Security is imperative in the future digital retail world

Why cybersecurity is a critical component of Enterprise Intelligence

verizon

From SmartBrief

Retailers are forever evolving to improve the customer journey. Technology has made the industry more connected than ever, blurring the lines between channels, but these advancements have also opened retailers up to cyberthreats. Working to protect customer and company information has become imperative to maintain customer trust and loyalty.

This paper will explore the primary cybersecurity challenges facing companies in the retail sector and examine technology solutions that help identify vulnerabilities and mitigate threats. Forward-thinking leaders are embracing digital innovation and changing the way they think of cybersecurity, shifting from a cost center to a tool that empowers the growth of their business.

Retail organizations that prioritize digital innovation to build smarter, more efficient and more agile enterprises will secure their future successes. Transformation starts by bringing together disconnected systems to create powerful, modular and intelligent solutions that can enable new functionality, thoughtful insights and faster decision-making. The result is Enterprise Intelligence.

Enterprise Intelligence is the result of setting aside old ways of working and using technology to capture an end-to-end vision of your organization as it operates. It means using your network to provide a secure platform for the latest technologies and partner solutions – including artificial intelligence, machine learning, IoT and more.

This enhanced digital customer journey, with incredible amounts of data to manage, creates additional risks of cybersecurity threats making it paramount that enterprises act to protect consumer credentials, payment data and company resources.

Security risks are significant

In recent years, data has become the most sought-after resource for companies and cybercriminals alike. In 2022, 629 retail security incidents were analyzed in Verizon's Data Breach Investigations Report (DBIR), with 241 breaches of confirmed data disclosure.[8]

Retailers must prepare for what's looming as new threats are always on the horizon. System intrusion, social engineering and basic web application attacks have increased at an alarming rate with the leading means being stolen credentials, phishing and ransomware.[8]

Some of the most significant cybersecurity vulnerabilities retailers face are:

- Compromised credentials, accounting for 45% of all breaches reported in 2022,[5] dominate both social engineering and basic web application attacks. The majority of web app attacks involve stolen credentials, underlining the importance of password safeguards.
- Ransomware attacks are on the rise and now consist of more complex breaches that occur on multiple fronts. In fact, ransomware attacks on retail increased by 67% year-over-year in 2022.[2]

67%

ransomware attacks on retail increased by 67% year-over-year in 2022.[2]

- PCI DSS v4.0 compliance, which helps to ensure that all companies that accept, transmit or store credit card information maintain a secure environment. Fines for noncompliance can range from $5,000 to $100,000 per month for the merchant.[1] The first deadline for compliance is March 31, 2024.

Retail organizations need to both identify and address their vulnerabilities as they move toward building an infrastructure that supports the needs of today. Cybersecurity must be their first concern when adapting.

Consequences of falling short

Failing to protect data can bring significant consequences to retailers, including loss of customer confidence and loyalty, tarnished brand reputation and financial impacts from ransomware and class action lawsuits from data breaches.

The motive for most hackers is money, stealing personal information because it is easiest to monetize. Ransom payments for the reacquisition of stolen data can be costly for retail organizations, with the average cost of a retail breach totaling more than $3.28 million in 2022.[5]

For retailers, a breach goes beyond just the financial consequences. The negative impact on an organization's customer relations can be severe. On average, 78% of consumers say a company's ability to keep their data private and secure is "extremely important," with the majority of consumers saying they will not buy a product from a company if they do not trust that company to protect their data.[6]

Top cybersecurity innovations

These incidents highlight one vital thing: the importance of safeguarding data at all costs. The consequences of waiting until a breach occurs are far too high.

To address today's cybersecurity challenges, retailers should invest in cutting-edge technologies that work to protect their data.

Cybersecurity technologies

- **Private networks**. 5G and private networks offer high speeds and low latency with the bandwidth to support advanced encryption and continuous monitoring for intrusion detection and response.
- **Zero-trust frameworks** verify every person and device every time, regardless of where they originate or whether they are already behind the corporate firewall.
- **Network detection and response.** Network monitoring and threat detection capabilities help shorten the time to detection, enable real-time response to threats, improve the ability to mitigate breaches, lessen the impact of breaches, and decrease or eliminate General Data Protection Regulation/California Consumer Privacy Act (GDPR/CCPA) compliance penalties.
- **IoT security and mobile device security,** such as credentialing, that mitigate the possibility of devices being used by hackers as an access point.
- **AI/ML.** Artificial intelligence is increasingly being used in cyber programs to identify vulnerabilities and threats, predict attacks on data and provide alerts and recommendations for response. Machine learning automates threat detection, which allows investigation and response efforts to start faster than ever before.
- **DDoS mitigation solutions** can help lift the burden of managing breaches off internal IT teams. These systems, along with the embedded security of private networks, provide them the ability to help combat large volume attacks quicker and deliver the intelligence to help distinguish good traffic from bad.

Getting started

Retail businesses that want to tighten cybersecurity and make the most of the rich data and smart technologies available to them can begin with a few simple steps:

- Begin with a complete security program evaluation.
- Follow up with a workshop or consultation to assess current programs and tech stacks for vulnerabilities.
- Partner with a reliable solutions expert to build a roadmap for streamlining the security portfolio and programs.
- Protect investments by working with a managed services provider whose expertise can include anything from consultations to private networks to fully managed security services.

Retailers are working to better respond to customer needs, creating not only digitally advanced stores but also smart digital shopping experiences. Those that make cybersecurity a priority and embrace Enterprise Intelligence can create a more innovative environment in store and online by making intelligent decisions that are contextual, consistent and guided by clearly articulated business objectives. And having a real-time view across every access point in the network ensures retailers are better prepared to respond to unexpected challenges while bringing new opportunities to their customers.

Learn more at verizon.com

References

1. https://www.pcicomplianceguide.org/how-can-your-pci-compliance-efforts-ultimately-save-your-business-money/
2. https://marketscale.com/industries/software-and-technology/why-are-ransomware-attacks-on-retail-so-common/
3. https://www.grocerydive.com/news/ahold-delhaize-usa-pulls-back-the-curtain-on-data/641086/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202023-01-26%20Grocery%20Dive%20%5Bissue:47602%5D&utm_term=Grocery%20Dive
4. https://www.ibm.com/reports/data-breach
5. https://securityintelligence.com/articles/cost-data-breach-retail-costs-risks-prevention/
6. https://www.prnewswire.com/news-releases/new-survey-finds-deep-consumer-anxiety-over-data-privacy-and-security-300630067.html
7. https://www.verizon.com/about/sites/default/files/Verizon-Business-Third-Annual-State-of-Small-Business-Report-2022.pdf
8. https://www.verizon.com/business/resources/reports/dbir/2022/retail-data-breaches-security/
9. https://www.verizon.com/business/resources/T244/reports/2022-payment-security-report.pdf

verizon

From SmartBrief