ESET INDUSTRY REPORT ON RETAIL:

Evolving threats to data and payments

TABLE OF CONTENTS

1 Introduction: Retail and the evolving threats to data and payments
3 - 4

2 E-commerce cybercrime: Treasure troves of credit cards for the taking
5 - 7

3 IIStealer: Jeopardizing the trust relationship between online sellers and buyers
8 - 10

4 Regulatory radar: Data protection and payment card standards
11 - 13

5 Take a deeper look at server security solutions
14

1

RETAIL AND THE EVOLVING THREATS TO DATA AND PAYMENTS

Brent McCarty
President
ESET North America

Under pressure from threats and technology adoption, retail evolves

In early spring 2020, buyers and sellers worldwide witnessed a decade of bullish retail growth collide with an unknown spectre: SARS-CoV-2, or COVID-19. Not since the Spanish flu have retail markets and consumer habits been so impacted by a virus that it changed behaviors at home, at work, on the street, and in stores. But this virus, in our time, also impacted the virtual marketplace and, even amid this transformative era of digitalization, has changed both the online environment and our online behaviors.

Several questions might be asked: What do these disruptions to the retail industry communicate about the current level of digitalization? Are the efficiencies created via digitalization robust? How should retailers balance opportunity and risk vectoring from IT infrastructure and e-commerce? And can cybersecurity help make or break our understanding of the retail industry's evolution?

By examining the linked online behaviors of customers, vendors, marketers, suppliers, and payment processors as a cross section of the retail industry, we can freshen our understanding of the threats in this new dynamic. In other words, considering the retail industry's quest to survive and thrive, which cybersecurity risks have grown and which have newly opened under retailers' feet? This report will aim to show how cybercriminals have evolved to better position themselves in the new retail landscape.

Transformation in the office...

In many locations, 2021 saw some concrete relief from the worst business impacts of the pandemic: Many shops, restaurants, and hotels reopened. However, the return to in-person work, dining, education, and shopping hung precariously in the balance.

Massive credit is due to public health officials and medical researchers who've been able to increase our understanding of the risks to public life. However, what's also changed is that a host of popular digital solutions, which in 2020 were just poised to have their moment, have now been battle-tested. These have enabled many business and retail services to be recast and return in a new guise. The majority of "us" see the evidence for this in the back office where, whether as a corporate employee or an entrepreneur, much of business moves via *Microsoft Teams* and *Zoom calls*, productivity and collaboration tools like *Microsoft Exchange*, and a host of managed services via Kaseya, for example, all of which have gone from popular to ubiquitous. But these business technologies have brought with them their own risks.

Among the leading business platforms are Microsoft Exchange for email services and Kaseya VSA for IT management, both of which *were targeted in early 2021*, with the consequences still being felt globally. These interruptions impacted the continuity of a variety of businesses — including enterprise retailers — with ESET and the wider security industry documenting the subsequent impacts, including ransomware, data exfiltration, and other interruptions.

To read more broadly about the impact from these large-scale attacks, find resources *here*, make a deep dive into *ransomware here*, or survey the threatscape in our *T2 Threat Report here*.

... and at the till

In parallel with an evolved threatscape impacting retailers' back offices, matters have evolved at the storefront too. With the massive uptick in online retail, direct sales, transport, and food delivery, unique challenges are driving the retail industry's exposure to risks via marketing, sales, and payments, along with the storefront IT environment and its associated tools, practices, and processes. The cybersecurity scene in 2021 demonstrated significant impacts on companies as large as enterprises and down to small entrepreneurial businesses, with customer databases, point-of-sale (POS) terminals, marketing automation tools, web search optimization tools, as well as payment processing platforms and services being at the sharp end of the spear of novel forms of credit and debit card fraud and data theft. To underscore the risks, many retailers were caught up in the January 2021 *Kaseya supply chain attack*, including leading Swedish supermarket Coop.

New tech, same focus on security

While retailers big and small have adopted new tech or further entrenched themselves in ever-maturing business platforms, risks are still mounting. What follows in this report largely pertains to risks facing software and IT infrastructure from malicious actors. However, another critical area will be explored as well — risks that relate to processes, technology usage, and platform administration.

