WHITEPAPER

2024

THE PRICE OF NEGLECT:

WHY RETAILERS CAN'T AFFORD TO IGNORE CYBERSECURITY

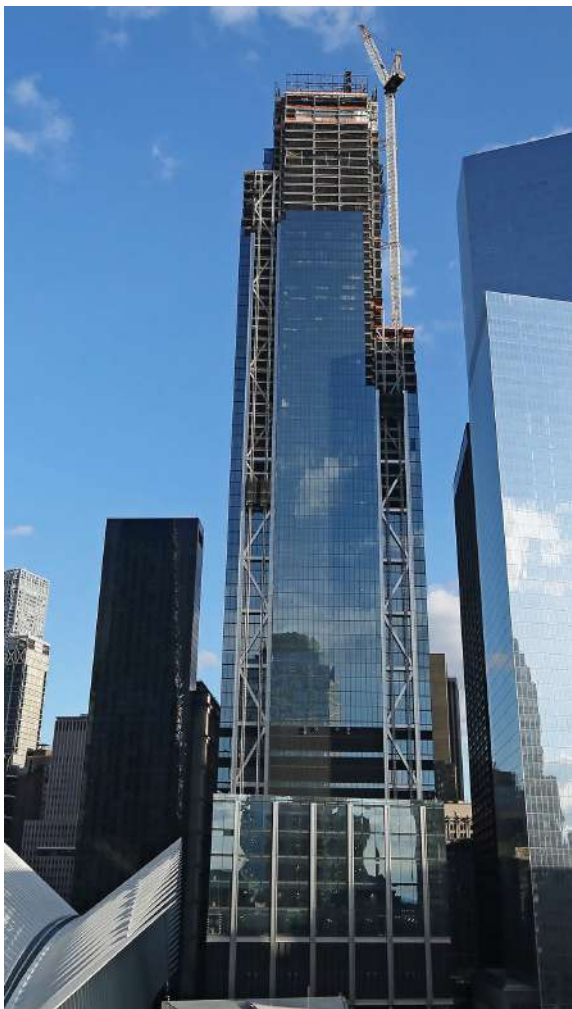
MAR
22

rewterz

Studies indicate the reach of the global retail industry is growing. In 2022, **McKinsey & Company** reported that one-fifth of all companies registered in the European Union belong to the retail industry, meeting one-third of total household consumption needs, with an annual revenue of **EUR $7 trillion.** The United States is not far behind. The National Retail Federation posits that the retail sector provides 1 in 4 jobs, with 52 million working Americans involved in the retail industry.

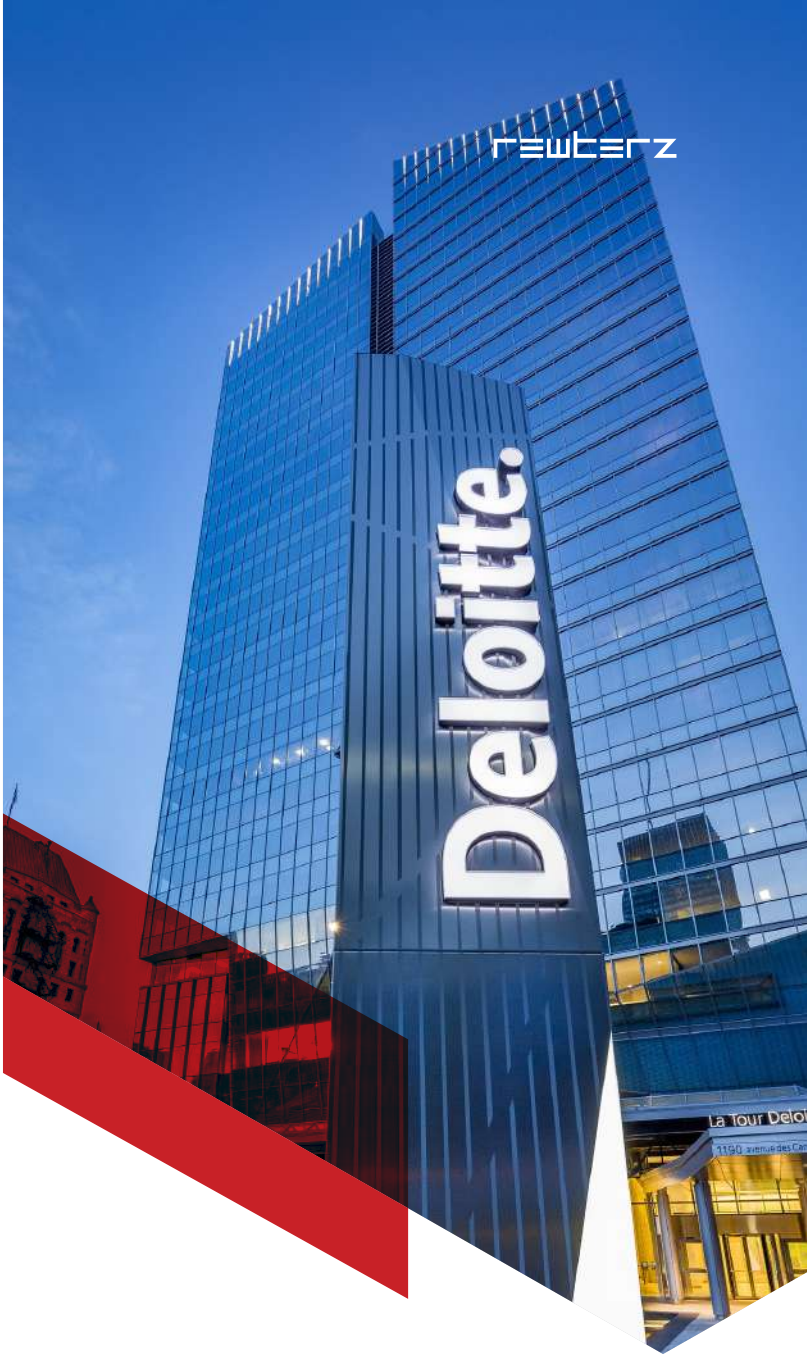
As the retail sector flourishes, so do complementary omnichannel experiences. Brick and mortar retail stores, such as those in shopping malls, are often supported by online shopping options. Whether online or in-person, there is unmistakable momentum in the shift from cash payments to "cashless" debit, credit card and mobile payments, with transactions expected to amount to over **USD 505 billion** globally by 2032.

