
How Healthcare Organizations Can Keep 'The Wolf' Away
Is your network at risk?
This HP eBook can help you find out.
command
alt

How Healthcare Organizations Can Keep 'The Wolf' Away

Print security is more than document security. Today's threats require attention to data in-transit and endpoint devices on the network. This is especially important for healthcare organizations. Use this eBook to see how **HP Print Security** can help you stay a step ahead.

Chapter 1: Today's Environment

Begin by reading our in-depth articles on the cybersecurity challenges today's healthcare organizations face. Find out what's keeping IT leaders up at night. Cybercriminals are like wolves – constantly lurking, ever alert for the weakest prey. In many organizations, networked printers are at the bottom of the security feeding chain, leaving them ripe for attack. Even one unsecured printer could put your whole company at risk. Learn how to protect yourself from attack.

Watch the video: **"The Wolf: The Hunt Continues"**

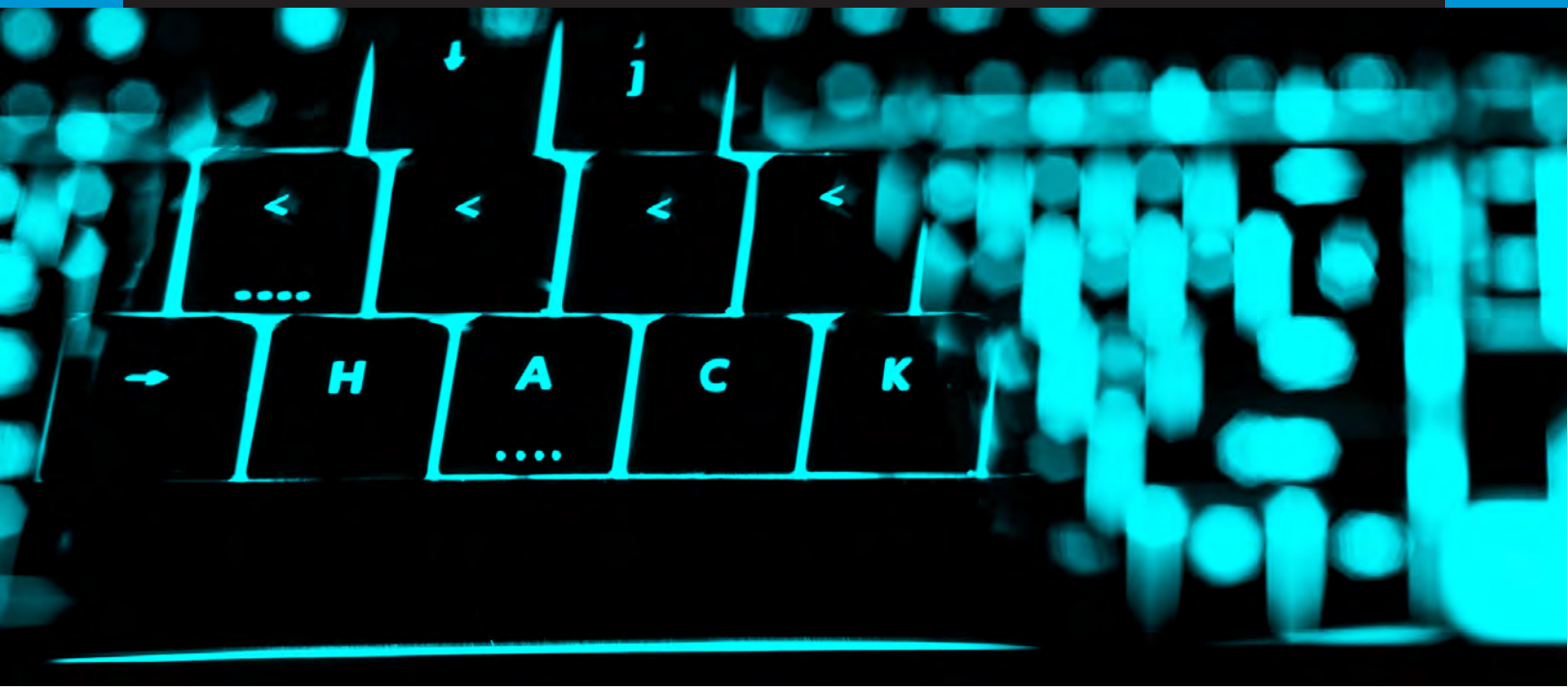
In HP's film, The Wolf targets patient records stored by one of the medical world's biggest records management companies. He hacks into a PC and later a hospital printer by using the printer's USB port to upload malware.

