Retail: Avoiding A Nightmare Before Christmas

Cybersecurity Series

By James Hughes, Chief Technology Officer for EMEA Retail, Verizon Business

The pandemic accelerated digital transformation in retail. With stay-at-home orders in place, consumers who were already accustomed to e-commerce expanded the products they purchased online, and those unfamiliar with online purchasing were compelled to start buying goods online. Retailers responded by digitizing their operations, and in one sense, the forced digital transformation was a silver lining of the lockdown.

However, if they weren't prepared, that digitalization presented new risks which in turn has been compounded by the explosion of new loyalty programs, gamification, augmented reality try on and other engagement and experiential capabilities deployed increasingly post pandemic. Linking the digital world and online channels to physical stores and pop-ups with gamified experiences is a growing trend and possibly introduces even more potential threats and risks.

Retailers should button up their cybersecurity as they head into the holiday season, since increased activity will potentially mean increased exposure. After surveying the retail cybersecurity landscape in its authoritative 2023 Data Breach Investigations Report (DBIR), Verizon has identified some of the biggest cybersecurity threats to retail. Here they are summarized below.

Scrooged: How compromised credentials can escalate

The challenge

Compromised credentials account for almost half (45%) of all breaches and are often used to carry out additional attacks. Other patterns, such as pretexting, a form of social engineering in which a threat actor pretends to be a trusted individual or institution, can be used in conjunction with stolen credentials to engage in more malicious activities, like introducing malware into a network or stealing more other sensitive information. In other words, compromised credentials can be a gateway to more expansive hacks.

The challenge for retail, more than most other industries, is people. The human element factors in almost three-quarters (74%) of all breaches, including compromised credentials and social engineering. The fact that retail contends with labor shortage, high rate of employee turnover, and a workforce that isn't digitally well-versed can leave retailers vulnerable to phishing and smishing. The holiday season only amplifies this vulnerability.

The potential solution

The good news for retailers is that even though compromised credentials and social engineering are widespread, they are often lo-tech attacks. As such, training can go a long way toward defending against them. Teaching staff how to spot and avoid common phishing, smishing, pretexting and other social engineering attacks can help prevent the majority of human-error–related breaches. Technologies like AR and VR can even be used for remote video training, which can be especially effective with temporary and seasonal workers.

Taking a zero-trust approach to cybersecurity, whereby all users are authenticated, authorized and continuously validated, can also be very effective. This model acknowledges the reality that security threats can come from anywhere, including from unsuspecting users from within an organization. A "never trust, always verify" approach also applies to applications and infrastructure. Being disciplined about authentication can plug system holes, while training can minimize personnel exposure.

The Grinch: Ransomware can be very expensive

The challenge

A single breach can have a major impact on a retail business, both financially and in terms of reputation. One of the costliest action types is ransomware. The median cost per ransomware more than doubled over the past two years to $26,000, with 95% of incidents that experienced a loss netting hackers as much as $2.25 million. Ransomware accounts for almost a quarter (24%) of all action types.

The potential solution

Considering social engineering, including pretexting, which nearly doubled year over year, is commonly used to introduce ransomware to a network, the training mentioned in the previous section can be useful in helping employees identify common tactics used to employ ransomware.

Investing in threat detection and response solutions is also critical. These solutions, which can help enable organizations to identify, prioritize and mitigate risks across environments and endpoints, can help prevent these kinds of attacks. Response solutions can be effective not only in thwarting ransomware attacks but also containing threats and preventing further exposure across an organization.

It’s A Wonderful Life: Keeping up with the latest regulatory compliance is critical

The challenge

Payment data theft is increasing dramatically across retail, accounting for 37% of breaches this year. Most of these breaches (70%) originate from web applications.

The potential solution

This underlines the need for PCI 4.0 compliance as soon as possible. As hackers become more sophisticated, adhering to the latest global technical and operational standards will be instrumental in helping to protect account data moving forward.

The holiday season magnifies retail’s existing challenges

The post-lockdown retail environment comes with new challenges, including an unpredictable supply chain and skittish consumers. The holiday season only exacerbates these challenges.

The opportunities for retailers are great during the holiday season, but so are the potential cybersecurity risks. It’s a golden opportunity for threat actors to take advantage of the shuffle of seasonal employees, decrease in IT staff levels, and extended server vulnerabilities. If those retailers that digitized in recent years have not put a proportionate cybersecurity plan in place, they’ll be that much more vulnerable this time of year. Just as retailers must be strategic and proactive about their inventory management heading into the holiday season, they must be proactive about protecting their organizations and their customers. Holiday season isn’t just a boon for retailers. It’s a spotlight. A data breach not only represents a greater financial risk during the holiday season. It also represents a great reputational risk. Investing in cybersecurity isn’t just smart. It’s necessary.