MFP Security

Is it part of your dealership's talk track?

by: Brent Hoskins, Office Technology Magazine

For a number of years, MFP security has been a part of the office technology industry. Early on, manufacturers saw that their MFPs were vulnerable to internal prying eyes and external intruders. Consequently, features such as using passwords to release print jobs to the output tray and self-encrypting hard drives emerged. The mission to ensure that documents and information are secure within the MFP realm has remained steadfast.

"We embrace security as a primary objective," says Bill Melo, chief marketing executive at Toshiba America Business Solutions Inc. (TABS). "In fact, we were one of the first manufacturers in our space to begin talking about security in a leading way as being paramount to what we do."

Security must be a primary objective for good reason, Melo says. "Today, probably more than ever, you regularly read about some new hack," he says. "The biggest one was the recent SolarWinds attack, which affected governments and some of the biggest corporations in the world. So, unfortunately, there are external threats — people from the outside who are trying to get into your infrastructure and either steal secrets or plant malware, ransomware, etc. There are people inside, too — disgruntled employees or otherwise — who may knowingly or unknowingly leave information exposed or, in some cases, seek to sell company information."

The MFP is an "important device" to keep secure because it is on the network, Melo says. "It is, conceivably, a gateway through which an external actor can get into the network," he says. "It's also a highly centralized, very commonly used product inside the office, principally used for recreating or distributing information, including very sensitive documents. So, MFP security is really important — probably more so than most people would think."

Are imaging devices without security measures in place actually vulnerable to breaches? "Oh yes, it has happened," Melo says. "We have some great videos that show — and thankfully not on Toshiba devices — where hackers have remotely accessed printers, mostly older models, printing off whatever they feel like from those printers; others have taken over and printed information from check printers."

Yes, says George Grafanakis, associate director of hardware product management at Sharp Electronics Corp., without security in place, the MFP could be breached. "There are many firewall features built into Sharp MFPs that help customers protect their data, such as IP/MAC address filtering, port management and more," he says. "If IT administrators are not using these features, they can be leaving doors open that could result in malware attacks. So, without MFP security in use, network ports can certainly create a path for malicious intruders."

Similarly, in sensitive environments without encryption, "the hard drive can be a treasure trove of confidential information and intellectual property for hackers and intruders," Grafanakis says. "If the data is not encrypted, it can certainly be compromised."

Likewise, there are features such as Sharp's Secure Print, whereby print jobs are released with a passcode, that protect documents from getting into the wrong hands. "Without them, a user who prints confidential documents would have to leave them on the output tray until picking them up, making it easier for prying eyes to see or steal the documents," Grafanakis says. "Plus, without authentication features, users could scan or send sensitive company information via email, or make copies without any tracking or accounting security. In addition, if there was no device admin authentication, intruders could easily access the device remotely, changing settings or stealing information stored on the device."

Fortunately, Grafanakis says, Sharp offers a broad range of security features that span its entire product line. "All are fully configurable based on customer requirements, ranging from SMB environments to highly secure government installations that require stringent mandates, including Common Criteria

certification," he says. "Most MFPs in the Sharp family support a full range of security features."

Of course, implementing MFP security features is an ongoing mission for the industry's manufacturers. TABS, for example, has developed the ability to remotely establish profiles in MFPs, via the company's e-BRIDGE CloudConnect, that meet certain desired security parameters, similar to how a person would set parameters in a browser to accept cookies, block pop-ups, etc., Melo says. "The device can then continually check to see if those profiles have been changed," he says. "If so, the device can request that it is automatically updated."

"Security is something that people cannot discount and is an area where salespeople can visibly address value. So, how much and how well they address this value equates to differentiation from competitors."

— Akisa Matsuda
Sharp Electronics Corp.

Steve Burger, vice president of technology innovation and new business development at Ricoh USA Inc., cites a similar recent stride with the launch of the company's Always Current Technology (ACT). "ACT enables the MFP's core platform to be updated as time goes on," he explains. "So, if I have an MFP and I want to add new technology or just stay current with the latest, we provide security updates among other updates that will automatically update your device. If there is a reported vulnerability, we can address that remotely and instantly, rather than waiting for someone to install a firmware update."

