The Printer Playbook

Strategy and insight for the enterprise

LaserCare™
MANAGED PRINT EXPERTS

Content

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Introduction: Information in the enterprise

All the headlines about the profusion of information aren't marketing hype. We've entered a new frontier in the information age, where petabytes of data are a mere click or tap away. We're living in a mobile, app-driven world in which people expect answers immediately. This is changing every aspect of society.

From a business perspective, this shift presents both opportunities and challenges. It's accelerating business processes and making employees more productive. As teams more easily share data and act on it, they can more quickly make decisions. On the other hand, information poses a security risk. As businesses become increasingly digital and networked, so does their sensitive and confidential information.

Enterprise organizations in every industry are grappling with this paradox. How do you enable mobile access to your network and its applications and devices without opening yourself up to attack?

Enterprise organizations in every industry are grappling with this paradox. How do you create more open, collaborative work environments, where employees can easily access and share information, without compromising information security? How do you encourage employees to use information to make better decisions without putting the enterprise at risk? And how do you enable mobile access to your network and its applications and devices without opening yourself up to attack?

The Printer Playbook examines the multifunction printer (MFP) within this broader context of information abundance. And it explores two important areas pertinent to the MFP's role in the enterprise—security and mobility.

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The networked MFP: Convenient and secure

Enabling convenient and secure access to information throughout the enterprise is a difficult balancing act. It involves a range of enterprise technologies and business considerations: the network, computers, and mobile devices; web applications; servers; intranets; and even privacy laws and compliance requirements—all of which require varying levels of access and security. The networked MFP is one such device to consider.

MFPs offer a range of information-sharing features, including basic functionality to print, scan, and email documents. They can also print documents directly from smartphones and tablets, and pull print jobs from the cloud. As such, they enable worker productivity and play an important role in enterprise workflow. But they're also equipped with hard drives and local storage, which enables them to store sensitive and confidential information. Essentially, any sensitive document that passes through an MFP, whether printed or scanned, is stored for some period of time on the hard drive. In that sense, an MFP is just like a computer and poses as much of a security risk as any networked hard drive.

Yet many enterprises neglect the potential security risk posed by MFPs. Research firm Quocirca recently reported that just 22 percent of businesses place high importance on printer security.[1] Moreover, the firm found that 70 percent of organizations report that one or more accidental data breaches occur through printing.[2]

More than 90% of organizations have security practices for desktops, laptops, and servers. Only 44% have security practices for their printers.

Source: HP Printer Security Research, Spiceworks Voice of IT Survey, January 2015

The good news, however, is that you don't have to prohibit mobile access to your networked printers in order to make them secure. Most MFPs offer a variety of security features that, when properly implemented, allow all the productivity and workflow benefits of printing from your mobile device without compromising on security.

In fact, if like most large IT organizations you support BYOD in the enterprise, your print management strategy should serve the needs of your mobile workforce. Employees who aren't offered a convenient mobile printing option will likely create their own work-around, flouting your security protocols in the process. Nearly 60 percent of security breaches are accidental, due to employee negligence or IT or business-process failure.[3]

[1] "Printing: a false sense of security?" Quocirca, 2013
[2] "The Mobile Print Enterprise," Quocirca, 2015
[3] "2014 Cost of a Data Breach Study: Global Analysis, Ponemon Institute," May 2014

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Secure printing in the enterprise

Start with securing your documents

Security measures to help you monitor and control access to confidential documents can be an important piece of an overall print security strategy. Documents left or abandoned on the printer output tray pose data security risks. If the wrong person picks up an abandoned document containing sensitive or confidential information, they could break any number of HR, privacy or securities laws. And breaking these laws often results in severe financial penalties.

Cutting down on abandoned or forgotten print jobs can help enterprises save money. Recent IDC research suggests a company with more than 1,000 employees spends more than $200 per employee in direct hard-copy costs.[4]

Don't overlook input trays

For some enterprises, even the printer input tray presents a potential security risk. For example, if you print on special paper for medical prescriptions or your payroll, that paper should be in a locked tray, otherwise people can easily remove it and use without authorization or anyone ever knowing. Regular paper might also be stolen, leaving departments to foot the bill. These costs can add up. IDG research shows that on average, companies spend five percent of annual revenue on document costs.[5]

Download this case study to learn how pull printing helped the Canadian Automobile Association of South Central Ontario increase efficiency, reduce waste, and decrease paper and toner costs.

