Why Print Security Matters in Healthcare

Healthcare organizations face unique cybersecurity risks, but solutions are available.

IDG
STRATEGIC MARKETING SERVICES

Why Print Security Matters in Healthcare

Healthcare organizations face unique cybersecurity risks, but solutions are available.

CONTENTS

Healthcare Ailing in Cybersecurity

When it comes to maintaining security, healthcare organizations sit between a rock and a hard place. Healthcare organizations must meet the challenges of protecting Electronic Medical Records (EMR) while, at the same time, providing authorized personnel with access to the information they need.

To keep patients safe, information must be accurate and delivered quickly. But hospitals are public environments with patients, clinicians, staff, visitors, and suppliers coming and going. Sitting among all this coming and going are a broad range of sophisticated—and networked—devices, ranging from computers and phones to IV pumps and X-ray machines. All of these devices are computers with network connections. And many of them have little to no security protections and are often unattended, each representing a potential entrance to the entire network.

74% of organizations have experienced an external IT security threat or breach in the past year.[1]

70% of organizations have experienced an internal IT security threat or breach. [2]

"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."

Beware "The Wolf"

Watch Christian Slater as "The Wolf" while he disables a healthcare organization's entire network through unsecured printers.

Watch video

Healthcare data attracts thieves

Healthcare organizations are a particularly attractive target for cybercrime because they're sitting on massive volumes of potentially vulnerable personal health and financial information. 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.

"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."[3]

Brookings Institute

[1] Spiceworks survey on behalf of HP, 2016
[2] Spiceworks survey
[3] Brookings Institute: Hackers, phishers, and disappearing thumb drives: Lessons learned from major health care data breaches, May 2016

Sure enough, in May 2017, malware known as WannaCry caused 37 of the health trusts in the UK's National Health Service to shut down, eventually spreading across 150 countries by seeking out vulnerable computers and networks across industries. Also in 2017, a similar attack infected hospitals in the U.S. and a major pharmaceutical organization.

Costs and consequences

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.

The Federal government can impose steep civil penalties for failure to comply with privacy and security rules. 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.

Unattended security holes

Because healthcare organizations are busy places with a constant flow of people moving around, it's particularly easy for a criminal to take advantage and utilize an unattended workstation to wreak havoc. A hacker can simply sit down and gain access to any data across the network—or use a USB drive to upload malware.

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.

Another often-unprotected device is the network printer, most of which feature USB ports with a direct path to the processor for code execution—a physically present hacker can upload malicious code that, when activated, can provide many ways to exploit data.

"Unfortunately, printers have joined networked computers, laptops, tablets and smartphones as increasingly popular entry points for hackers and careless (or unscrupulous) employees to breach networks, steal sensitive data, or cause digital mayhem," writes HP's Enrique Lores.

Hospitals have too much at risk to leave endpoints unprotected. A good first step is to take a systematic approach to reviewing networked equipment to find vulnerabilities. Then start plugging those security holes by performing software updates or replacing outdated devices with systems that have security built in. One good place to start is with your printers and imaging devices, which handle a lot more data than you might realize and are often left unsecured.

A Hidden Risk: Printing and Imaging Devices

Throughout the healthcare industry flows lots of valuable data, often in rushed environments by people focusing on issues far outside of security. While hospitals are increasingly using digital devices such as tablets and computer consoles in exam rooms to transmit information, hard copy information still plays a big role. Because of that, printing and imaging devices are still integral to healthcare environments.

Overlooked and undersecured

The fact is, printers, like other network devices, can pose an alarming cybersecurity risk. Printer attacks usually focus on the information flowing through the device, but multifunction printers (MFPs) and larger network printers are also attractive targets.

Most MFPs can store printed data electronically, for example print jobs stored in a cache. If left unsecured, a hacker could access a printer's cache and download documents containing sensitive data. Cybercriminals can also upload malware to unsecured devices, giving them access to spy on and exploit your network.

Because printing and imaging devices are everyday tools that require little or no expertise to use, they're often overlooked in security policies and best practices. However, networked printers and imaging devices may include operating systems, storage media, and software that the average user has no idea about—but a hacker does.

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.

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

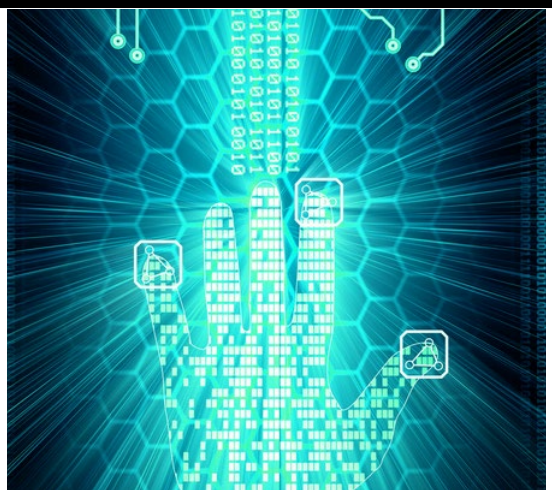
Protecting the data that flows into and out of printers and imaging devices is one level of security. But don't forget what these devices output, and which also contains lots of valuable data: paper.

