CYBERTHREAT INTELLIGENCE FOR RETAIL & E-COMMERCE
**Introduction**

Why is the retail and e-commerce sector targeted?

<table>
<thead>
<tr>
<th>Why is the retail and e-commerce sector targeted?</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lowering barriers to purchase</td>
<td>5</td>
</tr>
<tr>
<td>Consumer analytics</td>
<td>6</td>
</tr>
<tr>
<td>Payments systems</td>
<td>6</td>
</tr>
<tr>
<td>Data governance</td>
<td>6</td>
</tr>
<tr>
<td>The human element</td>
<td>6</td>
</tr>
</tbody>
</table>

**State of the Industry**

Cyberthreats targeting retailers

<table>
<thead>
<tr>
<th>Cyberthreats targeting retailers</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>8</td>
</tr>
<tr>
<td>Malware</td>
<td>10</td>
</tr>
<tr>
<td>EMV skimming</td>
<td>12</td>
</tr>
<tr>
<td>Digital skimmers</td>
<td>12</td>
</tr>
<tr>
<td>Weak authentication mechanisms</td>
<td>13</td>
</tr>
<tr>
<td>2FA</td>
<td>13</td>
</tr>
<tr>
<td>DDoS attacks</td>
<td>14</td>
</tr>
<tr>
<td>Third party exposure</td>
<td>14</td>
</tr>
<tr>
<td>Hacktivism</td>
<td>14</td>
</tr>
<tr>
<td>Regulation and legislation</td>
<td>14</td>
</tr>
</tbody>
</table>

How retailers can manage their cyber-risk

<table>
<thead>
<tr>
<th>How retailers can manage their cyber-risk</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive level engagement</td>
<td>17</td>
</tr>
<tr>
<td>Breach response readiness</td>
<td>18</td>
</tr>
<tr>
<td>Payment systems security management</td>
<td>18</td>
</tr>
<tr>
<td>Third party security management</td>
<td>18</td>
</tr>
<tr>
<td>Effective fraud prevention</td>
<td>19</td>
</tr>
<tr>
<td>Company-wide training</td>
<td>19</td>
</tr>
</tbody>
</table>

The role of threat intelligence

<table>
<thead>
<tr>
<th>The role of threat intelligence</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>20</td>
</tr>
</tbody>
</table>

Conclusions

<table>
<thead>
<tr>
<th>Conclusions</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>24</td>
</tr>
</tbody>
</table>
INTRODUCTION

The internet has changed the way that goods and services are bought and sold. The retail sector continues to undergo rapid transformation and investment in technology and innovation is the new cost of doing business. Consumer expectations are ever increasing, demanding high-quality experiences, products and services, both at the computer and on mobile. Meanwhile in the back end, customer analytics and enhanced third-party integrations are deployed to help contribute to higher margins and increased revenues. Digital payment systems are also being updated, particularly with the emergence of non-banking players in the payments industry, further supporting growth.

But these extraordinary innovations come with a price: an increased attack surface for cybercriminals to exploit and exposure to an increasingly virulent and sophisticated threat landscape. The breadth of cyber risks that retailers now face is significantly broader and attacks themselves more frequent than ever.

Fraud in the e-commerce sector costs about $6bn a year, while consumer banking takes a fraction of this hit at $1.7bn. Accenture has the cost of a breach at $11.43m for organizations in the retail sector. It’s clear that a successful attack can have a huge impact on the bottom line – whether through direct losses from business disruption, customer attrition through reputational damage, penalties from regulatory bodies, or most likely a combination of the three.

Unfortunately, in the rush towards digital transformation retailers and e-commerce companies are often behind the curve when it comes to their cybersecurity posture. Cybercriminals targeting this sector have developed advanced and often automated TTPs (tactics, techniques and procedures) to compromise and monetize stolen data. From convincing phishing campaigns tricking users into sharing personal and financial information, to account hijacking to commit fraud, to crimeware and targeted malware attacking PoS, digital payment systems and customer databases, digital risk has never been so high.

This whitepaper will focus on the issues that confront the C-suite in the retail and e-commerce sector, offering insight and guidance to meet the challenges they face today.

In particular, many of these issues can be combatted using targeted threat intelligence. This report will demonstrate how actionable information, delivered in real-time, reduces your exposure to potential fraud attempts by cybercriminals. It will also explain how to optimize your response in the event of a breach.

In today’s cybersecurity landscape, basic prevention techniques simply no longer work. Not a week goes by without another high-profile breach or its financial consequences reported in mainstream media. But why
are retailers still getting breached, despite the amount of investment in security products? Even the biggest retailers remain vulnerable with their advanced SIEM and endpoint solutions.

This paper explores why retailers of all sizes must take proactive steps to manage their cyber-risk. The first step is to understand why the sector is targeted. The following pages lay out the cybersecurity landscape for retailers, offering insight around trends, regulations, responsibilities for companies of all sizes, and finally how retailers large and small can seek to mitigate their risk defend themselves.
WHY IS THE RETAIL AND E-COMMERCE SECTOR TARGETED?

In recent years, the number of attacks specifically targeting retail has increased, with a report claiming that three quarters of retailers claim to have been a victim. The business impact is clear: reduced profits and drops in shareholder value; negative publicity resulting in diminished consumer confidence; millions in expenses relating to breach mitigation and associated fines. E-commerce companies, which live and die by online payments, are arguably at even greater risk. The sector is particularly vulnerable to fraud, for example through credential theft leading to account takeovers, false purchases and associated clean-up costs.