Expansion is good for business, but with it comes greater exposure to risk, as complex omnichannel services will increase the attack surface of retail operations. Retailers collect a large amount of personal data and credit card information, making them desirable targets for cyberattacks. Stealing payment and identity information can be considerably more lucrative than stealing goods; a fact that cybercriminals know well. The noteworthy TJX companies breach in 2007 reveals the magnitude of damage that cybercriminals can inflict. The American retail giant that owns popular companies such as TJMaxx, Marshalls and Homegoods, was targeted in a cyberattack that affected 45.7 million credit and debit card accounts.



WHAT KIND OF DATA IS VULNERABLE?

The top three most commonly targeted data in cyberattacks are cardholder data (by far the most desirable), personal data and intellectual property, according to a Deloitte analysis.



As businesses expand, so do their stores, distribution centers and data points. As this happens, the use of big data and complex data warehousing models becomes commonplace. The profile of retailers engaging in these data warehousing models is also shifting. Healthcare and pharmaceutical retailers, traditionally known for their store-fronts, are increasingly offering digital services, resulting in highly sensitive information about patients being stored in their networks.

Traditional data reservoirs within other industries are vulnerable as well. These include databases housing customer details, as well as strategic information coveted by rivals, like forthcoming store sites and demographic insights (such as average income or age of customers within a store's vicinity). A decade after the landmark TJX cyberattack, the Equifax data breach proved that companies in the future were no safer, as the personal information of 147 million people was exposed to cybercriminals. The staggering Marriot International cyberattack of 2018 further exposed system vulnerabilities, affecting 500 million guests' personal data, including identity markers, credit card information and passport numbers.

147
MILLION
People was exposed to cybercriminals

500
MILLION
guests' personal data affected

HOW IS DATA STOLEN FROM RETAILERS USED?

Stolen data can easily be purchased by parties with specific interests on the dark web, paid for by cryptocurrency or Western Union. More often than not, cybercriminals targeting retailers are motivated by money, and use sensitive information for fraudulent purchases, financial schemes or to launch phishing attacks.

Identity theft:
Once sold, credit card numbers and their accompanying security codes can be used to make clone cards for fraudulent purchases. Cybersecurity research explains that stolen Social Security numbers, residential addresses, complete names, birthdates, and other personally identifiable details can facilitate identity theft. For instance, perpetrators may utilize this information to obtain loans or credit cards in the victim's name, or to submit counterfeit tax returns.

Phishing scams:
Phishing involves criminals pretending to be someone trustworthy, such as a popular retailer, to prompt customers to reveal more sensitive information. Usually, a link is sent that will direct users to a fake website where they will be prompted to enter their financial details. That information is then stolen and used to exploit the unsuspecting user.

