AN OFFERING FROM BDO'S CYBERSECURITY PRACTICE

BDO CYBER THREAT INSIGHTS

2019 1st Quarter Report

SPECIAL FOCUS:
RECENT CYBER EVENTS IN THE RETAIL & CONSUMER PRODUCTS INDUSTRY

BDO

In this issue

PREFACE 1

THE RISE OF CYBER-ATTACKS IN THE RETAIL INDUSTRY 2

Prominent Cyber-Attacks & Threats to the Retail Industry 4

SPECIAL FOCUS: RETAIL & CONSUMER PRODUCTS DIGITAL TRANSFORMATION AND THREAT-BASED CYBERSECURITY WILL HELP MID-MARKET RETAILERS THRIVE 7

Middle-Market Retail Thrivers: Where Digital Comes into Play 8
Leveraging Digital Transformation to Thrive 9
Managing Growing Risk in Tandem with Increased Innovation and Cybersecurity 10

NOTABLE ATTACKS 11

Clothing Retailer Kathmandu Investigating Possible Customer Data Breach 11
Online Electronics Retailer Newegg Hit by Megacart Hackers Group 11
Macy's and Bloomingdale's Breach 11
Walmart Jewelry Partner Exposes Personal Data of 1.3M Customers Because of Misconfigured Database 11
Under Armour's Nutrition App MyFitnessPal Breach Compromises Data of 150M Individuals 12
Adidas Breach Exposes Online Customers' Personal Data 12
SHEIN Fashion Retailer Breach 12
U.K. Retailer 'Superdrug' Breached, 20K Customers' Data Held for Ransom 12
23K Fortnum & Mason Customers' Personal Data Exposed 13
Norwegian Cloud Service Firm Visma Hacked by Chinese Group APT10 13

BDO CYBER THREAT INTELLIGENCE (CTI) SERVICES 14

Threat Intelligence – "Proactive Detection of a Breach" 14
How does it work? 14

BDO CYBERSECURITY SERVICES 16

CYBERSECURITY LEADERSHIP TEAM 17

Preface

Make no mistake, the retail and consumer products industry is facing increasing number of sophisticated cyber-attacks from nation-state cyber-attackers, criminal cyber-attack-groups, and politically and socially motivated hackers, often planning, coordinating, and implementing cyber-attacks in an integrated manner on a national, multi-national, or global level.

Unfortunately, the global retail industry has not made sufficient investments in their cybersecurity policies, plans, procedures, and methods of defense, especially with their respective supply chain partners. As a result, the average cost of a cyber data breach in the retail industry continues to climb every year and so does the average cost of cyber liability insurance coverage.

Further, more and more companies are facing major lawsuits from their own shareholders, consumer protection groups, and federal and/or state government agencies for their negligence in providing an adequate information security program for their organization, often resulting in significant financial losses and negative impacts to their brand's reputation.

This issue of our BDO Cyber Threat Insights Report is entirely focused on the growing cyber threats to the global retail industry. The cyber-attacks on the global retail industry affect every consumer worldwide via: increasing prices of products or services, the potential compromise of personal identifiable information (PII), the potential theft of their personal credit information (PCI), the potential theft of their identity, the possible theft or loss of products once purchased, the potential loss of value of stock or other investments made in the retail industry, all as a result of cyber data breaches, cyber scams, and business email compromises.

Our BDO Cyber Threat Intelligence (CTI) team brings together top information security experts from the U.S. and Israel with extensive information technology and cybersecurity experience from the military, intelligence, law enforcement, public, and private sectors to assist our clients in understanding both the constantly changing cyber threat landscape and the complex cybersecurity regulatory environment to make well-informed business decisions on how best to invest in cybersecurity and data privacy.

We hope you will find this issue of our BDO Cyber Threat Insights Report to be both interesting and of value to your organization.

Regards,

GREGORY A. GARRETT, CISSP, CPCM, PMP
Head of U.S. & International Cybersecurity for BDO

The Rise of Cyber-Attacks in the Retail Industry

In the past decade, the retail industry has undergone major shifts worldwide due to the rise of the internet. As a result, the burgeoning e-commerce industry has significantly impacted the "classic retail" as enormous digital platforms like Amazon, eBay, AliExpress and TaoBao significantly accelerate the pace of digital transformation. In fact, the latest reports estimate that 10 percent of total retail business worldwide is generated by e-commerce.[1]

Although this increased reliance on the internet has begun a new chapter for the retail industry, it has also opened the door to ample vulnerabilities for cybercriminals. Financial information—especially credit card numbers—are considered a highly lucrative reward of a successful cyberattack because they can be quickly monetized (i.e., turned into cash or a cash equivalent), and therefore continuously traded on the Darknet. Consequently, prices for this kind of information have seen a relatively big spike. Globally, this has become an even bigger issue, because many breaches tend to be discovered in the very late stages of cyberattacks—and, in many cases, only after large amounts of data have already been stolen. According to research from IBM and the Ponemon Institute in 2018, breached organizations took an average of 196 days to detect the breach.[2]

1 https://www.infosecurity-magazine.com/news/value-stolen-card-amazon-account-1/

2 https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

Furthermore, between 2017 and 2018, the breach rate in the retail sector multiplied by 2.5 as 26 percent of companies reported being breached more than once.[3] Britain's Information Commissioner's Office (ICO) reported in Q1 2018 a total of 957 incidents affecting the retail sector in the U.K., which represents a 17 percent increase over the numbers reported back in Q3 2017.