No matter the size of the retailer or e-commerce company, cybercriminals see the industry as a whole as a prime target for cyberattack due to the data these companies hold. The more data you hold, the greater the target. Consumers' PII is intrinsically linked to payment or cardholder data needed to complete transactions or stored for targeted marketing later down the line. Software vulnerabilities or customer databases not using a sufficient level of encryption are ripe for attack. An attacker exploits either of these vulnerabilities and can exfiltrate payment information for customers, impacting the company’s bottom line in compensation costs, not to mention significant reputational damage. Even further, the company then gets hit by GDPR penalties for not taking responsible steps to comply with the requirements of the legislation.

Within the business itself, compromised employee login credentials can lead to account takeovers, identity theft, blackmail, spreading crimeware, fraud and other criminal activities (see our in-depth report into the Credential Theft Ecosystem for more detail). Sophisticated phishing campaigns targeting VIPs and employees have been known to cause havoc for an organization, while targeted malware against IT infrastructures of these organizations have also been discovered in the wild.

The potential financial gain for cybercriminals looking to attack the retail and e-commerce sector is huge. Correspondingly, the ways in which they can get their hands-on valuable data is ever increasing. There are several areas of concern for retail companies to consider.

LOWERING BARRIERS TO PURCHASE

Many businesses in the sector necessarily innovate in order to remain competitive. However, as their digital footprint expands, so does their attack surface. Many companies prioritize rapid profit-making innovation over security measures. Equally, continuously and incrementally improving legacy systems can result in “technical debt.” Simply put, delivering a customer experience that enables increased and faster purchases is seen as more important than maintaining robust security processes. Resultingly these innovations, combined with greater resources deployed by the adversaries, make the retail sector a highly attractive target to attackers.
CONSUMER ANALYTICS

Successful retail companies harness data-driven technologies, leveraging as much consumer information as they can legally get their hands on to help boost sales and improve efficiency. However, this data is not only valuable to the company to target customers, but inherently monetizable to attackers. The more data you have on the back end, the juicer the target. Once the data is exfiltrated, it might appear on forums or the dark web for sale. In turn, this can help propagate further attacks as sophisticated criminals can cross-reference the data with other dumps and build up a clearer picture of victims.

PAYMENTS SYSTEMS

Payment technologies, both traditional and new, present a number of opportunities for attackers. It is surprisingly easy to install malware on PoS devices, for example, which records data on every card used in the machine. There are also strains of malware which can create backdoors elsewhere in the organization, persist and spread through the entire network to infect millions of PoS devices and harvest huge amounts of data. These ‘skimmers’ are a threat that proliferates across the industry.

Meanwhile, a “mainstream shift in how payments are made” has been signaled by consumer attitudes towards mobile wallets and NFC, which is enjoying a CAGR of 32% to 2022. And this figure only uses data from Western markets; in China, for example, it is becoming increasingly rare to pay with cash or card. Furthermore, many companies seek to include automatic payment technology into their apps, but accompanying defensive measures are not yet up to scratch.

It is abundantly clear that the proliferation of online marketplaces mean that brands are ever more vulnerable. This is not least because scammers prefer digital transactions, being able to bypass chip and pin technology.

DATA GOVERNANCE

Many retailers tend to take a compliance-based approach to the data they collect and store. Though this is defensible in the face of stringent legislation including the GDPR, often this is at the expense of a secure data governance framework more generally. For example, there is often a reliance on third party providers (in customer service etc.), leading to gaps in control structures which attackers can take advantage of. Furthermore, now more than ever a successful breach could result in the initial data-gathering entity, the retailer, being punished. It is worth remembering that a compromise of just one provider opens the gates to a multitude of new targets.

THE HUMAN ELEMENT

As with all industries, retail is not immune from social engineering attacks. Phishing campaigns are in fact particularly successful in this sector, as a result of poor cybersecurity education among employees on one hand, and expansive brand footprints on the other.
Retail is particularly susceptible to phishing, cybersquatting and other social engineering attacks

A scenario where employees were hit by a phishing campaign containing stealer malware could compromise login credentials, and subsequently a retailer’s internal servers. Verizon’s DBIR 2018 records that 4% of people will click on any given phishing campaign. Even if the attack only affected a few employees, it only takes one compromised credential to enter the infrastructure and persist, causing damage when something juicy is found. By the time the breach is discovered, it is usually already too late.

On the other hand, the sheer volume of emails (marketing, payment confirmation, shipment info etc.) shared makes spotting a rogue attempt amongst legitimate content even harder.

The number of domains held by retailers, especially those who operate in more than one market, also mean that the companies and their customers can become victims of cybersquatting more easily since there are more domains available to target.

In summary, the retail and e-commerce sector is highly vulnerable to attack for a number of reasons, some unique to the industry and others more ubiquitous. The following section will review the state of industry, including an examination of the threat landscape.

