

Network Copier Security: Are you doing enough to protect information assets?

Remember Harold Nicholson, the former CIA agent who was convicted of spying for the Russians? Arresting in 1996, he is now serving a 23-year prison sentence for passing sensitive photos and documents to Russian handlers. In exchange for that information, Nicholson was paid \$300,000 in cash. This story resurfaced as Nicholson allegedly enlisted his son to collect an additional \$35,000.

A more recent lapse in security occurred when a New Zealand man discovered confidential files on an MP3 player he purchased in Oklahoma. The device contained home addresses, Social Security numbers and cell phone numbers of U.S. soldiers, along with military mission briefs and lists of equipment deployed to Afghanistan and Iraq.

These breaches illustrate that people intent on seeking personal financial gain are an ongoing threat, as are those that mishandle mobile technology—MP3 players, laptop computers, USB thumb drives, or any other digital media.

With that reality comes an imperative to prevent sensitive information from falling into the wrong hands. This has never been more urgent as layoffs reach historic highs. Indeed, with every pink slip comes the very real threat of information theft. Case in point: A Symantec and Poneman Institute survey found that more than half of workers who lost or left a job in 2008 said that they stole confidential company data¹. What's more surprising, this same survey found that 82 percent of IT departments said no audits of paper or electronic documents were done before the employees left their jobs.

Certainly, IT professionals protect their network infrastructure by installing firewalls, reliable anti-virus software and monitoring the network for security holes. However, there's a vulnerability sitting in full view—the network copier/MFP (multifunctional peripheral).

An MFP integrates copy, scan, fax and print functions into a single platform. However, if not properly protected, these sophisticated network devices pose a potential threat to information security. To address that threat, please read on. We've highlighted products that are engineered to help safeguard information assets and increase accountability across an entire enterprise.

Canon U.S.A., Inc. (www.usa.canon.com)

Canon imageWARE Secure Audit Manager software collect important job attributes, including a physical copy of all processed jobs, acting as an effective deterrent to information leaks. When documents are processed by Canon-branded MEAP-enabled imageRUNNER devices, the software tracks everything that that user does, ultimately capturing and archiving each image in a backend Oracle database. The Keyword Notification feature automatically notifies the administrator via e-mail whenever a pre-set keyword is detected in a scan job. This software provides companies with an effective and efficient tool to monitor the electronic transmissions of hardcopy documents.

eCopy, Inc. (www.ecopy.com)

eCopy ShareScan software operates across different MFP and scanner platforms, so scan operations can be performed on the device of choice, for example, a Canon, Konica Minolta, Ricoh or Xerox device, using one intuitive interface. An open architecture is important within mixed fleets, where each device uses its own proprietary functionality. IT administration is streamlined when scan activity occurs at eCopy ShareScan. Moreover, eCopy's security features can be deployed across all scanning devices within the enterprise—dynamic Active Directory and application authentication, document encryption, job logging, and secure deletion of temporary image files. Regardless of which device a user walks up to, the touch screen, with an easy to navigate graphical user interface (GUI) is the same. That consistent user experience is a key benefit, as is its ability to customize that experience to a customer's specific application needs, whether to improve business processes or enhance security.

Konica Minolta Business Solutions U.S.A. (www.CountOnKonicaMinolta.com)

Konica Minolta realized early on the importance of security issues in the digital age, where the risk of seriously damaging security breaches rises dramatically alongside rapidly growing worldwide communication possibilities. In response to these threats, Konica Minolta has taken a leading role in developing and implementing security-based information technology in its MFPs. In contrast to other MFPs in the market which are certified based on a security option or a specific function, they engineer and provide ISO 15408 Evaluation Assurance Level (EAL) 3 Security Certification for each product as a total system.

Konica Minolta has announced a partnership with ActivIdentity that has produced a Personal Identification Verification (PIV)-Compliant Card System that increases security and document control for customers using Konica Minolta MFPs and printers. Initially available to U.S. Department of Defense customers, the PIV-Compliant Card System can be used in conjunction with the Common Access Card (CAC) as well as the next generation CAC, a PIV-Compliant Identification Card.