Capture and route documents for efficient workflow

MFPs can do a lot more than simply print. They can "capture and route" documents directly from a printer. This allows users to scan, upload, and easily send documents to a variety of destinations: fax machines, e-mail addresses, and cloud or business applications such as Microsoft SharePoint®, to name a few. But this feature could also pose a security risk. Imagine if a rogue employee found a sensitive document on a printer and wanted to scan and email it to people who shouldn't see it? To help ensure "capture and route" isn't used for nefarious purposes, it allows you to specify who can use use the feature, as well as to whom those individuals can route documents.

"Capture and route" offers enterprises a range of benefits, including reduced document printing, storage, and shipping costs, elimination of dedicated fax lines, and even freed up office space.

Find out how Merck is using capture and route technology to streamline and digitize workflow. Click here.

MERCK

[4] "Tech Briefing: The Business Benefits of HP's Balanced Deployment," IDG

[5] "Tech Briefing: The Business Benefits of HP's Balanced Deployment," IDG

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Authenticate for a safe hand off

User authentication technology is one of the most effective ways to eliminate the risk of abandoned print jobs. To retrieve a print job, users must enter a PIN, or use smart cards or biometric scans, in order validate their identity. This helps ensure that a document never lands on an output tray without the intended recipient there to pick it up.

When combined with private or pull printing, a user can send a print job to a global queue (server or cloud) and then pull it down to any printer after authenticating with his or her credentials.

Pull printing also reduces cost and paper waste by making print-job retrieval more efficient. Pull printing can help reduce costs and waste by helping to eliminate unnecessary print jobs. It can also help reduce instances of printing on expensive specialty media. Instead, pull printing enables the person to go to any free printer to retrieve the document. This feature is particularly convenient for business travellers who may want to print documents from a main office, but retrieve them at a regional office. Pull printing also eliminates the “print and sprint” syndrome, in which people run to the printer to pick up a document with sensitive information before anyone else can see it.

Usage tracking and feature restrictions

As part of your overall print security strategy, you may want to monitor printer usage, and in some cases, restrict access to certain printer features for specific people or groups. For example, setting permissions for who can print in color, single sided, with special toner, or on oversized paper, to who can access the hard drive or scan and email documents; these permissions will help you mitigate security risks and reduce costs. And monitoring employees’ use of your printers allows you to manage the placement of printers to match printing needs.

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Protecting data

It's not always the information on your printer output tray or in its hard drive that poses a security risk. Sometimes it's the data on its way to your printer.

Without the right network security protections in place, data traveling to your printer could be intercepted by hackers, corrupted, or altered. To continuously protect the data on your network and help mitigate this threat, consider Internet Protocol Security (IPsec), SSL, or other data encryption methods. Just as connected computers and MFPs should be shielded from outside eyes, so too should be the roads that connect them.

Unprotected, an MFP's hard drive can be a data source hackers. That's because every document that moves through an MFP is captured and stored temporarily on the hard drive, including printed, scanned, and emailed documents. Additionally, MFPs equipped with user authentication capabilities will store user names, PINs, and other authentication information. The most effective way to protect data on the hard drive is to first encrypt it, and second, conduct daily or regularly scheduled disk wipes to erase the data. You can also safeguard your hard drive with disk image overwrite, choosing to either automatically remove data once a print job is completed or do so on a scheduled basis. It's also important that you perform a final hard drive data wipe prior to replacing or disposing of your printers.

Supporting remote and mobile workers

"At the office" has many meanings these days. Mobile computing and communications and an array of collaboration tools have enabled a mobile workforce that's equipped to work from virtually anywhere. Whether based at home or on the road, the remote and mobile worker is now an integral part of the modern economy. Often a salesperson or traveling executive, these workers rely heavily on their laptops, tablets, and smartphones.

