IDC

IDC ANALYST CONNECTION

Sponsored by: Sharp

The office multifunction printer (MFP) is an intelligent business processing hub that serves as an important on- and off-ramp for both paper-based and digitally based business information. Particular attention must be paid to this mission-critical device to ensure compliance with the organization's overall IT security initiatives.

Safeguard Your Organization's Sensitive Business Information with a Comprehensive MFP Security Action Plan

July 2021

Questions posed by: Sharp

Answers by: Keith Kmetz, Program Vice President, Imaging, Printing, and Document Solutions

Q. Why is there a need to address multifunction printer (MFP) security specifically? Isn't it addressed by the organization's overall IT security plan?

A. An overall IT security plan is a great first step, but it is only a piece of what is needed when considering MFP security. It is faulty logic to assume that MFP security is entirely covered under a broader IT security plan, and being behind a firewall is no guarantee of security on its own. Many organizations leave themselves vulnerable due to a lack of awareness of what is needed to provide for their total security requirements.

IDC believes that organizations should take specific action to address the unique characteristics of the MFP in their organizational security plan. Why? Unlike any other IT technology, the MFP addresses business information in both paper form (e.g., prints, copies, faxes) and digital form (e.g., scanning). To be truly secured, an MFP requires a security plan that addresses both formats to effectively corral this challenge. While office workers are bombarded with an exponentially growing amount of digital content to use and manage, the U.S. market is still expected to generate over 680 billion pages on MFPs in 2021, so there is an abundance of paper-based content available that needs to be secured too. The need to ensure that all this content, digital and paper, is accessible only by authorized users is of paramount importance.

Muddling the security challenge is that cloud and mobile technologies have emerged to offer the great organizational benefit of "anytime, anywhere" access to business information. However, this accessibility is a double-edged sword. Greater accessibility can also mean greater vulnerability, if the appropriate security solutions are not in place. If a security breach occurs, sensitive company information could fall into the wrong hands.

Q. What is the significance of ensuring a secure print environment? Where are the vulnerabilities?

A. IDC sees a broad base of security vulnerabilities across MFP use cases. These vulnerabilities can occur at the device level to the documents created/managed/distributed by the MFP or on the network.

At the device level, an unsecured MFP is subject to careless use or malicious attacks from inside or outside the organization. Remember, the MFP is a system. It has a display screen or user interface, memory, a hard drive, communication ports, and network ports where access to sensitive information may reside. All these access points represent opportunities to gain entry to the device as well as to other endpoints in the same computing environment. Steps should be taken to ensure authorization/authentication of all users to interface with the MFP. However, with so many other entry points available, MFP security needs to address more than just authentication to prevent a security breach.

The MFP is also responsible for documents at rest or in motion. If the documents are not properly secured when faxed or scanned to a destination, this information could be attacked or intercepted en route. Documents at rest include information still resident in memory or the device's hard drive. Specific to paper-based content, another document-at-rest vulnerability may exist in the output tray where sensitive prints, copies, and faxes could lie unretrieved and accessible to anyone passing by the MFP. Documents in motion (faxes, scans) can be intercepted and used if not secured with encryption.

The MFP is one of many technology citizens on the network, and every device connected to the network is poised to be an endpoint security risk. It is important to note that the MFP acts as a hub for a high level of business processing, meaning that not just printing and copying but also a wide range of document networked traffic must be monitored and secured. Thus, it is crucial that businesses pursue a comprehensive approach to security so that the organization's print and document infrastructure is adequately secured. Remember, organizations are only as secure as their most vulnerable network endpoint.

Q. Are there certain markets where security is vital to the organization?

A. All markets typically place a top priority on securing their workplaces, so the need and the desire to be secure have top-of-mind awareness. The ramifications of a security breach are significant, including bottom-line impact penalties such as fines or loss of business. Indirectly, the security problem could result in an uncalculated negative financial consequence due to damage to the firm's reputation as well as the use of valuable employee time and costs to correct it. On the other hand, a comprehensive print security plan offers numerous benefits to help shrink overall print costs, reduce organizational risk, and gain new efficiencies by lowering security incidents. All these benefits offer direct positive impact to the bottom line.

Regarding specific areas where security is critical, healthcare (HIPAA), financial services (GLBA, Sarbanes-Oxley), legal, education (FERPA), and government have mandated governance policies with respect to information used in these operations. These sectors often require access to sensitive personal or financial data information. Legislation governing these industries and organizations offers insight into how this content is to be managed and typically spells out possible consequences for a violation of this trust.

Q. Has the recent COVID-19 pandemic influenced any new developments for MFP security?

A. One of the complicating factors influencing the future of work is that the pandemic ushered in a significant increase in remote and home working. Organizations had to adjust overnight to major changes in how employees functioned during the pandemic, including how information was managed throughout the workday. Fortunately, a greater range of remote access technologies enabled office workers to maintain productivity, even while located in homes, during this crisis period.