Immediate costs

These are the largely unavoidable costs that include the immediate business and media impact, plus the cost of restoring the confidentiality, integrity and availability of data and systems. Immediate costs include:

- Forensic investigation costs
- Legal costs
- Customer notification costs
- Credit monitoring for customers
- Potential business interruption costs
- Public relations expenses
- Fraud costs
- Extortion costs
- Physical damage costs
- IT/business remediation costs

Slow-burn costs

These vary according to the type and severity of the event, and how it is handled, but typically include the long-term business impact and costs incurred by reimbursing victims, as well as reparation and the payment of penalties for failure to meet obligations. Slow-burn costs include:

- Third-party litigation expenses
- Customer churn from reputational damage
- Regulatory fines and penalties
- Share price impact
- Loss of management focus
- Loss of competitive advantage
- Loss of revenue

This graphic from KPMG illustrates the impact of a successful cyberattack on a business.
STATE OF THE INDUSTRY

As outlined above, companies in the retail sector are high-profile targets for cybercriminal organizations. As digital transformation continues apace, the number of attack vectors available to cybercriminals expands and threatens companies of all sizes. Breached consumer data presents a huge business risk to companies, but for every successful attack exfiltrating credit card details or PII, there is also a number of other threats that businesses need to defend against, such as DDoS attacks taking down a shopping website during the holiday season, or spoofed sites impersonating the real thing. Last year, malware attacks stealing data through e-commerce sites were particularly active in Europe and other emerging markets. Fraud in the e-commerce sector costs about $6bn a year, while consumer banking takes a fraction of this hit at $1.7bn.

CYBER THREATS TARGETING RETAILERS

This section will outline some of the most active cyberthreats faced by the retail industry. Security teams would do well to note that their resilience is charted against different threat categories.

<table>
<thead>
<tr>
<th>Threat category</th>
<th>Threat actor</th>
<th>TTPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Script kiddies; low-level; unsophisticated.</td>
<td>Exploiting known vulnerabilities; Uses freely available tools</td>
</tr>
<tr>
<td>Advanced</td>
<td>Sophisticated attackers; criminal groups; APTs.</td>
<td>Targeted malware; complex tools and methodologies; zero-day vulnerabilities</td>
</tr>
<tr>
<td>Emerging</td>
<td>Sophisticated attackers; criminal groups; APTs; nation states.</td>
<td>Research to identify exploits; new attack vectors enabled by emerging technologies</td>
</tr>
</tbody>
</table>
Phishing is one of the most effective attack vectors, combined with social engineering techniques to extract information from its victims.

**Phishing**

Phishing is a seminal technique used by cybercriminals to steal credentials and personally identifiable information (PII) from its victims. It remains one of the most effective attack vectors, due to the fact that it is normally used together with social engineering techniques to extract information from its victims. The sender tries to make the victim follow a link and enter credentials, PII information or install malware. When phishing is more targeted against an individual or a company, then it is known as spear phishing.

The success of the attack often depends on the level of social engineering and quality of communication. Often, attackers will use company logos and realistic-looking links to trick unsuspecting customers.

There are also more professional groups at play, such as FIN7. It has primarily targeted the retail sector with an eye on financial information. The group uses phishing techniques to distribute point-of-sale (POS) malware, often combined with remarkably bold social engineering techniques, such as calling up victims to ensure they open malicious files. Since appearing in 2015, the group has compromised hundreds of companies, thousands of POS terminals, and millions of payment cards. FIN7 has been linked to high profile breaches at Arby’s, Chili’s, Chipotle, Red Robin, Jason’s Deli, and Sonic. After a successful breach, FIN7 typically offers the compromised cards for sale on the underground card shop Joker’s Stash.

FIN7 should be considered a dangerous APT because of its rigorous and sophisticated procedures, proving in several occasions the ability to quickly evolve new strategies and adapt tools. The group has shown to be a particularly professional and disciplined organization, working following a regular office schedule, with nights and weekends off. The information on this threat actor is detailed in Blueliv’s Threat Context module. This sort of strategic intelligence information is critical to protect retailers from attacks.

Worryingly, in the retail sector there was a year-over-year increase of 78% in phishing attempts last year, and according to MediaPro 6% of retail employees proved to be a risk when it came to correctly identifying phishing attempts.

**Site Impersonation & Spoofing**

Fake websites pose a real risk to retailers. The importance of online shopping across the sector means that heavy investment in an optimum customer experience delivers new opportunities for cybercriminals to exploit.

The broader the offering, the higher the risk, since the retailer will necessarily have a greater number of URLs which can be impersonated. If, for example, a retailer has a number of different URLs in different languages to service different markets, their exposure is greater and customers may trust the site without questioning the authenticity of the page.
A carefully crafted spoof site will adopt the design of the target site, logos, fonts, tone of voice and often will have a similar URL – or one that looks legitimate enough to convince the visitor that the site is safe. The replica site may be used for a variety of purposes, including advanced phishing campaigns, spreading malware and capturing visitor information which can later be used for malicious purposes. It is important to increase resilience both internally and externally, by investigating potential site impersonations through threat intelligence and taking them down as soon as possible to protect the brand.

REFUND FRAUD
Fraudsters have developed an interest in conducting scams that involve obtaining refunds from major retailers under false pretenses. Like phishing, refund fraud does not use compromised payment card information but rather relies on social engineering techniques to secure the refund. Refund fraud vendors endeavor to make customer service representatives believe that there has been an issue in the shipment or delivery of the purchase. Common fabrications used by refund vendors hoping to secure a refund is that the package never arrived, the package was stolen, the package was empty, or that the items within the package were somehow sullied.

MALWARE
Malware stealers are widely-used by cybercriminals to acquire sensitive information. For example, according to a recent report, up to 87% of sites using the Magento ecommerce platform still remain at high risk of attack. This follows a major malware campaign stealing payment card data, resulting in 1.4% of all sites using Magento already compromised. Most of the victims were smaller, local businesses, demonstrating that cybercriminals simply do not discriminate based on size. Notably, without appropriate cyberdefenses, they will have had to wait to be notified by credit card companies that customer payment data had been compromised. This process might have taken months.