Many organizations are expanding the ranks of their remote and mobile workers. A mobile workforce allows them to lower real estate costs, extend their geographic reach, and offer flexible work schedules. But when remote workers are on site, how do you provide seamless and secure connectivity? How do you extend that connectivity to printing so that it's quick and easy? And it's not just mobile workers who want to print from their devices. With BYOD the norm and supported by many IT departments, today's office workers want to print from their smartphone or tablet of choice.

To minimize risks, most IT administrators hard wire their printers to the network, rather than using Wi-Fi connectivity. Similarly, they tend to not allow wireless connectivity between mobile devices and networked printers. Although this helps mitigate Wi-Fi security breaches, it makes mobile printing difficult—for the visiting executive and everyday employee. Even for organizations using a mobile device management (MDM) solution, mobile printing is still a challenge. You cannot access most network printers, for example, from an MDM environment.

Striking a balance between network security and access to network applications and devices, such as printers, is always a challenge. It's especially tricky with mobile printing, as the ranks of mobile and remote workers continue to grow.

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Secure mobile print solutions

Despite these roadblocks, there are mobile print solutions that are both user friendly and allow you to protect the network and sensitive business information. And that's a good thing, because many enterprises want that capability. A recent Quocirca report found that 83 percent of enterprises are interested in mobile print capabilities, but only 14 percent have deployed a mobile print solution.[6]

If you're among the IT administrators who don't allow mobile devices to access your network or infrastructure, peer-to-peer wireless printing can meet users' demands without compromising strict security standards. It allows employees to print directly from a mobile device to a printer, without having to access the same network subnet as the printers. By sidestepping the network altogether, peer-to-peer wireless printing allows you to maintain your BYOD secure network access approach while providing direct access to the company printers.

Printers with peer-to-peer wireless connectivity use 802.11b/g Wi-Fi technology and appear to users as a Wi-Fi network. But the connection is completely separate from your LAN and back-end infrastructure. You manage access to the device through a configurable passphrase that appears prior to connection, and your document is encrypted before it is wirelessly sent to the printer.

Near field communication (NFC) technology provides another way to make a peer-to-peer wireless connection between the printer and a mobile device. To support NFC-based printing, you accessorize your printer with an NFC antenna. To print from an NFC-enabled device, users simply open a document and touch their device to the printer's NFC antenna.

[6] "The Mobile Print Enterprise," Quocirca, January 2015

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Compliance

Laws to protect individuals' personal, financial, and health information have made compliance integral to every organization's strategy and operations. Whether it's an internal or external information security breach, exposing such sensitive information can bring not only stiff financial penalties, but often times an even bigger, costlier PR backlash. So regardless of the specific law—HIPAA, Graham-Leach Bliley, or the Sarbanes-Oxley Act—organizations must be more vigilant than ever in protecting sensitive or confidential data and documents. And you should never overlook your networked multifunction printers (MFPs) when developing an overall strategy and set of security measures to comply with these laws.

Unfortunately, many IT organizations fail to employ acceptable security measures for their printers. A recent Quocirca report revealed that nearly 90 percent of enterprises say they have suffered at least one data loss through unsecured printing.[7] And in a recent Spiceworks survey, fewer than 20 percent of respondents perceived their printers to be at moderate or high risk for security breaches.[8]

It's hard to say why so many enterprises fail to appreciate the potential security risks in MFPs. It's possible they're not aware of the security risks created by network connectivity and MFP features such as the ability to print, scan, email, store data, and browse the Web. These convenient information-sharing features can improve productivity and enhance workflow, but they can also open your organization to a variety of potential security breaches. The fact is, MFPs with these capabilities should comply with the same security measures as any computer on your network.

So what measures are they?

Printer auditing

An auditing tool can record and trace every user interaction on a printer, allowing you to track who is using the printer and what documents that person is printing, copying, or scanning. Coupled with feature restrictions for individuals or groups, you can control and monitor what people are doing with your printers, which helps mitigate the chance of a compliance-related security breach.

