FCW

A New Approach to Document, Data Security

Introduction

Several of the big trends in computing are converging on multifunction devices (MFDs), those print-fax-scan-copy workhorses found throughout the enterprise that every office depends on.

Given the rise of mobility and cloud computing and the paperless flow of data, you might think MDFs would be relegated to the periphery. But it turns out, the modern enterprise environment is anything but paperless. Moreover, MFDs have evolved a great deal. They've become network-connected hubs in the workflow of documents and data.

That's why security of MFDs has become an important imperative. So much data and so many documents flow in and out of these devices, they demand an updated, holistic approach to security. If all your IT group is doing is periodically wiping the hard drives aboard MFDs, it's leaving a host of vulnerabilities that can lead to real losses.

Think about it: A multifunction device may be connected via Ethernet, Bluetooth and WiFi. People thereby send data to the device. They also scan in data for distribution, possibly to a cloud. Faxes, even if they are never output to hard copy, represent another source of data coming into MFDs, from which they are distributed to their intended users. The latest devices have touch-screens so people can call up documents they need as well as scan in information. And they come equipped with software for designing document and data workflows.

This coincides with the rapid movement of organizations into the third wave – or to use market research firm IDC's term, third platform – in computing. This wave is extending the enterprise towards users, now more fully mobile than ever; and beyond data centers, many of which are giving way to commercial clouds that put data and documents outside of the organization's firewall.

The third platform presents new security challenges, including those surrounding an enterprise's MFDs.

Third Platform Defined

To understand the third computing platform, it's helpful to briefly look at where computing has come from.

The first wave consisted of mainframe processors coupled to terminals as the principal user way of getting information in and out. The minicomputer era replicated the enterprise mainframe at the business unit or functional level. An engineering group or marketing/sales could have their own minicomputer. Equipment, communications protocols, operating systems and applications were proprietary.

The second platform produced orders of magnitude more users by equipping everyone with a PC connected to a LAN and, beyond the LAN, the enterprise network. Internet and virtual private networks superseded proprietary WANs. Client/server applications ballooned to tens of thousands. Everyone had – and has – e-mail and a basic set of office productivity and collaboration applications at a minimum.

The third platform is emerging fast and co-exists with the second. It brings together several developments, chiefly wireless broadband, cloud computing, big data powering lightweight apps, and social media.

In the third platform, people use smartphones and tablets for enterprise computing. These devices mostly use reduced instruction set processors and mobile operating systems, not traditional desktop OSes. (Manufacturers have been working to converge mobile and desktop OSes but full integration is still a major release or two into the future.)

Mobile devices require new iterations of enterprise applications, and they have brought with them millions of native apps. Many of these have powerful enterprise potential. In fact, organizations in both the public and private sectors frequently incorporate consumer apps for functions such as note-taking, contact management, and communications into their internal app stores.

Because these devices have as their primary connectivity media WiFi and cellular voice/data networks, they offer nearly 100 percent mobility, enabling computing anywhere and at any time.

Compared to the mainframe and client/server eras, the third platform has produced a revolution in end user computing. It's certainly revolutionary in terms of scale. IDC estimates that by 2015, 1.3 billion workers will be mobile, representing 37% of the workforce. By the end of last year, some 128 million tablets and 722 million smartphones were in use worldwide.

The Third Platform and Workflow

As we've described, the third platform in computing is characterized by a convergence of mobility and cloud. In this model, mobile devices access data stored in clouds, creating a sort of virtual enterprise outside the organization's wired network and internal WLAN. The set-up produces a rich computing experience for users. But it also creates new and specific security challenges because it changes long-established workflow patterns. It alters the ways in which data and documents, devices, user access, and hard copy versions of information interact.

For example, a user may call for a document, say a spreadsheet or presentation, stored externally in a cloud, possibly in a virtual machine. That user may download the file to a mobile device, then later on print it using a mobile print application when he or she is in the office. The document and the data embodied within it may never have crossed the wired infrastructure.

With highly up-to-date workflows, mobile print can send a document to the same printer from wherever the user happens to be. If it is a confidential document, how long will it sit in an output tray? There's a new version of an old security risk, exaggerated by the fact that the person printing the document could be hours or days away from picking it up.