Although we will look at data protection regulations later, here it is enough to say that while security software plays a large role in helping guard databases and their access, applying best practices and proper configuration are key too. This is especially important to handle the case of disgruntled *employees* — especially *IT admins — who can unleash a heap of pain* on a retail business. To be concrete, large businesses have deployed products like HubSpot, Adobe Campaign, or Eloqua to manage massive databases used in marketing campaigns and for lead tracking. But these tools, which are complex in their own right, both secure opportunities and broaden risks. Due diligence with their use should not just be about the deployment of security software, but also system hardening along with a deep look at the configuration literature, such as what Oracle has published for *Eloqua administrators*.

With the stakes so high in 2022, and risks vectoring from inside and out — employees, software both used and neglected — cybersecurity ultimately becomes a means of securing opportunity. Think of the opportunities presented by Christmas, Black Friday, or Boxing Day. It is for, and on, these days that we see both brick-and-mortar shops and online stores seeking to further leverage the transformed retail landscape with tech. But these also mean that more players along the value chain are now invested in the "general" digital business solutions mentioned above, and increasingly in newer layers of technology that connect retail-oriented businesses to their customers and enable the exchange of goods and services.

Let's look at the cybersecurity implications of some of these technologies.

2

E-COMMERCE CYBERCRIME: TREASURE TROVES OF CREDIT CARDS FOR THE TAKING

Martin Kováč
Director of Global Digital Business

Handling payments online necessitates exposing money to the Wild West of the internet with all its rogue cyberbandits and dangers.

Where there is money, there are crooks

Even before the pandemic, innovations in payment technology were driving e-commerce on an upward trend. From payment apps to digital wallets and website plugins, the e-commerce era has opened new digital channels for cybercriminal gangs to steal money, as the expansion of new technologies to support e-commerce has not always been accompanied by the most secure practices. Pandemic-induced lockdowns have accelerated this expansion in many cases.

At the same time, cybercriminals motivated by financial gain have been hunting in every nook and cranny of e-commerce systems for any weakness that might open a door to the spoils. Handling payments online necessitates exposing money to the Wild West of the internet with all its rogue cyberbandits and dangers.

These crooks are especially a threat to online retailers by going after account credentials, credit and debit card details, and customer information. Yet retailers that accept card payments in store via point-of-sale (POS) software are no less at risk. POS software often runs on computers that are connected to the internet with insecure configurations. So, although there has been a shift from targeting brick-and-mortar businesses to e-commerce websites, the threat against POS systems remains alive and instructive of the same lessons for all retail businesses. Therefore, before turning to the threats facing e-commerce systems today, let's take a brief look at POS malware.

A shifting threat landscape: From POS to e-commerce malware

With the growth of the credit card market, POS software increasingly took its place in the front seat of handling payments for retail businesses. But, as is often the case with the introduction of new technologies, secure practices were something of an afterthought. With the large-scale *attacks* on the POS systems of Target in 2013 and Home Depot in 2014, the industry finally seemed to be shaken enough to want to improve the security practices of retailers, and so a lot of good work was done thereafter to secure POS systems. However, fast-forward to 2021, and the Coop supermarket chain in Sweden *closed 500 stores* in the wake of the Kaseya ransomware attack that crippled the systems of a service provider higher up the supply chain, thus disrupting the functioning of some of Coop's POS systems. Securing payment software along with the entire software supply chain is an enduring need.

In the cases of Target and Home Depot, the deployment of the malware to POS systems happened through the compromise of third-party access to the retailers' networks. These breaches showed the need for more robust authentication practices, like *multifactor authentication*, that would have made the stolen credentials less useful. They also showed how network segmentation would have stopped the attacker pivoting from a less sensitive area to one with more valuable information, such as where a POS system resides.

The Coop case was a disruption of payment services triggered by the exploitation of a vulnerable IT management tool — Kaseya VSA — used by a service provider that Coop's POS systems depended on. Nothing can be done to prevent such disruptions, except to provision all IT services and management in-house. In other cases, it is critical to have very fast patching practices in place (although that would not have helped in the case of Kaseya VSA, as a patch was still being developed) and to consider having an endpoint detection and response solution like *ESET Enterprise Inspector* that can detect the earliest signs of an attack.

Aside from these well-known attacks in the history of POS system security, other threats are ever present. For example, in 2020, ESET researchers discovered *ModPipe*, a backdoor that can access sensitive information stored in devices running a specific POS management software suite from Oracle, which is used by hundreds of thousands of bars, restaurants, hotels, and other hospitality establishments worldwide. The best security practices are to have multi-layered endpoint protection, such as *ESET Endpoint Security*, that can detect malware like ModPipe, and to ensure all devices are always running with updated operating systems and software.