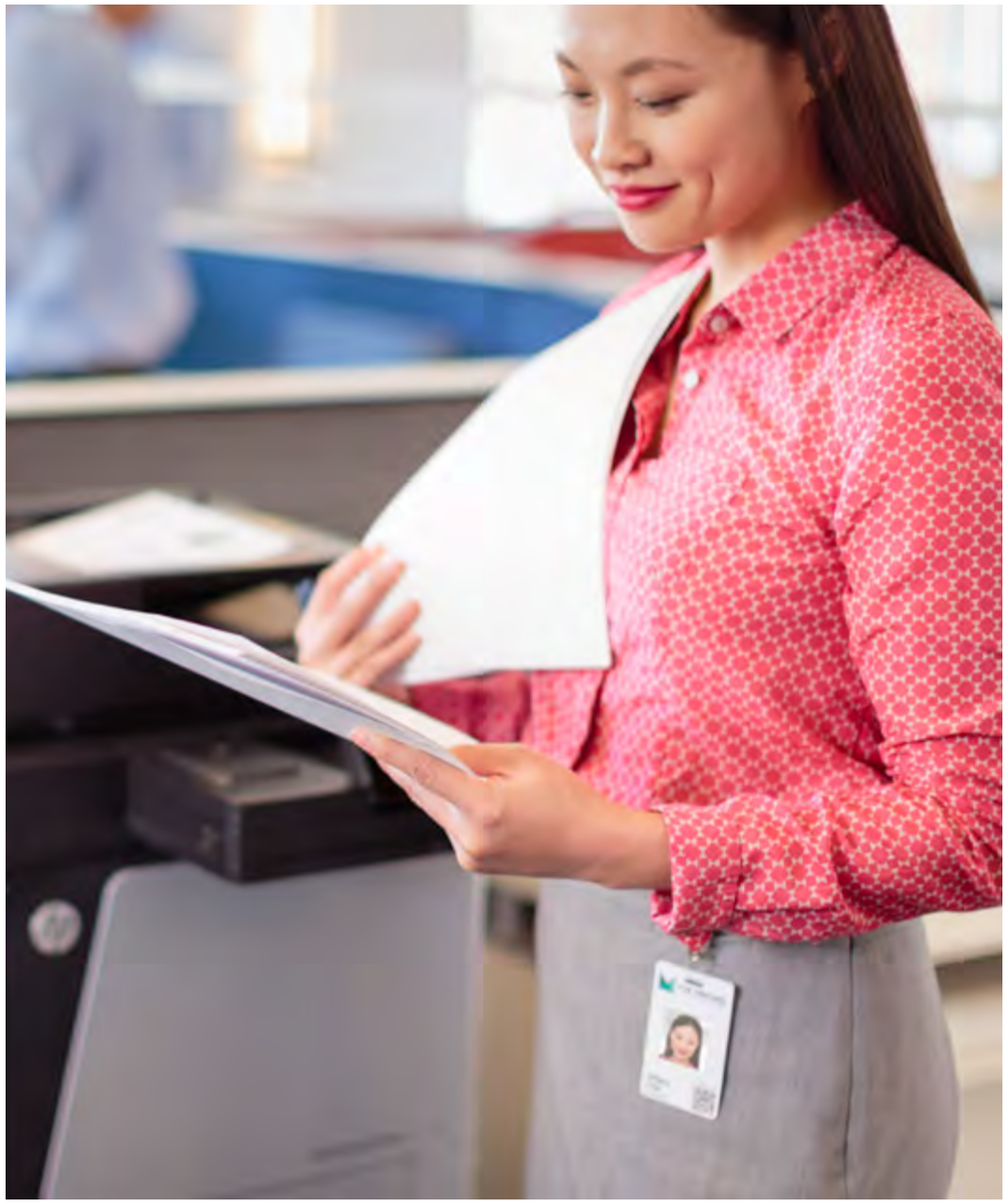
[7] "Managed Print Services Landscape," Quocirca, June 2014
[8] "HP Printer Security Research," Spiceworks Voice of IT Survey, January 2015

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Fleet management

If your idea of the perfect printer is one that simply works, you're not alone. Printer reliability and operational costs have long been a focus for IT, and for good reason. When you're tasked with manually managing a multi-vendor fleet of printers across multiple locations, the time required for each update, setting change, and support ticket adds up quickly. It's not surprising that many IT professionals focus on the cost and manageability of printers, rather than new innovations that can benefit the business.

