

Let's talk virtualization

Complimentary seminar on how to use virtualization to decrease application lifecycle costs

Technology **07**  
Leadership Series  
presented by GTSI & FCW[Click here for more information](#)[Login](#) | [Register](#) Search GCN  GCN Quickfind[GO](#)[Our Sites](#) | [Current Issue](#) | [White Papers](#) | [Subscribe](#) | [Blogs](#) | [eSeminars](#) | [Resource Center](#) | [Events](#) | [Jobs](#) | [FAQ](#)**GCN Hot Topics:**[Tech/Products Home](#) | [Authentication/ID Mgt.](#) | [Content/Record Mgt.](#) | [COOP/Telework](#) | [Data Mgt.](#) | [Defense IT](#) | [Enterprise Architecture](#)  
[Geospatial](#) | [Hardware](#) | [Homeland Security](#) | [IPv6](#) | [IT Mgt.](#) | [State & Local](#) | [Software Apps.](#) | [Web Strategies](#) | [Workflow/Collaboration](#)[GCN Home](#) > 03/19/07 issue

## Secure printing

Tools that help keep paper out of the wrong hands

By Drew Robb, Special to GCN

[Story Tools: Print this](#) | [Email this](#) | [Purchase a Reprint](#) | [Link to this page](#)[Listen to this story](#)

### RFP Checklist

Selecting the best secure-printing solution for your organization requires a close look at your existing infrastructure and workflow as well as consideration of future needs. Here are some critical questions you'll want to answer before investing in a specific solution.

- Do you need to provide security for an existing fleet of printers?
- Are you purchasing new printers in the near future?
- If so, do a thorough needs analysis to determine your desired printing capabilities (such as color, paper size, resolution) and speed. Also, bear in mind that some vendors provide printers with built-in security capabilities.
- Does the data need to be encrypted?
- Will it be decrypted at the printer or at the file server?
- Do you need to log what gets printed and audit the data?
- Do you need to restrict the number of copies or types of files an individual prints?
- Do all printers in your organization need security functions?
- Do you need to restrict who gets access to which printers?
- Will any printers have an external connection, either to send and receive faxes or for remote support?
- Is there already a security system in place?
- How does the user activate the print job?
- If so, does it employ a keypad, fingerprint reader or secure ID card?
- If it uses a card, is it HSPD-12 compliant?
- Does your current equipment have Common Criteria certification?
- What support is needed?
- What are the terms of the support contract?
- Will you have a vendor representative on site?

Sometimes the biggest threats to data are fairly low tech. Former national security adviser Sandy Berger made that point when he walked out of the National Archives with classified documents. There was no hacking of networks or decrypting of documents. Instead, it was as simple as carrying out hard copy on your person.

The fact is, despite billions of dollars being spent on securing federal IT systems, it's possible for the wrong eyes to see sensitive data at unsecured print stations.

Vendors are responding to the situation, but IT staff aren't sure how to assess the vendors' proposed solutions. "We see more vendors advertising secure printing, which leaves people wondering what they should do," said Ken Weilerstein, research vice president of Gartner Inc. of Stamford, Conn. "IT security directors have other things to worry about, so the decisions are left to people who are not security specialists."

While most printer manufacturers have some sort of secure printing offering, a full solution requires more than putting a keypad on the printer. Data needs to be protected in transit, and the printers need to be protected against hacks.

"The biggest mistake is to view secure printing as a separate, standalone application. It is one element of security and has to be looked at in that context," said Steve Reynolds, senior analyst for Lyra Research Inc., a consulting group in Newton, Mass. "The best way to do it is to take advantage of the security infrastructure you are putting in place for all kinds of things."

### Threat diversity

An obvious low-tech security risk is the wrong person picking up a sensitive document from a shared printer.

"Sometimes you print a document and get a phone call before you pick it up," said Chuck Jarrow, vice president and deputy general manager of the IT Services Group at government contractor L-3 Communications Corp. "You might have some very sensitive data sitting out there."

Last spring, International Data Corp., a Massachusetts consulting firm, released a survey showing that more than half of respondents had found other people's documents on their shared printer. E-mails were the most commonly found item, but 24 percent found financial data and 18 percent found personnel records.

The simplest way to solve this issue, of course, is to buy personal printers. "Printers are so cheap these days, the easy way is for everyone to have their own printer," said Bruce Schneier, founder and CTO of Counterpane Internet Security Inc., a managed-security-services company in Mountain View, Calif.

But this strategy only works when users have private offices. It's also more expensive to support a large number of private printers than having networked shared printers.

Another approach often used in high-security installations is to put the printer behind a locked door. But, again, that's not always practical for general office use.

Then there is the matter of device and network security. This is particularly becoming an issue with multifunction peripherals (MFPs), which combine printing, copying, scanning and faxing. Some devices even have their own Web page for access by remote personnel. And, as we have witnessed with other computing devices, more features mean more potential security holes.

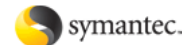
### What to do?

The technology conference that puts it all into perspective.

### Symantec Government Symposium 2007

July 19, 2007 | Washington D.C.  
Ronald Reagan Building and International Trade Center[REGISTER NOW](#)

Confidence for a Connected Government.