Muratec America, Inc. (www.muratec.com)

Muratec's OfficeBridge™ software solution supports Inbound Fax Routing, enabling users to receive faxes directly to e-mail. With the increased emphasis on security, IT doesn't want sensitive fax messages printing at the device for all to see; they want to route messages directly to an e-mail inbox. Inbound Fax Archival also serves as a permanent audit trail, as a copy of each received fax is stored to a network folder. The administrator has the ability to retrieve a given document, perhaps in the event of a security breach or litigation. Outbound Fax Archival also captures an image of each document sent outside the organization. Other embedded Muratec security technologies include user authentication, which validates network user names and passwords (through Microsoft Active Directory), password-protected PDF, PIN masking, secure fax Reception and secure print.



Denine Phillips, Contributing Writer

Software/Solutions

- [CANON U.S.A. ANNOUNCES AVAILABILITY OF THE COPYblue MEAP KIOSK VERSION 2.1 SOLUTION](#)
- [Laserfiche Poised to Integrate with Microsoft SharePoint Server 2010](#)
- [Print Audit 6 Now Available for Macintosh OS X](#)
- [Latest A2iA CheckReader Release Provides For Even More Recognition and Image Quality Analysis](#)
- [AnyDoc Software Certifies OPEX DS1225 Scanner for Enhanced Document and Data Capture](#)
- [Sign Version of EFI PrintSmith Management Solution Now Available](#)

Ricoh America Corporation (www.ricoh-usa.com)

The GlobalScan Family of products addresses security requirement by using the employee's existing network log-in credentials (used at their workstations) for authentication at the MFP control panel. Once validated, the user can scan to e-mail, folder, fax and/or DMS. Card Authentication (optional) supports single sign-on and the ability to control access to restricted features. Using HTTPS, e-mail communication from the GlobalScan Server-enabled MFP is secured using 128-bit encryption technology. By leveraging the core security features of compatible MFPs, and GlobalScan Family products, Ricoh provides assurance that information assets introduced into their electronic workflow were fully protected from unauthorized access.

Sharp Imaging and Information Company of America (www.sharpsec.com)

Sharp MFP log file monitors all device activity for auditing purposes, either on the device itself—where the first page of each scan is retained, or via third-party software, where every page is stored on a back-end server. And with scan to e-mail, authentication rules can be enforced that only allow the employee to scan to their e-mail inbox or desktop, no other destinations. Security is enhanced because documents cannot be sent outside the organization. This type of authentication is associated with an Account Control List (ACL), where permissions are based on authentication settings established by the administrator. Securing network printing is also possible, using PIN Print, where the user must enter a code at the device to release the job; Pull Print uses third-party software to send the file to a server where any authorized individual (on the LAN or WAN) can print the job; My Folder Print uses Sharp's OSA™ Platform to enable users to browse to and print documents stored in their network folder.

Xerox Corporation (www.xerox.com)

Xerox MFPs are equipped with a wide range of security features to protect data. The Image Overwrite security option electronically shreds information stored on the MFP's hard drive, either automatically (at job completion) or on demand. Data residing on the hard drive is encrypted, as is data communicated over encrypted network protocols, like SSL, IPSec and SNMPv3. For full access control, authentication and authorization privileges can be granted to all device services on a per-user basis via Active Directory. The embedded fax subsystem separates fax telephone line and network connection to prevent unauthorized access to a user's environment. And audit log tracking records the date and user of every job the device processes. Secure print prevents the unauthorized viewing of private documents when printing to a workgroup MFP by safely storing print jobs at the device until the user enters a PIN to begin the printing process.

Additional Security Solutions

There are many security solutions available today that address specific vulnerabilities, including, but not limited to, the following:

- ▶ CAC (Common Access Card) Authentication: The MFP user inserts their Department of Defense-issued CAC into a card reader attached to the MFP before accessing device functions.
- ▶ E-mail Encryption: SSL (Secure Sockets Layer) technology encrypts mail communications so messages can only be read by the recipient.
- ▶ Hard Drive Overwrite: After each scan operation, the latent image data stored on the hard drive is overwritten with a random sequence of 1s and 0s. Look for ISO 15408 certification.
- ▶ IP Filtering: A host-based firewall filters traffic by IP address and port number.
- ▶ MAC Address Filtering: Provides network access control via the 802.1X protocol.
- ▶ Removable Hard Drive: The MFP's hard drive is mounted externally, allowing for removal and storage.
- ▶ Network Port Security: System administrator can enable or disable IP ports, controlling the different network services provided by the print controller to an individual user.
- ▶ WPA (Wi-Fi Protect Access): Used in conjunction with the IEEE 802.11b Wireless LAN option, to provide assurance that data is protected by allowing only authorized users to access the network.

1 Symantec and Poneman Institute polled nearly 1,000 adults who lost their job in 2008.