Critically, most malware isn’t discovered for a considerable amount of time, further putting retailers at risk. Take Hudson’s Bay retail group, for example, hacked in February 2018 resulting in around 5 million credit card accounts stolen and 125,000 offered for sale on the dark web. The attack was a long-term compromise of data and metadata for point of sale and credit card transactions, exfiltrated to the cybercriminals. It was concluded that the malware infection could have been in place for as many as 500 days. The duration of this attack displays a clear necessity to invest in proper prevention and detection systems to avoid or detect intrusions inside the private network.

BANKING TROJANS
Banking Trojans are a malware type specifically designed to obtain banking and payment data from their victims. In 2018 Kaspersky identified the main malware families using e-commerce brands to steal from victims. All of these are banking trojans, best known for targeting users of online financial services to obtain banking and payment data from their victims.

Trojans have multiple functionalities that allow them to steal the victim’s...
information, such as man-in-the-browser techniques, keystroke logging, and form grabbing. Blueliv monitors botnet configurations as new functionalities have started to spread among banking trojans in recent years. These functionalities include webfilters, dnsfilters and webinjests. These functionalities are defined and detailed in our recent report on The Credential Theft Ecosystem.

A webinject is a technique used to intercept data after it is decrypted from SSL but prior to its display in the browser. Consequently, it gives the trojan the ability to modify the response of a webpage’s server. That response is leveraged by trojans to request further information from the victim to perform fraudulent transactions, among other activities.

The main targets of this type of attack are organizations in the financial service sectors, but in recent years it is clear that the target has shifted towards retail. The perpetrators perform these attacks in an attempt to get hold of users’ credentials through tampered login panels and perform fraudulent activities in their name.

These samples are mostly distributed through spam mail campaigns and exploit kits, which usually employ a loader to drop the actual trojan. This distribution process is rigorously detailed in our report Chasing Cybercrime: Network insights into Vawtrak v2. It is available online and provides deeper insights about these infection methods.

If infected, retailers trusted by their customers can be abused by cybercriminals. It should be noted that another potential danger for retailers are bots which have already infected the system through a different vector. For example, cybercriminals have been known to use backdoors to install custom malware and move laterally within a network in order to mine sensitive data. Threat intelligence is crucial, not just for looking outside the network, but seeing what’s already inside too.

RANSOMWARE

The goal of ransomware is to infiltrate and take control of a retailer’s infrastructure. When ransomware malware successfully infects a machine, it encrypts all important files and data. It then asks for a ransom, in return for the key victims must use to decrypt their files. Although ransomware attacks’ popularity has ostensibly decreased in recent months, they must still be considered a dangerous and destructive threat for retailers.

Ransomware-as-a-Service is a business model where ransomware software can be leased to any client willing to pay the price. Instead of developers using the malware exclusively, they offer its usage to third parties for an affordable price or by receiving a percentage of the proceeds.

This business strategy makes RaaS a particularly dangerous threat due to its indeterminate client base. From regular users with bad intentions to companies interested in disturbing the performance of their competitors, anyone with the ability to pay could be a potential threat actor.

Often RaaS developers try to make their products attractive for unskilled users, creating intuitive online management portals for deploying and tracking the rented ransomware. They even let clients configure some parameters, such as the ransom price or message shown to the victims.
Just like regular software business models, some RaaS even have their own customer support teams, helping clients use the software by solving issues. This model of cybercrime business is win-win for malware developers; they develop powerful yet easy-to-use software for others to deploy, and they receive a cut of the proceeds.

Retailers should be particularly cautious about ransomware, given the highly competitive landscape of their marketplace and importance of reputation. The significant financial impact is unlikely to be the ransom itself but rather the business disruption, similar to DDoS attacks.

MOBILE APPS
Retailers must look out for malicious apps impersonating their brand, but also specific malware targeting mobile phones. The use of smartphones for purchasing items has increased exponentially in recent years and correspondingly malware developed to target this trend has also grown. Account takeovers and fraudulent transactions are rampant, and it is only recently that retailer apps are using authentication techniques during comms between the app and servers to confirm healthy usage.

POS MALWARE
Despite being among some of the simplest forms of cyberattacks, card detail stealing PoS malware is highly effective. A combination of hard-to-detect data-exfiltrating malware, legacy hardware which is difficult to patch, and general OS vulnerabilities mean that this particular threat is common and difficult to defend against. An investigation into the breach of Forever21 in 2017, for example, found that attackers had gained network access and installed malware to harvest credit card data.

EMV SKIMMING
EMV security protections have attempted to stem the tide of massive breaches of track data resulting from PoS malware compromise. Unlike magnetic stripe data, which remains the same until the card’s expiration and is not encrypted, the information stored on EMV chips is encrypted. On cards using dynamic data authentication (DDA), the data is encrypted uniquely each time, while the encryption for static data authentication (SDA) cards remains the same for each transaction.

The fixed nature of the encryption on SDA cards renders the cards less secure than their DDA counterparts. A multitude of unverified EMV skimming and writing software exists on cybercriminal forums and marketplaces. Indeed, since the introduction of EMV protections, cybercriminals have sought new and creative ways to circumvent these measures.

