The Ups and Downs of Data Breaches in Retail

Cybersecurity Series

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

For many, the holiday season represents the "most wonderful time of the year," but for retailers and online merchants, it can be the most challenging time of the year. Managing inventory, supply chain and staffing in the face of surging consumer demand is a tall order. Complicating the already-monumental task is the accompanying spike of hacker activity. An increase in online transactions can translate to more opportunities for threat actors. At a time when retailers should be their most vigilant, their attention is pulled in many different directions. If they haven't already, now is the time for retailers to fine-tune their cybersecurity preparedness. Here are some of the biggest cyber threats for retailers and how they can plan for them.

PCI data theft down, but stolen credentials up

Historically, payment card information has been a chief target for threat actors attacking retailers, but this year's Data Breach Investigations Report (DBIR) revealed a marked drop in this data category, with only a quarter of breaches resulting in PCI data theft (down from 37% last year). This development is surprising given the short-term fraud opportunities that payment cards present. Though it's not immediately apparent what accounts for this year-over-year drop, it may have something to do with PCI 4.0, which became mandatory in April 2024. Organizations working toward compliance have likely tightened their payment processing standards ahead of this year's deadline. Whatever the reason may be, organizations mustn't become complacent, as a year-over-year drop could be a statistical anomaly that does not hold up in 2025.

While compromised PCI data is down, the incidence of stolen credentials is rising. Last year, stolen credentials made up 35% of the data compromised; this year, that number climbed to 38%. Might the steady rise of stolen credentials also have had an impact on the drop of PCI theft? Are credentials simply easier to steal? Time will tell, but it's important to note that stolen credentials can be more damaging, as they may lead to additional data breaches.

Phishing is down, but pretexting is up

Pretexting supplanted phishing as the top social action, which may be a function of growing awareness of cybersecurity best practices. Phishing depends on lapses in judgment, vigilance or knowledge, as do several social engineering tactics.

verizon business

As such, educating one's workforce on common phishing tactics, for instance, and running simulations to test their awareness can go a long way toward defending against phishing and other social engineering attacks. The reduction in phishing may be one benefit of this rising awareness.

As we at Verizon Business have pointed out in recent years, most threat actors aren't as they're portrayed in fiction: criminal masterminds who utilize the most cutting-edge technologies. They tend to seek out the easiest payday, which is why a simple, straightforward tactic like phishing has been the hacker's go-to for years. If you limit access to the path of least resistance, however, they'll likely explore other avenues, which may begin to explain why pretexting, a more involved social engineering tactic, is up. Pretexting is a key component of business email compromise (BEC) attacks, which can be very costly for an organization, as it can involve high-level executives who often have access to a company's most sensitive information.

Applying those insights

Don't be complacent about cybersecurity training

As mentioned above, an educated workforce can be an effective risk mitigator, but the fact that phishing is down does not mean that it will stay down. It's important to maintain that cybersecurity standard moving forward. In fact, training may need to become more sophisticated to be able to identify more sophisticated pretexting attacks. Smarter solutions may also need to be employed at scale to thwart pretexting attacks.

Maintaining PCI 4.0 compliance

This past April deadline was just the first phase of PCI 4.0. The second phase will prove a more challenging set of requirements to meet. The decrease in PCI data theft is a positive development, but, like with phishing, just because it's down this year doesn't mean it will necessarily stay down next year. Maintaining compliance through the next phase will help organizations maintain a high standard for protecting payment processing. Organizations may want to tap consultants for this next phase.

Adapting alongside threat actors

Understanding the threat is always the first step of addressing the threat. A broader insight to be gleaned from the trends outlined above is that threat actors, when denied one path, will often find another way. PCI data theft is down, but stolen credentials are up. Phishing may be down, but pretexting emerged as its replacement. Part of mitigating risk is tracking its evolution and adapting accordingly.