[Latest News](#) | [WashingtonTechnology.com](#) | [FCW.com](#)

### GCN.com

The latest technology news from [GCN.com](#)

- [NIAP certifies Enterprise Linux 5](#)
- [New high-speed encryption for fiber links](#)
- [DARPA to raise robot army](#)
- [Bill Vass | Different tasks, different chips](#)
- [FCC chair focuses on broadband](#)

A better view of public service.

Check out our wide range of government display solutions.

[Learn More](#)

**NEC**  
necdisplay.com

### TOP JOBS FROM LOCAL EMPLOYERS

- [Electronic Technician](#) / InHand Electronics, Inc.
- [Chief Information Officer](#) / Office Of Comptroller Of The Currency
- [Experienced Buyer's Agent Wanted on Busy Team](#) / Keller Williams Realty

[All Top Jobs](#)

- What do support and materials cost? The most common printer security strategy is to control access to printer output with a keypad, card reader or biometric device attached to the printer. When the user sends the document to the printer, a dialog box appears offering the option of using either secure or standard printing.
- Will you lease or buy the equipment? If you choose secure printing, you enter a code at your workstation. The job would then go into a print queue, either on a print server or on the printer itself, and the job would sit there until the user goes to the printer and—if a keypad device is being employed—enters the password to release the job for printing.
- How is equipment disposal handled? Alternatives include smart cards and biometric devices. L-3 Communications, for example, has started using fingerprint readers for some of its own internal printing needs, as well as for some of its customers.
- Does your current printer infrastructure integrate with any other enterprise security software? "For an organization that suddenly finds it needs secure printing, biometric access is a very cost-effective way to do it and a very quick way to do an implementation," Jarrow said.
- How does the security software interact with user applications? L-3 has employees stationed at the offices of some of its customer agencies to provide tech support. Adding keypad security to printers would have been one way to enhance security, but Jarrow prefers a biometric approach.
- Is any additional middleware or custom programming needed, or does it just show up as an option on the print screen? "There was a group we worked with that had printers with a keypad release mechanism, and they got rid of them because they were more trouble than they were worth," he said. "You need to look at your people, and if they can't remember their ZIP code, they won't remember their printer code."
- What type of user training is needed for each printer security solution you're considering?
- Does the vendor conduct the training?

Instead, he purchased a fingerprint system from Silex Technology America Inc. With it, a fingerprint reader is plugged into a USB port on the user's workstation to register a fingerprint. Then, if a user opts for a secure print job, he uses a fingerprint reader at the printer to release the document. Since L-3 started using the system, Jarrow said, he has seen a lot of interest from clients.

"We talked to one agency that had grown tired of people forgetting their codes and calling the help desk to get the number reset," he said. "They were very intrigued by this solution since users can't leave their finger back at the computer."

#### Wire worries

The interconnectivity of modern printing equipment also creates additional security holes.

"It wasn't that long ago where we had separate printers, and the copier was only connected to the power supply," says Weilerstein. "Today they have an increasing number of functions, are connected to the network and might also be connected to the phone line."

While it is more common for hackers to try to access databases or document storage systems, printer files have two distinct attractions. The first is that they show what documents are currently in play in an organization. The other is that print documents are easy to read.

Bob Forte, senior systems engineer for Levi, Ray and Shoup Inc. of Springfield, Ill., likes to conduct demonstrations of how even a free network sniffer can produce clear copies of printer files.

"People don't feel they have a vulnerability in their print data streams," Forte said. "In actuality, any basic line data or PCL [Printer Command Language] is pretty readable."

He advises encrypting all printer files and only decrypting them at the printer. This is especially critical if the printer file is being transmitted to a remote location. LRS has print encryption software, and some printer vendors, including Hewlett-Packard Co. (Capella) and Lexmark International Inc. (Printcrypton), have decryption options on their printers.

Then there are remote workers who are physically outside the network but who need to print documents inside the office. "Printing can take advantage of the security and encryption that is already there, a VPN tunnel or 128-bit encryption that is available with the Web," said Lyra Research's Reynolds.

#### Taking control

Another important factor to consider is controlling who is printing what. "The most common problem is not knowing what users are printing," said Bill Feeley, CEO of Software Shelf International Inc. of Clearwater, Fla. "If management has no way to run reports on who is printing, what is being printed [and] where jobs are being printed, they have no way to implement any kind of security."

Software Shelf sells the Print Management Plus software that is used by the General Services Administration, NASA and other agencies. While it's most commonly used to set quotas or restrict who can print in color as a way to cut costs, it also provides an audit trail to see who is accessing and printing what documents.

In addition, a user can be blocked from printing documents from specific applications or documents that have designated key words in the title. For example, anyone not on the human resources staff would be blocked from printing anything from the HR Management System.

"The point here is that the other elements of computer systems are being tightened up so paper is one of the few remaining places you can take information out of the agencies without leaving a trace," Weilerstein said. "If you try to download the information to local storage there might be rules blocking it, but not with printing." Unless, of course, you have installed print management software to prevent this.