DIGITAL SKIMMERS
Digital skimmers have received attention recently targeting EMV technology. The number of threat actors operating under the umbrella term “Magecart” and leveraging digital skimmers increased significantly, demonstrating that steps to eradicate credit card-related fraud has shifted cybercriminal resources to other vulnerabilities.
Digital skimmers are scripts designed to steal data entered into online payment forms, and threat actors use these on the compromised websites of e-commerce entities or third-party suppliers. Research suggests that the actors often use vulnerabilities in the website/CMS or take over the hosting/CMS accounts to facilitate crime.

Magecart groups first started appearing in 2015, attacking the e-commerce platform Magento outlined above. Later in 2016, they hacked numerous e-commerce websites. The groups injected JavaScript code into the sites allowing the attackers to capture the credit card information introduced in the payment form. Since these attacks, it seems that the group established the modus operandi of injecting JavaScript code to exfiltrate the customer’s payment data. Last year saw a number of Magecart megabreaches, including breaches at Ticketmaster, British Airways, and Newegg – the consequences of these hacks are still being felt. Customers are inconvenienced, maybe defrauded but certainly losing trust and goodwill. The companies meanwhile must face not only high rates of attrition after such incidents, but also massive financial penalties. For example, in the UK the Information Commissioner’s Office has hit BA with an all-time record fine for failing to protect their customers’ data.

WEAK AUTHENTICATION MECHANISMS

Many retailers rely on user login credentials in order to deliver a personalized customer experience. However, without strong authentication mechanisms such as 2FA or MFA, there are vulnerabilities which can be exploited.

A major breach was reported by Macy’s in June 2017, where an unauthorized third party gained access to customers’ first and last names, full addresses, phone numbers, email addresses, birthdays and credit card numbers with expiration dates. It was suggested that the breach involved the use of legitimate credentials to break into the network, which could have been compromised in a number of different ways. For more detail on how credentials are stolen, please see our in-depth report into the Credential Theft Ecosystem.

2FA

2-factor authentication has long been touted as a broadly infallible way to authenticate accounts. However, mobile malware has been identified that intercepts authentication codes, putting individual users, and trust in your brand, at risk. Further, a tendency for customers to synchronize multiple devices including phones with a brand website, increases the chance of compromise.

DDOS ATTACKS

Retailers which rely heavily on online shopping to generate revenue are particularly susceptible to distributed denial of service, or DDoS attacks. An increased availability of off-the-shelf tools for unsophisticated attackers means that the barriers to entry have massively decreased in recent years.

Attacks target the bandwidth of e-commerce sites and are designed to...
disrupt business function, severely damaging traffic and databases. As a result, a successful attack, well-timed to hit during a busy shopping period for example, can lead to huge losses. Even a smaller attack which overloads servers and takes a site down for a few seconds could frustrate customers enough to shop elsewhere. Equally, attackers might seek to extort money from a retailer by simply threatening a DDoS attack.

These types of attacks are a significant risk to retailers, since revenue will likely be disrupted as a direct result of an attack. Furthermore, costs for remediation and even customer compensation should be added to the bill. We expect that DDoS attacks will continue in the near future, surpassing 2 Tbps and include more ransom demands to increase the financial benefit.

THIRD PARTY EXPOSURE

While retailers should invest heavily in their own cybersecurity infrastructure, third party vendors can create a weak link in the chain. Emerging payment technologies are being embraced by retailers and consumers alike, but these present additional risks. According to Deloitte, few consumer businesses regularly review and test their vendors’ cybersecurity capabilities. The Ticketmaster breach, for example, occurred through malicious JavaScript code delivered via a third-party live chat widget, loaded on Ticketmaster’s payments page.

Data breaches often start with the compromise of suppliers, contractors and vendors. It is important to note that it is not just the individual victim’s problem if their data is exfiltrated. It can affect the e-commerce company too – according to one report up to 90% of login attempts are actually cybercriminals attempting access.

This risk also extends to talent. There are considerable difficulties in hiring and training IT professionals, and so outsourcing to vendors for back end development (for cloud integrations, app development, mobile payments for example) can leave retailers at risk to new cybersecurity challenges.

HACKTIVISM

Though companies of all sizes are competing against each other in the marketplace, hacktivists do not make the same differentiation and can attack any retailer as a result of grievances held against a particular organization. If a major company is involved in some controversy, the knock-on effect could be significant across the sector. Where hacktivists fail to penetrate one company, they might have better luck at their competitor, drawing attention to the weaknesses of the sector as a whole – and causing significant reputational damage in the process.

REGULATION AND LEGISLATION

All online businesses are subject to a considerable amount of regulation worldwide. This legislation not only regards data privacy for consumers, but also places obligation on companies themselves. The EU GDPR, for example, enforces that companies should “implement appropriate technical and organizational measures to ensure a level of security appropriate to risk.” Given that retailers have a high level of risk due to the amount
of data they control, there is a significant onus on them to invest in cybersecurity tools and solutions to minimize the impact of cyberattacks on the enterprise that could affect their business and customers. In recent years a greater understanding of cyber-risk has forced relevant regulatory bodies to take action. Though compliance requires significant investment, responding to these challenges encourages a greater understanding of cyber risk and a more effective approach. For more detail on how threat intelligence can mitigate the impact of GDPR, see our special whitepaper here.
HOW RETAILERS CAN MANAGE THEIR CYBER-RISK

To put it simply, it is not possible to protect all data, networks, applications. Organizations must put in place proactive security measures that help them prioritize detection and response, enabling them to react quickly to incidents. This section covers a number of strategies and mechanisms that retailers of all sizes can implement.