Indeed, it may come as a surprise that in 2021 some retail businesses still use unsupported operating systems, like *one premier golf club* in the UK that was using Windows XP, which reached its end of life in 2014, and running POS software on it. With all the financial and sensitive data being run through this device, it would make for a very dangerous outcome if it were targeted, including the potential for *huge consequences under GDPR*.

From the point of view of regulation, the year 2021 brought added pressure on U.S. fuel retailers with the imposition of the *EMV liability shift* for Automated Fuel Dispensers (pumps) on April 17. With this mandate, which has been in rollout since 2015, the big credit card companies American Express, Discover, Mastercard, and Visa have placed the burden of credit card fraud on retailers that continue to accept card payments via swipe of the *magnetic stripe* instead of insertion or tap of the EMV chip and PIN.

While regulation is playing catch-up to reflect the increased security offered by the use of the EMV chip, technologies like Apple Pay and Google Pay have forged ahead with new innovations in payment security. When using these services, merchants don't receive actual credit card numbers; instead, virtual account numbers are generated for every payment. This has made Apple Pay and Google Pay *even safer options* than an actual credit card with an EMV chip and PIN.

An e-commerce shakedown

Returning to e-commerce, we can see a similar industry-shaking experience as that of the Target and Home Depot breaches when in 2018 we heard about the skimming of hundreds of thousands of payment card records from the *Ticketmaster UK* and *British Airways* websites. These websites were among the first in a long chain to fall prey to a variety of very crafty payment card-stealing malware.

A common modus operandi of card-stealing crooks is to inject into legitimate websites scripts that can steal the payment data of website customers as they are paying for their goods. In 2020, a cybercriminal group known as Keeper compromised the websites of *more than 570 businesses* in 55 countries around the world. In another 2020 campaign, one of the Magecart gangs victimized *more than 2,800 online stores* running on Magento, a popular e-commerce platform, with web-skimming malware.

Considering the need for many businesses to turn to e-commerce as a result of the pandemic and the increase in online purchases by consumers, online revenues have naturally increased in tandem. Shopify, another popular platform for creating online stores, almost *doubled its revenues* in the second quarter of 2020. According to an *analysis* by Deloitte, this surge is in part due to consumers' willingness to pay more for the conveniences offered by online buying in a pandemic world. Thus, businesses that increase their e-commerce capabilities are strategically teeing themselves up to drive the most competitive advantage in the market. The catch? Such high levels of potential money flow also act as strong magnets for financially motivated criminals.

IIStealer: Snatching e-commerce transaction data

A multitude of tricks and tools to swipe credit and debit card data via e-commerce websites have been spotted in the past few years. Card-stealing malware has been found hidden in *CSS files*, *social media sharing icons*, and even *favicon metadata*. However, despite the ingenuity demonstrated by malicious actors, many buyers and businesses still fail to realize the significance of these threats. Until they see unauthorized transactions on their credit card bills, as the credit card holders, or they discover security anomalies on corporate servers, as the IT administrators, many instances of online credit card theft will likely go completely unnoticed. This is precisely the danger with *IIStealer*, one of the sneakiest examples of credit card-stealing malware to compromise e-commerce servers.

IIStealer, which was discovered by ESET researchers, monitors website visitor traffic for HTTP POST requests to check out and pay for items. The malware saves the information from these requests (e.g., credit card details) into a log file for later exfiltration from the compromised server. Meanwhile, the website continues generating HTTP replies so that shoppers pay for items as expected.

To exfiltrate the saved data, the malicious operators send the compromised server a specially crafted HTTP request that signals IIStealer to embed the collected data in the HTTP response to that request. Using HTTP, IIStealer swipes any credit card data shared by website visitors, leaving IT admins with little opportunity to suspect something is amiss. This subterfuge of disguising the stolen data within legitimate website traffic is not uncommon. A trick used by other malware is to *hide the data to be exfiltrated in .JPG files*, creating the appearance that nothing more than images are being downloaded from the website.

If a website uses HTTPS — remember the *padlock* in the browser address bar? — to protect website traffic with SSL/TLS encryption, this would provide no help against IIStealer, as it waits for requests to be decrypted on the server side before logging information from them.

