OLIVER WYMAN

CYBER-ATTACKS

The Increasing Risk For Retail

Cyberattacks are an unfortunate reality and major source of damage in today's digitally focused business environment. Successful cyberattacks have the potential to cripple companies through significant legal fines, reputational repercussions, and overall financial strain. The financial impact of attacks on retailers have reached hundreds of millions in the past. As retailers increasingly shift to a digital environment — and particularly as COVID-19 accelerates online purchasing — it is more important than ever for retailers to invest adequately in cybersecurity safeguards.

In the past few years, disruptive cyberattacks on retailers have become more common. These companies had implemented advanced cybersecurity measures in some cases, but professional hackers nonetheless were able to install malware to harvest confidential customer payment information, resulting in a massive breach of customer data. According to Bloomberg, nearly 400 million customer records were exposed through the attacks on these companies.

Compared to other industries, retail is more vulnerable to cyberattacks due to the nature of its online traffic and the design of its e-commerce websites. To encourage customer spending, user-friendliness is a top priority in the design of retail website, and robust security can be seen in conflict with making online shopping a pleasurable experience. The fear is that robust security measures can make the purchasing process seem time consuming and difficult, driving customers to abandon purchases. As a result, many retailers have shied away from implementing important best practices, such as two-stage purchase verification. This reticence only serves to increase the likelihood that retailers will be a prime target for hackers — increasing the need to act now to implement cybersecurity best practices.

HOW ARE RETAILERS BEING ATTACKED?

Retail is changing at a rapid pace, so much so that cybersecurity and IT professionals are facing cyberattacks for which they are unprepared. The following examples detail cyberattack schemes specific to the retail industry. (See 2018 Credential Spill Report for an extensive description of these types of cyberattacks).

MOBILE IN-STORE PAYMENTS

Retailers have developed their own apps to allow customers to pay in-store. If attackers obtain access to customers' log-in credentials, those attackers can even shop in-store unnoticed. Attackers view in-store purchasing as lower risk, as they receive items immediately.

BUY ONLINE, PICK UP IN-STORE

Buying online and picking up in-store is a convenience that many retailers now offer. Unfortunately, scammers have started exploiting this convenience. Since there is a quick turnaround time from the moment the item is purchased online to when it is picked up in-store, this purchasing method poses less risk to scammers than traditional purchasing methods.

ADD NEW PAYMENT

In this scheme, attackers hack into existing accounts and upload stolen credit card information. This is a preferred strategy for scammers because they can leverage the good purchasing history of the hacked account, increasing the likelihood that the transaction will be approved. Alternatively, hackers can create fake accounts with no purchase history, but this method has a lower success rate.

RETURN WITHOUT RECEIPT

Select retailers allow customers to return items without receipts. While this practice provides an added value to customers, it also is often exploited by scammers, who hijack an account and purchase items online, then return the items in-store without the receipt.

STEPS RETAILERS CAN TAKE TO MITIGATE CYBER RISK

Retailers need a proactive approach to cyberattack, as a failure to act quickly will leave them and their customers vulnerable. We have observed that there is an evolving set of best practices that companies can deploy to protect customers and safeguard against the hackers who are constantly innovating their cyber weapons.

TRAIN YOUR EMPLOYEES AND VERIFY THEIR ACTIVITIES

Employees are the most important asset to a company; however, employees also can be the greatest liability in the context of cybersecurity. According to Experian, employees accounted for 59 percent of security incidents in 2014, and the unauthorized use of computers by employees accounted for $40 billion in losses, just for US companies alone according to Experian.

Not only should companies run enterprise-wide cybersecurity training, they also must vigilantly monitor data flow and usage within their internal units. Cybersecurity training programs need to educate employees on cybersecurity best practices, such as the importance of using virtual private networks (VPNs) when working remotely, how to identify phishing scams, using strong password protection, enabling firewall protection, and more. With proper data governance in place, companies will have visibility enough to spot and stop internal data breaches in a timely manner.

EMBRACE SECURE PAYMENT PROCESSES

Retailers need to embrace the mobile wallet payment trend, as this payment method is notably more secure than traditional methods of credit card payments. Mobile payments utilize tokenization, which allows credit card payments to be processed without exposing actual account details that could potentially be compromised. If the token is stolen, the issuing credit card company will simply issue a new one, and the cardholder's primary account number (PAN) is safe.

In addition, retailers need to keep up with industry payment standards such as PCI DSS, which is a set of standards that ensures all parties involved in accepting, processing, storing, or transmitting credit card information maintain a secure environment. Embracing these more secure payment processes will help protect against future cyberattacks.

