@CBP # 07-04/05/06
Tower A, Singapore 486025
Phone: + 65 6812 4051
Fax: + 65 6324 4051