In the third platform with its new, cloud and mobile enhanced workflows, the MFD still figures prominently. People print remotely, as we've described. But data and documents go both ways. Local, in-office users scanning in documents are likely to select a cloud location as the destination, later to be recalled by a mobile user.

This means it's time to re-think user authentication processes and access privileges to multifunction devices. In government applications, it means paying particular attention to how remote access to MFDs can be accomplished in such a way that the organization stays in compliance with laws and regulations for information privacy and national security.

In short, MFDs have evolved along with the mobile-cloud approach to computing. They've become, in effect, the on- and off-ramps to cloud-hosted applications, data and documents. With mobile users and cloud resources, people operate untethered from the traditional enterprise network, but they come back in via the MDF. To maintain security and compliance, you need non-traditional ways of managing and tracking this activity.

Workflow, Security, and Multifunction Devices

Perhaps it's their legacy as unconnected devices that causes people to overlook the security vulnerabilities associated with multifunction devices. The first copiers were connected to nothing more than the electrical outlet. People brought paper to them, stood there while the machines cranked out copies, then marched the originals and the copies back to their desks for collating and hand-distributing.

That all went the way of the pink telephone message slip and the typing pool. Today's network-connected MFPs are the hubs of complex data and document workflows.

Organizations face tangible potential for loss of money and intellectual property in these new workflow environments. Consider these horror stories:

- In one famous case, Singapore banking officials found in the hands of one employee copies of confidential faxes meant for legislators.
- Several documented instances have shown employees who inhabited cubicles near a group printer and helped themselves to someone else's output. In one case, an employee monitored confidential information on mergers and acquisitions and made millions by trading on that information.
- A computer trade magazine reported that in a single month, two Medicaid data breaches occurred at the state Medicaid office level. Employees transferred private, confidential data to personal e-mail accounts.

If you see a pattern here of insider, employee breaches, you're not off the mark. IDC reports that 79 percent of reported data breaches come from employees with trusted access to organizational resources. In all, 81 percent of employees have access to confidential information. The same research found that organizations face significant consequences of cybercrime, with the 2013 average so far hitting the $9 million mark, and rising 5 percent each year. The number of occurrences is also on the rise, driving up the costs of compliance.

Zero In On MFP Security

Unfortunately, hackers don't find it particularly difficult to hack into MFDs that aren't properly secured. Often, the bad actors plan their moves carefully, with breaches routinely taking place during work hours.

Properly securing MFD begins with simply understanding that they are vulnerable in the first place. Dennis Amorosano is senior director of solutions marketing and professional services at Canon U.S.A., Inc., a leading manufacturer of enterprise grade MFDs. In presentation after presentation, he laments that the devices are not widely considered vulnerable on the network, but they should be. In fact, he says, lack of consideration is what makes them vulnerable in the first place.

But think about the MFD for a moment. It has a display, keyboard, hard drive, a network interface card, WiFi and Bluetooth. It's accessible to mobile users, and it offers not just output but also document distribution.

What are the main data-theft vectors involving multifunction devices? Here are the main ones:

- Weak authentication and access. All users are not equal. They have differing levels of privilege on the network and different sets of applications. Yet too often they have equal –meaning full and open – access to crucial MFDs. A corollary danger is weak authentication of guest users, often in the same organizations that have careful restrictions on guest WiFi users. Some even go so far as to have separate, unsecured WLANs for guests. Why leave MFDs unsecured?

- Lack of auditing of user activity. Too often, network logs leave out data generated by MFD usage, concentrating instead on individual computers and servers.
- Paper everywhere. Output trays on the devices or collection bins are nearly always left open and unsecured. Every organization has tales of salary schedules or other personal information carelessly printed out and sought for pickup only when it's too late and the wrong eyes have seen the information or, worse, have copied and distributed it.

Yet all of this is avoidable.

Solutions For MFD Security Vulnerabilities

Knowing your security weaknesses is the start of eliminating them. Clearly, MFDs need to have all of the security essentials. The organization needs to know who is using the devices, and from where, and how information assets are being used.

