Are your multi-function printers a security risk?

Here are five key strategies for safeguarding your data

Executive Summary

Security breaches can damage both your operations and your reputation, and repairing them can cost your company dearly. While most companies take great pains to protect their computers and servers, many neglect a potential weak spot in their security: multifunction printers (MFPs).

MFPs are capable of printing, transmitting, and storing sensitive information, both electronically and on paper. Like any other networked device, they need to be protected against both malicious attacks and simple employee carelessness in order to keep valuable data out of unauthorized hands. This white paper will discuss several security challenges involving MFPs, the potential consequences and costs of failing to mitigate MFP threats, and five key areas in which IT decision-makers can act to lower the risk.

Printer Security Challenges

Copiers and printers have become such basic office fixtures that employees commonly assume they can't possibly be a security risk. If they think about controlling printer usage at all, it may only be as a way to manage the cost of paper, toner, and other supplies. However, today's MFPs are integrated into the larger IT infrastructure. They must be secured to safeguard sensitive business information, employee and customer privacy, and help provide regulatory compliance. To do so, IT managers must address these challenges:

- Controlling physical access to the company's MFPs, not just by ensuring only employees can use them, but sometimes by limiting the devices a particular employee can access.
- Ensuring groups and individuals can use only the MFP features appropriate for their roles and responsibilities.
- Restricting who can open, print, and transmit electronic documents—email, PDFs, scans, and faxes—as well as how, where, and to whom they can be sent.
- Securing paper documents to prevent them from being stolen, misplaced, or simply seen by the wrong person.
- Protecting data stored on an MFP, such as user documents, device settings, and address books.
- Determining who accessed which documents, when, and from which MFP, both to help guard against information leaks and to create an audit trail for compliance purposes.

Consequences of Security Breaches

At best, failing to secure MFPs can lead to the extra supply and maintenance costs associated with uncontrolled usage. At worst, it creates a gaping hole in a company's information security procedures.

In one instructive case, a news reporter found that many MFPs awaiting resale in a warehouse still retained electronic copies of documents from past users. One machine contained a police department's list of targets for a major drug raid. Another spat out the answer to a fraudster's prayers: pages of a construction company's payroll records, complete with names, addresses, Social Security numbers, and photocopied checks. A third delivered pages of medical records ranging from prescription records to cancer diagnoses, forcing a health care organization to notify people that they may have been affected by this violation of federal privacy law.

Whether accidental or deliberate, data exposure leaves companies open to the risk of fines and other legal penalties

Of course, many companies know to erase devices' hard drives before disposing of them, but with no ability to detect or prevent unauthorized use of MFPs, malicious or careless users can expose sensitive information to loss or theft even while the machines are still in the supposed safety of the office.

Whether accidental or deliberate, data exposure leaves companies open to the risk of fines and other legal penalties for noncompliance, loss of reputation and customer confidence, loss of competitive advantage, lawsuits, and even embezzlement or fraud. MFP security features are a small investment compared to the potential costs of a data breach. By implementing them and following best practices for using them, IT managers can significantly reduce that risk.

Best Practices for Securing MFPs

Like a general-purpose PC, today's MFPs contain hard drives, memory, and a CPU. Many even use mainstream operating systems such as Windows and Linux. As a result, many security best practices that apply to network devices apply to MFPs as well. At the same time, best practices have also evolved and expanded to cover MFP specific functions. These five preventive measures can help protect MFPs against data loss, unwanted use, and the risk of compromising sensitive or confidential information:

1. **Device security:** Security for the multi-function printer starts with the MFP itself—and, as with any network device, an MFP policy should include methods of managing both who can use it and how. At the most basic level, this involves authentication, either with a PIN or password or by swiping an employee badge or other physical object on a reader. Users must be required to authenticate at the printer for every task, from copying a paper document to retrieving a print job sent over the network.