From the point of view of customers, there is often no way of knowing whether the e-commerce website they are shopping on is afflicted by server-side malware such as IIStealer. Instead of allowing a website that hasn't built a reputation for security to handle payment data, a better option is to use a trusted third-party payment gateway.

From a business's point of view, protecting visitors' payment information should be paramount. This can be done by integrating a payment gateway into their e-commerce websites. Popular choices include PayPal, Apple Pay, Google Pay, Amazon Pay, and Alipay, among *others*.

Vulnerabilities and phishing aplenty

Using one of these payment services, however, does not entirely remove the threat of theft so much as it shifts the playing field. Cybercriminals are just as cognizant of the reputation enjoyed by some payment services, meaning that the most popular brands are often abused as a guise for malicious campaigns. For this reason, merchants and customers alike should be aware of a number of *frauds* and *impersonation* tactics to swindle them out of their funds.

A common threat to both buyers and sellers is phishing, with *one of the most spoofed brands* being PayPal. Whether the phishing starts with an email or an *SMS text message* posing as a popular payment service and claiming that there was "unusual activity on your account," the best policy is to not click on any links and to contact service providers directly to verify the provenance of the message.

Merchants should also be aware of the ever-present plague of vulnerabilities that can affect their chosen e-commerce plugin. In 2020, attackers exploited *security flaws in WooCommerce* (a popular WordPress plugin and e-commerce engine for websites), enabling them to scan for other WordPress targets and to connect to the website's database and query it for WooCommerce-related data, such as the total number of orders and payments.

Server security tips

Having considered some of the threats facing e-commerce today, here we offer a few more tips to help protect your e-commerce server:

- Use dedicated accounts with *strong, unique passwords* for the administration of the server.
- Require *multifactor authentication* on all administrative and more privileged accounts as an extra protection step.
- Regularly update the server's operating system and applications, and carefully consider which services are exposed to the internet to reduce the risk of server exploitation.
- Protect customer data at rest with *encryption* so as to render it useless to thieves.
- Consider using a web application firewall, as well as a security solution such as *ESET Server Security*, on your server.

3

IISTEALER: JEOPARDIZING THE TRUST RELATIONSHIP BETWEEN ONLINE SELLERS AND BUYERS

Zuzana Hromcová
Malware Researcher

Unfortunately, the good behaviors of internet users to avoid suspicious websites and to verify that websites are protected with SSL/TLS encryption provide no help in avoiding IIStealer.

One of the unique threats mentioned in this report is IIStealer. Although Martin Kováč highlighted the deceptive nature of this malware, an important implication that needs to be spelled out here is the immediate and universal access to data granted by compromising a server. IIStealer is a malicious extension for Internet Information Services (IIS), which is Microsoft's web server software. Thus, all the network communication flowing through a server running IIS and infested by IIStealer is open to the purview of the attackers, including passwords, usernames, and payment information from e-commerce transactions.

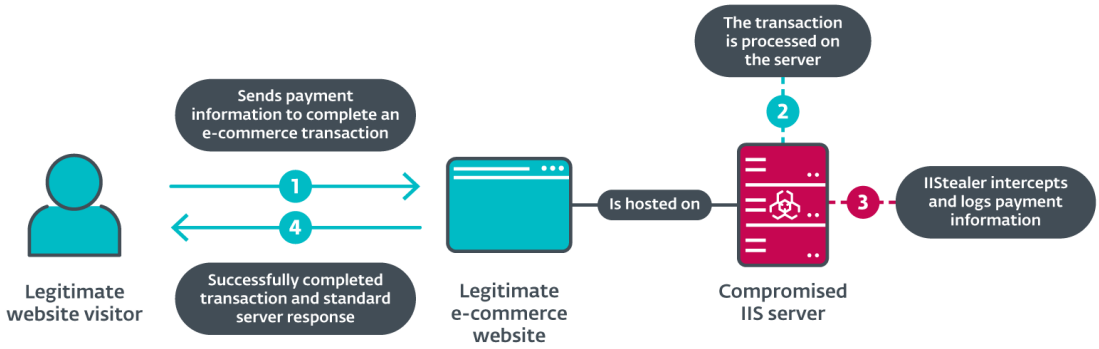
Unfortunately, the good behaviors of internet users to avoid suspicious websites and to verify that websites are protected with SSL/TLS encryption provide no help in avoiding IIStealer. Even if the e-commerce website is trusted and the communication channel is secure, from the perspective of website visitors there is no way of knowing the security state of the servers hosting the websites they are visiting. Yet that is where their data are processed and, unbeknownst to them, pilfered. One question that might arise then is, "How real is the threat of IIStealer?"