Paper chain compliance risks

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. This poses a big compliance risk. 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.

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.

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.



Because printing and imaging devices are everyday tools that require little or no expertise to use, they're often overlooked in security policies and best practices.

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 their documents, or delay in picking them up.

Applying more controls over when and how documents are printed, and who has access to the output trays, should be included in any security policy within a healthcare organization. This starts with creating a print security framework that includes devices with security built in, like **HP Enterprise printers.**

How to Approach Multi-layered Print Security

Data breaches are on the rise, as are the costs associated with them. Ransomware that holds company data hostage as encrypted files until ransom money is paid, DDoS 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.[4] This overlooked yet common vulnerability exists because, as technology market 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."[5]

Plugging the hole

IDC proposes a systematic approach to print security that covers these best practices:

1. Survey your fleet

Identify printing and imaging vulnerability points. A network access controller or asset management tool that discovers devices on a network can help streamline this process.

2. Update firmware and patchware

Patch and update printer firmware and software as soon as updates are available. IDC points out that many manufacturers offer management tools for monitoring and patching their printers, simplifying the job of keeping printers up to date. 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.

3. Close open ports

Close any open ports the printer may have shipped with that you don't actually need. These 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.

4. Limit Wi-Fi and Bluetooth

Disable unneeded Wi-Fi and Bluetooth functionality on printers. Or, if it is required, add mobile authentication and encryption.

5. Use pull v technology

Onboard storage media such as hard drives full of stored print jobs represent additional potential vulnerabilities on a printer, as do unattended output trays. Pull printing—in which a user specifies a network printer and then starts printing only when at the printer—can reduce the risk of sensitive documents falling into the wrong hands. Requiring the user to enter a PIN on the control panel adds another layer of 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

How HP can help

Printers from HP, such as **HP LaserJet** and **HP PageWide Enterprise** printers, offer best-in-class security features to keep your data safe and protect your networks in three main areas: device security, data security, and document security.

Device security

HP can help defend your network with the world's most secure printing[7] —including devices that can automatically detect and stop an attack.

[4] Spiceworks survey of 309 IT decision makers in North America, EMEA, and APAC, November 2016.
[5] IDC, "The Printer Is an Endpoint: Proactively Addressing the Security Vulnerability," 2016.
[6] HP Development Company, "Keep The Wolf Away: Security Risks in 'The Wolf' Films and HP Solutions," June 2017.
[7] "Most secure printing" claim based on HP review of 2016 published security features of competitive 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. For a list of printers, visit: hp.com/go/PrintersThatProtect. For more information: hp.com/go/printersecurityclaims.

- **Intrusion detection:** HP Sure Start and run-time intrusion detection protect at startup and during operation. If malware is detected, the printer automatically reboots. At each startup, HP Sure Start validates the integrity of the BIOS code and self-heals if necessary.
- **Update authentication:** HP Enterprise printers also include whitelisting to help ensure that only authentic, digitally signed HP firmware is loaded into memory.
- **Output monitoring:** HP Connection Inspector evaluates outgoing network connections to determine what's normal, stop suspicious requests, and automatically trigger a self-healing reboot. Stop malware from "calling home" to malicious servers, stealing data, and compromising your network.
- **Policy enforcement:** 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

To protect data, you must make sure that only authorized users can access devices and the networks they are connected to.

- **Access control:** Fleet-wide authentication solutions can require users to enter a password or PIN, or scan their badge or fingerprint. HP solutions include HP Universal Print Driver[9] and HP Access Control for PC network printing, and HP JetAdvantage Connect and HP Access Control for mobile users.
- **Data encryption:** Data in transit should also be encrypted. Data traveling between PCs and the network is often encrypted, but data flowing to and especially from printers is often overlooked. Administrators should use Wi-Fi and network encryption protocols along with solutions like HP Universal Print Driver, HP Access Control, or HP JetAdvantage Connect.
- **Certificates:** Apply signed certificates to network printers and MFPs. Save time by using HP JetAdvantage Security Manager to automatically install and renew certificates.

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.

Document security

HP offers several authentication and pull print solutions for a variety of situations and IT environments.

- **User authentication:** HP Access Control Secure Pull Print is a server-based pull print software solution that can be set to require all users to authenticate before retrieving their job.
- **Cloud storage:** 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.
- **User control:** HP Universal Print Driver is a free print driver solution that includes a secure encrypted printing feature for sensitive documents. It allows users to send a print job to be held until they release the job via a PIN at the device.
- **Swipe access:** The HP Proximity Card Reader lets users quickly authenticate and print securely at a printer or MFP using their existing ID badge.

A partner in HP

HP Print Security Services and specialists can help with print security assessments, planning, deployment, and ongoing management. HP Print Security Advisory Services can help 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 organizations maintain security settings compliance across the printer fleet.

HP understands healthcare security challenges and how to meet them. Whether it's in a clinic, a visit room, a doctor's office, the back office, a provider's home office, or a health insurance company, HP has the print solutions to help organizations reduce risk while improving efficiencies.

Learn more at **HP Print Security.**

[8] HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager. Competitive claim based on HP internal research on competitor

[9] The HP Universal Print Driver is available for download at no additional charge at hp.com/go/upd.