Your first step is not necessarily technical, but rather an organizational realignment. Specifically, MFDs are often the purview of the facility's management department and not IT. That should change so that the locus of cybersecurity expertise "owns" any output device on the network.

A first basic technical step is encryption of the hard drives on MFDs and erasing them at periodic intervals. But, as we've noted, this is where output device security ends for too many organizations.

Beyond these standard steps, you'll find a host of controls to devices, documents and the network. Canon has incorporated them into its imageRUNNER ADVANCE Series security suite that accompany its MFDs. Coupled with Canon's Multifunctional Embedded Application Platform (MEAP) for creating customized document workflows, these capabilities enable a much higher level of security and control than simple hard drive encryption and hope.

For starters, the organization must institute restrictions on who can call up, print, or send documents. Institute a menu of assignable privileges based on the user's role. You can configure today's devices to offer designated, role-based functions, and only the designated ones. For example, the organization may want to restrict who can scan engineering drawings or financial information. You can limit logical destinations of faxes or other document formats down to just one or two, and this can be configured per user. In short, with the right software solution you can customize an MFD for each user.

But authentication-based device restrictions can also apply at the workgroup or department level.

Also consider hardware tokens to restrict access. Hundreds of thousands of civil servants and members of the military are using access cards issued under Homeland Security Presidential Directive 12, known as PIV cards, or DOD's common access card. These are capable of both physical and network access control, and they offer a readily available route to enforcing MFD access policies.

For users without cards of this type, IT can activate password control on devices, just as in the early copier days when plug-in hardware "clickers" were required to gain access to the precious copier and organizations operated them on a charge-back basis. For devices that support it, establish user logon and privileges using individuals' Active Directory profiles.

Don't overlook personal printers and MDFs. Many federal agencies have been diligently rooting out and removing personal printers, not so much for security as for saving power consumption

and reducing use of paper on the theory that if people have to walk 10 or 100 feet to an output device they'll think twice about hitting the PRINT button. But those outlier devices carry the same security vulnerabilities as departmental or workgroup MFDs and should therefore be included in any security plan.

For MFDs in highly sensitive environments, you can equip them with removable hard drives that administrators lock up after hours.

Document Security

Here again, before cyber controls are applied to documents, the organization should establish policies on physical output itself. These are difficult to police and enforce, but their establishment can set a tone that says to employees how important data and document security is. Consider a policy that sends a technician to shred all documents in a tray if not retrieved in, say, 30 minutes.

Better yet, available software can secure printouts by stopping the process at the final output step, storing the printout until the specific user arrives and releases with a password. Or, a user can print a document, then go to an MFD on the network to actually execute the printout and retrieve it.

A number of technologies are available for document security. These involve authorization for access to documents, marking documents with electronic watermarks to enable audit trails and controls on copying so receivers can verify whether the copy was authorized. Consider software for encrypting individual documents or applying digital signatures to Portable Document Format output to let recipients check authenticity.

Canon's imageRUNNER ADVANCE Series also supports fax forwarding, in which the MFD, rather than outputting the fax to hard copy, sends it to the designated recipient at his or her desktop or mobile device.

It's critical to know who accessed which documents. Sometimes time of day can be critical to revealing a security problem. For instance, an individual entrusted with access, print and send rights who exercises them in the middle of the night could raise a red flag. So it's important to establish logging and auditing software for each MFD.

Network Security

MFDs, as network devices like servers and PCs, should be treated as such in terms of cybersecurity. That means turning on WPA security for MFDs with WiFi connectivity. It means applying the same security controls as you do with computers, such as SSL encryption, address and port filtering and monitoring and remote on/off control for USB ports. Combined, these restrict usage of devices to only authorized users or addresses

In summary, the third platform of computing has combined with the tremendous gains in multifunction device capability to produce real gains in mobility, flexibility and efficiency. They've also produced new security challenges. With the right thinking, and application of technologies such as Canon imageRUNNER ADVANCE Series, users and agencies can enjoy full mobility and security in an environment of digital and hard copy documents.

For more from Canon, please visit www.usa.canon.com/advance.