Real-world use of IIStealer

ESET telemetry reveals that IIStealer was active in the U.S. between September 2020 and January 2021, and that it targeted e-commerce websites. The samples of IIStealer that we analyzed looked for checkout and payment page URIs that were hardcoded, meaning they appear to have been tailored for specific e-commerce websites. Of course, IIStealer can target e-commerce websites in other countries as well, but we did not observe this, having only limited visibility into IIS servers via ESET telemetry. This limitation is partly due to the fact that it is still common for businesses to not protect their servers with security software.

As the figure below demonstrates, website visitor traffic that requests checkout and payment pages is intercepted and logged by IIStealer. The adversary can then contact the server by sending a special request to the e-commerce website—IIStealer will intercept this request and modify the server response by adding the payment information collected from the customers.

IIStealer: data interception



IIStealer: data exfiltration

Mitigation tips

The threat of IIStealer puts the trust relationship that should exist between sellers (the servers) and buyers (website visitors) into jeopardy, unless IIS server administrators can educate themselves on and adhere to best security practices. For this reason, IIS server admins are advised to:

- Only install native IIS modules from trusted sources.
- Regularly check:
  - the `%windir%\system32\inetsrv\config\ApplicationHost.config` file,
  - the `%windir%\system32\inetsrv\` folder, and
  - the `%windir%\SysWOW64\inetsrv\` folder

  to verify that all the installed native IIS modules are legitimate. In other words, verify that they are signed by a trusted provider or installed on purpose.
- Notify all parties involved in the case of a successful breach so that they can react quickly.
- Read the full white paper on IIS malware, *Anatomy of Native IIS Malware*.

Although the burden of handling IIS threats lies squarely on the shoulders of IIS server admins, web developers can limit the damage with the following tips:

- Do not send the password to the server, even over SSL/TLS.
- Instead, use a protocol such as *Secure Remote Password (SRP)* to authenticate users. This protocol removes the need for an unencrypted password to be transmitted to the server. It also removes the need to rely on server-side hashing, as IIStealer can still use the hash to reauthenticate.
- To handle payment transactions, use the services of payment gateways by trusted third-party providers, to avoid processing the sensitive payment information on your server.

Finally, for website visitors, the following tips can help reduce the impacts caused by having your payment card details stolen:

- *Keep an eye on your credit statement* for small or unusual payments: Often small amounts are processed to test whether the cards are valid.
- If you spot something unusual, notify your bank immediately.

Podcast on IIS malware

If you'd like to hear more about IIS malware, subscribe to the ESET Research podcast on any of the popular podcast applications, including *Spotify*, *Google Podcasts*, *Apple Podcasts*, and *PodBean*.

4

REGULATORY RADAR: DATA PROTECTION AND PAYMENT CARD STANDARDS

Tony Anscombe
Chief Security Evangelist

Securing the retail industry's IT infrastructure, which includes payment systems, entails a host of complex technical challenges. Some pertain to direct risks to technology, for example, to software both embedded and at the application layer. Others pertain to secondary, but still serious, risks related to the technical implementation of industry standards and regulatory obligations.

Back in 2004, to protect data and reduce the risk of fraud, the payment card industry created a set of standards known as the *Payment Card Industry Data Security Standard* (PCI DSS). Merchants that accept payments via a credit card or a debit card, where the transaction is processed through the credit card payment system, are required by the major credit card providers to comply with this standard. In addition, merchants are also required to meet a minimum level of security when they store, process, and transmit cardholder data. PCI DSS has been adopted across the globe, and since 2006 has been governed by the Payment Card Industry Security Council.

Fifteen years later we can see that the PCI DSS and privacy legislation such as the European Union's General Data Protection Regulation (GDPR) display many similarities in regard to payment card data. Some privacy legislation could even be viewed as including the PCI DSS.

GDPR, for example, has specific requirements covering payment card data. In a way, this promotes the PCI DSS from being merely an industry standard to one mandated by legislation. However, this also means that while in some territories the PCI DSS is effectively a piece of legislation accompanied by penalties and the oversight of regulators, in other territories it remains the responsibility of industry to regulate its own standards, with payment processing powerhouses such as Visa and Mastercard potentially imposing fines for non-compliance. This becomes more complex in some territories, for example in the United States, where PCI DSS is not required by federal law, though some states have legislated it or equivalent provisions. If in doubt about these legislation requirements, it is recommended that you seek professional legal advice.

