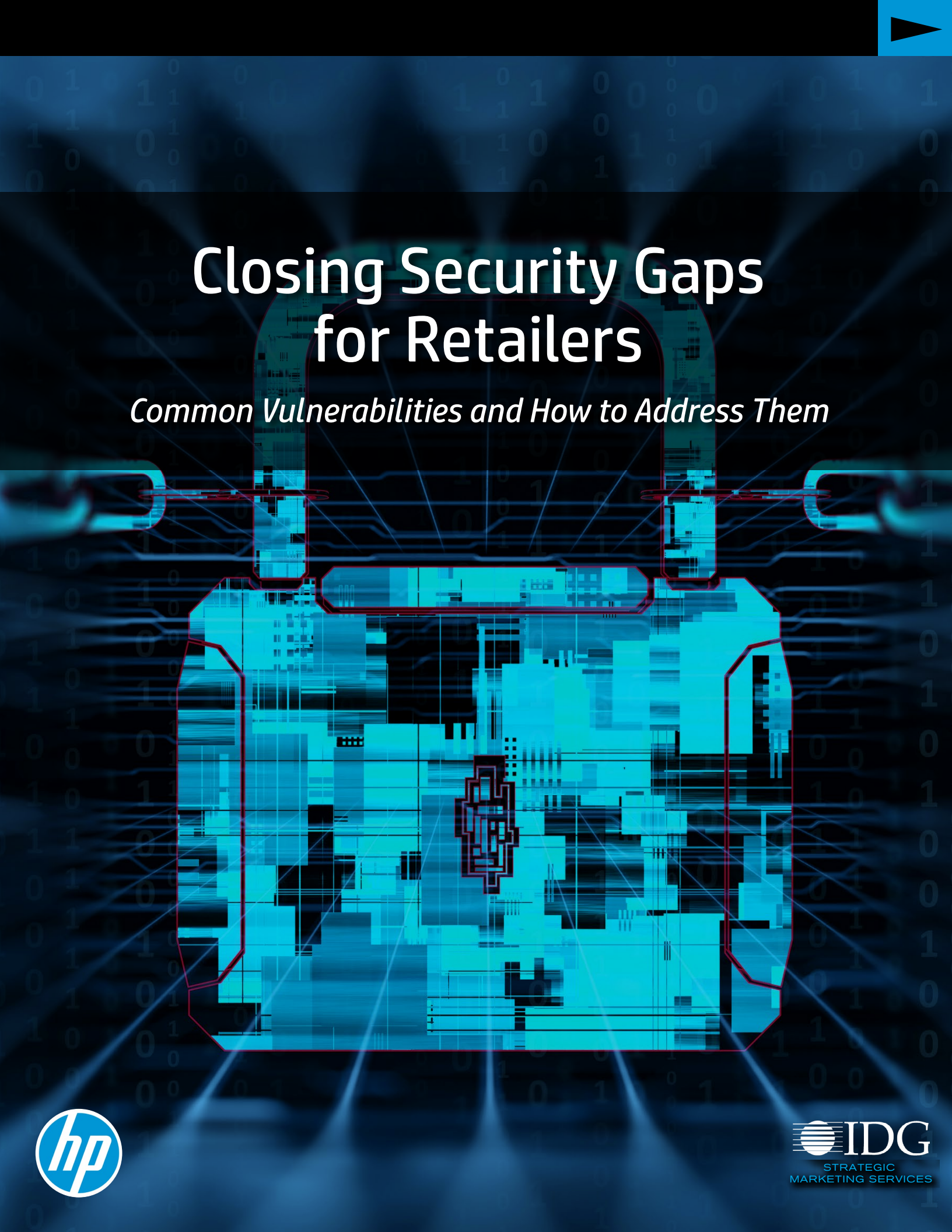
Closing Security Gaps for Retailers

Common Vulnerabilities and How to Address Them



IDG
STRATEGIC
MARKETING SERVICES

Closing Security Gaps for Retailers

Common Vulnerabilities and How to Address Them

CONTENT

The Retail Industry is Under Attack:

Brick-and-mortar Outlets Particularly Vulnerable

When it comes to cybersecurity, retail organizations face a full spectrum of challenges. They're attractive targets for cybercrime due to the amount of consumer information they collect during a retail transaction, including credit card numbers, but retail operations typically aren't managed with security in mind.