EXAMINE VENDORS' CYBERSECURITY PREPAREDNESS

Cyberattacks on suppliers have the potential to temporarily compromise or cripple a company. This was the route used to target Ukraine in 2017, when the NotPetya computer virus rapidly spread worldwide and caused billions of dollars in damage — making it the costliest cyberattack in history. To build a comprehensive and foolproof cybersecurity regime, companies must proactively examine their suppliers' cybersecurity capabilities and maintain an up-to-date blueprint on how to prevent security breaches from compromised vendors.

STRESS TEST THE SYSTEM

To test the strength of their cybersecurity, companies should regularly try to "hack" their own systems, or even better, hire a professional hacker to conduct an attack. By stress testing the security of the IT system in place, companies can better understand their own cybersecurity weaknesses and institute proper improvement measures ahead of real attacks.

RE-EXAMINE SERVICE OUTAGES

If a high-risk system has experienced an unusual glitch that was initially attributed to technical faults, it is worth checking again: reexamination may unearth hacker activities and their link to a company's previously unexplained technical difficulties. Glitches often are signs of hackers testing their target's cyber defense systems. UK government agencies, for example, are examining whether a trading outage at the London Stock Exchange in August 2019, which was initially blamed on a software hiccup, may instead have been caused by a cyberattack aimed at disrupting markets.

CONFIRM RAPID-RESPONSE CAPABILITIES

Regular cybersecurity exercises can help identify a company's vulnerabilities to cyberattacks and confirm that processes are in place to respond at short notice. Executives should know what they need to communicate to a broad range of stakeholders — regulators, employees, customers, counterparties, and investors — to get their company back up and running quickly post-cyberattack. And after a company has mitigated immediate harm from an attack, it may need to do a broader, deeper inspection, as the hackers could be searching for ways to inflict even greater damage later.

Assessing cybersecurity capabilities also includes ensuring access to external resources. In the case of a nation-state attack, law enforcement authorities may be able to step in with their investigative expertise and resources. Updating insurance arrangements is another important measure companies can take to mitigate the financial impact of future cyberattacks.

RETAILERS NEED TO ACT NOW

The Thales Data Threat Report from 2019 revealed that most retailers feel confident with their cybersecurity preparedness, with 66 percent of global retailer respondents describing their security levels as “very secure.” But while many companies are becoming more vigilant and agile about cyberwarfare, the rapidly evolving tactics of hackers can mean that today’s well-deserved confidence may easily become tomorrow’s fatal flaw. With the accelerated shift from brick-and-mortar to e-commerce due to the COVID-19 pandemic, it is even more imperative that retailers reassess and revamp their cybersecurity capabilities on a frequent basis. Promptly implementing the best practices outlined above can ensure cyber security keeps pace with accelerating and novel threats.

ABOUT OLIVER WYMAN

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

In the Retail & Consumer Goods Practice, we draw on unrivaled customer and strategic insight and state-of-the-art analytical techniques to deliver better results for our clients. We understand what it takes to win in retail: an obsession with serving the customer, constant dedication to better execution, and a relentless drive to improve capabilities. We believe our hands-on approach to making change happen is truly unique — and over the past 20 years, we've built our business by helping retailers build theirs.

For more information, please visit www.oliverwyman.com

CONTACTS

SIRKO SIEMSSEN
Global Retail & Consumer Goods Practice Leader
sirko.siemssen@oliverwyman.com
+49 89 939 49 574

MARIA MIRALLES
Retail & Consumer Goods Practice Lead, EMEA and LatAm
maria.miralles@oliverwyman.com
+34 615 036 406

FREDERIC THOMAS-DUPUIS
Retail & Consumer Goods Practice Lead, North America
frederic.thomas-dupuis@oliverwyman.com
+1 514 3507208

PEDRO YIP
Retail & Consumer Goods Practice Lead, Asia
pedro.yip@oliverwyman.com
+852 22011705

RONAN GILHAWLEY
Retail & Consumer Goods Practice Lead, Australia and New Zealand
ronan.gilhawley@oliverwyman.com
+61 410 668440

RAINER MUENCH
Retail & Consumer Goods Practice Lead, Germany
rainer.muench@oliverwyman.com
+49 89 93949461

NORDAL CAVADINI
Retail & Consumer Goods Practice Lead, Switzerland
nordal.cavadini@oliverwyman.com
+41 44 553 37 64

COEN DE VUIJST
Retail & Consumer Goods Practice Lead, The Netherlands
coen.devuijst@oliverwyman.com
+31 20 541 9790

SALIM POONAWALA
Retail & Consumer Goods Practice Lead, France
salim.poonawala@oliverwyman.com
+33 1 45023660

DUNCAN BREWER
Retail & Consumer Goods Practice Lead, UK
duncan.brewer@oliverwyman.com
+44 20 78527760