Why MFPs Matter to IT
Part IV: Ensuring Security on the Network

Contents

August 2008

Author:
Jeffrey Coffed
Worldwide Product
Marketing Manger
Xerox Corporation

Why MFPs Matter to IT
Part IV: Ensuring Security on the Network

Executive summary

In the 21st century, and with information as the key asset of every organization today, security is essential to the office—for documents and for any devices connected to the network. And the network is today's business hub.

The threat is very real and the stakes are growing at exponential rates. A breach in the security of an organization's documents can result in unauthorized use of sensitive or proprietary information. It can lead to harmful disclosure, stolen or compromised intellectual property and trade secrets. And for many organizations, these security breaches can end with costly fines and litigation, to the tune of hundreds of thousands to millions of dollars.

When it comes to networked multifunction devices, or MFPs, additional vulnerabilities can be present because these devices can print, copy, scan to network destinations, send email attachments and handle incoming and outgoing fax transmissions. For those in IT, it's critical to the security of an organization's network to make sure that security infractions can't happen through network-connected MFPs—or at the devices themselves.

The Computer Security Institute (CSI) estimates that the cost of a successful security attack averages $345,000, with 46% of companies reporting a security incident in the past 12 months.

— CSI Survey 2007, www.gocsi.com

After all, attacks can originate in unexpected ways:

- The phone line attached to an MFP could be used to access the network
- The web server used to manage the MFPs and printers is vulnerable to attack
- Unprotected electronic data at rest on the hard disk, or in motion to/from the device
- Malicious emails can be sent from an MFP with no audit trail.

Just about anyone can launch attacks against a network and a company's information assets if an MFPs physical and electronic access isn't securely controlled and protected. Those attacks can be as simple as someone picking up documents left in the MFPs output tray, to malicious worms pulling sensitive documents off the network.

An MFP's entire system, along with any device management software on the network, must be evaluated and certified in order for IT and all the workers of an organization to be certain that their documents and network are safe and secure from information predators—or even from internal security breaches.

In this respect, not all MFPs are equal. A comprehensive approach, based on foundational, functional, advanced and usable security, is critical to the information assets of today's businesses.

Executive summary, continued

The 5 areas where documents generated by MFPs are most at risk:

1. **From the desktop**: A file can be seized en route from the desktop to the server and used either in its existing form or modified and even exploited externally.

2. **At the server**: Jobs sent to the MFP for printing typically sit unprotected on the server queue. At this stage, an internal hacker can pause the printing queue, copy a file, and restart the queue without noticeably disrupting the system.

3. **Between the server and the MFP**: This is another point where documents are traveling unprotected—while on the way to the MFP device, information is fully exposed to anyone who can tap into the network.

4. **On the MFP**: All information sent to the MFP is stored in the device's hard drive. MFP hard drives can typically store about as much information as a PC hard drive.

5. **Left in the output tray**: In most office environments, it is common to pick up printed materials that belong to a co-worker. There are also cases when printed documents are left or forgotten at the printer, leaving information open and available to anyone with access to the machine.

—From "Plugging the MFP Security Gap," by Mason Olds, IT World Canada (www.itworldcanada.com), September 1, 2006

Foundational security: table stakes for every business

Any device intended to operate in today's increasingly networked and Internet-connected offices requires many security capabilities—no matter what size the company. IT managers need to ensure that network communications will support the appropriate security protocols for the business. In addition, administrative access to network security and other sensitive configuration settings must be controllable, locally and over the network. For some device vendors, these fundamental network protocols and access controls are offered as options. But IT managers should be aware that, increasingly, these baseline capabilities must be built into every device that IT connects to the network.

With MFPs increasingly popular additions to today's networked offices, and because they can print, copy, scan and fax documents, MFPs ramp up the productivity of many enterprises. But it's their connectivity to the network that makes MFPs vulnerable to security attacks. Mason Olds, author of "Plugging the MFP Security Gap," posted on www.itworldcanada.com, on September 1, 2006, stated that a report commissioned by McAfee in July 2005 cited that cyber crime cost US organizations $400 billion in 2004, with 2,000 new threats emerging *each month*, compared to only 300 threats just two years earlier. Today it pays for every enterprise to take steps to protect the information that is sent, shared and stored via their connected MFPs. These protections and safeguards are necessities, not options.