This isn't news to retailers, who typically have their online consumer portals buttoned up security-wise. But cybersecurity in physical retail locations is a different story. Many retail operations are becoming increasingly connected with mobile and Wi-Fi technologies, if not increasingly secured. Each piece of equipment that is connected to the location's network—ranging from point-of-sale (POS) devices to printers—represents a potential gateway to sensitive data.

Once a criminal has access to the enterprise network, anything is possible. The infamous Target breach of 2013, for example, reportedly resulted from exploiting an HVAC vendor's credentials to access the retailer's supplier portal in order to seize POS system data.

Beware "The Wolf"
Watch Christian Slater as "The Wolf" while he disables an organization's entire network through unsecured printers.
Watch video

In 2016, the retail industry represented 22% of all data-breach incidents—the largest single share of the total reported by Trustwave[1]. In 2017, fast-food chains Arby's, Sonic Drive-In, and Wendy's reported major compromises to their POS systems, as did retail chains Forever 21, The Buckle Inc., and Brooks Brothers, along with the Whole Foods grocery chain.

A data breach can have immediate costs. The Ponemon Institute has estimated an average of $3.62 million per incident.[2] Data breaches, and even false reports of data breaches, can drive customers away, tarnish a retailer's reputation, and diminish goodwill.

While the retail industry will probably never escape its status as a top target for cybercrime, retailers can take some basic steps to better secure their physical facilities.

A Target-commissioned report following the breach said that "consultants were able to directly communicate with point-of-sale registers and servers from the core network. In one instance, they were able to communicate directly with cash registers in checkout lanes after compromising a deli meat scale located in a different store."

This starts with understanding the primary sources of security weakness.

"With credit and debit cards serving as a de facto currency for many transactions today, modern cyber criminals have found it is more efficient to hack into computer databases to steal consumers' names and card numbers than to rob a bank for cash."

National Retail Federation[3]

[1] 2017 Trustwave 2017 Global Security Report

[2] Ponemon, 2017 Global Report on the Cost of Cyber Crime, August 2017

[3] National Retail Federation, Data Security, 2017

Two Main Sources of Security Weakness

The retail industry is notoriously low-margin, so budgets are limited for things like equipment upgrades. Retailers tend to hang on to their equipment until it's totally non-functional and must be replaced. This means that outdated and unsecured equipment hangs around for awhile, and retail infrastructures tend to include a random jumble of equipment types and makes, which is difficult for creating comprehensive security policies and meeting compliance.

The retail industry is also becoming increasingly competitive as online retailers and low-cost foreign markets drive price points ever lower. In the face of such challenges, it's no wonder that retailers prefer to focus investment in areas that will increase sales and efficiency.

According to the RIS/Gartner Retail Technology Study, top investments in retail are focused on unified commerce, personalized marketing, and customer engagement. Security may appear as a line item at best, if at all.

To start, retail operations can improve security by investing in two key areas: updating legacy equipment and training employees in security best practices.

Legacy systems pose threats

The retail industry overall is behind on security investments. For example, U.S. payment card networks shifted fraud liability from issuers to merchants in 2015, yet half of retailers are still leaving themselves at risk by using older, non-EMV payment terminals instead of the more secure chip-card readers. According to the Cisco 2017 Annual Cybersecurity Report, just 52% of retail organizations consider their security infrastructure up-to-date. This ranks below other industries at 59%.

The problem with having a lot of outdated equipment around, including equipment like thermostats and printers, is that each unit represents a potential security breach. And a lot of legacy equipment is impossible to secure. Even if your equipment isn't directly linked to your valuable data like a POS, it may still be part of the network that includes your data. A skilled hacker could exploit a networked but unsecured device as a portal to the rest of your network, including your valuable data. The Target breach mentioned earlier is a vivid example of this.

These loose security practices at the store level makes retailers a prime target for cybercrime. Any info that feeds through a scanner for example, such as employee info, credit card numbers, or customer data, can be intercepted.

Retailers should review their security frameworks to identify needed upgrades, both long and short term. Sometimes, increasing security in lower profile equipment, like printers or HVAC control systems, can gain you some security improvements now, while you plan for larger changes like POS systems in the longer term.

The people problem

Not only are retailers heavily reliant on aging technology, but their workers often lack basic security training. According to one survey, just 29% of retail employees can identify common best practices to prevent cyber and data privacy incidents.

