APG CASH DRAWER®

PROTECT YOURSELF

8 Security Best Practices
For Retailers

The retail industry is a favorite target of cyber attackers. Hackers know a successful attack on a retailer can give them access to the data of thousands or even millions of payment cardholders. Cybercriminals can sell that data for a tidy profit to other criminals on the dark web who use it for fraud, identity theft, and phishing attacks. Cybercrime is big business; it's projected to cause damages of *$6 trillion by 2021* on organizations of all types and sizes.

When it comes to cyber threats, retailers have a lot at stake. They operate on thin margins and have to protect their brands. A breach that compromises the private information of customers can erode trust, prompting many to take their business elsewhere. *Nineteen percent* of consumers in a KPMG study said they would stop shopping at a retailer following a breach, and 33 percent said they would do so temporarily.

A strong cybersecurity posture, therefore, isn't optional for retailers. It is an absolute must. Retailers that fail to take proper measures to secure customer data, as well as their own, risk being penalized if a breach is found to have been caused by non-compliance of relevant regulations. For many retailers – especially smaller, independent shops – security is a big challenge because they lack the requisite skills and knowledge, in which case they must seek help from solution providers that can implement security solutions to protect them.

Security is a multifaceted endeavor, especially in retail where there are so many potential points of attack: – POS systems, card readers, email, Wi-Fi, e-commerce sites, and, of course, the physical stores themselves. Retailers must approach security holistically, making sure to cover all systems and areas where an attacker can exploit vulnerabilities to spread malware infections and steal valuable data. A comprehensive retail security strategy must include the following eight components:

Measures for POS protection include running endpoint monitoring and threat detection solutions, encrypting all data introduced to a payment processor, limiting applications on POS systems to only those that are absolutely necessary, and applying security patches as they become available to keep all software up to date.

1 POS SECURITY

Retailers live and die by their POS systems. Unsecured POS software and hardware such as card readers and receipt printers can cause serious problems. For one thing, any retailer found to be in violation of PCI -DSS standards, which are meant to protect owners of payment cards, can incur monetary fines and even lose the ability to accept card payments. Proper security and compliance are critical because POS threats are introduced constantly.

Measures for POS protection include running endpoint monitoring and threat detection solutions, encrypting all data introduced to a payment processor, limiting applications on POS systems to only those that are absolutely necessary, and applying security patches as they become available to keep all software up to date. Retailers also should conduct vulnerability testing periodically and require workers to use strong authentication (more on that below) to access POS systems.

With payment processing, it's best to use a payment gateway outside of the POS terminal with no direct connection. The payment gateway communicates with the POS terminal via the network (or internet) where the POS simply requests transaction approval. The payment gateway or device activates and handles the transaction with end-to-end encryption (E2EE) and notifies the POS of an approval (or decline). This eliminates the risk of any credit/debit card data being compromised on the POS terminal itself.

2 E-COMMERCE PROTECTION

Retailers must protect their online storefronts as zealously as they do physical POS stations. As with the POS, PCI regulations apply to online transactions, so retailers must ensure that they have the proper controls in place to protect web shoppers.

There are many ways for hackers to attack an e-commerce site, including the use of bots to change pricing and other information, Trojan horses that trick users into performing an action that turns out to be harmful, brute force attacks to guess passwords, and attempts to break into databases attached to online storefronts. Preventing these malicious acts requires a multilayered approach that uses firewalls, malware detection, monitoring, encryption, and strong user authentication to protect the website and all applications, servers, and databases connected to it.

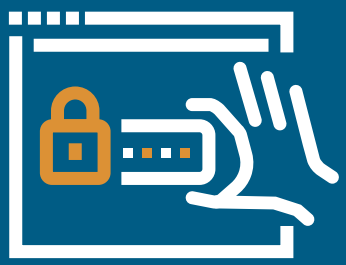
3 USER AUTHENTICATION

Reliable user authentication policies are critical in two primary ways: – to ensure that internal users follow security protocols and to accurately identify customers. Both require strong authentication practices. Internal users should be required to use strong passwords, (eight characters minimum that mix upper and lowercase letters, numbers, and symbols), as well as a second authentication

$6,000 000 000 000

Cybercrime is big business; it's projected to cause damages of $6 trillion by 2021.

Nineteen percent of consumers in a KPMG study said they would stop shopping at a retailer following a breach, and 33 percent said they would do so temporarily.



Internal users should be required to use

STRONG PASSWORDS

(eight characters minimum that mix upper and lowercase letters, numbers, and symbols) as well as a second authentication method for the most sensitive applications.

A DATA BACKUP and RECOVERY STRATEGY

are central to busines continuity plans.

method for the most sensitive applications. Common examples of the latter include one-time PIN codes transmitted by email or text. Passwords should be renewed periodically – monthly or quarterly – to minimize the chances that hackers will guess them. Users should never use the same password in more than one place.

While two-factor authentication is less common for authenticating online shoppers, retailers should consider it, especially with big-ticket purchases. At minimum, users should be required to create strong passwords or passphrases – consisting of nonsensical word sequences, such as PineFlyAlmost – to protect their identities. Properly identifying customers with strong authentication will become that much more crucial as retailers implement multichannel strategies, allowing users to switch back and forth between devices.

4 ENDPOINT MONITORING

In the past, deploying antivirus (AV) software may have been sufficient to protect endpoints, but that is no longer the case. AV typically focuses only on known threats and cannot defend against newly introduced malware strands. This is why businesses need a combination of 24/7 endpoint monitoring and data analytics to defend against all kinds of threats.