There is a solution. A fleet management tool enables you to manage all your printers remotely, through a single management console. For instance, you can auto-discover new and existing printers on your network, and remotely configure those printers so they adhere to your corporate printer policies. You can also remotely configure settings for entire groups of printers to add or disable features like auto-duplex printing, color printing, and document scanning. These remote management capabilities eliminate the need to dispatch IT support personnel for every printer change or update, helping to reduce printer-fleet management costs.



Fleet management tools also allow you to easily create and maintain the security settings for all your printers. They include features to:

- Create and automatically deploy a single security policy across your entire fleet
- Secure new printers the moment they are added to the network
- Maintain printer security compliance through automated monitoring and risk reporting
- Automatically deploy and update printer security certificates
- Schedule automatic printer security assessments and remediation

Fleet management tools also offer visibility into the ways in which individuals and groups use printers, allowing you to spot important trends and usage patterns. For example, are people printing in color or black and white? Are printers being under- or over utilized? Is usage increasing or decreasing month over month? The ability to answer such questions allows you to proactively manage your printer fleet and enforce the right printer policies.

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Recognizing security risks

Input tray

Unlocked input tray Sensitive documents may be forged or altered.

Protect sensitive paper from theft and tampering by using a lock that requires a physical key.

Access to special paper Unauthorized users with access may forge documents

Help prevent fraud with the HP and TROY Secure Document Printing Solutions. hp.com/go/gsc

Output tray

Unsecured print jobs Anyone can see what's printed.

HP Access Control Secure Pull Print offers multiple forms of authentication. hp.com/go/hpac

Abandoned print jobs Sensitive information may be intercepted.

HP JetAdvantage Private Print is a cloud-based pull print solution included with your printer purchase. hpjetadvantage.com

Mobile printing Employees on the go may send print jobs to multiple printers.

HP's wireless direct and touch-to-print solutions allows users to print from their mobile device to the nearest printer. hp.com/go/businessmobileprinting

Networked devices Users in BYOD environments may expose the network to malware.

HP's wireless direct and touch-to-print solutions allows users to print without connecting to the company network. hp.com/go/businessmobileprinting

Control panel

Unsecured access panel Users can set features, change permissions or disable the entire fleet.

The JetAdvantage Security Manager offers centralized management of printer fleet security settings and device certificates. hp.com/go/ipsc

Unrestricted feature access Documents can be uploaded and sent to individuals or business applications.

Ensure scans are protected with document encryption features with HP Capture and Route. Control where users are able to route scans and monitor content for information governance. hp.com/go/documentmanagement

Printer hard drive

Unsecured hard drives Hard drives may be removed.

Protect devices from theft and tampering by using a lock that requires a physical key for removal. Disable physical ports.

Unencrypted hard drives Past print jobs, user credentials and other data may be downloaded.

Securely overwrite stored data and remove safely remove sensitive information.

Network

Unsecured network Printing and imaging jobs can be intercepted or altered

The HP Universal Print Driver (UPD) provides print job encryption and decryption. hp.com/go/UPD

Unmonitored fleet Different security settings for devices on the same network

HP ArcSight Printer Integration offers real time monitoring of printer endpoints as well as corrective actions. hp.com/go/SIEM

Manual printer updates Significant resources required to periodically update printer firmware

HP Webjet Admin can help reduce cost and resources to maintain printer fleet firmware upgrades. hp.com/go/wja

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Interactive Assessment

Secure Print Analysis

Assess your printer security strategy

Get started

Are your printers vulnerable to attack?

It’s time to find out

“An unsecured multifunction printer is a prime target for hacking into the enterprise.”

