SIX COVID-19 CYBER SECURITY INSIGHTS
FOR RETAILERS

Introduction

Today's outlook for retailers is a mixed bag. Consumers may be finding deals from distressed retailers. However, the shutdown has been a brutal reality for many segments within the retail industry. Although COVID-19 vaccines are on the horizon to offer hope, retailers still face major challenges. The reliance on digital technology has increased due to the coronavirus pandemic. Analysts expect this trend to persist even after the pandemic subsides. Here are some guideposts for securing your retail business during this volatile time of transition.

A report on the first half of 2020 states there were 4.83 million cyberattacks, a 15% increase over the prior year. [1]

Fewer retailers means less competition and more cyber risk

If you're a retail organization and you've survived to this point, then things are looking good for your market share with fewer competitors to contend with.[2] However, this also means there are fewer retailers for cybercriminals to attack. A report on the first half of 2020 states there were 4.83 million cyberattacks, a 15% increase over the prior year.[3] For example, an APT group called FIN11 attacks point-of-sale (POS) in retailers, restaurants, and other industry sectors. Recent attacks by FIN11 have stolen data and extorted ransomware payments from retailers using CLOP ransomware attacks.[4]

[1] Mary K. Pratt, 6 security shortcomings that COVID-19 exposed, CSO Online, Nov 16, 2020.

[2] Teresa Rivas, How COVID-19 Changes Are Actually Helping Some Retail Stocks, Oct. 7, 2020.

[3] Mary K. Pratt, 6 security shortcomings that COVID-19 exposed, CSO Online, Nov 16, 2020.

[4] Ravie Lakshmanan, FIN11 Hackers Spotted Using New Techniques In Ransomware Attacks, The Hacker News, October 14, 2020.

Under these conditions, it is vital for retailers to prevent malware from entering their IT environments. Sandboxes that allow traffic to pass into your environment while spending up to 5 minutes to identify threats already in the network is no longer acceptable for threat prevention. Your solution for advanced threat prevention must stop today's multi-vector threats outside your environment including your data centers, cloud deployments, SaaS, and endpoint and mobile devices. As a further backstop, it's prudent to have purpose-built ransomware protection that blocks bot behavior within networks and backs up files for rapid restoration.

> The pandemic has accelerated existing trends in the economy towards the increased use of technology, remote work, and automation.[5]

COVID-19-caused shifts to more digital likely permanent

Walmart's latest quarterly report stated that the discount retailer's online sales grew by 79 percent as customers eschew in-store visits for online transactions.[6] According to U.S. Federal Reserve Chairman Jerome Powell, the economy we knew is probably a thing of the past. The pandemic has accelerated existing trends in the economy towards the increased use of technology, remote work, and automation.[7] In support of Powell's assertion, Apptopia reported the average daily downloads for popular digital grocery apps Instacart, Walmart Grocery, and Shipt have surged since February.[8]

Yet with all this progress, one must remember that software developers can't be rushed to bring new products to market without adequate security testing. The new software that powers online transactions, curbside services, touchless checkout, contactless-delivery services, and other COVID-19 related technologies likely contain flaws that grow retailers' threat surfaces. Application security as well as preventative malware protection and DLP controls are increasingly needed in today's business climate.

---

[5] Anneken Tappe, The economy as we knew it might be over, Fed Chairman says, CNN Business, November 12, 2020.

[6] Melissa Repko, Bertha Coombs, Walmart earnings top expectations as customers' new shopping habits send e-commerce sales soaring 79%, CNBC, November 17, 2020.

[7] Anneken Tappe, The economy as we knew it might be over, Fed Chairman says, CNN Business, November 12, 2020.

[8] Adam Blacker, Instacart and grocery delivery apps set consecutive days of record downloads, Apptopia.com, March 2020.

Employees working from home add risk

Retailers, like businesses in other sectors, are asking corporate employees to work from home to prevent COVID-19 spread. This introduces security risks from employees' unprotected home WiFi, routers, and IoT. Retailers must adopt secure VPN communications with remote workers as well as endpoint protections, document security, and protection for SaaS to prevent account takeovers in insecure home offices.

Streaming via social media boosts sales and threats

Whether live streaming sales demonstrations or using on-demand video, retailers are discovering that streaming content on social media is offering a new revenue stream much like per-inquiry advertising does on television. For example, Dong Ming Zhu, chairwoman of Gree Electric, recently sold more than US$43.8 million worth of home appliances in a three-hour live stream event.[9] Retailers engaged in streaming should provide security and compliance controls on their Facebook pages, Twitter accounts, LinkedIn pages, and other streaming venues with security measures that utilize social network APIs.[10]

---

[9] Jia Jen Low, Retail-streaming is the future of e-commerce and will save retail, T_HQ, June 9, 2020.

[10] Keeping Social Media Accounts Secure is Much Harder Than You Think, Check Point, as viewed November 17, 2020.

Supply-chain disruption means more automation

Putting products in customers' hands has become more challenging due to COVID-19. Supply chains rely heavily on human workers to fulfill orders particularly in the last mile. Automated IoT devices such as robots and autonomous vehicles are taking up the slack.[11] However, these connected devices generate more customer data to protect and further expand a retailer's threat surface outside traditional security perimeters. Dedicated IoT security is now a priority as retail supply chains become more automated.

> International cybersecurity workforce needs to grow by 89% to close skills gap.[12]

COVID-19 further strains cyber-security staffing

Given the difficulty of finding cyber security professionals under normal circumstances, illnesses due to COVID-19 can increase the burden on remaining staff members. To help your security staff maintain added strain, it is vital to consolidate security controls under a central management system to simplify visibility into threats and streamline security administration across your total environment: datacenter, cloud, mobility, POS, social media, supply chain, and other elements.

Consolidated Security Architecture pulls it all together for COVID-19 and Beyond

Technology change is constant in the retail industry. Retailers must be technically agile to meet changing consumer behaviors as well as in cyber security. Using consolidated security architecture streamlines retail security practices end-to-end. When you need to upgrade your advanced threat prevention, ransomware protection, cloud security, social media protection and any of the other 60 security controls experts recommend for retailers during the COVID-19 pandemic, consolidated security architecture lets you add them quickly on-demand.

[11] Western Digital, 5 Changes in IoT Data Storage Since the Pandemic, IoT for All, October 21, 2020.

[12] International Cybersecurity Workforce Needs to Grow By 89% to Close Skills Gap, by Scott Ikeda, CPO, November 24, 2020.

" The Check Point Infinity Total Protection model covers all current threats. I don't have to choose different vendors for specific tasks or challenges. Everything is included.

- Kim Moberg, IT Manager, Eurowind Energy

Consolidated security architecture also reduces the burden on managers and administrators who can monitor and administer all security controls through a single interface. COVID-19 has accelerated the retail industry's digital transformation. For greater agility and effectiveness it's time for retailers to adopt preventative security bound together by a consolidated architecture across all environments.

To obtain further information on how a consolidation security approach can better protect your organization, click here to discover Check Point Infinity.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com