Next-generation endpoint security tools use machine learning to identify new threats and quarantine them to protect environments against infection. Retailers, being among the most targeted businesses by hackers, need this kind of protection to foil hackers and, if an attack succeeds, respond swiftly and effectively to minimize damage – and protect their customers' data.

5 EMAIL PROTECTION

Many cyber-attacks originate with phishing emails, and most ransomware infections start with a user clicking an infected URL or attachment. Phishing works because it preys on fear and curiosity by making emails look like they are coming from a legitimate source and persuading users to click on the URL or attachment.

Preventing email-borne attacks requires a combination of technology and user awareness. Retailers should deploy anti-phishing and anti-spam tools to catch suspicious emails, but that isn't enough. A user can still make a bad decision even with the tools in place, which is why investing in awareness and education programs is critical. Effective training typically involves phishing simulations that teach users how to identify suspicious emails and ongoing reminders about the dangers of opening attachments and URLs. Employees should be mindful of requests coming from managers or executives requesting the transfer of funds or purchase of gift cards. These are often fraudulent scams that appear to be coming from an internal connection with a similar email alias.

6 WI-FI NETWORK/COMMUNICATIONS

Retailers increasingly offer Wi-Fi connections to customers in stores as a conve-

Wi-Fi networks used for business should have security controls such as:

- Firewalls
- Endpoint Protection
- Encryption
- Strong User Authentication

Preventing email-borne attacks requires a combination of technology and user awareness. Retailers should deploy antiphishing and antispam tools to catch suspicious emails.

nience, -- and to capture customer information for marketing purposes. However, Wi-Fi networks open to the public should be separate from those used for business functions such as inventory, HR, and POS. Mix the two, and you're asking for trouble because data on public Wi-FiI networks is more likely to fall into unauthorized hands.

Wi-Fi networks used for business should have security controls such as firewalls, endpoint protection, encryption, and strong user authentication – the same types of protections that should be in place for communications between stores, corporate headquarters, clouds, and data centers. In addition, retailers also should instruct employees who travel never to use public Wi-Fi for sensitive corporate data and, instead, connect to critical business applications, databases, and cloud services through secure VPN connections. Retailers should also change Wi-Fi passwords regularly following the best practices listed above.

7 SURVEILLANCE SYSTEMS

In addition to protecting their digital assets, retailers have to secure physical stores to prevent shoplifting, fraud, and employee theft at the POS. Deploying a surveillance system with CCTV or IP-connected cameras not only helps to secure physical spaces but also acts as a crime deterrent. CCTVs paired with intelligent POS hardware can time- and date- stamp footage to pinpoint suspicious activity or transactional discrepancies . Whether to choose IP-based or CCTV cameras comes down to business needs and budgets. IP systems offer advantages such as higher resolution, wireless connections, and scalability, but in some settings, a CCTV system may be more suited to a company's needs.

8 BUSINESS CONTINUITY

No security strategy is complete without a business continuity plan. If a business suffers a cyber-attack or physical operations are interrupted by a natural disaster, a company needs to resume operations as quickly as possible. A data backup and recovery strategy are central to business continuity plans. Retailers need to back up all of their critical data and have it ready for quick recovery. Increasingly, businesses are turning to cloud-based services for data backup because of their affordability and scalability.

Business continuity is about more than technology. It also involves policies and procedures that all employees need to follow in the event of a cyber-attack or disaster. *Plans* should include contact information, meeting points for employees, and contingencies for temporary relocations. Retailers should make sure all employees are aware of the overall plan and their individual responsibilities under the plan. Periodic drills and revisions help ensure that the plan stays current and workable.

> *Preventing these malicious acts requires a multilayered approach that uses firewalls, malware detection, monitoring, encryption, and strong user authentication to protect the website and all applications, servers, and databases connected to it.*

CONCLUSION

Retailers cannot afford to be lax with security, be it in physical spaces, their IT networks, or websites. It can take a long time to recover from a security breach, especially if customers lose trust in the company. Digital theft, data breaches, and security related to new payment methods erode a consumer's trust in a brand, making security a business essential.

Hacking and cybercrime are a common occurrences that sometimes compromise the payment card information of users at the POS. Fear of card and personal data breaches is a reality in our society, and as a cash management solution manufacturer, this bodes well for cash use . Although proper security poses some challenges for retailers because of the technology and skills that a comprehensive security strategy requires, help is available from security providers. Retailers with a solid security strategy are more likely to succeed in today's business environment.

Digital theft, data breaches, and security related to new payment methods

erode a consumer's trust in a brand, making security a business essential.

APG Cash Drawer, LLC
5250 Industrial Blvd. NE
Minneopolis, MN 55421

+1 763-571-5000

sales@us.cashdrawer.com

APG Cash Drawer, with over 40 years of experience, manufactures a wide range of highly durable and reliable cash drawers that are delivered quickly to the marketplace. APG has built a reputation as the supplier of choice for cash management solutions for retail, grocery and hospitality, and quick serve for thousands of customers throughout the world. Whether it's our general application cash drawer, custom designed solutions, or the SMARTtill ® Cash Management Solution, our products and brand are differentiated by our ability to deliver innovative technologies that globally enhance efficiency and security at the point of sale. To learn more about our products, visit www.cashdrawer.com

M-43-412 Rev. A