Angele Boyd, IDC Analyst Connection

Today’s multifunction printer does more than simply print. It scans, sends and stores potentially sensitive information. Innovations surrounding networked printers help streamline business processes and increase productivity. At the same time, implementing those additional features may leave your fleet vulnerable to attack. If your printer fleet connects like your computer fleet connects, it should be protected in the same way.

The HP Secure Print Analysis Tool will reveal the range of printer security options now available, and offer guidance on how you can calibrate your strategy accordingly against six printer security categories. Take the assessment to quickly evaluate your printer security practices and capabilities. Find out where you’re doing well, and where you may be falling short. It’s quick and easy.

When you’re done, you’ll receive a summary of your current printer security practices, and recommendations on what you should do next.

[1] “HP: Protecting printers with enterprise-grade security,” Moor Insights & Strategy, 2014

The six printer security hot spots

Network security features & standards
Multifunction printers have hard drives and network access. They can be hacked like computers and be an entry point for malware and viruses.

Fleet management
Lack of central control of printers can lead to inefficient, incomplete, and time intensive efforts by IT to establish and maintain security settings on printers.

Mobile print security
In the absense of a user-friendly mobile device strategy, employees may implement workarounds that could violate established security policies.

Document security
Output trays are an easy way for sensitive data to fall into the wrong hands. Unprotected input trays could lead to special paper – like check stock–being stolen.

User authentication & access control
Without requiring user credentials, it’s possible for sensitive documents to be retrieved by any user. Anyone who can access printer settings can exploit permissions.

Printer hard drive security
Printing and imaging devices store user credentials and other sensitive data that can be accessed if it’s not encrypted or periodically erased.

Start now

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Your recommended actions

The summary of your results below offers advice on how to improve your printer security practices over six key areas. Print this summary and use it as a checklist for future discussions about your organization's printer security strategy.

Network security features & standards

802.1x or IPsec network standard to encrypt data between computing devices and networked printers

Apply the 802.1x or IPsec network standards to encrypt data in transit. Encryption makes files nearly impossible to read if intercepted.

Set administrative passwords to change printer / multifunction printer settings

It is highly recommended that your organization apply administrative passwords to lock down the printer / multifunction printer control panel, as well as use SNMP passwords to manage networked devices.

Apply digital certificates or encryption keys to printers and other network endpoints

Save time by using a printer fleet management tool to automatically apply digital certificates to network printers and multifunction printers.

Only purchase printers with encrypted hard disks

Choose print devices with encrypted hard disks or deploy disk erase solutions to remove sensitive data.

Fleet management

The ability to track users and know when and what they print, scan, copy, or e-mail from networked printers

Apply a user authentication solution to track all printing activities and maintain corporate security and compliance standards.

The application of corporate security policies when adding a new printer to the network

Establish a standard level of security configuration, such as a hardening checklist. Use a fleet management tool to automatically apply it to new printers.

Updating printing devices – including regular firmware upgrades

A printer fleet management tool ensures your devices are up to date with the latest device protection and security features.

Management of SIEM software to detect security threats

Include printers as part of your IT ecosystem and use security intelligence and event management (SIEM) software to detect and take corrective action on printer security alerts.

Mobile print security

User authentication & tracking for mobile device printing

Use a managed mobility solution that includes print client authorization with secure authorization tokens, integration with VPN or MDM solutions, as well as specific end user set-up and policy settings.

Limit mobile printing for authorized users only

Deploy a user authentication solution with passphrase, PINs or LDAP authentication to allow mobile device printing.

Corporate print security policies applied to mobile device printing

Apply your overall print security policy to your mobile device printing.

Wi-Fi Direct or Wireless Direct peer-to-peer wireless printing

Peer-to-peer wireless printing allows users to print without connecting to the network or the same subnet as the printers.

Document security

Managed access to sensitive preprinted forms, such as checks or prescription paper

Secure (locking) input trays help prevent the theft of sensitive paper, such as payroll checks, prescriptions and birth certificates.

Requirements and procedures for privacy regulations such as HIPAA

Apply a private or pull-print solution to authenticate users before releasing the print job to the output tray.