Chapter 2: Point of View

This section of the eBook addresses the need for healthcare organizations to be more proactive about security vulnerabilities. For example, are you ignoring a gaping hole in your network? What steps are you taking to reduce malware? It examines the security controls you should implement to improve compliance, and how to avoid becoming "cyber-prey." So what security measures should your organization implement to protect confidential documents? That's the question we posed to members of the **IDG Influencer Network** for our **crowd-sourced article.**

According to IDC, "printers have not received the attention that other cybersecurity threat vectors received. The vulnerability and the corresponding threat is real, very real. Organizations of all sizes must take steps to address the concern and address it quickly. Cybermiscreants are voracious copycats. Once a threat vector has been exploited for gain by one malicious actor, others follow quickly."[1]

continued >



And in its 2017 MarketScape Security Solutions Vendor Assessment, IDC states, "Neglecting to secure the print environment as part of an overall IT strategy leaves an organization vulnerable to significant internal and external cyberthreats." Further, "organizations looking to develop a comprehensive print infrastructure security strategy should seek out solutions and services to extend protection well beyond the device."[2]

IDC named HP a leader in its latest MarketSpace, saying "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."

CONTENTS

[1] "The Printer Is an Endpoint: Proactively Addressing the Security Vulnerability," IDC, November 2016
[2] "IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment," IDC, October 2017

Healthcare Ailing in Cyber War

Cyber criminals exploit vulnerabilities faster than healthcare organizations can adjust their cyber defenses.

Cybercriminals prey on the weak, and they've concluded that healthcare organizations are among the most alluring – sitting on massive volumes of potentially vulnerable personal health and financial information. At the same time, growing regulatory requirements leave these organizations threatened by steep compliance penalties if a breach occurs.

At the close of 2016, Experian's Data Breach Resolution unit predicted that healthcare would be the most targeted sector for cyber criminals to exploit. Sure enough, in May 2017, malware known as WannaCry caused 37 of the health trusts in the UK's National Health Service to shut downs, eventually spreading across 150 countries seeking out vulnerable computers and networks across industries. In June, a similar attack infected hospitals in the U.S. and a major pharmaceutical organization.

Like other attacks in recent years, the malware locked up computers and displayed a notice demanding ransom to unlock the systems. "Hospitals have been a common target because the culprits know how critical digital records are for treating patients," noted a report from the *Bloomberg* news service.

"Many NHS computers are running very out-of-date software which can have serious security flaws," the UK's Daily Mail newspaper reported. "At least 10 health trusts still rely on the Windows XP operating system, released in 2001."

Keeping pace with criminals

Part of the problem is that cyber criminals are moving faster to exploit vulnerabilities than organizations in healthcare and other industries can adjust their cyber defenses. In the case of WannaCry, the *Los Angeles Times* reported, "The tactic itself wasn't innovative or surprising, exploiting a flaw in several versions of Microsoft's Windows operating system that was well-known and well-publicized. A patch Microsoft issued in March to fix the issue could have taken businesses and organizations just a day or two to test and install."

But it's not just reliance on PCs with old software that makes hospitals particularly vulnerable.

"Hospitals not only have thousands of computers, phones and laptops: they also have thousands of medical devices connected to the network," John D. Halamka, M.D. and Chief Information Officer of the Beth Israel Deaconess System, wrote in an article for the PBS NEWSHOUR web site. "IV pumps, X-ray machines, and heart monitors sound like appliances, but in reality they are computers with network connections. Many of these medical devices have little to no security protections because manufacturers never assumed they would be attacked."