However, homes were never designed to be cybersecurity perimeters. Hacking activity rose during this period as malicious actors preyed on the vulnerability of technologies typically used in home environments. Hackers capitalized on the weakness or absence of essential security measures in work-from-home environments needed to protect content. In a recent IDC survey, respondents were asked about their organization's top IT challenges and the work-from-home print challenges faced by employees. Security vulnerabilities and worries was the sole item to make the top 3 list of challenges for both IT overall and print specifically.

IDC anticipates that a hybrid workforce — one in which employees have the flexibility to work from different locations — will account for a much greater percentage of work now and in the future. The pandemic served to reinforce the idea that workers can be productive outside of the conventional office with 24 x 7 access to technologies necessary to getting work done. Culturally, organizations learned that employees could be trusted to work competently outside of the direct watchful eye of management. This change does mean that management will need to put new policies in place to address the security conundrum, inclusive of specific print security programs to address devices, documents, and network connection. While the pandemic ushered in greater work flexibility for the employee, this flexibility also potentially raises the organization's vulnerability and security threat levels if it is not well managed.

Q. What are the appropriate steps to take when considering an MFP security strategy?

A. There are multiple steps to take when considering an MFP security strategy. Hopefully, organizations have already embarked on this initiative, but even if they have not yet done so, the opportunity to act is still available to them and should be initiated.

Organizations should start by getting executive buy-in to the proposed MFP security plan. The work needed to put a plan in place should go more smoothly with executive-level support. Print should be part of an overall IT security strategy, but the MFP security plan should also include print-specific policies and procedures to guide access and use of this technology.

The plan should be long term in nature with mechanisms to address worker behavior as well as the use of technology in the office and in home/remote locations. Some basics to consider for the plan are working on automating certain business processes with attention to security; multifactor authentication for all employee access to technology; specific language for bring your own device (BYOD) and working remotely; and establishing specific governance policies for the use of company data.

Organizations should look for a provider with a strong history and background in security. IDC's research has confirmed that security capabilities have a high influence on MFP purchasing decisions, so organizations should consider picking a provider that demonstrates a history and emphasis on security. They should see if the vendor is active in security market initiatives and has enlisted key partnerships with known security providers. The MFP provider should demonstrate an ability to respond to an organization's security plan and provide an offering that aligns with the organization's goals. A multilayered approach that addresses security in hardware, software, and network services should be a priority to ensure a high level of security.

There are numerous key security features to look for in the provider's portfolio. Passwords and user authentication are givens, and more will be necessary to ensure a secured print environment. While there are many MFP security features to review and consider, a few MFP-specific capabilities that are less obvious but that should be considered as part of the MFP security solution are as follows:

- Providing encryption features to protect resident information in the device's memory and hard drive as well as for documents in motion (e.g., scanning, faxing)
- Having secure updating of firmware/BIOS/OS as well as protection that detects attacks and restores firmware/BIOS/OS to the original state
- Securing all communications ports (e.g., network connections, fax lines)
- Using application whitelisting to ensure that only authorized applications/files can access the MFP
- Offering pull printing (e.g., enter a PIN at the MFP to initiate printing)
- Having an audit log to track/monitor use
- Offering an end-of-life plan to erase any remaining content still resident in the device's memory and hard drive
- Implementing company security policies to govern employees' use of business-related information

At a minimum, organizations should make sure the offering adequately addresses the security of the device, documents at rest and in motion, and the network. While no security plan can be 100% foolproof, taking the action to design and implement a comprehensive MFP security plan will allow organizations to recognize and react to threats quickly as well as minimize the potential impact.

About the Analyst

Keith Kmetz, *Program Vice President, Imaging, Printing, and Document Solutions*

Keith Kmetz is the Program Vice President of IDC's Imaging, Printing, and Document Solutions programs. He is responsible for all written research in these areas, including analysis on the printer, multifunction peripheral (MFP), and 3D printing markets as well as related transformational hardcopy software/services developments.

MESSAGE FROM THE SPONSOR

Organizations of all sizes rely on a broad range of technologies to help make daily activities and communication more efficient while protecting against network intrusions and malicious attacks. The adoption of modern platforms, such as mobile and cloud services helps streamline workflow, but also creates new security challenges for IT administrators. The more open and intricate these platforms become, the more vulnerabilities there are for organizations to face that could put sensitive information and business continuity at risk. Sharp MFPs and single function printers provide strong information security features that help protect data-in-transit and data-at-rest, as well as auditing features to facilitate compliance with industry regulations, such as HIPAA, FERPA, Gramm Leach Bliley and others, so organizations can work simply smarter. For more information, visit: sharpusa.com/security.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.