Xerox reduces the risk for connected MFPs

MFPs evolved from copiers almost ten years ago. The guts of an MFP are essentially computer components—complete with a hard drive and memory—so that it can capture and manipulate image data and convert it into bits and bytes. Every time someone prints, scans, copies or faxes a document, the MFP retains that information in its memory, where it's vulnerable to attack by unauthorized users. That's why it's so essential for any MFP to be tested extensively for security vulnerabilities in its software before it goes to market.

That's also why all MFPs require all the security precautions and updates of other network peripherals. There's an inherent risk with any device that contains software, because it's always possible that new ways to break the software will be discovered. Xerox takes any security vulnerabilities seriously and moves immediately to provide a downloadable patch to solve any security vulnerability, via www.xerox.com/security.

Xerox provides more security for potential entry points to its MFPs than any of its competitors. It also continues to update those security functions on a regular basis. IT managers will find that Xerox offers the broadest range of multifunction systems that meet the internationally recognized standard for security, which is why they've earned Common Criteria full system certification.

—Based on "Xerox Multifunction Systems and Network Security—What You Should Know", www.xerox.com

Functional security: more than security kit certification

Once foundational security is established, additional security requirements are driven by the specific functions offered by each device connected to the network.

In the case of MFPs, these functions also require multiple protections. For example, unlike typical office printing, network scanning is a potential "on-ramp" to not only the local office network, but also the Internet itself. On top of that, the scan-to-email function increases vulnerabilities and security issues to address. IT managers will want to choose MFPs with software that integrates securely with email systems.

Likewise, the fax function has its own set of security requirements. These include isolating its telephone connection from any local network interaction to avoid "back door" access to the device. Many MFP manufacturers don't separate the faxing function from the rest of the device, opening it up to easy security breaches. With embedded fax functionality, which is featured on Xerox MFPs, companies can prevent unauthorized access to the device via the fax subsystem because it's internally separated from other network functions.

As for printing and copying, maintaining security over electronic data can in fact be easier than controlling hard copies, because IT can build security measures into electronic file properties. Making sure that their multifunction systems encrypt data traveling on the network, along with to and from devices, prevents any unauthorized viewers from accessing print and scanned documents as they travel to file servers or other network repositories. This requires either encrypting the connection to the Web user interface or by employing device management through software that supports encryptions.

> ***"Unlike other document services vendors, Xerox has the entire multifunction system evaluated, rather than just a security kit or an individual security feature."***
>
> **—Recharger Magazine, "Xerox MFPs Earn Int'l Security Standard," April 27, 2007**

Xerox CentreWare Web helps IT administrators manage and secure all networked devices

CentreWare Web is free, Web-based device-management software that installs, configures, manages, monitors and reports on all SNMP-compliant networked printers and multifunction devices in the enterprise, regardless of the manufacturer. It also helps IT staff protect against unauthorized network or device changes with Windows® 2000 and/or NT4 native security. For more information and to download the software and print drivers, see xerox.com.

—From office.xerox.com, CentreWare Web sell sheet

Functional security: more than security kit certification, continued

But hard copies can be tougher to trace back to a security breach once the documents have left a locked file cabinet or office—or picked up by the wrong person at the MFP's output tray. The first step in protecting key documents is to create and maintain an authentication system on all communications produced by a company's MFPs. This creates an audit trail of accountability for all users of the device. By putting a validation system in place, with user names and passwords, network authentication restricts workers' access to scanning, emailing, secure printing and faxing features, as needed. And with additional system administration authentication, no one can make configuration changes to the network or the device without the proper log-in for authentication.

Functional security: more than security kit certification, continued

The following security functions have been included in Xerox common criteria certifications*:

Encryption with secure protocols—Xerox MFPs encrypt the data traveling on the network to and from the devices to prevent unauthorized access to documents as they travel to file servers or other network repositories.

Authentication—By validating user names and passwords prior to use, network authentication restricts workers' access to scan, email and fax features as needed. System administrator authentication requires authorized administrators to log in to the device in order to make configuration changes.

Internal audit log—The multifunction systems can maintain audit logs of activity to help track the path of documents, an important feature for organizations that must comply with federal regulations, such as the Health Insurance Portability and Accountability Act (HIPAA).

Firewall—A built-in firewall manager allows Xerox MFPs to manage all communication access to authorized users.

Image Overwrite Option—This option electronically "shreds" data stored on the device's hard disk during routine job processing. This electronic removal of data can be an automatic function after every job or set to be performed when a user specifically requests it.

Embedded Fax—Unprotected fax connections in multifunction devices can be a back door into the network. Xerox is the first manufacturer to offer Common Criteria-certified products that assure complete separation of the fax telephone line and the network connection.