Considering the high employee turnover and influx of temporary seasonal workers in many retail environments, it's no wonder retail employers have a hard time keeping up with security training, let alone consistently enforcing security policies. That's a recipe for exploitation from internal as well as external threats. For example, "hire attacks," where contingent workers sign on to work a busy holiday season, can leave retailers vulnerable to corporate espionage and other mayhem from insiders.

According to the National Retail Federation's 2017 National Retail Security Survey, employee theft and insider crime accounts for almost one-third of "inventory shrinkage," just behind losses from shoplifting and organized retail crime activities.

Retailers can't stop at simply securing their perimeters or digital firewalls. They need to ensure security within their premises as well. Including security training in employee onboarding process is one step. Upgrading to devices with built-in security, such as data encryption and secure login, adds an extra layer of security and confidence.

Networked Printers: A Forgotten Security Gap

A large retailer could be spending millions of dollars on cyber security to protect their data and in-store surveillance systems to cut down on "inventory shrinkage." However, there is one common blindspot they're probably not thinking about: networked printers. Unsecured devices can expose the entire network to a cybersecurity attack.

According to one survey, 61% of large enterprises have experienced a print-related breach.[4] Despite this threat, a Spiceworks survey found that 43% of surveyed organizations ignore printers in their endpoint security practices.[5]

Overlooked and exposed

Because they require little if any technical skills to operate, printers and other imaging devices are often overlooked in the security infrastructure. Decision makers may not be security minded, or IT decision makers may simply have their hands too full to worry about the many other endpoints in a typical retail operation to prioritize print security.

However, many print devices incorporate software-implemented communications "ports" that provide potential points of vulnerability for criminals to exploit with internet protocols. Others have USB slots that could allow an attacker to upload malware to the network, collect sensitive data, and transmit it over the internet.

And it's not just sophisticated cyber schemes that threaten the print environment. Documents left unattended in a printer output tray could allow a passerby to quickly scoop up confidential information, potentially causing compliance violations if customer data is involved.

But there are solutions, ranging from simple—such as printer access policies—to sophisticated, such as printer malware protection and managed print services. The key is to take printer security as seriously as any other retail security component.

---

[4] Quocirca, "Print Security: An Imperative in The IoT Era," January 2017

[5] Spiceworks survey of 309 IT decision-makers in North America, EMEA, and APAC, on behalf of HP, November 2016

A Multilayered Approach to Security

To combat security challenges, retailers need multi-layered security strategies that ensure there are no weak links waiting for cyber criminals to exploit.

Update legacy equipment

The first place to start is with retail hardware. Today's technology can build in security, all the way down to the BIOS level. Encrypting devices can prevent spyware from collecting usable data, and strong user authentication and printer "pull" technologies can provide only authorized users the ability to receive documents.

Don't rely on manual procedures

Workers across all industries are notoriously bad at following security best practices—security just isn't part of their core duties, so it tends to fall outside of their focus. Retailers in particular can't expect to rely on manual security procedures, especially with the fluid nature of their workforces. Instead, they should seek to equip IT staff and managerial teams with automated security solutions that take human error out of the equation and streamline day-to-day operational requirements.

Defend your devices, data, and documents

In addition to tightening up security policies and implementing best practices, retailers can look to modern printers from HP that contain sophisticated technologies to make them active parts of the security defense. Today's printers can incorporate continuous monitoring and intrusion detection; when malware is detected, they automatically reboot to prevent the execution of malware and can even self-heal the internal BIOS.

HP Printers: An Ally in the Cybersecurity Fight

Components of a print security solution can be relatively simple, such as employing locked input trays that prevent misappropriation of items such as paycheck forms.

HP can help you defend your network with the world's most secure printing[6] — including devices such as **HP LaserJet** and **HP PageWide Enterprise** printers that can automatically detect and stop an attack. HP's print security experts can help you develop and deploy an end-to-end imaging and printing security strategy, with a broad portfolio of solutions featuring encryption and configuration administration as well as BIOS and firmware protection options.

In recognition of HP's competitive strengths in print security, IDC recently positioned the company as a leader in the IDC MarketScape: Worldwide Security Solutions and Services 2017 Vendor Assessment. According to IDC, "HP's approach to security takes the entire print and document infrastructure into account, beginning with locking down the device and extending into all aspects of device usage and content protection." [7]

Printers from HP offer security features to keep your data safe and protect your networks from harm in three main areas: device security, data security, and document security.