As a result, governments became stricter about enforcing data security regulations, which meant harsher requirements and heavy fines to those who failed to comply. For example, in early 2018, the U.K. mobile retail firm Carphone Warehouse was fined £400,000 because of a data breach that occurred back in 2015 and compromised the personal data of about 10 million customers. To date, this is one of the largest fines ever issued by the ICO.[4]

In 2004, the Payment Card Industry (PCI) created the Data Security Standard (DSS) to increase security controls around credit card information and reduce credit card fraud incidents,[5] but almost 15 years later, many retailers still are not PCI-compliant. The retail industry is decentralized and complex, incorporating many different technologies such as artificial intelligence (AI),[6] the internet of things (IoT)[7] and blockchain,[8] and is constantly shifting between e-commerce, social commerce[9] and even e-commerce with software-as-a-service (SaaS).[10]

Research analyzing about 1,400 U.S. retail domains from October 2017 to March 2018 found that more than 90 percent of retailers failed to pursue at least four PCI DSS key requirements, and an astonishing 98 percent of them struggled to withhold the key security requirements to maintain secure systems and applications.[11]

To further illustrate the problem, just before that period, other researchers found a sample of about 1,600 AWS S3 buckets misconfigured, which exposed sensitive data to malicious intent.[12]

Additionally, a study published in February 2019 found that 64 percent of insider threats are a result of human neglect (i.e., human error or lack of security awareness amongst employees).[13] Another study stated that 83 percent of the companies reviewed reported they had an incident where employees accidentally exposed customer or business data.[14] The lack of cybersecurity prioritization in the retail industry has become an executive management and board-level issue—many companies continue to deploy poor cybersecurity strategies or no strategy at all,[15] which critically exposes the retail business environment to malicious intent that can cripple retailers and cause significant financial losses.

3 http://go.thalesesecurity.com/rs/480-LWA-970/images/2018-Thales-Data-Threat-Report-Retail-Edition-es.pdf

4 https://www.itgovernance.co.uk/blog/dixons-carphone-5-9-million-payment-cards-compromised

5 https://www.pcicomplianceguide.org/faq/

6 https://www.forbes.com/sites/forbestechcouncil/2018/11/21/pragmatic-ai-for-retail-an-introduction/

7 https://www.i-scoop.eu/internet-of-things-guide/internet-things-retail-industry/

8 https://www.forbes.com/sites/stevenbarr/2018/09/05/three-things-retailers-need-to-know-about-blockchain-today

9 https://www.zdnet.com/article/e-commerce-can-not-deliver-what-consumers-want-but-social-commerce-can/

10 https://www.nchannel.com/blog/saas-ecommerce-platforms/

11 https://www.infosecurity-magazine.com/news/over-90-of-us-retailers-fail-pci/

12 https://www.scmagazineuk.com/misconfigured-amazon-s3-buckets-allowing-man-in-the-middle-attacks/article/1473869

13 https://dtexsystems.com/2019-insider-threat-intelligence-report/

14 https://pages.egress.com/2019-Data-Privacy-research.html

15 https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/factsheets/grant-thornton---cyber-security-concerns---retail.pdf

PROMINENT CYBER-ATTACKS & THREATS TO THE RETAIL INDUSTRY

Supply chain cyber-attacks, where malicious actors breach third-party service providers to execute attacks on companies utilizing that service, are becoming more frequent across nearly all industries—including retail. The supply chain attack vector became prominent in 2018, and that trend is continuing in 2019. The destructive malware attack on the information technology (IT) supplier of the 2018 Winter Olympic Games is a good example, and other supply chain players have been attacked as well: accounting firms, law firms and even cleaning service providers all have been compromised and used as penetration vectors to the actual intended targets.

Supply Chain Cyber-Attacks via Point of Sale (PoS) Providers

The retail industry is highly susceptible to supply chain attacks via PoS software or devices. In late February 2018, a major provider of PoS solutions was hacked and infected by malware, compromising more than 130 outlets. The PoS provider, North Country Business Products (NCBP), revealed that hackers compromised its IT system a month prior to the outage and later planted the PoS malware on the networks of some of its customers.[16]

Among the list of businesses affected were Dunn Brothers Coffee, Zipps Sports Grill and Someburros. A third-party forensic investigation concluded an unauthorized entity deployed malware into these businesses between Jan. 3-Jan. 24, 2019. The malware was able to access cardholder names, credit card numbers, expiration dates and CVVs.[17]

This incident surfaced just one of the latest vulnerabilities exploited via a PoS provider. For example, in early 2018, it was revealed that a flaw in Oracle's PoS system affected more than 300,000 payment systems worldwide. The vulnerability (CVE-2018-2636) was first detected by researchers from ERPScan who found it affects Oracle MICROS PoS terminals and allows attackers to read sensitive data from devices.

Later that year, 239 locations of coffee shop chain Caribou Coffee had their PoS systems infected with malware after a breach at its PoS vendor. More recently, in early February 2019, U.S. restaurant chain Huddle House revealed hackers targeted a third-party provider's PoS system and used its remote assistance tool to deploy info-stealing malware at multiple locations.[18]

Mobile point-of-sale (MPoS) devices could easily become targets, too. In August 2018, researchers detected vulnerabilities with common MPoS vendors, determining most could have enabled malicious actors to steal sensitive information from the devices.

In March 2018, while investigating a large PoS malware campaign, researchers identified a new and sophisticated variant of a PoS malware dubbed "PinkKite" that included built-in persistence mechanisms. The new strain, which has an exceptionally small footprint of less than 6KB, obfuscates its activity by encoding stolen credit card details via a double-XOR encryption, making it harder to detect.[19]

While PoS attacks are not classified as breaches (as they rarely result in the compromise of data), any interruption to operations could result in tremendous losses for retailers, and in practice, they are a major threat to the sector.