Secure Print—This feature prevents unauthorized viewing of hardcopy documents by holding jobs in the MFP's queue until a PIN is entered at the device.

—Source: Recharger Magazine press release, "Xerox MFPs Earn Int'l Security Standard," April 27, 2006

* *As of April 2006, the NIAP had certified 30 of Xerox's office digital color and black-and-white multifunction systems.*

Advanced security: locking down sensitive information for specific industries

While laying a secure foundation and making sure the print, copy, scan and fax functions are secured may be enough for some businesses, those that handle especially sensitive information will want additional layers of security to protect against any unauthorized viewing or misuse of information. These include legal, healthcare, financial services and government organizations, which require extra caution and control. In many of these situations, the best solution is a combination of secure device features and either the device manufacturer's or a third-party's software to provide additional layers of security for day-to-day operations.

For those environments that need the utmost in security, the security solutions must lock down mission-critical information to make sure it doesn't fall into the wrong hands. IT managers will want to make sure the solutions allow for restricted access, trackable usage, and protection of confidential data that flows through the network.

By evaluating the security level an enterprise needs, IT managers can determine how many layers of security are needed and for which users certain actions and protections will apply. Considerations include securing users, the image data, the output, and document rights, which also requires special document tracking. Securing the audit trail completely means being able to track and monitor every page that's scanned, printed, copied or faxed, especially if the enterprise has to meet federal regulatory guidelines such as Sarbanes-Oxley, Graham Leach Bliley and HIPPA.

For networked MFPs, this requires advanced architecture, to protect each user's data from unauthorized access by other users. It also requires authentication and authorization, with multiple options for secure user access. Advanced security also means that the MFPs in use comply with the most stringent industry and government-mandated standards and regulatory compliance. Again, Common Criteria Certification is a must. Common Criteria for IT Security Evaluation (ISO/IEC 15408) is an internationally recognized set of standards that define security requirements and establish procedures for evaluating the security of IT systems and software. This certification makes it easier for businesses and agencies to meet the high-level security requirements and increasing regulations in the government, military, healthcare, legal and financial sectors.

> ***"Xerox has the most Common Criteria Certified MFPs of any vendor, and is the only vendor to receive certification for the entire device, rather than just for a kit or specific feature."***
>
> **—Russell Peacock, President, Xerox Office Group**

Advanced security: locking down sensitive information for specific industries, continued

Xerox MFPs: ensuring start-to-finish security on every job

Device Access Password Protection—Administrative set-up screens and remote network settings cannot be viewed or altered without a personal identification number (PIN). This controls access to all device functions.

IP Address Restriction—Administrative set-up screens allow access to be restricted for specific IP addresses to control communications with specific network clients.

Secure Print—Holds jobs until the job owner enters a PIN to release those jobs for printing. This prevents unauthorized viewing.

Embedded Fax—Prevents unauthorized access to the device via the fax subsystem because it's internally separated from network functions. No other multifunction device manufacturer has obtained third-party certification that fax and network lines are separated.

Image Overwrite—Electronically eradicates data process to the hard disk during print, scan or email operations by repeatedly overwriting the data.

—Source: Xerox Market Brief, "Meeting healthcare regulations for security & privacy"

Usable security: for protection from beginning to end

It's one thing to make networked devices and their functionality secure. But if security features aren't easy to use, and workers aren't aware of the correct processes to follow to keep information secure, all the effort and investment will be for nothing.

Of course, the reasons appropriate security features aren't fully utilized are because they're difficult to set up and / or inconvenient to work with on a daily basis. IT managers will want to make sure that the MFPs they connect to the network are not only going to make their organizations more productive and secure, but also that they're easy to use, with a minimum amount of training and Help Desk support. For these reasons, it's wise to choose devices from a manufacturer that offers continuity among its device features and interfaces, at the desktop and at the console.

And as the organization's needs grow and change, it also makes sense to choose MFPs from a vendor that is able to grow and adapt to the needs of the enterprise. From this standpoint, MFPs are increasingly the choice of networked offices because manufacturers are continually adding more technology "on the box."

One example of this added technology is Xerox's Extensible Interface Platform (EIP), the software platform that allows developers to use standard Web-based tools to create server-based applications that can be configured for the MFP's touch-screen user interface. This allows a Xerox MFP to adapt to the way an enterprise works, versus the other way around, and permits additional opportunities to not only customize functions and create time-saving applications for workers, but also to create specific applications for highly sensitive document jobs. Xerox introduced EIP two years ago, but it has long been a leader in both security and usability features for office devices.

