Document and Endpoint Security

Checklists and Discussion Guides

Contents

Use this eBook as a guide to help your organization make the best choices for protecting business documents and securing the multifunction printers and devices that create them. We've also included lots of downloadable checklists to make the information easier to share and use.

Overview: Reducing Risk in the Document Domain

No one can afford to ignore information safety, especially when it involves documents.

A Widespread Concern

Document security affects many industries—healthcare, finance, government, education, pharmaceutical, retail, manufacturing and more. According to one IT study,[1] 90% of U.S. organizations experienced leakage or loss of sensitive or confidential documents over the 12-month period studied. Not surprisingly, InfoTrends research has also identified security as one of two main IT initiatives among U.S. businesses.[1]

Different views. Same risk.

The need for information security is pervasive, but it means different things to different functions within an organization. The executive suite and the legal team want to protect intellectual property from competitors and keep customer financial and personal information safe from hackers. Employee records and personally identifiable information create concerns for Human Resources. Industry regulations and mandates add more complexity. In healthcare, organizations must maintain the security of patient records as a part of its regulatory compliance efforts.

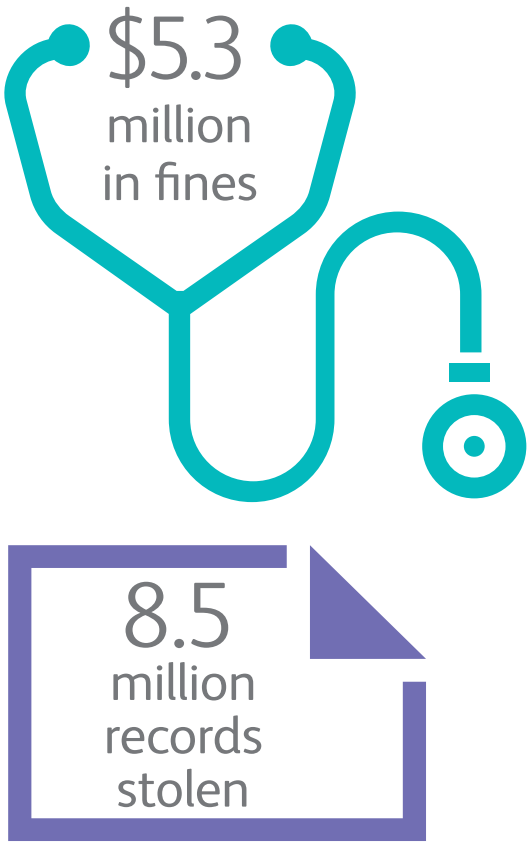
And what about IT? Well, you're involved in all of it.

Here are just two examples of what happens when organizations put themselves in harm's way from unsecured paper documents:

In 2011, the U.S. Department of Health and Human Services, citing HIPAA, fined two hospitals a total of $5.3 million for improper management of paper records.[2]

A Florida bank agreed to pay the state $850,000 plus an additional $125,000 to a charitable organization after an employee stole records containing credit card numbers, bank account information and other personal data of 8.5 million customers.[2]

Many more examples are just a search away.



[1] *Document Security and Compliance: Enterprise Challenges and Opportunities*, InfoTrends, April 2013.

[2] *Paper Chase: The Huge Security Risks Now In Your File Room*, Forbes, March 2012.

Taking the Security Threat Seriously

This threat isn't going away, so take measures to ensure safe practices in all your document infrastructures and processes.

As you explore security solutions, you'll find a vast array of pitches, proposals and plans. Trying to absorb all this information may, at best, delay your progress. At worst, it could ruin your investment.

This eBook will help you focus on the important factors involved in a document security strategy. You'll understand what questions to ask and why, what things to make sure are in place, how to keep users in the picture and how to evaluate possible partners and solutions.

Use these **checklists and discussion guides** to ensure your Managed Print Services (MPS) partner keeps the data on your multifunction printers (MFPs) as safe as possible. Learn more about specific capabilities that ensure the security of your MFP endpoints.

We've divided the information into categories for user-related issues, device factors and how to vet an MPS partner to help with document security. Read straight through or jump to a particular section. **Share this eBook** with your colleagues who are also involved in document security choices.