Moreover, the frequency and magnitude of Denial of Service attacks, and in particular DDoS attacks, have been growing year-over-year—especially because "DDoS-as-a-service" is becoming cheaper and more widely available.[20]

These services are often powered by botnets such as Mirai, Srizbi, WireX and Hajime, among others. It's worth noting that two massive DDoS attacks—the largest at that time, 1.7Tbps and 1.35Tbps—were executed several days apart in 2018 against a U.S. Internet Service Provider (ISP) and GitHub, respectively,[21] by exploiting vulnerable memcached servers rather than using botnets.[22]

16 https://www.infosecurity-magazine.com/news/pos-firm-hacked-malware-deployed-1/

17 https://www.zdnet.com/article/pos-firm-says-hackers-planted-malware-on-customer-networks/

18 https://www.infosecurity-magazine.com/news/huddle-house-suffers-pos-malware/

19 https://securityaffairs.co/wordpress/70266/malware/pinkkite-pos-malware.html

20 https://www.csoonline.com/article/3180246/hire-a-ddos-service-to-take-down-your-enemies.html

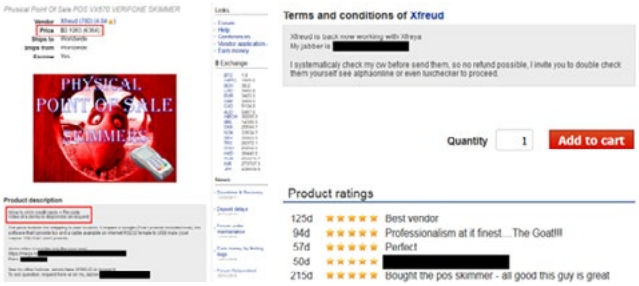
21 https://www.zdnet.com/article/new-world-record-ddos-attack-hits-1-7tbps-days-after-landmark-github-outage/

22 https://www.zdnet.com/article/memcached-ddos-the-biggest-baddest-denial-of-service-attacker-yet/

PoS Skimmers in the Retail Industry

One form of attack unique to the retail industry is PoS skimming. These devices glean credit card and pin data from cards physically swiped during purchase. In the past, these devices were bulky, conspicuous and hard to install, but they have advanced and become much smaller, easier to conceal and easier to install in recent years.[23]

The screenshot below shows a PoS skimmer intended for a Verifone device and listed for €364 on a Darknet market called "Dream Market." The vendor, "Xfreud," is a reputable seller with multiple other listings and high ratings.



The most active hacking group using this attack vector is called Magecart—a collective of at least six different hacking groups all operating in various ways to exploit the same attack vector.[24] Among the victims of attacks attributed to the group are ABS-CBN, British Airways, Feedly, Ticketmaster and an online electronics retailer called Newegg.[25] The name "Magecard" is also used by another hacking group for an online credit card skimming malware.

Phishing – BEC Scams and Social Engineering Attacks

Business Email Compromise (BEC) scamming, often called "spoofing," is one of the most widespread forms of cyberattacks in recent years. BECs (also known as "Man-in-the-Email" or CEO/CFO attacks) are carried out through a variety of social engineering methods and tools. According to the latest data from the FBI's Internet Crime Complaint Center (IC3),[26] more than 78,000 BEC incidents were reported with an excess of $12.5 billion stolen between October 2013 and May 2018. Moreover, these types of attacks appear to be growing, with stolen funds rising by 136 percent since December 2016.

So far, this type of attack has been relatively easy to execute. In one of the most common scenarios, the attacker impersonates an executive in a company and asks the target (often someone in a financial department) to wire transfer money for reasons of urgency and business criticality. In retail and some other sectors, these attacks involve supply chain. Attackers often impersonate a customer, supplier or even a legal representative.

The Russian group Carbanak carried out a variation of this attack to infect its targets with malware. About 30 minutes after sending an email with a malicious document attached, the attacker will make a phone call to the corresponding representative in the company encouraging the employee, under some pretense, to open the malicious document. Once it is confirmed that the document is opened, the attacker hangs up. This tactic was reported in various sectors and businesses, from hospitality to retail.

23 https://krebsonsecurity.com/tag/pos-skimmer/

24 https://techcrunch.com/2018/11/13/magecart-hackers-persistent-credit-card-skimmer-groups/

25 https://www.riskiq.com/blog/labs/magecart-newegg/

26 https://www.ic3.gov/media/2018/180712.aspx

Fraudulent Websites

Retailers are also particularly at risk because consumers can be attacked by fraudulent websites impersonating merchants. Attackers often lure targets to the fake websites via different methods such as phishing emails, spear phishing, etc. Once accessed, the websites serve a malicious payload such as an exploit or malware.

In cases of targeted attacks, attackers create custom content tailored to their targets and their targets' interests. These websites often download malware or redirect the users to various fraudulent services that trick them into providing sensitive information such as login credentials or credit cards details.

Another common technique involves creating a website with a minor, almost undetectable change in a trusted URL. For example, malicious actors registered the domain google[.]com in an effort to impersonate Google.com (note that the little "g" is, in fact, a Latin character). This method is growing; now, entire domains are registered in various languages that have similar characters to English, consequently making it difficult to identify a fake URL.