EXECUTIVE LEVEL ENGAGEMENT

First and foremost, the C-suite must be fully engaged with cybersecurity strategy. Protecting the enterprise against an ever-evolving dynamic threat landscape is no longer the remit of the CIO, CISO or the IT team. Cybersecurity is everybody’s job – and the C-suite is responsible for establishing and promoting an appetite for cyber-risk management across the business.

Perhaps more so than in other industries, the role of the CMO is very important here. A breach has the potential to significantly damage a brand’s reputation. Marketing’s unique role within the company means that CMOs should try to measure how cyber risks could impact the business (from image, revenue, customer attrition etc.), and importantly, use their position to promote appropriate cyber hygiene and security behavior in and out of the company.

On one hand, the exponential growth of content created online makes companies much more vulnerable to brand abuse, spoofing and impersonation. It is easier than ever to create false customer experiences, difficult to monitor and fast to reproduce. Marketing in particular must be informed and should analyze any security threats that could impact brand reputation or customer experience. CMOs need to ensure that employees involved directly and indirectly on any projects which involve brand risk includes a security assessment in each of the actions, projects and processes developed.

On the other, a digital marketing infrastructure that the CMO and their team leverages to reach customers is massively exposed to digital risk. Connected software and hardware must be constantly monitored to ensure robust security protocols, such as the front end of the website and its associated plugins – they increase the company’s attack surface and offer an opportunity for attackers to penetrate the company infrastructure. As a result of ongoing testing, a good relationship with the IT team is required to prevent, detect and mitigate potential threats in production.

Consumer-focused businesses can gain a better understanding of their threat landscape by deploying threat intelligence solutions, not only for...
detecting existing threats but also ensuring that new technologies are sufficiently secure before rolling them out. Knowing that a product or service is secure is a claim to be made by the commercial team – security itself is growing concern for both companies and buyers.

Therefore, the level of security provided by a company can positively impact their propensity to purchase (specifically online products), and CMOs should promote this if they can back up the claim.

Overall, it is critical to create a strong culture of cybersecurity within the organization. This should extend from the management team all the way down to the newest hires, with encouragement to fully understand the risks of using certain technologies.

Frequent company-wide training is encouraged, and though cybersecurity education is critical in any enterprise regardless of size, a robust risk culture in larger companies is particularly important simply because of the scale of both technology and staff.

Risk increases due to the greater probability of insider threats too, so a strong culture of risk reporting and increased interaction between departments, smoothing the flow of information, is also encouraged.
BREACH RESPONSE READINESS

Reputation is critical to retailers. A negative brand perception can have a weighty impact on the bottom line. In this regard, it should be priority to ensure a high level of breach response readiness, in order to minimize disruption in a breach situation which is all but inevitable.

Retailers should consider an action plan from the outset, with a leader who has the political capital within the organization to push through tough decisions at short notice. Scenario planning and rehearsals are also key, as well as keeping an eye on what is happening out in the market – other companies’ mistakes needn’t be your own. It also helps to make the assumption that any breach will eventually hit the public domain and be difficult to message. As such, appointing a spokesperson and preparing crisis communications plans in advance are constructive efforts. Finally, preparation should extend to building relationships with other teams that can help in the event of a breach, both inside and out of the company. These should include law enforcement, legal teams, public relations experts and threat intelligence providers that can help manage breach response.

PAYMENT SYSTEMS SECURITY MANAGEMENT

No payment system is 100% secure, and it is clear that one of the most valuable targets to cybercriminals is payment data. It is therefore critical to both businesses and consumers that payment systems are secured as far as possible, and there are a number of steps that retailers can take in order to ensure this.

Much of these mean constant review and evaluation of existing mechanisms. All payment technologies (especially those that use third parties) should be rigorously and continually monitored, with regular vulnerability scans to keep up to date with the latest security patches. Processes that keep an inventory of payment endpoints such as PoS devices are also encouraged.

It is also recommended that companies create a structure that maps out the lifecycle of transactions. By doing so, retailers can better understand both the technologies and business groups involved, and their associated risks from e-commerce platforms to call centers to accounting teams.

THIRD PARTY SECURITY MANAGEMENT

Where retailers work with third parties, steps should be taken to hold them accountable. Businesses who necessarily share customer data with external partners should push for the highest level of security, and often third-party providers number in the tens if not hundreds, depending on the size of the retailer. To help manage this, a tiered framework can help segment and assess these companies based on the level of risk they present to a business. For example, a third-party payment provider might be a tier 1, given the information they process, against a packaging
partner who might manage less valuable data and be tiered lower. In short, the trend towards decentralizing operation functions means developing and implementing a comprehensive third-party risk program is critical. It is prudent to define requirements for third-party vendors at the procurement stage, and regularly monitor whether they fulfill them. Threat intelligence modules can support with this goal, outlined in more detail below.

**EFFECTIVE FRAUD PREVENTION**

Fraud attempts by cybercriminals can find success in a number of different ways. It is not only defrauding customers of their personal information, but the retailer out of goods and with the potential to cause significant reputational damage. When it comes to customer credential theft, for example, just one good credential can open the door to an organization and cause havoc. A cybercriminal might impersonate a real customer to steal goods or execute fraudulent transactions – and the majority of the time it is the retailer who will have to assume the cost.

These kinds of attacks are usually carried out by threat actors who want a quick win from the stolen credentials. It is not common to see this from advanced threat actors, as they would use these accounts for a different purpose (reshipping, money laundering, gift card fraud etc.; see our Credential Theft Ecosystem report for detail). However, this kind of attack costs retailers and e-commerce companies a significant amount of money, which increases every year.