Xerox security: protection now and in the future

Xerox scientists are busy readying the next generation of security technologies to prevent tomorrow's cutting-edge security attacks and keep documents safe as they travel between the paper and digital worlds.

DataGlyph® technology, micro-printing, print-mark technology, such as Glossmark® Correlation Marks, fluorescence, infrared print security and erasable paper are just some examples of the technologies being developed and perfected from Xerox labs around the world.

— Source: Xerox document, "Your New Workplace"

Conclusion

With the proliferation of networked multifunction devices in today's offices, and the amount of information that is sent, stored and shared via those MFPs, the security of those devices should be among the top concerns of IT managers.

While its connectivity is a major benefit and makes an MFP highly productive, the same connectivity also opens it up to security threats unless the device is secure at every level: network access, users, image data, output, and audit trail. Because an MFP is often the information hub in the office, it must be secure online and at the device itself.

Security breaches can happen anywhere and in unexpected ways. For these reasons, an MFP's entire system should be evaluated and certified in order to ensure security of an organization's key asset: its information.

A comprehensive approach to MFP security—from foundational, functional, advanced and usability standpoints—is essential for IT managers to ensure that their connected MFPs are able to protect an organization's data, its users, and the organization itself from the damage and expense caused by security attacks.

For more information

Xerox, renowned for its technological innovation, has focused that innovation on the challenges IT faces on a daily basis. We offer proven expertise in improving document and business processes, and put that expertise to work every day around the world, liberating thousands of IT professionals from the tedious and resource-intensive hassles of managing their output infrastructure.

Xerox is committed to ensuring that our customers' businesses run at top efficiency, with services and service availability levels aligned with today's organizational demands and designed to minimize the impact of your IT workload.

The full portfolio of Xerox services is a comprehensive array of offerings, customized to address specific business and IT management requirements. Xerox service expertise includes dedicated technicians who respond to all support calls, along with trained analysts and engineers who are ready to be on-site when needed. In addition, Xerox offers new administrative technologies to simplify processes, plus full Internet support:

- Local support team of dedicated sales consultants, technical specialists and analysts
- Online services for Web-based administration tasks
- Online Support Assistant and self-help tools
- Xerox Office Services for end-to-end management of the printing and imaging environment
- Office Document Assessment and Xerox Office Productivity Advisor Services
- Device-Centric Services™, Xerox's DRM Platform for the Future[†]

Look for more in the "Why MFPs Matter to IT" series, including:

- Part I: Validating the Technology
- Part II: Managing the Print Environment
- Part III: Transforming Business Processes

Learn more about how Xerox can put our forward-thinking to work for you.

Contact your local Xerox provider, or visit www.xerox.com/solutions.

[†] Smart eSolutions client is a free download from www.xerox.com/smartsolutions and installs on your PC. It's available for a range of Xerox network-connected devices, including Phaser® printers, Document Centre®, WorkCentre® and WorkCentre Pro. It also includes award-winning CentreWare® Web device-management software. CentreWare Web is free and can be downloaded from www.xerox.com/centrewareweb.

For more information, continued

About the author

Jeffrey Coffed, Worldwide Product Marketing Manager with the Xerox Corporation, is a marketing professional with 18 years' experience in the high-tech sector. He has worked in all phases of marketing, including strategy, product marketing, growing channels, developing programs, training, marketing communications and events. Currently, he's responsible for the marketing of Xerox's high-end color MFP portfolio.

Prior to joining Xerox, Jeff served as a product marketing manager with Hitachi Data Systems. He was responsible for the company's flagship products and led Hitachi to the enterprise digital-storage market-share leadership position. During his tenure at Hitachi, he was a key contributor in several high-profile product launches, authored several white papers and articles, and worked with the global sales force to increase revenues.

From 1988 to 2000, Jeff held progressively responsible positions with ATTO Technology, Caslon & Company, Dartnell Enterprises Incorporated (DEI) and EDS. He developed the marketing plans and programs for ATTO Technology and helped to create its channel partner program. At Caslon & Co., he supported the member companies of the Print on Demand Initiative (PODi), a not-for-profit corporation dedicated to educating various market segments about the benefits of print-on-demand technology. With DEI, he led the company's marketing efforts and started is Office Imaging Division.

Jeff began his career with EDS as a systems engineer, after graduating with a Bachelor of Science degree in management science from the State University of New York, with concentrations in marketing and computer science. He is presently working on his Six Sigma Green Belt certification.