"Cybersecurity vulnerabilities and intrusions pose risks for every hospital and its reputation," the American Hospital Association advises. "While there are significant benefits for care delivery and organizational efficiency from the expanded use of networked technology, Internet-enabled medical devices, and electronic databases for clinical, financial, and administrative operations, networked technology and greater connectivity also increase exposure to possible cybersecurity threats that require hospitals to evaluate and manage new risks."

Any connected endpoint device represents a potential security vulnerability. Healthcare organizations are also adding more and more devices as they take advantage of Internet of Things (IoT) technology solutions aimed at improving efficiencies, saving costs, and improving health outcomes.

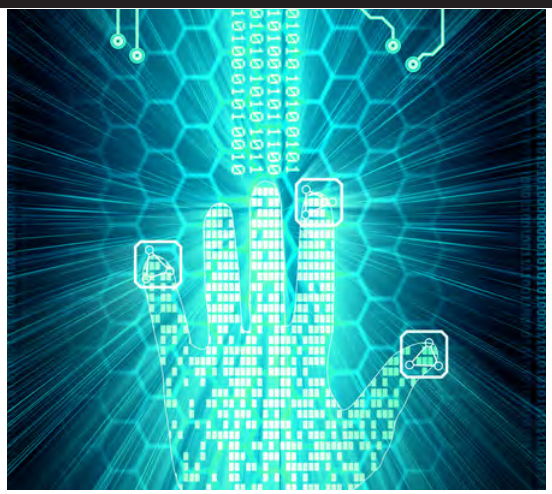
"Healthcare organizations are also charged with managing all the IoT devices in their network," HIT Infrastructure warned. "Adopting a device management solution that gives IT administrators complete visi-

bility and control over the network is crucial to successful implementation."

Hiding in plain sight

In some cases it may be easier to plan for cyber security when adopting new systems. It's also easy to overlook commonly used devices that may not be generally viewed as points of vulnerability.

Printers and imaging devices represent one such vulnerability that needs to be addressed. These everyday tools require little or no expertise to use, are increasingly networked, and are often left unattended. When there are unsecured devices, the entire network can be exposed to a cybersecurity attack.



The key to warding off the pain of cyber security incidents is to make sure that all connected devices are incorporated into an organization's network security protection plan.

Consider, for example, just a partial list of points of attack using one networked imaging or printing device:

- **Ports —** Unauthorized users can access the device via unsecured USB or network ports to upload malicious code that, when activated, can provide many ways to exploit data.
- **Storage media** — Imaging and printing devices often store sensitive information on internal drives or hard disks, which can be accessed if not protected.
- **BIOS and firmware** — Firmware that becomes compromised during startup or while running could open a device and the network to attack.
- **Cloud-based access** — Unsecured cloud connectivity may expose data to unauthorized users.
- **Network intercepts** — Printing and imaging jobs can be intercepted as they travel over the network to/from a device.

Cybersecurity pain management

Just one lowly, networked multifunction printer, if unprotected, could result in painful ramifications, including identity theft, stolen proprietary information, a tarnished brand image and reputation, and litigation.

There's also the potential penalties for regulatory and legal noncompliance. The Health & Human Services Office for Civil Rights can impose **civil penalties up to a maximum of $1.5 million** annually in cases involving failure to comply with privacy and security rules, and criminal violations can result in prison terms.

The key to warding off the pain of cyber security incidents is to make sure that all connected devices are incorporated into an organization's network security protection plan. With printers, for example, administrators should consider the following:

- **Encryption of data and print jobs** traversing the network and stored in local media
- **Secure erase of data** to ensure sensitive information is not left unprotected
- **Disabling** unused ports and protocols
- **Access control**s to ensure only authorized personnel can configure devices
- **Real-time threat detection,** automated monitoring, and built-in software validation
- **Advanced authentication** to limit usage to authorize personnel

These preventive security tools are available in current products. But they need to be part of a comprehensive, consistently enforced network security strategy. The IT security team has to account for every possible point of vulnerability because the cyber-criminal only needs to find that one point left exposed.

To learn how to protect your organization from cyber risks, go to HP Print Security.

Health Data Increasingly Attractive to Criminals

It contains valuable information such as Social Security numbers and home addresses and thus is worth more to hackers than other types of data.

