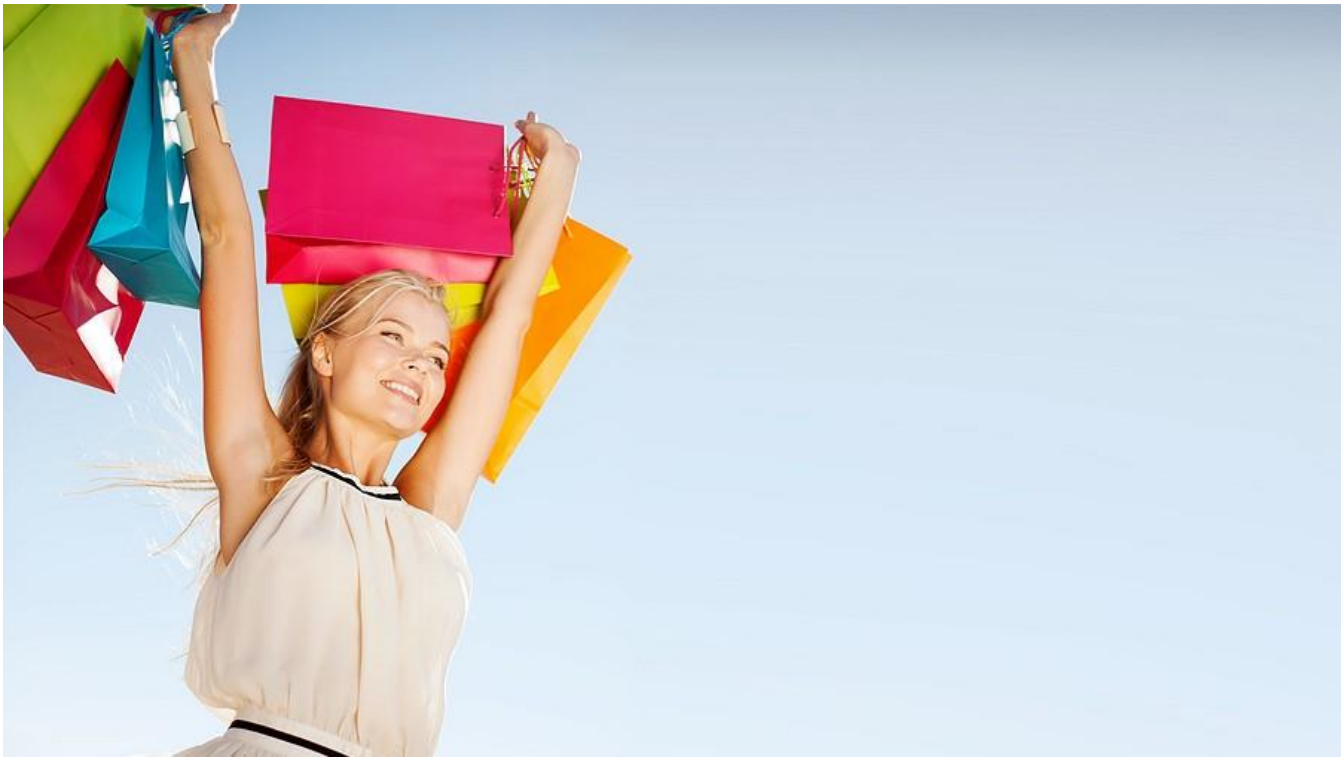
How to Battle Retail Cyber Security Threats and Win



When a retailer experiences a cyber breach, millions of customers feel the pain. Consider the 10 million individuals victimized when threat actors successfully infiltrated fashion retailer JD Sports. A breach of Walmart subsidiary Bonobos affected another 7 million. A combination of factors makes retail cyber security threats a top business concern.

To begin with, retailers hold a vast quantity of valuable data, from credit card information to sensitive personal details. The information allows retailers to personalize their marketing efforts, and it makes shopping easier for customers. But that insight and convenience comes with associated risk.

The rise of omnichannel retailing opens additional risk avenues by widening the attack surface. Threat actors look for vulnerabilities in websites, IoT devices, and POS systems. They exploit weaknesses in the supply chain to gain access to high-value targets. And they use phishing to target a revolving and sometimes poorly trained workforce.

Businesses that invest in solutions to protect against the top retail cyber security threats position themselves for a safer and more prosperous 2024.

Ransomware Still a Top Threat

According to a report by Corvus Insurance, ransomware attacks increased by 95 percent in 2023. Ransomware can affect everything from e-commerce platforms to POS systems, customer databases, and inventory management systems.

Technology advancements such as AI and ransomware-as-a-service have made it easier for threat actors to carry out successful attacks. Fortunately, advancements in cyber security solutions provide a powerful defense.

To prevent ransomware attacks and minimize the damage they cause, retailers need to strengthen endpoint protection and email fortifications. Geo blocking will help prevent foreign hackers from accessing business systems. Additionally, retailers should assess and improve their data backup and recovery practices.

E-commerce Threats Require Multi-faceted Approach

E-commerce threats can take a variety of forms in addition to ransomware. For instance, hackers hijack customer accounts to steal sensitive personal data, and they impersonate legitimate companies with fake online stores. Threat actors also infiltrate the systems used to manage gift cards or process returns online.

Protecting against e-commerce attacks requires a multi-faceted approach, beginning with multi-factor authentication and strong password policies. Timely patch management for all systems also helps to close vulnerabilities that hackers can exploit. And improved security awareness training for employees will educate them about social engineering techniques.

Protecting against brand impersonation proves particularly tricky. DMARC for email validation makes an essential starting point, but it will not solve the problem on its own. Regular monitoring with Google Alerts will help detect impersonators. Businesses should also collaborate with platforms such as social media to report intellectual property violations.

Data Skimming Prevalent Online and on POS Systems

Hackers use data skimming to steal credit card information when customers make online or in-store purchases. To implement data skimming, they install malicious code on websites and apps or attach physical devices to card readers.

To protect credit card data, retailers should implement firewalls to control traffic between the POS network and external networks. They should also inspect card readers regularly for tampering and quickly install the latest security patches to keep hackers from exploiting known vulnerabilities. And they should ensure data encryption both in transit and at rest.

Access Management Critical to Address Supply Chain Attacks

In a supply chain attack, threat actors infiltrate a third-party vendor that provides services to the retail business. Because small vendor companies may have weak security but also insider access to the retailer, they offer a valuable back door for attackers to reach their main target. And because the attacks target an outside system, they can prove difficult to detect.

To guard against supply chain attacks, retailers must strengthen access management. Zero trust architecture, for instance, requires identity verification every time any user, device, or application attempts to access the system. Additionally, privileged access management will provide visibility into the actions taken by privileged accounts that hackers may target.

Mitigate Retail Cyber Security Threats with Comprehensive Solution

Retail businesses present a tantalizing target for threat actors. However, with cyber security solutions specifically designed for the retail sector, business owners gain the confidence they need.

eMazzanti Technologies has provided technology solutions, including comprehensive cyber security, for retailers for over 20 years. Take steps now to enhance productivity and support safe and speedy transactions.