Such strides point to the reality that many MFP security efforts are taking place in the background, and while of great importance, are not necessarily a key focus of end users. Says Burger, speaking in particular of self-encrypting MFP hard drives: "We want our users not to worry about it. 'You picked Ricoh, you picked one of our dealer partners, we've got your back.'" Says Sharp's Grafanakis: "Sharp designs MFP products so that when security measures are in place, that minimizes the impact on users and allows them to proceed unobstructed in their workflows with the confidence that their data is protected."

Of course, many end users are likely unaware of the vulnerability of their MFPs when it comes to document and information security. Says Burger: "Does everyone know there is a hard drive in the MFP? Probably not." Says Grafanakis in agreement, while also identifying those workers who are paying attention to MFP security: "Most users pay little attention to MFP security as they go about their business. However, IT departments pay very close attention and make back-end security mostly invisible to users."

Are your salespeople making MFP security part of the talk track in the selling process? If not, there is good reason to do so. "Security is adding value," says Akisa Matsuda, associate director of software product management at Sharp, noting that often "salespeople struggle" when competing on price. "Security is something that people cannot discount and is an area where salespeople can visibly address value. So, how much and how well they address this value equates to differentiation from competitors. That leads to the ability to better convince customers to agree with the pricing."

The security talk track should be geared to the nature of the work environment and users of the MFP, Burger says. "How much security does the customer require based on the workflow they're doing?" he says. "If I'm in a marketing role and I'm creating a PowerPoint presentation, the content might not require the same level of security as in other company functions, such as in finance, where I have confidential financial information and want the MFP to be pretty secure."

Of course, there are companies and business environments where security is paramount and sales reps must be proactive in discussing security, Burger says. "In the RFPs of bigger customers, we are seeing stricter security requirements," he says. "Then, in certain departments and verticals, such as HR, health care and, as noted, finance, there are unique workflows and security requirements."

Despite suggestions to make security a part of the talk track, it is not always included, even with the manufacturers' efforts to educate sales reps on how to address security issues. "It's an uphill battle to some degree, because it's a lot easier for them to talk about prices, features and 'how fast your MFP is and how many pages it can staple,'" Melo says. "However, those sales reps who talk about security well are rewarded. At the very least, it lets customers know they are talking to someone who knows his or her stuff. In the best case, when someone has a great story to tell, it will help make the sale. We certainly encourage that discussion every time. I think we have provided some good tools and good education for people to have that discussion confidently and successfully."

Are you and your reps taking advantage of the resources your manufacturers offer? Via its Encompass StoryTeller presentation platform, TABS, for example, offers a print and MFP security presentation that sales reps can use in the selling process. It addresses such topics as the importance of

security and print security vulnerabilities. "We try and make it really easy for our dealers to present the information because once made aware, customers respond to it," Melo says. "If they are told 'there's a potential fox in the hen house,' people are going to react to that."

Similarly, a 32-page PDF, titled "Ricoh Security Overview," can be downloaded from Ricoh's website. It, too, can be shared with customers and describes, among other topics, Ricoh's layered approach to security. Likewise, Sharp offers a 28-page PDF, the "Security Suite Reference Guide," via its website. "It is divided into four sections — the internal threat, the external threat, mobile and the cloud," Matsuda says. "We have answers to all kinds of aspects of the environment so salespeople can work with customers to design the security measures that will be required around their MFPs."

"We try and make it really easy for our dealers to present the information because once made aware, customers respond to it. If they are told 'there's a potential fox in the hen house,' people are going to react to that."

— Bill Melo
Toshiba America Business Solutions Inc.

Unfortunately, the workplace challenges presented during the COVID-19 pandemic have resulted in a rise in hacking and the potential of a company facing a security threat, Matsuda adds. "Every single organization and end user must have the awareness of the need for MFP and network security," she says. "This is an opportunity for dealers to be innovative and become true partners with compelling security services." ■

Brent Hoskins, executive director of the Business Technology Association, is editor of Office Technology magazine. He can be reached at brent@bta.org or (816) 303-4040.