KYND

Cyber risks in the retail industry

The retail industry has undergone rapid digital transformation over recent years to improve business operations, cut operating costs, and ultimately achieve a seamless purchasing experience and service for its customers. With more businesses pivoting to an omni-channel retail strategy, particularly with COVID-19 forcing the rapid shift to e-commerce, it has become easier for retailers to reach new markets by breaking the barriers of location and time.

This increased reliance on technology, however, makes retailers much more vulnerable to cybercrime than ever before. From limited funds devoted to cyber security, to legacy and highly distributed IT environments, combined with a wide variety of new endpoints (e.g., mobile Point of Sale (mPOS) sales, interlinked stock and inventory applications, numerous vendor management systems, etc) – it all contributes to retailers' expanded attack surface for cybercriminals to exploit.

Due to the nature of the business, retailers also process and store large amounts of customer and employee data, as well as a significant amount of financial information. Without a strong capability for responding to a cyber incident, the reputational damage and ensuing legal repercussions of one single data breach can adversely impact a company.

Business exposure and implications

Distributed denial-of-service (DDoS) attacks

DDoS extortion attacks - malicious attempts of flooding website/systems with an overwhelming volume of requests - are common against the retail sector as they're relatively easy to deploy, and the damage to the retailer is immediate and costly. The attackers execute a DDoS attack, issue a ransom demand, and threaten to continue the attack until the payment is made. Whilst many companies prefer to pay the ransom because it appears to be the fastest way to resolve the problem, they are consequently identified as a "good" target and are likely to be a DDoS attack victim again in the future.

Data breaches

Data breaches exposing valuable customer information have become a significant issue for trading businesses. With most major retailers having adapted to operating online, creating a personal customer account in order to purchase goods or use online services has become normal practice. Cybercriminals, in turn, use these accounts as one of the attack vectors to gain access to Personally Identifiable Information (PII) and financial details - to either use the data themselves to make fraudulent purchases or sell it on the 'dark web'.

Failure to adequately protect customer information in case of a data breach can not only cause major disruption, significant reduction in share price, and lasting reputational damage, but also lead to substantial GDPR fines of up £18 million or 4% of annual global turnover - whichever is greater - that can adversely affect the business.

IP infringement and domain spoofing

The rapid growth of e-commerce has prompted cybercriminals to take advantage of the essential role that websites play on the Internet by registering domain names that appear related to existing brands. Bogus websites mimic legitimate sources by copying sources by copying their logos, images and style to trick unsuspecting customers into entering their credentials, giving up their personal or financial information, or even installing malware on their devices.

As a result of such cyber-attacks, businesses may also incur legal costs associated with defending issues of IP infringement.

Supply chain cyber risk

Complex and diverse global supply chains, ranging from manufacturers and stock supply, up to payment providers, require retail businesses to provide their third-party vendors with access to their corporate systems and network in order to maintain frictionless daily operations. Often the intermediaries involved don't have the same cybersecurity standards and protection, and as a result, are used by opportunistic cybercriminals as a conduit into the retailer itself.

Key industry statistics

83%

of the top 30 U.S. retailers have connections to a vulnerable third-party asset, with nearly half of them having vulnerabilities posing an immediate cyber risk[1]

440m

customer records compromised as a result of a major data breach suffered by Estée Lauder at the beginning of 2020[2]

£1.45m

was the amount of ransom paid to cybercriminals by FatFace to restore its data following a successful cyber attack on its systems in January 2021[3]

228 days

was the average time retail companies took to identify breach, taking 83 more days to contain it, as of 2019[4]

What types of risks exist?

There is a variety of different threats that the retail industry could be impacted by, but the most common include:

Phishing
Malicious emails designed to look like genuine emails which encourage employees to click – infecting their computers or stealing passwords in the process.

Viruses
Code which infects computer systems, corrupting or deleting data.

Hacking
An individual or group attempting to gain access to company systems with the intent to steal or destroy data.

Ransomware
A malicious programme which locks access to company files and data until a ransom payment is made, after which time access may be restored.

Case Study

Type
A global fashion retailer suffers a serious data breach as a result of a concerted cyber-attack on its computer network.

Scenario
In late September 2018, a U.S. based global online fashion company announced that there had been a significant data breach over the course of the summer that resulted in the theft of almost 6.5 million customer records, including their email addresses and encrypted passwords.

Sting
The breach was first uncovered in August when the IT team noticed suspicious activity on their internal network. It was then discovered the attackers had installed a "backdoor" in the retailer's servers – a type of malware that negates standard authentication procedures, giving the perpetrators the ability to remotely access customer databases.

Investigation
The company immediately hired a well-known forensic cybersecurity firm as well as an international law firm to conduct a thorough investigation and prevent any further breaches. During the investigation, the backdoor malware was confirmed to no longer exist on the servers. It subsequently transpired that the hackers were able to infiltrate servers through back door entry points, which were later also closed and removed. The apparel company offered a one year identity theft monitoring service to its affected customers.

Conclusion
Customer data is one of the most valuable assets that any organisation holds – and is a primary target for cybercriminals as it can be monetised very quickly. As retailers continue to collect more PII data, implementing a comprehensive data protecting strategy that includes adequate employee training, appointing cybersecurity representatives and vetting third-party partners – has become a critical necessity for companies.

KYND

KYND's analysis of key cyber risks of the top* 100 world's largest retail companies
*by turnover and excluding Amazon

Ransomware Risk

55% of retailers had at least one external internet service exposed which would place them at a higher risk of a ransomware attack.

Email Spoofing

89% of retailers were vulnerable to having their email addresses spoofed.

Vulnerable Services

55% of retailers were running at least one service, such as an email server or web server, with a well-known vulnerability to cyber attack.

Out of Date Software

85% of retailers had at least one service that was using software which was out of date, no longer supported and vulnerable to cyber attack.

Certificate Issues

74% of retailers had at least one security certificate which had expired, been revoked or distrusted.

How KYND can help

- With just a website name, KYND reveals your organisation's cyber risks
- Instantly KYND lets you know if your emails are spoofable or if you're vulnerable to a ransomware attack
- KYND provides clear and easy recommendations without using technical jargon
- KYND continuously monitors and alerts you instantly if any new cyber risks are found

Get in touch

broker@kynd.io

www.kynd.io

References:
[1] https://www.securitymagazine.com/articles/94137-of-top-30-us-retailers-have-online-vulnerabilities-posing-cybersecurity-threats, 2020, Security Magazine
[2] https://threatpost.com/estee-lauder-440m-records-email-network-info/152789/, 2020, Threat Post
[3] https://www.cybernewsgroup.co.uk/fat-face-pays-2m-to-conti-ransomware-gang/, 2021, PSBE Cyber News Group
[4] https://www.ibm.com/security/data-breach, 2019 Cost of a Data Breach Report, 2019, IBM & Ponemon Institute