The faster organizations detect these compromised credentials the better. Using threat intelligence modules, if these are discovered within days of compromise (rather than the usual months) then the impact of an attack can be massively reduced.

**COMPANY-WIDE TRAINING**

Formal cybersecurity training can mitigate risk for retailers. Not only should this focus on internal security, but also on how employees manage their own personal information, BYOD, login credentials generally – constant vigilance in any scenario is key to minimizing company-wide risk.

It appears that many retailers aren’t training their employees adequately. This may be down to costs, high employee turnover, or simply resources to manage. However, establishing a dedicated function within your organization and providing regular learning opportunities should go far to developing a culture of cyber-hygiene within the organization.

On a more operational level, regular internal phishing tests to help employees better identify potential threats, combined with real-life threat scenario simulations are also positive steps that can be taken. By evaluating the results of these simulations, retailers can identify gaps and potential vulnerabilities (including among staff) and seek to plug the holes before it is too late.
THE ROLE OF THREAT INTELLIGENCE

Cybercrime – just like retail – is an industry with its own collaborative models. There are services for hire and marketplaces and information exchanges on the open and dark web, allowing cybercriminals to be agile in targeting retailers.

Attackers are constantly innovating, so defending an organization against cyberthreats means fighting a fast-moving target. Because of the sheer range of threats outlined above, it is often difficult to both prioritize them and respond effectively in a timely manner. Anticipating threats, responding to alerts or investigating incidents demand considerable resource, not to mention talent, both of which are usually in short supply across the industry.

There is a solution to this. Threat intelligence is actionable information, delivered in an automated way so that organizations can detect threats both inside and outside their network, and prioritize their responses. The reason it is so important is that it allows security teams of all sizes to focus their resources on the most crucial threats targeting their networks and infrastructure.

Threat intelligence is also extremely effective in helping identify and protect critical assets, such as customer and payment information, as well as intellectual property. It can help retailers define what is of interest to attackers, where these assets are located, and how they can be accessed. Armed with this information, security teams are able to put in place appropriate defense measures ahead of time.
THE BENEFITS OF REAL-TIME, DYNAMIC THREAT INTELLIGENCE

High quality threat intelligence helps accelerate threat and fraud detection, prioritization and incident response capabilities. By focusing scarce cybersecurity resource where it is needed most, retailers can mitigate the impact of cyberattacks and minimize their risk of future attacks and fraud attempts.

How Blueliv gathers and processes data from millions of sources in the open, deep and dark web, extracting what is relevant to you.
It is a game-changer for retailers – a new strategic weapon which obliges security teams to rethink their approach to include intelligence in their overall strategy. Real-time threat intelligence ensures that you maintain visibility of the threat landscape so that your security infrastructure is able to respond to the latest threats and fraud attempts. This includes detecting fraud and malicious activity already inside your network, analyzing it and helping your security team understand the attackers’ objectives.

Most vendors push a one-size-fits-all approach – you either buy or you don’t – and heavily featured service offerings: a manually-generated, report centric service which uses human analysts to identify specific threats.

However, fully modular and automated intelligence is available, using customer information to identify closely targeted threats. Blueliv’s modular architecture allows retailers to address individual use cases, breaking down the broad problem of external threats into more addressable projects. Automation provides speed and scale, so customers get fresh information, not aged reports.

The clear benefit of cyberthreat intelligence delivered through modules is that it works to a pay-as-you-need model. Retailers are able to select modules which are most relevant to their business and plug the gaps in their cybersecurity infrastructure. Below, Blueliv modules relevant to retailers are briefly outlined.

**CREDENTIALS**

Credentials are the gateway to your organization’s infrastructure, and it only takes one compromised password to cause havoc. This module identifies leaked, stolen and sold user credentials in real-time on the open, deep and dark web, along with information about relevant malware used to steal it. A combination of sinkholes, honeypots, crawlers and sensors are continuously searching for compromised credentials – the sooner these are identified, the sooner they can be retrieved, and the impact mitigated.

Crucially, this includes the identification of stolen credentials of customers and third parties relating to a company, i.e. individuals outside the network. Targeted threat intelligence is the only way to identify stolen login data outside your company’s perimeter. However, the threat is extremely high since hackers use stolen credentials in a majority of successful breaches. Credential detection can also mitigate the impact of fraud through account takeovers. The sector is particularly vulnerable to this fraud which can lead to false purchases and associated clean-up costs borne by the retailer.

**DOMAIN PROTECTION**

This particular module is especially important to retailers. Fraudulent domains are a risk to end customers, with the goal of stealing information and damaging your brand. Effective phishing and cybersquatting campaigns can be mitigated by proactive detection, where retailers can take effective countermeasures in time. Additionally, retailers can protect their VIPs against social engineering attacks, since they tend to be the biggest targets.

Protecting domains also means monitoring unauthorized sellers. Most brands can sell through multiple retail channels both off an online. If products are being sold on massive online marketplaces a company might
not even see this brand abuse. Threat intelligence can help.

**CREDIT CARDS**

Dig deep enough and you can find all sorts of credit card data online. This module can dramatically reduce losses from theft and fraud of credit and store cards. Our unique methodology retrieves stolen credit card data and provides necessary information to help organizations mitigate the damage. Crucially for retailers, we can also identify compromised PoS devices, protecting end clients by detecting infected endpoints.