According to FBI history, when asked why he robbed banks, legendary criminal Willie Sutton responded, "Because that's where the money is." Today's cyber criminals are attacking healthcare networks because that's where they can gain access to vast stores of personal health information, often left vulnerable from weak security points.

A Brookings Institution report noted that "Healthcare data contains valuable information such as Social Security numbers and home addresses and thus are worth more to hackers than other types of data. Since they can sell these data files for a premium price on the black market, hackers have a strong economic incentive to focus their hacking attacks on the healthcare sector."

It might surprise you that the network printer, often sitting unattended, is a potential gateway to exploit healthcare data and leave your organization exposed to costly compliance penalties in the event of a breach.

Looks can be deceiving

Although they require relatively little technical skills to use, networked printers and imaging devices are actually very sophisticated computer devices, and may include operating systems, storage media, and software that the average user has no idea about.

That device sitting in the corner may include a File Transfer Protocol (FTP) software-based server. In March 2017, the FBI issued a Private Industry Notification warning that criminals are actively targeting FTP servers "operating in 'anonymous' mode and associated with medical and dental facilities to access protected health information (PHI) and personally identifiable information (PII) in order to intimidate, harass, and blackmail business owners."

According to Security Intelligence, "Anonymous FTP, as it is called, does not require any authentication before granting access to the files on the system. It has long been recommended that a server with this service host only public files. But smaller health care offices may use older, less sophisticated systems that could have been either misconfigured or not properly maintained."

Not just data at risk

The FBI advises that "Cyber criminals could also use an FTP server in anonymous mode and configured to allow 'write' access to store malicious tools or launch targeted cyber attacks."

The ramifications of this vulnerability extend far beyond capturing data, according to a Dark Reading report: "Companies also run the risk of cyber criminals storing malicious or incriminating content on their server. They can use this as the foundation for a ransomware attack, threatening to publicize their possession of this information unless they pay. A hacker could use an anonymous FTP server to store and sell pirated software, involving the business in selling stolen goods."

> *"Healthcare data contains valuable information such as Social Security numbers and home addresses and thus are worth more to hackers "*
>
> *Brookings Institution report*

It should be clear by now that there's no such thing as a low-risk network-connected device. But there are ways to ensure that your printer is not a weak link in your network security chain. **To learn how to protect your organization from these risks, visit HP Print Security.**

The New Pandemic: Healthcare Data Breaches

Assaults on healthcare organizations aren't likely to abate any time soon.

Exposed medical data can cost healthcare companies millions of dollars in federal and state fines, civil actions, corrective action plans, credit monitoring, ID theft, and lost business from current and future customers.

HHS' Office for Civil Rights can impose **steep civil penalties** for failure to comply with privacy and security rules, and criminal violations can result in prison terms. In 2016, Advocate Health Care Network paid **$5.5 million in fines** for multiple violations that jeopardized electronic health records of more than 4 million patients.

Healthcare organizations are a favorite target of cyber criminals due to the nature of personally identifiable and personal health information stored in databases. These are lucrative targets that provide criminals with opportunities for identity theft, financial fraud, and falsified drug prescriptions.

Held for ransom

Another opportunity for criminals is ransomware, which locks up infected computers and can spread to other networked devices, disrupting normal operations ranging from records access to scheduling operations.

The assaults on healthcare organizations aren't likely to abate any time soon.

"After two years of a steadily increasing cyber threat landscape that resulted in record numbers of patient records compromised, health organizations extorted financially, and hospital operations disrupted very publicly, 2017 is likely to be just as interesting," predicts an *Health IT Security* perspective. "Hackers will continue to go after networks, systems, and applications that have been misconfigured or are not maintained properly."

Many organizations, though, may not have adequately prioritized endpoint security, which can be exploited by a physically present hacker. Any connected intelligent device is a potential gateway for cyber criminals.

"All medical devices face a certain amount of cybersecurity risk," a recent Health & Human Services **cybersecurity task force report** advised. "The risk of potential cybersecurity threats increases as more medical devices use software and are connected to the Internet, hospital networks, and other medical devices. This connectivity also improves healthcare and increases the ability of healthcare providers to treat patients."