PCI DSS provides guidance on cybersecurity for six control objectives:

1. Build and maintain a secure network and systems
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

*Full PCI Security Standards *Here*

When compared with some privacy legislation, such as the *California Consumer Privacy Act* (CCPA), PCI DSS offers very specific guidance on the need for "reasonable cybersecurity."

*An updated *PCI DSS (4.0) is due in March 2022*

Diverting transactions or data for ransom — well, both!

Security risks to personal data, especially when processed and/or stored at scale by businesses and institutions, already triggered a torrent of malicious activity targeting retail well prior to the pandemic. As of late, this has been compounded by the change in the modus operandi of ransomware attacks where data is exfiltrated by the attacker prior to the malicious activation of the malware that denies a company access to its systems and data.

Need more detail on ransomware?

See our 2021 white paper

Looking further, both personal data and privacy received another boon of attention when the World Health Organization formally raised COVID-19 to the world's attention on January 9, 2020. Soon thereafter, much of the world became extremely reliant on digital infrastructure, with remote working, home schooling, and online retail dominating our lives. And as the pandemic progressed, technology became paramount for vaccine rollout, initiating strategies to record and manage testing, track virus transmission rates, and, more recently, issue vaccine passports. This creates a host of data and privacy concerns for both governments and businesses globally.

Sitting on the other side of the fence, cybercriminals, chasing both data and revenue, have rapidly deployed new approaches to undermine *COVID-19 relief efforts*, and to extract more from the retail sector too.

There are significant parallels between the malicious tactics on display when leveraging COVID-19 in malicious campaigns and targeting retail. This in large part tracks to the fact that the criminal actors involved have a complete skill set to conduct phishing campaigns, SIM swapping scams, ransomware attacks, and man-in-the-middle attacks (to steal credit card/transaction data), just to name a few. With respect to COVID-19, *December 2020 saw a number of novel scams* offering the sale of masks, tests, and "cures" on social media, and leveraging social engineering to scare users into buying or sharing personal information. By the summer of 2021, criminal efforts evolved to the point of even *spoofing vaccination passport apps* to access personal data. Critically, the *skill set deployed against COVID-19-related targets of opportunity are entirely relevant to targeting consumers and businesses* in various retail processes.

The very data that is so critical to retailers' digital marketing and sales efforts is also a source of risk. How? Via the fact that all these digital activities have expanded regulatory and compliance risks that impact both e-commerce sellers and brick-and-mortar retailers via the improved digital efficiencies sought with partners, suppliers, staff, and the digitalization of transactions.

What COVID-19 demonstrated about digitalization of retail

While GDPR and other privacy-driven regulations like CCPA in the U.S. had pushed businesses globally to meet a basic level of data protection and clients to demand it, COVID-19 accelerated retailers' precipitous dive into e-commerce.

The massive jump in scale of digital activities triggered by the pandemic, including retail, has thrown out any notion of a maturation of process. Instead, the conversion to e-friendly business approaches has moved well beyond data protection regulations compliance and has introduced vast numbers of businesses to the intense threat environment that has always hovered over retailers' pursuit of digital opportunity.

New (to you) tech brings risks and scope for poor practice

The many tools used to support e-commerce offer at least three attractive targets for digital threats. The first, poor or malicious practices by employees responsible for maintaining sales and marketing platforms and databases. The second, poor configuration of and vulnerabilities in software on network, endpoint, and point-of-sale devices — all of which support today's IT-intensive retail environment.

And lastly, a rising number of transactions, where, for example, we see *projected retail sales amounting to around 26.7 trillion U.S. dollars globally* by 2022. *Retail sales in the U.S. alone* are projected to reach 5.23 trillion U.S. dollars by 2022. These hefty sums clearly attract the attention of malicious actors, and thus it is no surprise to see the retail sector featured among the top five industries targeted in 2020 in IBM's *X-Force Threat Intelligence Index*.

With increasing threats and risks to customer data coupled to complex legislation and standards requirements, it is important that businesses take the security of consumer data, whether payment card transactions or stored customer data, very seriously. Failing to do so weakens consumer confidence and could bring a regulator to your door.