**MALWARE**

As outlined above, malware attacks are increasingly sophisticated, targeted and much harder to detect than before. This module allows you to detect malware seeking to steal sensitive information or commit fraud, including those which are successfully targeting other companies in the retail sector.

**SOCIAL MEDIA**

Retailers should ensure that trust in their brand remains high. Social media and search engine monitoring of an organization’s digital footprint helps find websites not authorized to use your brand, logos, assets claiming partnership affiliation assets and more, so proactive steps can be taken to shut them down.

**DATA LEAKAGE**

The larger the organization and the more third parties it engages, the greater risk it has to manage. This module monitors whether an organization’s sensitive documents have been leaked on the internet, deep web or P2P networks, intentionally or otherwise.

**HACKTIVISM**

By monitoring global hacktivism activity on social networks, the open and dark web, retailers can protect their infrastructure before a potential attack happens. Using an advanced early-warning system and active geolocator, the module generates targeted threat intelligence to shield against potential attack vectors.

**MOBILE APPS**

As more retailers create new digital platforms to engage with clients, cybercriminals are busy creating malicious and illegal applications, hiding in plain sight in non-official marketplaces. They lure away customers and steal valuable data, with the potential to have a significant negative impact. This module specializes in detecting applications claiming affiliation to retailers or using company assets without authorization, to protect both brand and reputation.

**DARK WEB**

Retailers of any size should seek to boost their awareness of what’s going on in the underground, observe malicious activities targeting their organization and proactively prevent future attacks. This module delivers a serious advantage to security teams by putting a spy in the enemy’s camp: retailers become better informed about criminals targeting their organization and customers, can proactively prepare countermeasures, and find already-compromised data before the impact is too severe.
CONCLUSIONS

This whitepaper has sought to highlight the challenges that retailers face. Many are fighting an uphill battle. Staying competitive in today’s marketplace means new technology initiatives are being rolled out on tight timelines and tighter budgets, and cybersecurity isn’t baked in from the outset as it should be. In retail in particular, all data held should be viewed a strategic asset to the company, from customer information to product IP. In doing so, retailers recognize that this makes the data immensely valuable targets to cybercriminals, who pose a huge risk to business in the event of an attack or fraud attempt.

Ultimately it all comes down to making the right investments. Retailers need to try and stay one step ahead of their attackers. Innovation within the company and collaboration with external suppliers helps assess and strengthen cyber resilience in critical areas. Blueliv has been working with very well-known retailers for many years, building a deep understanding of their strategic cybersecurity needs and the industry-specific threats they face. Modular, pay-as-you-need cyberthreat intelligence provides a robust platform with which to complement retailers’ existing cybersecurity setups, whatever the size of the organization.

In sum, proactive fraud detection and threat monitoring through threat intelligence should be supplemented by a process of continuous cyber-hygiene within the organization. This can help prevent attacks, as well as mitigate their impact when one happens.

Using intelligence, features dedicated to CVEs, for example, provide security teams with continuously updated and intuitive information to quickly add context to disclosed vulnerabilities that could be affecting other retailers. The massive Magecart breaches are a good example of this – understanding the relationships among these CVEs and entities is crucial to correlate them efficiently with tools, actors and TTPs. Often actors use various types of tools and techniques to profit from vulnerabilities and succeed in an attack; by correlating CVEs with campaigns and other indicators, real-time, dynamic intelligence can aid actor attribution and resultingly, threat prioritization.

When it comes to fraud detection, intelligence can provide real-time notifications for credentials and stolen credit or gift cards. The market generally is mainly focused around detecting and retrieving cards that have been leaked or dumped on darknet sites or underground forums. At this stage, it is often too late to prevent fraud from occurring. However, Blueliv’s crawlers, honeypots and other proprietary techniques enable its customers to often intercept cards before they are sold on the black market and therefore reduce this risk of fraud. Another unique differentiator offered by Blueliv is also the provision of information around compromised PoS devices, the most common source of compromise.

The bad guys are constantly testing new ways to exploit your infrastructure, so remaining static when it comes to your security protocols is a sure-fire way to get breached. This includes performing periodic internal security reviews, red-teaming, and an ongoing process of education among all employees.

By setting the right tone for cybersecurity within the organization, retailers can drive awareness on everyone’s responsibility to help mitigate cyber-risk. More and more we are seeing retailers of all sizes pursue cybersecurity policies to help them become more resilient. In fact, investing in tools to mitigate cyber-risk can actually start to be seen as a brand differentiator. Retailers can build a reputation for consumer protection and transparency about how customer data is used, and the steps which they take to defend against cybercrime.
REFERENCES

About Blueliv

Blueliv is Europe’s leading cyberthreat intelligence provider, headquartered in Barcelona, Spain. We look beyond your perimeter, scouring the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to protect the enterprise and manage your digital risk. Covering the broadest range of threats on the market, a pay-as-you-need modular architecture means customers receive streamlined, cost-effective intelligence delivered in real-time, backed by our world-class in-house analyst team. Intelligence modules are scalable, easy to deploy and easy to use, maximizing security resource while accelerating threat detection, incident response performance and forensic investigations. Blueliv is recognized across the industry by analysts including Gartner and Forrester, and has earned multiple awards for its technology and services including ‘Security Company of the Year 2019’ by Red Seguridad, Enterprise Security and Enterprise Threat Detection 2018 category winners by Computing.co.uk, in addition to holding affiliate membership of FS-ISAC for several years.