Active methods to prevent tampering and alteration of documents

A chemical reacting toner can dramatically reduce the potential for fraudulent alteration of documents.

Special document features to avoid copying or counterfeiting of documents

Multifunction printers can embed fraud protection (i.e. UV inks, watermarks, custom logos, signatures, security fonts) into documents.

User authentication & access control

Require users to provide network credentials to use imaging & printing devices

User authentication methods such as passphrase, PIN, LDAP authentication, proximity cards, smart cards or biometric access controls are effective ways to prevent sensitive documents from falling into the wrong hands.

Printer feature restrictions such as limits on who can scan to network, scan to email or scan to fax

Restrict certain printer features by user or department to reduce costs and security risks.

Require device passwords to access printer settings and administrative features

It is recommended that only IT staff and other authorized individuals be allowed to set-up and configure printer settings.

Limit walk-up use of printer in a public location

Assign printer feature permissions to individuals or groups as well as lock-out walk-up features such as copying.

Printer hard drive security

Printer hard drive encryption

Hard drive encryption is highly recommended to prevent the theft of information stored on the printer's hard drive.

Same day print job removal / clean up

Erasing the printer's hard drive every day is one of the simplest ways to reduce the risk of printer security breaches.

Secured printer disposal / recycling

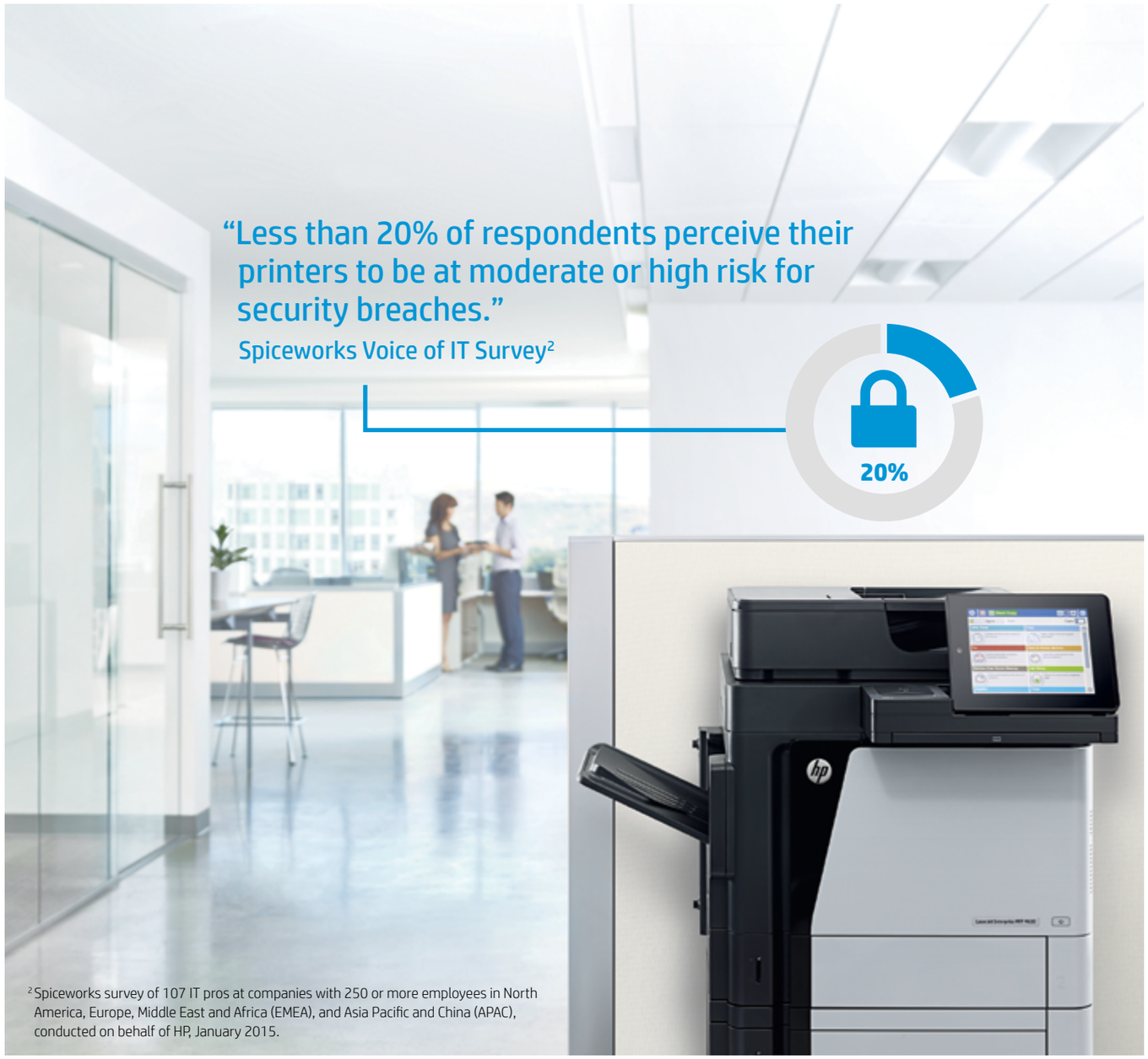
It is critical that data on a printer hard drive is erased or otherwise removed before the printer is replaced, recycled or taken away for disposal.