   Authentication also enables multiple levels of access control tied to the PIN, password, or an access card. The MFP should be capable of managing multiple levels of access restrictions by individual, department, group, or job responsibility. At the most restrictive level, users (including guests) should only be allowed basic functions like printing and copying. Other levels can give employees access to other functions, such as sending documents electronically, storing them on the printer or server, or accessing them online—but only as their job requires. Only system administrators should have access to the highest level of functions, such as network configurations, system configurations, and printing protocols.

MFPs configured to let users transmit electronic documents should include an additional layer of password-based security to protect the confidentiality of fax numbers and email addresses. In addition to restricting who can access the printer's address book, this security feature should also restrict who can add, remove, or edit address book entries.

The print driver itself should also include security features. In addition to the ability to track use by password for print-job accounting, a well-secured print driver will also give administrators the ability to create custom driver settings that both limit access to features and specify default settings. Using this function, administrators can define, enforce, and prohibit various settings—for example, ensuring every print job includes a watermark or force mandatory mailbox or secure password protected printing.

Device security on a multi-function printer should also include the ability to control access to the device's USB interface in order to prevent some or all users from attaching thumb drives or other USB devices.

Finally, any third-party custom solutions running on the MFP must themselves be secure to prevent malicious users from using them to compromise data integrity. The MFP's vendor should verify the integrity of these applications in a way that enables the MFP to sense any modifications and block the altered application from running.

2. **Information security:** Once IT administrators are confident they've chosen a device that's physically secure, they can move on to safeguarding the security of the data the MFP handles, both in hard copy and electronically.

Preventing paper documents from falling into the wrong hands is often a matter of not committing data to paper until the right hands are there to claim it. An MFP should include secure printing functionality that holds documents in the print queue until the user authenticates at the printer. For additional security, the system administrator should have the option of encrypting data as it travels across the network to the printer. In offices that handle large amounts of sensitive data, the administrator can designate one device to permit only encrypted print jobs, or even require encryption for all print jobs on all devices.

Many MFPs that contain a hard disk have the capability to store user files, similar to a file server. Security-conscious administrators will, at a minimum, want to limit the type of files that can be stored at the MFP and password-protect the storage space to restrict users' ability to store and retrieve documents. In situations where data security is mission-critical, administrators may choose to disable file storage altogether.

To further discourage unauthorized copying or transmission of sensitive information, administrators should also consider using other MFP features, individually or in combination:

- Secure watermarking, the ability to embed user-defined text in the background of a print or copy job so that it remains invisible in the original, but appears when the printout is photocopied.
- The ability to encrypt PDFs sent by email or stored on a file server, so that only users with the correct password can view, print, or edit them.
- The ability to add a digital signature to verify a PDF's source and authenticity.
- The ability to embed tracking information visible only to administrators.

5 Ways to Safeguard Your Data

- Control access to the MFP and its functions at the group, individual, and activity level.
- Ensure data is secure at every stage of the workflow.
- Use all available tools to protect sensitive documents from loss or theft.
- Include MFPs in standard network security measures.
- Capture, audit, and archive all device activity information.

- The ability to restrict copy/send/fax permissions not only by user, but by document.
- The ability to integrate Adobe LiveCycle Rights Management ES for tighter control over PDFs, from access permissions and distribution tracking to setting an expiration date after which the PDF will not open.

For the highest level of data privacy, an MFP also needs features to protect the data, both in storage and in transit. Strong encryption is key to protecting data while stored on the MFP hard disk, as data travels over the internal network, as it waits in a print queue, or when transmitted over the Internet. The MFP should support the Advanced Encryption Standard (AES), recognized in the industry as a strong encryption algorithm to protect electronic data, and use it for hard disk encryption, PDF file encryption, and encrypted printing.