SPECIAL FOCUS:
RETAIL & CONSUMER PRODUCTS

Digital Transformation and Threat-Based Cybersecurity Will Help Mid-Market Retailers Thrive

In 2018, retail continued contending with a steady drumbeat of bankruptcies, burdensome debt, disruptive new entrants and shifts in buying power across generations—all of which increased the pressure to innovate. In addition to these more traditional business challenges, the vast amount of personally identifiable information (PII), including valuable financial information like credit card numbers, that retailers possess also make them a lucrative target to cyber-attackers.

In fact, the threat of cyber-attacks for all businesses is rising. The number of global ransomware attacks alone doubled in 2018 compared to 2017, as attackers began more effectively targeting critical business systems, according to Verizon's 2018 Data Breach Investigations Report.

While coming up with a focused business strategy amid disruption and increased cyber risk is already tough for any business, it's even more so for mid-market retailers saddled with greater resource constraints.

In fact, just 37 percent of mid-market retailers say they are actively thriving today, while more than half (54 percent) say they're merely surviving, and 9 percent admit to struggling, according to ***BDO's Retail Rationalized Survey.***

Rationalizing Retail

To thrive (versus just survive) in today's environment, retailers must:

- Be realistic about their true strengths, choices and opportunities
- Have a strong sense of purpose
- Ensure appropriate information security and data privacy
- Understand that innovation will only generate positive ROI if it's based on a solid financial foundation and strategic choices

The retail success formula, which distinguishes between the strugglers, survivors and thrivers in today's world, is no longer based on who can check every box for a product or service. It's about who has the clearest focus, the most thorough business.

MIDDLE-MARKET RETAIL THRIVERS: WHERE DIGITAL COMES INTO PLAY

When it comes to which retailers are thriving, a lot of it comes down to technology adoption and digital transformation.

An overwhelming majority of pure play e-commerce businesses (84 percent) are thriving, meaning they're profitable and experiencing robust growth. Meanwhile, more than half of traditional retailers (including big box, department store, discount and specialty retailers) are just surviving, as they catch up to optimizing physical assets and bolstering online and attractive price offerings.

Who are **Thrivers**?

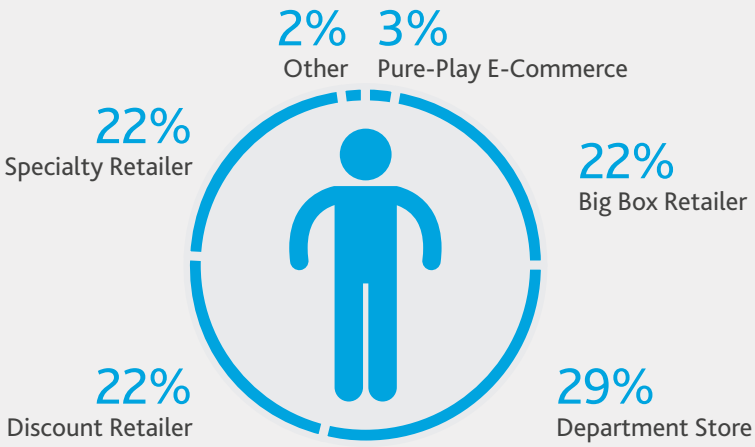
PORTRAIT OF A THRIVER:

- E-commerce-centric
- Technology early adopter
- Exclusive products as competitive advantage
- Cite less convenience as greatest weakness
- Planning ahead for the worst

Who are **Survivors**?

PORTRAIT OF A SURVIVOR

- Risk-averse
- Technology laggard
- Customer service as competitor advantage
- Cite higher prices as greatest weakness
- Using outside capital to remain stable