BUSINESS IMPACT ON RETAILERS

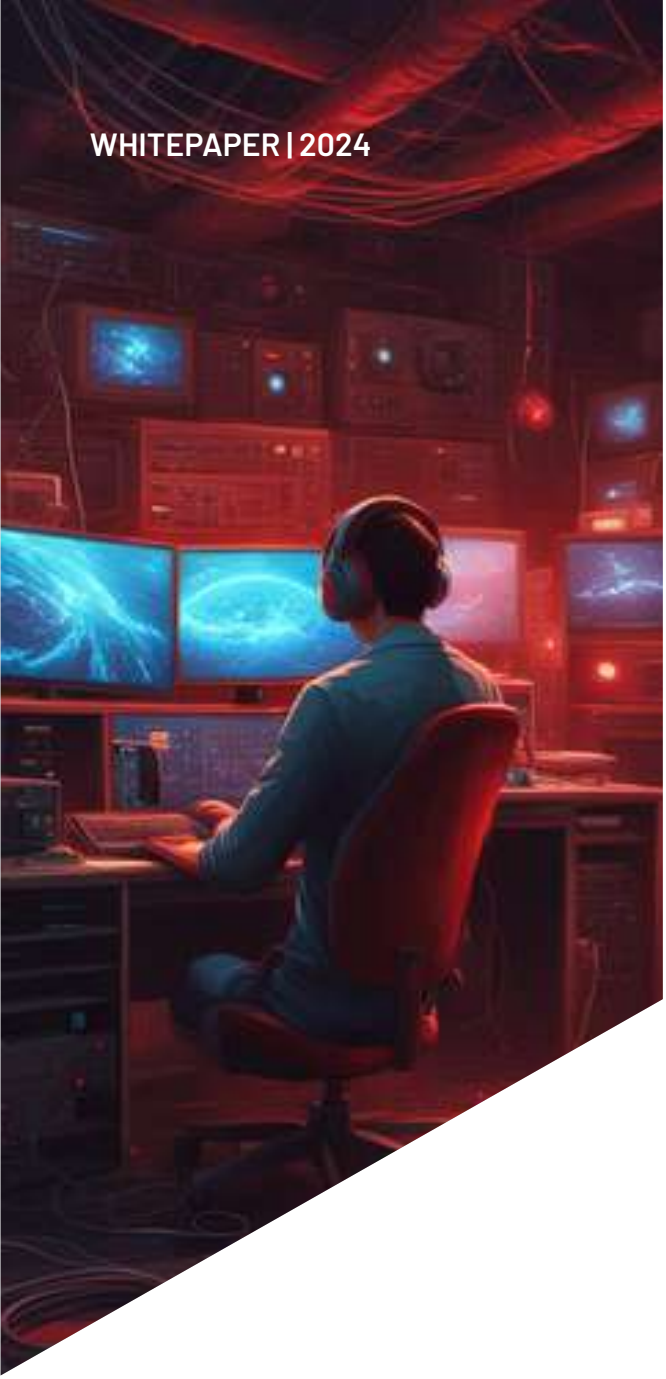
Whether the attacks are personal or profit driven, they inflict damage to the breached organization's reputation and levels of consumer trust, with considerable financial implications as well.

Increased severity and duration of the breach can tarnish a company's standing and stock value significantly. Yet no matter what the magnitude, a data breach is always worrying to clients, investors and employees and can alter the Company's value in both measured and imperceptible ways.

Cyberattacks can also compel companies to compensate affected customers financially. In 2013, one of America's largest retailers, Target Corporation, was victim of a data breach that compromised the data of 70 million customers. Apart from large sums of money spent in remediation, the Company paid USD 292 million in class action lawsuits in the wake of the cyberattack. The attack garnered extensive global media attention, resulting in substantial harm to the company's reputation and sales. Financial ramifications included a decline in the company's stock price throughout the subsequent quarter and into the fiscal year, substantial fines, and other expenses.

70
MILLION
Consumers' personal information exposed

$292
MILLION
Paid in class action lawsuits in the wake of the cyberattack.



EMERGING THREATS IN RETAIL: WHAT ARE THE POINTS OF ENTRY?

Cloud services and the Internet of Things (IoT):

Retailers are increasingly aware of the benefits that cloud services and the Internet of Things (IoT) can have on streamlining and backing up their data, revolutionizing the way shopping centers and retailers operate. However, with increased adoption, these new technologies can also become vulnerabilities. As more data is stored in the cloud, its security needs also expand.

E-commerce and Mobile Payment Systems:

Increasing e-commerce and mobile payment systems has facilitated criminals in targeting shopping centers through cyberattacks. In retail, criminals employ methods like point-of-sale (POS) skimming or malware to pilfer credit card data.

Third-Party Vendors and Partners:

Increasing reliance on third-party vendors and partners can make it tougher for shopping centers to secure their systems and data. Shopping centers and retailers depend on external vendors and partners for essential functions like marketing, supply chain management and payment processing. Cybercriminals may exploit these third-parties to access sensitive data.

Current, Departing or Ex-employees:

Insider threats in retail are often overlooked. Vulnerabilities occur as employee turnover remains high. Seasonal and short-term employees, with little allegiance to the company, but with systems access can be points of insecurity.

Complex Supply Chains:

Cybercriminals increasingly target weak links in supply chains to attack. Supply chain security is becoming increasingly important as vendors often do not have end-to-end oversight and control over their supply chains.

New Technologies:

Shopping centers and retailers are adopting novel technologies to keep shoppers engaged and to speed up customer identification and payment processing. These personalized experiences such as facial recognition and augmented reality can present new security challenges, as cybercriminals can target these systems to steal sensitive data.

CONCLUSION

As the retail industry responds to fundamental shifts in customer preferences and embraces new technologies, it must keep a complementary focus on maintaining control of its data. Identity theft and phishing scams are currently two major ways in which credit card information, personal data and intellectual property are being compromised. As businesses expand and traditional brick and mortar shops are supported by omnichannel experiences, a thoughtful and comprehensive cybersecurity plan will be required to maintain data integrity, financial security, and customer confidence.