When everyone is well informed and on the same page, you can be more confident in your document security decisions.

User-Related Issues: The Human Side of Document Workflow

Research and experience tell us the riskiest part of a document process might be the people who use it.

Research has found that the human factor accounts for 35% of data breaches.[3] Yet this risk often gets overlooked and, as a result, employees can be your biggest threat. Knowledge workers and other employees may mean well, but they're human. They make mistakes. In some instances, they find shortcuts, so they can do more with less. And sometimes, they make document security decisions that put the organization at risk.

What to do? First, tap in to analytics to find out how your users are working with documents and devices.

User analytics can answer questions like these:

- Who is printing outside business hours when few employees are working?

  Business impact: cost, security

- A key person has resigned. What has he been printing recently?

  Business impact: security

- Has an employee scanned or emailed content to an unauthorized location like a public cloud?

  Business impact: security, compliance

"Employees and negligence are the leading cause of security incidents, but remain the least reported issue."

—Ponemon Institute Study[3]

35%

of data breaches are due to human error.[3]

[3] *2013 Cost of Data Breach Study: Global Analysis*, Ponemon Institute.

The Value of User Analytics

Partner Qualifications Checklist

MFPs and other printers may generate hard-copy business documents, but it's users who drive the process. That's why a user-centric view of document output—and input—is essential for a total picture of your document environment. Without understanding what users are doing with their documents and devices, you may miss opportunities to modify behavior and reduce risk and expense within your organization.

Every organization has information that must be protected. User Analytics lets you see who is accessing, printing and scanning certain types of documents and intellectual property. User Analytics can capture that information and present it as clear, useful visualizations.

You can then decide if additional safeguards are needed.

Checklist: Can your MPS partner handle analytics?

> Download checklist

An MPS partner may be able to help you with user and document analytics. Here are some signs a provider is up to the task:

- ☐ Maps your current-state and benchmarks to your peers, based on years of data collected from MPS clients.
- ☐ Compares your current state to where you want to be.
- ☐ After data capture and analysis, your partner creates a road map for ongoing improvements to document processes.
- ☐ Uses tools and comprehensive reports to turn raw data into actionable steps.
- ☐ Supplements quantitative methods with qualitative data gathered through client surveys and user workshops to reveal why documents are printed and stored.
- ☐ Supports change management to ensure adoption and sustained success.

User Analytics can guide you to further services and solutions that drive sustainability, productivity and security.

User-Related Security

How to Monitor Who Prints Document Information in Your Organization

Checklist: Network Authentication and Authorization

> Download checklist

Network Authentication

Security improves when administrators limit access to certain users.

- ☐ Can authorized users simply log in with an ID card for secure access to device functions?
- ☐ Can these authentication and authorization sessions be tracked?

Information Access

- ☐ What confidential information is accessible through your documents?
- ☐ Who has access to the information?
- ☐ What controls are in place to manage this information on output devices?