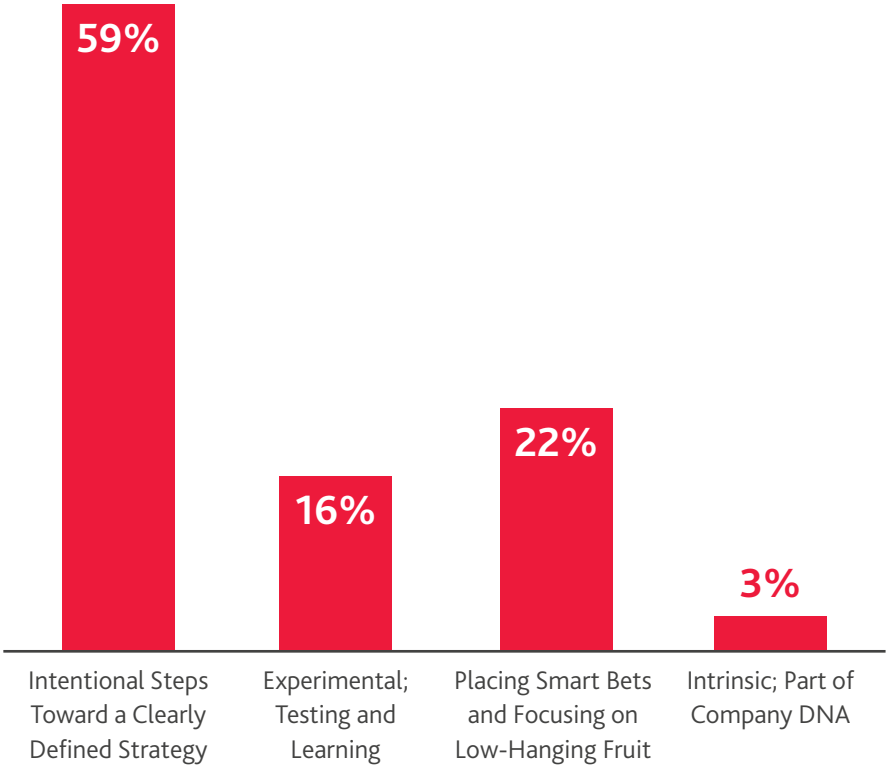


LEVERAGING DIGITAL TRANSFORMATION TO THRIVE

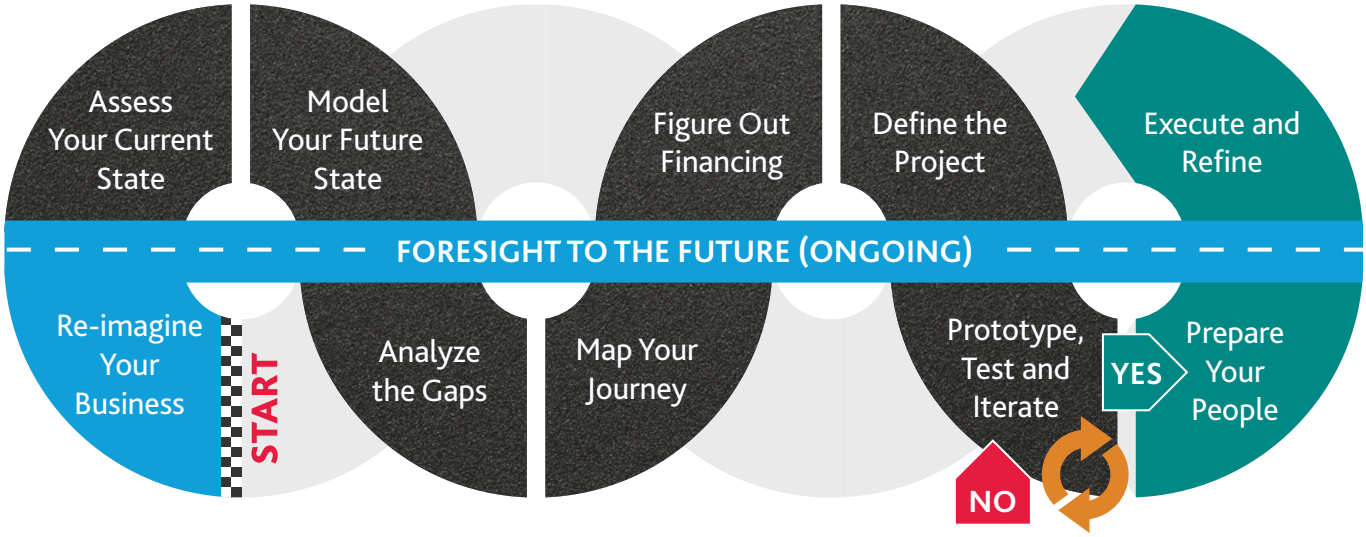
As mid-market retailers work to intentionally refocus their business strategy to thrive, it's clear that e-commerce and other digitally-enabled offerings with appropriate information security will become a greater part of their business.

In fact, a notable portion of mid-market retailers expect such digital initiatives to reward them with increases in both revenue and profitability. Nearly half (48 percent) of retailers **expect their digital investments to increase their revenue by 1-9 percent** in the next three years, and 18 percent expect them to drive revenue growth of 10 percent or more, according to [BDO's 2019 Middle Market Digital Transformation Survey](). Forty percent, meanwhile, **expect digital investments to increase their profitability by 1-9 percent**, and 27 percent expect them to grow profits by 10 percent or more.

MID-MARKET RETAILERS' CURRENT APPROACH TO DIGITAL TRANSFORMATION



Taking intentional steps toward a clearly defined digital transformation strategy will be critical and involves a 10-step journey.



Source: *BDO's Digital Transformation Playbook for the Middle Market*

MANAGING GROWING RISK IN TANDEM WITH INCREASED INNOVATION AND CYBERSECURITY

As digital transformation becomes a core part of retailers' strategy, they'll have to prioritize threat-based cybersecurity in tandem.

Threat-based cybersecurity is a forward-looking, predictive approach. Instead of (or in addition to) focusing solely on protecting critical data assets or following the basic script of a generic cyber program, threat-based cybersecurity concentrates on investments in the most likely risks and attack vectors based on an organization's unique threat profile. For example, this framework looks different for a pure play e-commerce entity than for a hybrid e-commerce or specialty retailer because the most likely attack vectors are different for each.

Threat-based cybersecurity approaches go hand in hand with innovation, as security serves as the backbone to digital transformation—and can even be an innovation catalyst.

"Taking on digital transformation initiatives like adopting an emerging technology, investing in a new technology or even building a new technology are key to not only increasing operational efficiencies, but also to bolstering cybersecurity, as both security and privacy should be embedded into the initiative's design and architecture. When an organization overhauls its IT infrastructure, its security risks undergo an overhaul, too. Old vulnerabilities may be mitigated or even eliminated, while new ones are introduced. The process of implementation will require a fresh look at how data is accessed and used, and can help retail companies shift their security resources accordingly, in conjunction with an external threat monitoring system."

GREGORY GARRETT
Head of U.S. and International Cybersecurity for BDO

Learn more about how BDO can help retailers craft a threat-based cybersecurity approach in line with their **digital transformation playbook**.