U.S. privacy regulations and evolving cybersecurity laws

Following the EU's enactment of GDPR in 2018, implementation of data privacy regulations also began to gain pace at the state government level in the U.S.. Legislators in California passed the *California Consumer Privacy Act* (CCPA) in 2018, which has been implemented since 2020. At the end of 2020, California's Proposition 24 was passed, meaning the *California Privacy Rights Act* (CPRA) will become effective in 2023. The CPRA makes significant additions to the CCPA — which itself could be seen

as falling short of GDPR in some areas, although in others it went further. These additions include:

- the concept of household data in addition to merely individual data, as emphasized in the GDPR;
- extending protection to California residents even when outside the state for temporary or transitory purposes;
- the right to opt out of the sale or sharing of personal data to third parties. Companies must include a "Do Not Sell or Share My Personal Information" link on website home pages.

While similar protections exist under the GDPR, they are less clear — a data subject needs to opt out of marketing purposes and additionally withdraw consent for processing activities.

With broad agreement on the need for federal consumer privacy legislation realized in the *Consumer Online Privacy Rights Act* (COPRA) in December 2019 and the Biden administration's apparent recognition of the need for federal privacy legislation, we will likely see a host of initiatives. Indeed, Vice President Kamala Harris has a strong record in privacy enforcement, as witnessed by the amended and strengthened *California Online Privacy Protection Act* (CalOPPA) during Harris's time as California's state attorney general. Also, several Obama-era staffers who contributed to the consumer bill are back in the driver's seat.

As the pandemic continues, there will likely be considerable focus on healthcare providers and agencies that have been party to contact tracing, testing, and vaccination. Currently, some of the processes for collection of personal data may not be as scrutinized due to urgency and medical need. It should be expected, however, that this latitude will likely be removed and the cybersecurity requirements for such data will be strengthened and enforced.

This is also true globally, where the internet creates an environment that breaks down international barriers, given that everything is accessible in the same cloud. Privacy legislation is not a set-and-done process; it is an evolving process that is likely to require continual modification, especially when considering new technologies such as artificial intelligence, the Internet of Things, and other advancements in technology. This demonstrates that there is a need for standardization and harmonization both within and among states, countries, and continents across the globe. All consumers should be awarded the same data privacy rights by companies and organizations regardless of their location.

Privacy legislation is undoubtedly a topic that will remain a priority for legislators and an enduring concern for businesses in 2022. As such, readers should keep in mind that both the opportunities and efficiencies brought to bear by the technologies mentioned in this report and beyond demand enhanced respect for security practice and adequate investment, as well as ongoing engagement in the dialogue around business standards and regulatory burdens.

5

TAKE A DEEPER LOOK AT SERVER SECURITY SOLUTIONS

A server security solution is designed to protect the central servers of an organization from threats.

Companies nowadays allow employees to save files to company network shares, yet often without adequately protecting their network shares from malicious files. A single employee saving a malicious file to a network drive can instantly cause a cascade effect that renders your organization's files inaccessible.

Alternatively, many websites are hosted on servers that do not have any security software to protect them. Servers are typically a more sought-after target due to them containing or processing sensitive data, such as payment card details and passwords.

Unfortunately, retailers have large and growing threat surfaces to contend with, and need to prioritize prevention, defense, and remediation at all times. This is due both to the increase of regulatory burdens and the need to automate marketing, the online shopping experience, as well as the logistics around delivery.

Thus, when an attack or data breach occurs, organizations are typically surprised that their defenses were compromised or are completely unaware that the attack even happened. After the attack is finally discovered, organizations then reactively implement mitigations to stop this attack from being repeated.

Taking a proactive approach by installing a server security solution turns the tables on these flawed paradigms. *ESET Server Security* provides advanced protection to all general servers, web servers, network file storage, and multipurpose servers. It pays special attention to ensure the servers remain stable and conflict-free to keep maintenance windows and restarts at a minimum level in order to not disrupt business continuity.

ESET Server Security also supports ESET's *cloud sandbox* and *endpoint detection and response* technologies, meaning that companies can build robust, multi-layered endpoint defenses that span the prevent, detect, and respond phases of your security model.

ABOUT ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit **www.eset.com** or follow us on **LinkedIn**, **Facebook**, and **Twitter**.

Contributing Editors:

James Shepperd, ESET Content Manager
Rene Holt, ESET PR Writer II

Additional contributions from:

ESET Creative Studio