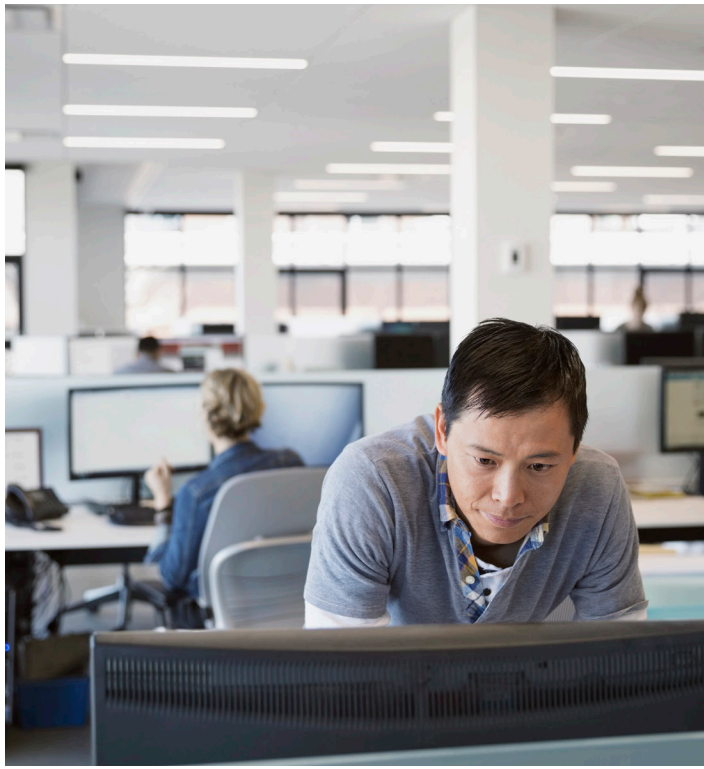
Device Security Policy

Consider access to network assets, not just to the information.

- ☐ Have you created a security policy for access and printing to network assets?
- ☐ Does the provider collaborate with best-in-class security companies like Cisco and deliver embedded hardware security solutions and services through the cloud?

Employee Guidelines

- ☐ What measures are in place to ensure employees adhere to guidelines?



Mitigating Risk in Document Workflow

A Quick Guide to Reducing Information Risk

Not every security challenge is new or unique. Some common problems already have a solution that's supported by Managed Print Services (MPS).

Document Workflow Risk: What's your concern?	Mitigation
Print goes to the wrong printer	Pull printing
User forgets printed document, leaving it abandoned at the printer	Pull printing
Documents left on desk or in conference room	Clean desk policy
Confidentiality and information privacy	Digitize workflow
Documents misclassified or not labeled confidential	InfoSec policy
Slow transaction time waiting for signed documents	Digitize workflow
Unauthorized scanning of confidential documents	Device-based scanning controls

How does your organization rate for document security?

Tips for Keeping Document Information Safe

Consider these five ways to work more securely:

1

Document Repositories

Maintain one version of the truth. This makes it easy to find the latest version of a document and harder to use wrong or outdated information, which can interfere with compliance efforts. Hard-copy documents can easily be scanned directly from MFPs to a secure online repository and maintained under the same security and retention policies as electronic content.

2

Print Policy

Make sure employees understand why print policies are needed (secure confidential information, reduce cost, reduce impact on environment) and engage users in ways that make them willingly compliant.

3

Document Classification

Documents containing confidential information must be clearly labeled and employees educated on what those labels mean and how to handle those documents. Information publishers should learn how to secure documents in repositories that have appropriate authentication and access controls.

4

Secure Print

This capability reduces unauthorized viewing of documents sent to printers and reduces the possibility of data loss or breach.

Jobs should be stored safely at the device until the document owner releases them by entering a PIN, logging in to the device or swiping an ID badge.

5

Secure User Access Through Unified ID System

User access to scan, email and fax features can be restricted by verifying user names and passwords in network directories prior to allowing these functions.

- Can access permission be controlled per user and per service? Some businesses need this flexibility.
- Are these security measures managed centrally at a network domain controller?
- Is all activity monitored and recorded in a security audit log for applicable accounting or regulatory requirements?

Managing by Cloud

MPS Partner Capabilities Checklist

The cloud has helped eliminate the need for on-premise servers, essentially enabling anywhere, anytime access to applications, platforms and services. But is it completely safe?

As more of your documents and work processes move to the cloud, it's essential to partner with an MPS provider that not only facilitates your journey, but collaborates with best-in-class security companies like Cisco to keep your information secure.

Checklist: Can your MPS partner help you move to the cloud? > Download checklist

Managed Print Services (MPS) can support your move to the cloud in a number of ways. Here are some signs that your partner is on the right track:

- ☐ Implements cloud content solutions to provide a secure central repository for all your documents hosted in the cloud.
- ☐ Delivers personal and office productivity capabilities for improved collaboration, so users can freely collaborate while maintaining enterprise security.
- ☐ Digitizes routine office processes, such as document review and sharing, replicating the functions traditionally supported by paper, so documents can be secured in the cloud.
- ☐ Deploys workflow automation solutions to make tasks deemed important easier to accomplish for increased productivity and to lessen the risk of data breaches caused by human error.
- ☐ Provides embedded hardware security solutions in the cloud through partnership with best-in-class security companies like Cisco.