Notable Attacks

CLOTHING RETAILER KATHMANDU INVESTIGATING POSSIBLE CUSTOMER DATA BREACH

On March 13, 2019, New Zealand-based outdoor clothing and equipment retailer Kathmandu Holdings, Ltd. reported it was investigating a possible breach. According to the company, it detected unauthorized access to its website platform between Jan. 8-Feb. 12. As of March 14, it is still unknown whether customers' personal information and payment data were compromised.[27]

ONLINE ELECTRONICS RETAILER NEWEGG HIT BY MEGACART HACKERS GROUP

In September 2018, it was revealed that online computer hardware and consumer electronics retailer Newegg, Inc., fell victim to the prolific hacker group known as Megacart for more than a month between Aug. 13-Sept. 18.[28] It's worth mentioning that this was reported just a day after the attack on Filipino media conglomerate ABS-CBN's online store, which was also attributed to the group.[29]

According to researchers from RiskIQ, the attackers injected about 15 lines of obfuscated JavaScript code into the e-retailer's checkout process, which enabled them to siphon payment card data.[30] It is unknown how many customers were affected; however, the U.S.-based online retailer receives between 45 to 50 million visits a month.[31]

MACY'S AND BLOOMINGDALE'S BREACH

In early July 2018, Macy's notified customers that Macys.com and Bloomingdales.com were breached, compromising data of an unknown number of customers. The incident reportedly involved "unauthorized access to personal information" and took place between April 26-June 12.[32] After detecting the intrusion on June 11, Macy's blocked the affected customer profiles. In the company's statement, it assured customers that no CVV or Social Security numbers were compromised.

WALMART JEWELRY PARTNER EXPOSES PERSONAL DATA OF 1.3M CUSTOMERS BECAUSE OF MISCONFIGURED DATABASE

The publicly accessible bucket, discovered on Feb. 6, 2018, belonged to Limogés Jewelry. It contained an MSSQL database backup with the personal information of more than 1.3 million people in the U.S. and Canada—including names, addresses, zip codes, phone numbers, e-mail addresses, IP addresses and plaintext passwords.[33]

27 https://uk.reuters.com/article/kathmandu-hldg-data-breach/nz-retailer-kathmandu-holdings-flags-suspected-data-breach-at-websites-idUKL3N2100EO

28 https://www.zdnet.com/article/magecart-claims-another-victim-in-newegg-merchant-data-theft/

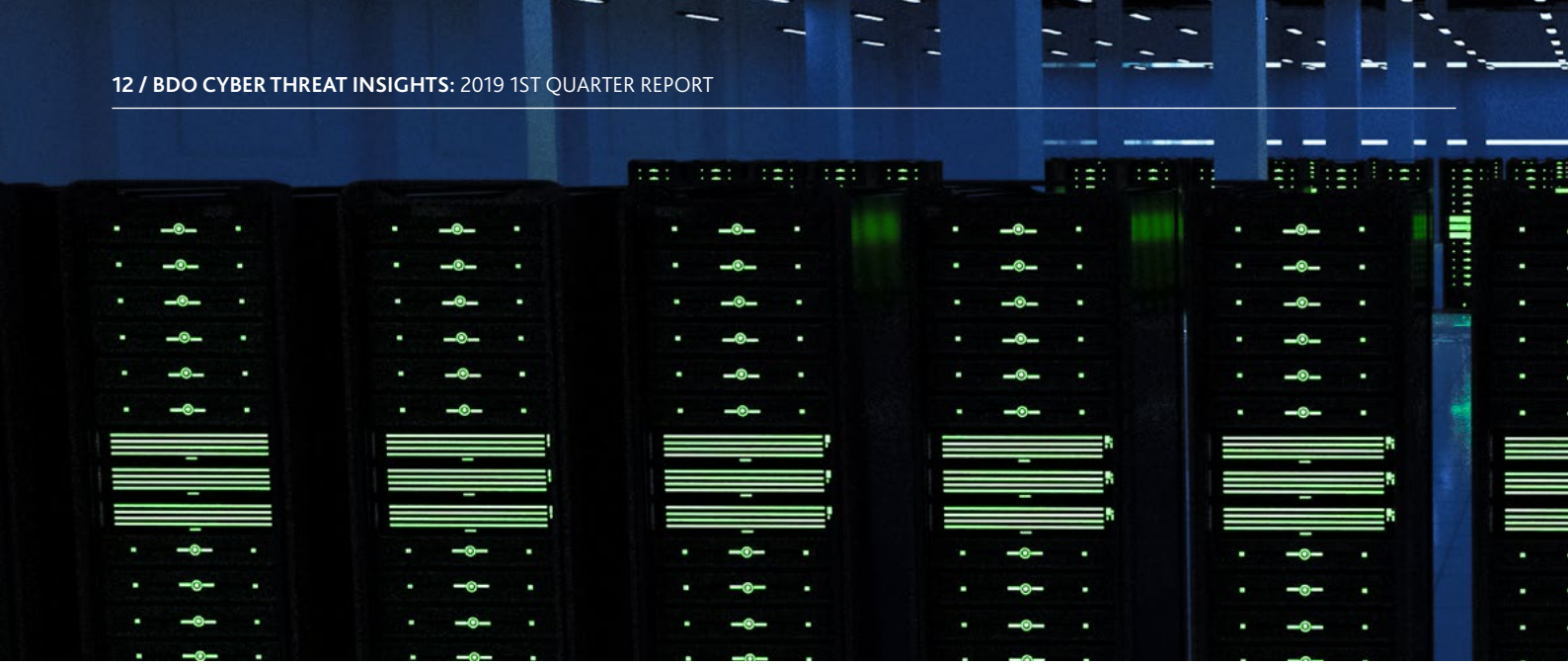
29 https://www.zdnet.com/article/broadcasting-giant-abs-cbn-customer-data-stolen-sent-to-russian-servers/