Secure technology that bites back

Watch "The Fixer" starring Jonathan Banks to see how HP technology helps you fend off "The Wolf."

Watch video

Device security

HP Sure Start and run-time intrusion detection are included on HP Enterprise printers to protect at startup and during operation. If malware is detected, the printer automatically shuts down and reboots the device. Every time a printer is turned on or restarts with an error, HP Sure Start automatically validates the integrity of the BIOS code and self-heals if necessary.

HP Enterprise printers also include whitelisting to help ensure that only authentic HP firmware—digitally signed by HP—is loaded into memory. HP Connection Inspector evaluates outgoing network connections to determine what's normal, stop suspicious requests, and automatically trigger a self-healing reboot.

When a reboot occurs—or any time a new device is added to the network—HP JetAdvantage Security Manager automatically assesses and, if necessary, remediates device security settings to comply with your pre-established company policies.[8]

Data security

HP solutions include HP Universal Print Driver and HP Access Control for PC network printing and HP JetAdvantage Connect and HP Access Control for mobile users. This helps ensure that only authorized users can access devices and the networks to which they are connected. Fleet-wide authentication solutions can require users to enter a password or PIN, or to scan their badges or fingerprints.

Data traveling between PCs and the network is often encrypted, but data flowing to and from printers is often overlooked, leaving it vulnerable to hackers. HP Universal Print Driver, HP Access Control, and HP JetAdvantage Connect, combined with Wi-Fi and network encryption protocols can secure data in transit.

---

[6] "Most secure printing" claim based on HP review of 2016 published security features of com-petitive in-class printers. Only HP offers a combination of security features that can monitor to detect and automatically stop an attack then self-validate software integrity in a reboot.

[7] IDC MarketScape: Worldwide Security Solutions and Services 2017 Vendor Assessment, IDC, October 2017

[8] HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager. Competitive claim is based on HP internal research on competitor offerings (Device Security Comparison, January 2015) and Solutions Report on HP JetAd-vantage Security Manager 2.1 from Buyers Laboratory, LLC (February 2015).

Applying signed certificates to network printers and MFPs adds another layer of data protection. Using HP JetAdvantage Security Manager saves time by automatically installing and renewing certificates.

Document security

Unclaimed print jobs are one of the most common ways in which sensitive data is exposed. Any printed document is at risk of being stolen by an unauthorized person if the intended recipient isn't there when it comes out of the printer. Additionally, documents often are sent to the printer and forgotten—left unattended for anyone to claim. This is a key concern for the HR department, which prints a high volume of sensitive employee documents due to frequent associate turnover.

Retail organizations should deploy a "pull print" and user authentication solution so that documents are not printed until the user authenticates at the device using identification security protocols. HP offers several authentication and pull-print solutions for a variety of situations and IT environments:

- **HP Access Control Secure Pull Print** is a server-based software solution that can be set to require all users to authenticate before retrieving their jobs.
- **HP JetAdvantage Secure Print** provides an option for print jobs to be sent and stored in a secure cloud queue until the user authenticates and prints the job.
- **HP Universal Print Driver** is a free solution that includes a secure encrypted printing feature for sensitive documents. It allows users to send print jobs to be held until they release the jobs via a PIN at the device.
- **The HP Proximity Card Reader** lets users authenticate quickly and print securely at a device using their existing ID badges.

Retail organizations should deploy a "pull print" and user authentication solution so that documents are not printed until the user authenticates at the device.

Now is the time to take proactive steps to reduce risk and help secure data:

- **HP Print Security Services** and specialists can help with print security assessments, planning, deployment, and ongoing management.
- **HP Print Security Advisory Services** can help retail organizations assess vulnerabilities and compliance, develop a custom print security policy, and make process and technology recommendations for improved security.
- **HP Print Security Governance and Compliance** can help retailers maintain security settings compliance across the printer fleet.

Your partner in print security

Creating a complete imaging and printing security strategy requires coordinated protection of devices, data, and documents, plus comprehensive monitoring and reporting solutions. With HP Secure Managed Print Services, you're more secure on every level, so the trouble that's out there stays out.

For more than 50 years, HP has been partnering with leading retailers, supplying the technical expertise and business savvy to help position them at the forefronts of their industries. This experience gives HP unique insight into your needs to reduce costs, increase productivity, ensure data security, and drive profitability. HP has the print solutions—and the industry's most recognized print management software—to help you reduce risk while improving efficiencies.

Learn more at **HP Print Security.**