> *"All medical devices face a certain amount of cybersecurity risk"*
>
> *Health & Human Services cybersecurity task force*

Physical interference

Many healthcare organizations may not realize that printers can be a physical insertion point for malware that can be used to exploit enterprise networks. For an eye-opening view of how such an exploit could lead to massive exposure of electronic records, watch Christian Slater's hacking portrayal in episode 2 of HP's **The Wolf**.

Fortunately, there are steps you can take to protect your organization from such threats. Printing technology from HP provides security protections such as encryption, configuration administration, as well as BIOS and firmware protection. But the best technology won't protect you from inadequate security policies. It's important that healthcare organizations establish requirements for unattended devices, implement and enforce access authorizations, and monitor usage.

To learn more, go to HP Print Security.

Paper Chain Compliance Risks

Healthcare organizations can't afford to ignore the potential risks of paper-based breaches

Networked printers are an essential element of organizations and an often-overlooked compliance risk. Recent cyber attacks have no doubt awoken healthcare IT organizations to the dangers of ransomware phishing assaults. But security teams shouldn't overlook the dangers of printed personal health information lying in output trays of printing devices that may be wholly or partly unmonitored.

According to the Department of Health & Human Services, between September 2009 and September 2016, personal health information of more than 168 million people was impacted in 1,688 breaches that affected more than 500 people. And paper records accounted for 23% of larger breaches.

Paper costs can sting

This is a serious compliance issue. One health organization settled a compliance violation for $475,000 after it failed to notify in a timely manner that more than 800 operating room schedules that contained protected health information had gone missing.

HHS' Office for Civil Rights (OCR) has picked up the pace of violations enforcement, and a key reason is increased auditing. OCR's Phase 2 HIPAA Audit Program, initiated in 2016, reflects more aggressive enforcement, including walk-through audits.

HIPPA audit case studies reported by Health Management Technology detail user access issues for which two organizations were examined.

"From a security perspective, the auditors make sure that computers that are unattended have been logged off per policy, passwords are not 'taped to the keyboard,' printers and fax machines are not where the public could remove confidential information, that locked rooms are indeed locked, and that badge access to secure areas is being utilized," according to the publication.

Protect the document

It's typical in a work environment for printers and imaging devices to be in open-access areas. With nobody monitoring a device, and frequent foot traffic, it's not difficult for an on-site criminal or a passerby to quickly lift documents that have been left unattended in an output tray.

Lax control over printed documents is a growing problem as many organizations expand mobile device access to workers on the go. Such workers may print remotely and forget about them, or delay in picking them up.

Protecting documents requires a combination of policy and technology. On the policy front, healthcare organizations should implement and enforce clear cut access-authorization guidelines.