Review security policies of printer repair and service companies

It is important to control who has access to networked printer settings

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

It’s time to think differently about your printers



[2] Spiceworks survey of 107 IT pros at companies with 250 or more employees in North America, Europe, Middle East and Africa (EMEA), and Asia Pacific and China (APAC), conducted on behalf of HP, January 2015.

Explore the following resources to fortify your printer security strategy.

Audit your printer security strategy and identify the solutions that make sense. Learn about **HP Printing Security Advisory Services**

Partner with HP’s global network of printing and imaging experts to optimize your printing and digital workflow. Explore **HP Managed Print Services**

Learn how to reduce IT costs and enhance employee productivity through centralized printer fleet management. Discover **HP JetAdvantage solutions for fleet management**

Deploy a single security policy across your entire printer fleet, and monitor each device for non-compliance. Check out **HP JetAdvantage Security Manager**

Discover more about HP printing solutions at **hp.com/go/printsolutions** or contact your HP representative.

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Conclusion

As people become increasingly reliant on their mobile devices, and their ability to quickly access and share information becomes essential to their job, how enterprises balance convenient and secure access to information is critical. Those that can strike the right balance and empower employees with information, while at the same time safeguarding its sensitive data, will be the best positioned to succeed in today's information-centric economy. The networked multifunction printer, with its array of security and information-sharing features, will play an important part of that success.

Resources

HP JetAdvantage solutions for security
HP JetAdvantage offers a full suite of embedded and optional print security features and solutions that integrate with your overall IT strategy.

HP Imaging and Printing Security Center (IPSC)
HP IPSC offers a streamlined, policy-based approach for securing your fleet of HP printers and imaging devices. Deploy, monitor and remediate your printers and imaging devices through a single security policy.

HP Capture & Route
With HP Capture and Route, it's simple to capture a document and route it to where it's needed. Now documents can become more accessible and easier to find, distribute, and track. This increases productivity and streamlines processes, while supporting record retention, document security, and privacy requirements.

HP Prescription Printing Solution
Assists with helping to meet government requirements.

HP Patient Identification Printing
Increase safety and efficiency with laser-printed wristbands that feature color and photographic identifiers over and above two-dimensional and linear bar codes.

HP Distributed Workflow Solutions for Healthcare
Help reduce healthcare costs and improve patient care with Enterprise Content Management (ECM) solutions that streamline and automate paper-based document processes.

HP Check Printing Security Solutions
Embeds fraud prevention technologies to control check printing and help combat fraudulent alterations to the finished check.

HP Compliant Document Capture Solution for Financial Services
Capture, archive and track regulated documents, email and faxes, providing improved productivity and can reduce operating costs.

LaserCare™
MANAGED PRINT EXPERTS
(800) LASER-20 | www.lasercare.com

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.