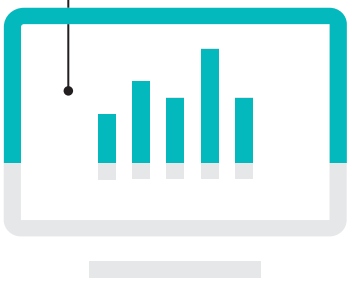
Device Factors: What to Know about Securing Endpoints

Your network—the PCs, the servers—need protection, but who thinks about the vulnerability of your multifunction printers? Small and medium-sized businesses create millions of impressions of their data each year using printers and copiers, and much of this information is vulnerable.

Don't underestimate what's at risk. The security of your document domain can't be taken for granted, but the networked imaging systems in your organization can become allies instead of risks.

57%

have already increased the security budget earmarked for endpoint security, analytics and incident response.[4]



66%

of organizations have re-evaluated their endpoint security policies, processes and tools to plan for improving endpoint security.[4]

85%

plan to spend more on endpoint security.[4]

[4] *2014 Endpoint Security Survey* developed and performed by ESG Research and sponsored by Guidance Software.

How Vulnerable Are Your Endpoints?

Use these checklists to discuss security needs and gaps with your team and your partners.

Checklist: Important Device Security Factors

> Download checklist

Device Vulnerability

- [ ] What possible vulnerabilities might expose your devices to attack?

Device Behavior Variability

- [ ] How can you ensure devices comply with the policy for network assets?
- [ ] What's the enforcement process?

Network Assurance

- [ ] Do you have a policy and process for approving device firmware before deployment?

Remediation Assurance

- [ ] What happens if a device falls out of compliance with the security policy?
- [ ] Are you alerted when this happens?
- [ ] What's needed to bring it back into compliance? Do you have a remediation policy?
- [ ] How do you know the policy is in place?

Reporting

- [ ] When a network asset comes out of compliance, can you capture data for reporting?
- [ ] Is there an audit trail?

Where is your document-based information most vulnerable?

Checklist: Device Vulnerabilities

> Download checklist

Fax/Network Separation

- [ ] Unprotected fax connections create a potential open back door into your network. Is there complete separation between phone lines and network fax connections?
- [ ] Do devices include a network firewall to prevent unauthorized external access to your systems through a network connection?

Image Overwrite

- [ ] Can the device be configured to automatically overwrite files stored on the disk?
- [ ] Does your partner have a documented policy for how they purge or destroy hard drives from machines removed from service?

Data Encryption

- [ ] As data moves in and out of multifunction devices, is it secured with cutting-edge encryption?
- [ ] What about data stored within the device on the hard drive? Extensive encryption on a device hard disk protects sensitive data at rest and in motion.

Security Across the Device Lifecycle

Checklist: Ongoing and End-of-Life Device Security

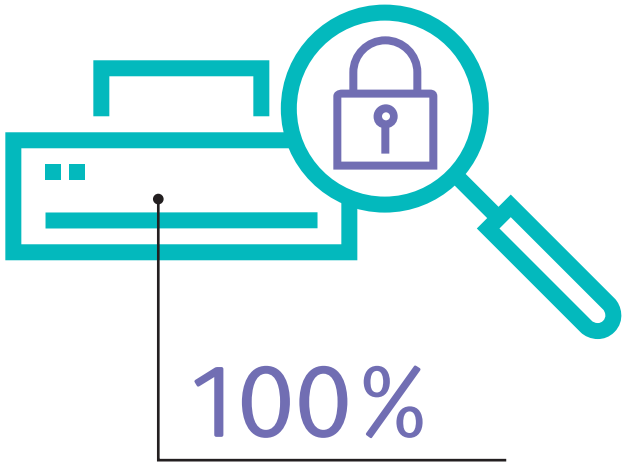
> Download checklist

Security Patch Program and Communications

- [ ] Does the MPS partner work with vendors who offer an active security patch program? This means they monitor for new vulnerabilities on devices, just as OS software developers track new viruses that target software.
- [ ] Can you sign up for a feed and receive immediate alerts when a new bulletin and patch are posted?