#### Don't fear the feature

Printer manufacturers keep adding features, and since additional features can mean additional vulnerabilities, the first reaction of some IT managers might be to disconnect the fax line and disable any other features that aren't absolutely essential.

But vendors are adding extensive security features as well. (Most vendors also offer white papers on their Web sites detailing these features.) In addition, Lexmark, Sharp Corp. and Xerox Corp. have received National Security Agency Common Criteria certifications and some HP LaserJet models are undergoing evaluation. But even this type of certification doesn't provide a complete answer.

"Agencies should look for certification such as the Common Criteria certification, but the problem is that the

certification only shows that it has been tested for a specific threat," Weilerstein said. "Vendors say it is like a Good Housekeeping seal, but in reality it is just one product tested for one threat."

Also, agencies will want to check to see what features their existing security vendors can provide in relation to printing.

"The whole subject of secure printing is being increasingly rolled into the general elements of security that people are enabling on their networks," Reynolds said. "It is less a standalone application these days as it is just another application in a suite of things that people are enabling."

#### Security Printing

Vendor	Representative Product(s)	Notes
Capella Technologies Inc. Anaheim, Calif. (888) 232-4200 www.capellatech.com	SecureJet, VeriUser, MegaTrack	MegaTrack is a Windows-based application for recording and monitoring printer usage. VeriUser is an authentication system for Hewlett-Packard MFPs. SecureJet controls user access to HP printers with keypads, ID cards or proximity devices.
Hewlett-Packard Company Palo Alto, Calif. (800) 727-5472 www.hp.com	Printers and management software	A wide range of laser and ink-jet printers with associated management and security features; some models currently under review for Common Criteria certification.
Kyocera Mita America Fairfield, N.J. (703) 469-2350 www.kyoceramita.com/us	Printers and multifunction devices; Equitrac Secure Print Release	Equitrac software works with keypads or card readers for secure printing.
Levi, Ray and Shoup Inc. Springfield, Ill. (217) 793-3800 www.lrs.com	VPS	Secure printing software that encrypts print files while in transit.
Liquid Machines Inc. Waltham, Mass. (877) 885-4784 www.liquidmachines.com	Liquid Machines Document Control	Software that lets users set access and print policies for documents; works with 65 different applications, including Microsoft Office, Adobe Acrobat, Sharepoint and Visio.
Oce-USA Chicago (773) 714-8500 www.oceusa.com	Printers and associated software	Nine models have achieved Common Criteria certification; some come with built-in fingerprint readers.
Ricoh Corp. Alexandria, Va. (703) 317-0800 www.ricoh-usa.com	Printers, Data Overwrite Security System, removable hard drives	The company offers optional removable hard drives for printers, so the data can't be accessed by others. Customers also have the option of overwriting data on printer drives, rather than just erasing it.
Silex Technology America Inc. Salt Lake City (801) 748-1199 www.silexreseller.com	SecurePrint	Biometric network printing security system; works with any workstations and printers that have a USB connection; replaces keypad access with a fingerprint reader.
Software Shelf International Inc. Clearwater, Fla. (727) 445-1920 www.softwaresshelf.com	Print Manager Plus (several versions)	Printing management software to control costs and improve security; includes user authorization and restrictions on what documents users are able to print, and audit logs to see who printed what.
Xerox Corp. Stamford, Conn. (800) 275-9376 www.xerox.com	Wide range of printers; Xerox Secure Access Unified ID System	The Secure Access Unified ID System works with existing student or employee ID badges; can use a keypad code for a second layer of security.

More news on related topics: [Communications / Networks, Hardware, IT Security](#)



#### MARKETPLACE

Products and services from our sponsors

#### ■ The Big Picture in Disaster Recovery- Free Webinar

In this discussion, industry experts from VMware, Double-Take Software, and Silver Peak discuss how to "put the pieces together" for an effective disaster recovery plan. They discuss new trends in data protection technology that span all areas of IT.

#### ■ Find State & Local IT Bid Opportunities

Get access to thousands of state and local procurement opportunities, key government contacts, incumbent and competitive data and more, by searching INPUT's State & Local Vertical and Geographic Opportunities database. Get a Free Trial.

---

■ **Planning to Prime on an IT Services IDIQ Contract?**

Will you be prepared to win task orders under the contract? Privia automates your processes for wired and unwired opportunities, connects you to teaming partners and centralizes past performance data to quickly process winning task order responses.

---

■ **Want to know your CIS security score?**

The CIS has developed detailed IT security benchmarks which will help make your computer more secure. Click here to download the Belarc Advisor which will automatically show you how secure your system is compared to the CIS benchmark configurations.

---

■ **Project Portfolio Management by Métier**

Learn how your peers are using Métier to reduce costs, manage resources better and predict their project success. Free PMI workflows and templates with software purchase. Contact us for a customized demo and educational white papers!

---

[View more products and services...](#)

[Buy a link now](#)

---

[Home](#) | [About GCN](#) | [Contact GCN](#) | [Customer Help](#) | [Privacy Policy](#) | [Editorial Info](#) | [Advertise](#) | [Link policy / Reprints](#) | [Site Map](#)



© 1996-2007 1105 Media, Inc. All Rights Reserved.