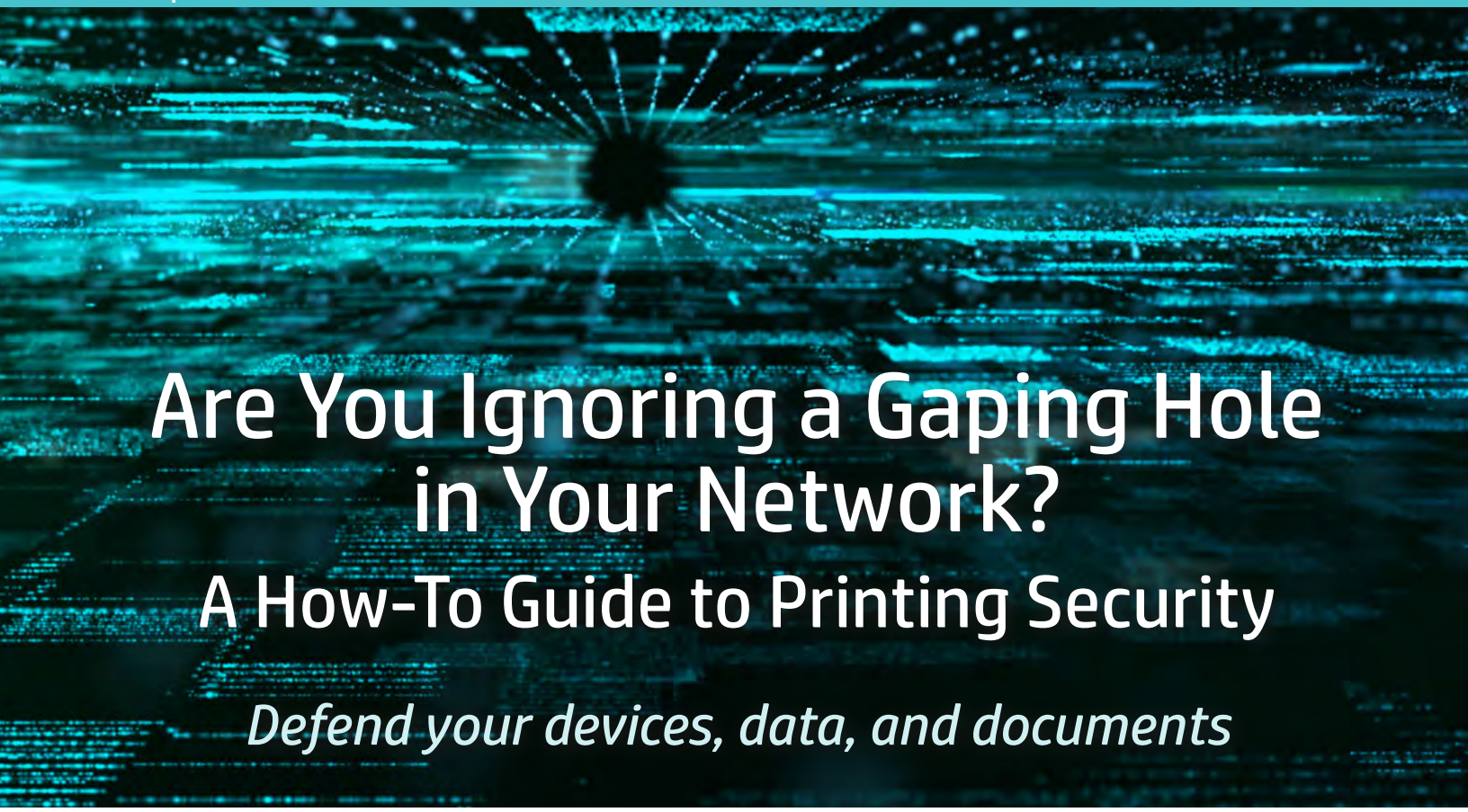
Simple to sophisticated solutions

Components of a print security solution can be relatively simple, such as employing locked input trays that prevent misappropriation of special payments used for printing items such as paychecks or prescriptions.

Or print security can be as sophisticated as HP's comprehensive access control system modules that provide print authentication, auditing, authorization, accounting, and secure "pull" printing capabilities that are scalable across the healthcare organization. (Pull printing stores print jobs in the cloud or on the user's PC—users authenticate at their chosen print location to pull and print their jobs.)

Other tools that organizations can consider include requiring a secure badge to release a print job, or allowing users to assign a PIN when they send a print job that can only be completed when they enter that PIN at the device.

Healthcare organizations can't afford to ignore the potential risks of paper-based breaches. **To learn more about how to protect your organization from these risks, go to** HP Print Security.



Are You Ignoring a Gaping Hole in Your Network?

A How-To Guide to Printing Security

Defend your devices, data, and documents

Imagine this scenario: An asset management company is hacked by a cyberterrorist who exploits unsecured printers in order to leak details of the firm's impending merger with another company. The hack costs shareholders $1.2 billion overnight as their stocks plummet, and the companies involved nearly go under.

The scenario—detailed in the film **The Wolf** by HP Inc. and starring Christian Slater—is fictitious, but the dangers posed by vulnerable printers are very real.

That's because although many IT departments rigorously apply security measures to individual computers and networks, printing and imaging devices are often overlooked and left exposed. And unsecured devices can expose the entire network to cybersecurity risks.

Printers: A weak link

And those risks are higher than ever. The number of data breaches is on the rise, as are the costs associated with breaches. Ransomware that holds company data hostage as encrypted files until ransom money is paid, distributed denial of service attacks that can take down company websites, and a proliferation of viruses all increasingly threaten the data and reputations of organizations around the globe.