30 https://www.riskiq.com/blog/labs/magecart-newegg/

31 https://www.similarweb.com/website/newegg.com#overview

32 https://www.scmagazine.com/home/security-news/data-breach/unauthorized-party-accesses-macys-com-and-bloomingdales-com-customer-accounts/

33 https://threatpost.com/walmart-jewelry-partner-exposes-personal-data-of-1-3m-customers/130486/



UNDER ARMOUR'S NUTRITION APP MYFITNESSPAL BREACH COMPROMISES DATA OF 150M INDIVIDUALS

In late March 2018, sports clothing and apparel company Under Armour reported that its nutrition app, MyFitnessPal, suffered a data breach that affected 150 million users. According to the company, the breach was limited and only exposed usernames, email addresses and passwords. This indicated Under Armour employed adequate segmentation between this information and their other more sensitive databases.

Furthermore, Under Armour reassured users that all the passwords were hashed, thus making them harder for attackers to use as cracking hashes is incredibly time-consuming. However, it was later revealed that while most of the passwords were hashed with an advanced hashing algorithm, bcrypt,[34] others were hashed using an outdated and weak function called SHA-1. [35]

ADIDAS BREACH EXPOSES ONLINE CUSTOMERS' PERSONAL DATA

The second-largest sports clothing and apparel company in the world, Adidas AG,[36] reported in June 2018 that its U.S. website was breached, exposing "limited data" of online customers, including contact information, usernames and encrypted passwords. However, the company claimed that there are no indications that any of the company's other websites were breached, and that no credit card or other sensitive information was accessed.[37]

SHEIN FASHION RETAILER BREACH

In late September 2018, online fashion store SHEIN announced that it suffered a security breach affecting about 6.5 million users. The attack took place in June but was only detected on Aug. 22. The nature of the attack is unknown, as no technical details were revealed and SHEIN did not disclose the vector of the attack, only stating that hackers executed "a sophisticated criminal cyberattack on its computer network." According to the company, there is no evidence that any financial data was compromised, and SHEIN stated that it does not store credit card information in its systems.

U.K. RETAILER 'SUPERDRUG' BREACHED, 20K CUSTOMERS' DATA HELD FOR RANSOM

In August 2018, the health and beauty retailer Superdrug Stores, PLC, reported that it fell victim to a security breach that supposedly compromised details of 20,000 customers. According to Superdrug, the hackers obtained customers' names, addresses, and in some cases, dates of birth and phone numbers. Superdrug stated that some customers' points balances may have been accessed, but it reassured customers that no payment or card information had been taken.

The hackers held the data ransom for an undisclosed sum. Superdrug was provided with details of 386 customers to prove the validity of their claims, and Superdrug's spokeswoman said they were able to verify that the details were indeed from Superdrug customers.[38]

34 https://auth0.com/blog/hashing-in-action-understanding-bcrypt/

35 https://www.wired.com/story/under-armour-myfitnesspal-hack-password-hashing/

36 https://www.pledgesports.org/2018/01/10-biggest-sports-brands-in-the-world/

37 https://www.digitalcommerce360.com/2018/07/02/adidas-suffers-data-breach-with-millions-of-customers-potentially-at-risk/

38 http://www.itv.com/news/2018-08-21/superdrug-customer-details-hit-by-hackers/ https://www.infosecurity-magazine.com/news/superdrug-held-to-ransom-after/

23K FORTNUM & MASON CUSTOMERS' PERSONAL DATA EXPOSED

In July 2018, it was reported that luxury retailer Fortnum & Mason exposed the personal data of 23,000 of its customers due to a breach of its online form service provider, Typeform.[39] The latter suffered a breach on June 27 that resulted in attackers downloading a "partial backup" of its customer data.[40]

The affected Fortnum & Mason customers voted for the company's food and drink awards via the Typeform survey in the "TV Personality of the Year" category. Most of the affected customers only had their email addresses compromised, but the attackers also obtained a small, unreported amount of customer names, home addresses and social media usernames.

NORWEGIAN CLOUD SERVICE FIRM VISMA HACKED BY CHINESE GROUP APT10

Techerati posted details about an attack by the Chinese group APT10, which is part of the Cloud Hopper attack campaign.[41] The Norwegian firm Visma, which provides cloud solutions for more than 850,000 clients around the world, experienced a breach in its network in August 2018. According to a report posted by Rapid7 and Recorded Future, the attack was carried out by the Chinese attack group APT10,[42] though it cannot be attributed to this group with full certainty.

The attack was designed to target cloud services to obtain user information. The attackers stole login details from Citrix and LogMeIn (used by Visma employees) about two weeks after the first propagation in the firm's network. They then used these login details to distribute a malware which spread to several computers in the firm's network and enabled access to sensitive information.

The attackers used the tool Mimikatz (named pd.exe) to steal login details and leveraged scheduled tasks via the Microsoft BITSAdmin utility to transfer files from their C2 to the Visma network.

Examination of network logs revealed an employee's credentials were stolen and used to authenticate the network outside of his normal working hours. Throughout August 2018, the attackers regularly logged into the Visma network during typical Chinese working hours.

Two weeks after the initial intrusion into the network, APT10 implanted its Tochilus malware via a C2 server that communicates with Salsa20 and RC4 encryption. After entering the system, the attackers reached information on the Visma systems through WinRAR files which were transferred to a Dropbox account—a method AP10 has used previously. Visma's Operations and Securities Manager Espen Johansen told Reuters the attack was halted before client networks were breached.