Hard Drive Removal

- [ ] Does the partner work with vendors who offer options for hard drive removal before a system is disposed of or turned in after a lease?
- [ ] Do they make recommendations on the most effective way to rid hard drives of data?
- [ ] Are trade-ins and returns that will be re-manufactured overwritten or reformatted?
- [ ] How are trade-in hard drives disposed of and “shredded”?
- [ ] What is the process regarding hard drives on competitive devices?



Security for the life of each device.

Vetting an MPS Partner: How to Evaluate Your Partner's Security Credentials

Best Practices Lead to Best Results

Checklist: Partner Security Qualifications and Best Practices

> Download checklist

Security Analysis

- ☐ Does the partner work with you to assess security needs, identify where your information lives, how it's transferred and greatest areas of risk?

Recommendations for Devices, Placement and Optimization

- ☐ Will the partner help you select the best devices for security purposes? There are many things to consider. Sometimes the most secure device is a locally connected one.
- ☐ Are any devices hidden from view, such as systems in copy rooms? This increases opportunities for security breaches, and a qualified partner would note this in their security assessment and recommendations.

Commitment to Security Innovation

- ☐ Does the partner work with vendors who invest in ongoing security research, development and engineering? Xerox, for example, has many research centers worldwide and devotes a percentage of revenue to security and other critical research, development and engineering projects.

Integration with Minimal Disruption

- ☐ How invasive are the partner's security measures? Organizations avoid needless complications and disruption when they don't have to install third-party applications or software on their workstations. Automated approaches supported by skilled service teams ensure interruptions for security measures are kept to a minimum.

Analysis and Reporting

- ☐ What technologies and automation does the partner use to ensure data quality and accuracy?
- ☐ How frequently does the partner proactively meet about security and other issues?
- ☐ What kinds of reports are available?

Continued >

Checklist: Partner Security Qualifications and Best Practices *(continued)*

> Download checklist

MPS Security Software

- [ ] Does your MPS partner provide software tools to send and receive information from devices using a secure protocol?
- [ ] Does your MPS partner work with Cisco ISE to enforce security requirements based on user, device and access context as well as mobile device compliance with corporate policy?
- [ ] Can the MPS software be configured to send the device only information the client allows, such as "Restrict IP address information from being transmitted"?
- [ ] Does the partner work with MPS vendors whose back office is certified by ISO 27001 as a secure facility?
- [ ] Can the partner's software interrogate the MFP or printer fleet for device firmware levels and determine if they align with your security policies?

Standards-Based Technology

Endpoint device security can impact your ability to comply with regulatory and industry demands.

- [ ] Are the products the partners deliver designed to support standards and regulations like HIPAA, Sarbanes-Oxley, the Gramm-Leach-Bliley Act and FDA 21 CFR Part 11?
- [ ] Does the partner work with vendors who seek third-party validation of device security by participating in the International Common Criteria for Information Technology and Security Evaluation program for certification?
- [ ] Do those vendors submit the entire device for evaluation, not just a security kit? This matters to high-security enterprises like government agencies purchasing MFPs with hard drives. It ensures extra protection is built into the device.

Be Informed and Confident about Your Document Security Decisions

What's next?

If you use the tools in this eBook to guide your team's security discussions and decisions, you can be confident you're moving in the right direction for your organization. You'll be well prepared for the next step—talking to your MPS partner.

Ready to speak to an MPS provider about document security? Get in touch.

About Xerox

Xerox is an $11 billion technology leader that innovates the way the world communicates, connects and works. Our expertise is more important than ever as customers of all sizes look to improve productivity, maximize profitability and increase satisfaction. We do this for small and mid-size businesses, large enterprises, governments, graphic communications providers, and for our partners who serve them.

We understand what's at the heart of work – and all of the forms it can take. We embrace the increasingly complex world of paper and digital. Office and mobile. Personal and social. Every day across the globe – in more than 160 countries – our technology, software and people successfully navigate those intersections. We automate, personalize, package, analyze and secure information to keep our customers moving at an accelerated pace.

For more information visit **www.xerox.com**.

©2017 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries. BR20992