Yet only 18% of companies monitor printers for threats, according to a Spiceworks survey sponsored by HP.[1] This overlooked, yet extremely common point of vulnerability exists because, as technology market

1 Spiceworks survey of 309 IT decision makers in North America, EMEA, and APAC, November 2016.

intelligence firm IDC notes in a recent report on printer security, "the printer is an endpoint" on enterprise networks—one that enterprises need to more proactively address. Moreover, "printers are IoT devices that are highly vulnerable to attack because of the requirements of keeping them open and accessible to the entire organization."[2]

Pull printing — in which a user specifies the printer to print to over a network, and then starts printing only when at the printer — can reduce the risk of sensitive documents falling into the wrong hands.

Plugging the hole

According to IDC, Step #1 for securing printers on an enterprise network is to identify printing and imaging vulnerability points. A survey of potentially vulnerable endpoints will be greatly helped by a network access controller or an asset management tool that can discover devices on a network.

- **Patching and updating printer firmware and software** as soon as updates are available will also help close known vulnerabilities. IDC points out that many manufacturers offer management tools for monitoring and patching their printers, making the job of keeping printers up to date that much easier. As the report says, "the vast majority of breaches occur because of a lack of hygiene." In other words, keeping printer software up to date is key to reducing security risks.

- Next, IDC recommends **closing any open ports** the printer may have shipped with that aren't actually needed in a given environment. These ports may include a wide range of TCP and UDP ports intended for telnet, FTP, and web access that could present unnecessary vulnerabilities if they are not used by an organization.

- Add to that list **unneeded Wi-Fi and Bluetooth functionality on printers.** In HP's The Wolf, the cyberterrorist loads malware from his phone onto a printer through an unsecured Wi-Fi or Bluetooth connection. HP recommends turning off Wi-Fi and Bluetooth access on printers that don't need it (or, if it is required, adding mobile authentication and encryption).[3]

- **Onboard storage media** such as hard drives full of stored print jobs represent additional potential vulnerabilities on a printer, as do unattended output trays. The cyberterrorist portrayed in The Wolf, for example, steals sensitive information in the form of a printed report left in an output tray.

- **Pull printing**—in which a user specifies the printer to print to over a network, and then starts printing only when at the printer—can reduce the risk of sensitive documents falling into the wrong hands. Such documents can be further secured on many printers by requiring the user to enter a PIN on the control panel. Onboard printer storage that encrypts and then regularly erases print jobs can help secure documents before and after they are printed.

How HP can help

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

HP business printers are protected from attack by continuous self-monitoring. The printer's BIOS is checked on every startup to ensure that it is unaltered. A firmware check next ensures that only authentic HP software needed for running the printer loads to memory. And monitoring during operation stops attacks that might occur while a printer is running—all without intervention from IT personnel. In the event that a printer is compromised, HP Sure Start—the only self-healing BIOS in the industry—forces the printer to immediately reboot and overwrite corrupted code with an embedded, isolated clean copy.[4]

HP printers protect sensitive information in transit by encrypting it over the network with encryption standards and tools including HP Universal Print Driver Secure Encrypted Print. Sensitive information on the printer is secured with encrypted drives and with optional HP Trusted Platform Modules that generate certificate private keys at the printer.

Unfortunately for the financial firm in The Wolf, none of these features was in place at the time the company was attacked. But, fictional though it is, this example can serve as a warning for real-life companies that still need to secure those most vulnerable devices at the edge of their networks: their printers.

To learn more, go to HP Print Security.

2 IDC, "The Printer Is an Endpoint: Proactively Addressing the Security Vulnerability," 2016.

3 HP Development Company, "Keep The Wolf Away: Security Risks in 'The Wolf' Films and HP Solutions," June 2017.

4 Applies to HP Enterprise-class devices introduced beginning in 2015 and is based on HP review of 2016 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. A FutureSmart service pack update may be required to activate security features. For a list of compatible products, see hp.com/go/PrintersThatProtect. For more information, visit hp.com/go/printersecurityclaims.