This attack method surely raises concerns among many companies in the Western world that rely on cloud services.

39 https://www.itgovernance.co.uk/blog/fortnum-mason-customers-personal-data-exposed-in-breach

40 https://nakedsecurity.sophos.com/2018/07/03/typeform-data-breach-hits-thousands-of-survey-accounts/

41 https://techerati.com/news-hub/chinese-state-hackers-attack-norwegian-cloud-computing-firm/

42 https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf

BDO Cyber Threat Intelligence (CTI) Services

THREAT INTELLIGENCE – "PROACTIVE DETECTION OF A BREACH"

Situational awareness is "the perception of environmental elements and events with respect to time or space, the comprehension of their meaning and the projection of their future status," while intelligence is "the ability to acquire and applied knowledge and skills."

BDO Cyber Threat Intelligence (CTI) is a combination of both: the objective of acquiring knowledge and skills to support better organizational ability and anticipate cyber events that could impact the future status of the business environment.

The BDO CTI Reports are based on research performed by the BDO Cybersecurity Centers. Our Cyber Threat Intelligence Centers in the U.S. and Israel work as an integrated team to transform reactive organizational situational awareness into proactive situational awareness to Cyber Threats. This enables an organization to better understand the likelihood and characteristics of a breach and enables an additional layer of proactivity in the detection of unidentified breaches that might be happening.

HOW DOES IT WORK?

Cybersecurity Research

Our Cyber Research teams reverse-engineer cyberattack techniques, malicious code and lateral movement to identify actual targets and methods used by different perpetrators with different malicious agendas.

Online Fictitious Identities

Our Cyber Intelligence team maintains online fictitious identities to enable their activity within threat communities, to infiltrate an online forum or create a connection with suspected threat actors or hackers, and establish online 'chatter' platforms, to establish 'trusted' conversation environments.

Monitoring Cybercrime Forums

Our Cyber Intelligence team monitors various cybercrime forums to identify premeditated attacks on organizational networks or personnel by monitoring any type of hostile chatter regarding these 'targets.'

Monitoring Data Leakage Platforms

Our team can trawl hacker-oriented data leakage platforms to identify specific data leakage that might lead to a potential attack against an organization.

CONTACTS:

TOMMY BABEL
Head of Cyber Resilience & Threat Intelligence Services
BDO Cyber Security Center, Israel
tommyb@bdo.co.il

NOAM HENDRUKER
Director, Head of Global Consulting Group
BDO Cyber Security Center, Israel
tommyb@bdo.co.il

BDO CTI DELIVERABLES

BDO Cybersecurity Services

PAYMENT CARD INDUSTRY (PCI)

- PCI assessment and remediation
- Third-party assessments

INFORMATION GOVERNANCE AND DATA PRIVACY

- Data mapping
- Data privacy assessments
- Data privacy strategy and implementation
- Privacy officer consulting
- Information governance assessments

CYBER INSURANCE

- Cyber insurance claim preparation
- Coverage adequacy evaluation

CYBER RISK ASSESSMENTS

- Risk assessments against multiple frameworks
- Cyber risk remediation

INCIDENT RESPONSE

- Data breach investigations
- Network/host active threat monitoring
- Threat hunting - exec, enterprise, nation state, insider
- Threat intelligence - deep/dark web, social media analysis
- Training & testing - 1st responder, table top, RED team, simulations
- IR data analytics

CYBERSECURITY STRATEGY, POLICY AND PROGRAM DESIGN

- CIO & CISO advisory services
- Cyber strategy consulting
- Regulatory compliance
- Government relations consulting

CYBER THREAT INTELLIGENCE

- Dark web recon
- Dark web analysis
- Social media

MANAGED SECURITY SERVICES

- Email and network attack threat assessments
- Security Operations Center (SOC)
- Penetration testing
- Vulnerability assessments
- Cloud migration & security
- Virtual desk-top services
- Cybersecurity education, training, & simulations
- Security Incident & Event Management (SIEM)

Cybersecurity Leadership Team

GREGORY GARRETT
Head of U.S. & International Cybersecurity
Tel: +1 703-770-1019
ggarrett@bdo.com
Resident Country: USA

GRAHAM CROOCK
Director, IT Audit, Risk & Cyber Laboratory
Tel: +27826067570 or +27824654539
gcroock@bdo.co.za
Resident Country: South Africa

JASON GOTTSCHALK
Partner, Cybersecurity Practice Leader
Tel: +44 (0)79 7659 7979
jason.gottschalk@bdo.co.uk
Resident Country: UK

STEPHAN HALDER
Senior Manager, Forensic, Risk and Compliance
Tel: +49 40 30293 169
stephan.halder@bdo.de
Resident Country: Germany

LEON FOUCHE
Partner and National Cybersecurity Lead
Tel: +61 7 3237 5688
leon.fouche@bdo.com.au
Resident Country: Australia

SANDRA KONINGS
Partner, Cybersecurity Practice Leader
Tel: +31 (0) 6 5150 8151
sandra.konings@bdo.nl
Resident Country: Netherlands

ANDREAS VOGT, PH.D.
Partner, Head of Section BDO Security & Emergency Services
Tel: +47 48171714
andreas.vogt@bdo.no
Resident Country: Norway

OPHIR ZILBIGER, CISSP, CRISC
Partner, Head of Cybersecurity Centre
Tel: +972-52-6755544
OphirZ@bdo.co.il
Resident Country: Israel

People who know Cybersecurity, know BDO.