For the highest level of data privacy, an MFP also needs features to protect the data, both in storage and in transit

The MFP should include functionality that simplifies the process of erasing critical data. To avoid any chance of data leaving the building when the MFP is moved or disposed of, administrators should use tools to overwrite all user data areas on the hard drive. It may also be wise to set routine print job processing to erase previous print job data automatically.

On devices equipped with hard disk encryption, one further layer of protection is the use of a Trusted Platform Module (TPM). A TPM is a tamper-resistant chip that stores sensitive security information, such as encryption keys, separately from the encrypted data on the hard drive. This also ensures that the hard disk will only operate on the MFP that contains the original TPM; if it's removed or tampered with, the MFP cannot decrypt passwords and other information it needs to function. Administrators using the TPM must be sure to back up the encryption key in a secure location so they can retrieve the encrypted data if the TPM chip is lost or damaged.

MFPs equipped with fax capability may also raise concerns. To protect the data network, these MFPs should have fax capability that only accepts fax-related protocols and does not allow for remote access type connections. This ensures the local network cannot be accessed via the phone line. To minimize the chance of virus transmission, the FP's fax function should examine the format for received faxes and discard any that do not conform to the format's definition of a fax image. Administrators can also help protect data privacy by routing faxes into secure storage and requiring users to authenticate in order to retrieve or print them.

3. **Network security:** Best security practices for multi-function printers also protect sensitive data by placing them on internal networks which are protected by firewalls or others security devices, thereby prohibiting direct access from the Internet. In this, MFPs are much like other networked devices: they require controls that limit network access, manage the use of network protocols and ports, and deter viruses and other malware.

   System administrators must be able to enable and disable FTP, SMTP, HTTP, IPP, RAW, SNMP, and other common protocols at the device level to block unnecessary connections. For tighter control, they should also be able to restrict MFP use by IP address, allowing only certain addresses or ranges of addresses to send or receive documents. In addition, the MFP device should be able to handle common encryption protocols such as SSL and IPSec to protect data as it travels over the internal network.

Finally, MFPs that support wireless connectivity must support strong wireless encryption and authentication standards. They should also automatically disable the wired interface so that no data bridging or routing is possible between the wired and wireless connections.

4. Monitoring and management: Some companies have just one printer, and others have dozens or hundreds. Either way, system administrators need an easy way to monitor MFP usage to ensure compliance with company rules and regulatory requirements.

The best solution is a single, secure point of control that allows IT staff to set up, configure, update, and manage every MFP from one central console. This lets them troubleshoot, restrict access at the device or function level, and lock out unauthorized access attempts quickly, without time-consuming travel to the printer's physical location.

Canon recognizes that security is as important as print quality

5. Logging and auditing: In a data-centric world where data exposure can carry heavy penalties, IT leaders must be able to track MFP usage at the document and user level, both for data security and for regulatory compliance purposes. Best practices in logging and auditing require an MFP with tools that can record, trace, and restrict interactions involving both electronic and paper documents.

Especially sophisticated systems are able to embed invisible tracking information in the background of electronic documents.. If someone tries to copy this document on the MFP, the printer can either block the attempt to copy or scan, and/or log the attempt. The administrator can then use the trace function to establish a chain of custody, including each time the document was copied or printed, by whom, when, and where.

These logging and auditing tools should work with printer accounting management software to track usage at the department, group, and individual user level, both to enhance data privacy and to eliminate wasteful use by enforcing billing codes and usage limits. For best results, administrators should be able to capture, archive, and report on all copy, scan, print, fax, and send jobs, with records that include searchable metadata to simplify later retrieval.

Performance + Security = Canon

With years of experience developing multifunction printers, Canon recognizes that security is as important as print quality. Its new imageRUNNER ADVANCE devices put all current best practices for printer security into effect simultaneously, with powerful standard and optional tools that meet or exceed the requirements of stringent government and industry certifications and regulations. Properly deployed, Canon imageRUNNER ADVANCE devices increase productivity—while significantly reducing the risk of exposing sensitive data through malice or mischance. ■