By Aaron Hale

# Could a Data Breach Sink Your Fleet? *(Part 2)*

Take action today to keep your organization's printing devices secure. Not doing so could cost you.

Do an Internet search for "default password" and include the OEM of your fleet devices. Next, go to the search engine Shodan.io and type your copier fleet OEM name into the search field.

By taking the actions above you can see just how vulnerable printing devices can be. And this is nothing more sophisticated than a simple web search. Imagine what the bad guys can accomplish with the resources available on the dark web.

In part one of this article, I talked about the ever-present threat of a security breach that could compromise your organization's intellectual property, user identity and personal information, potentially costing the organization a significant amount of money. The average cost in 2016 of a breach in the education sector alone was $300 per record.* To put that in context, the average total cost of a data breach in 2016 was $7.6 million.

There are two approaches to mitigating this scenario. One is "hardening" your fleet devices and the other is implementing user controls through print management solutions that provide protections such as user authentication, secure print and auditing technologies.

Copiers and MFPs can be "hardened" to ensure that they are not exposed to the outside and thus more vulnerable to attack. The term hardening implies that the configuration has safeguards put in place to restrict access to the device's connectivity features and functions such as turning off certain volatile ports. This would include USB ports in addition to network ports. It also means, ensuring that Secure Socket Layer (SSL) transport protocol is in place with an up-to-date version to mitigate against known threats (poodle, shellshock, heartbleed, etc.). Certificates must be authorized and validated with a signature and the level of encryption should be at the highest possible. The rule of thumb with hardening is simple: if you don't use it, turn it off.

Keep in mind that when these devices arrive from the OEM warehouse, they may be configured in a manner that leaves them wide open by default. Ask your vendors to perform this service, then call in any resident IT personnel to assist them with the implementation.

## Primary Areas to Secure

There are five primary areas of MFPs and copiers that require attention: Protocol Security; Hardware Security; Data Security; Managing Access; and Centralized Management. Your vendor should be able to provide detailed information that will enable your staff to perform the hardening service.

Most print management software solutions today provide features and functions that can help you to control your most volatile threat risk: the user. Protecting the perimeter with a firewall is all fine and good, but the real challenge is protecting the data within your domain. Numerous studies show that data breaches often originate within the organization, either from a lack of user awareness and mindfulness or from malicious worker behavior such as disgruntled employees looking to cause harm to the organization or enterprising thieves seeking to profit from stolen IP or customer personal information.

## Authentication and Authorization

The first step in controlling access is authentication of the end user via pin codes, passwords and proximity cards. No less important is user authorization. Print management solutions allow

*Aaron Hale is a senior advisor for Canon Solutions America's Enterprise Services & Solutions division. He can be reached at:*

**ahale@csa.canon.com**

* NEC (Net-Centric Enterprise Solutions), 2017

administrators to create unique user roles with unique permissions for the specific features and functions on the device they have access to. By leveraging an Active Directory (AD) employee database or through LDAP (Lightweight Directory Access Protocol), or even a local directory setup on the device, a user who is introduced to the device through authentication may only be authorized to print and copy documents. Another user may not be able to scan documents, but can fax, print and copy.

### Pull Print (a.k.a., Secure Print)

How many times have you walked by a fleet device and observed a pile of paper lying in the output tray? You may innocently rifle through it looking for your job, right? You didn't intend to infringe on someone's sensitive information, but there it is. When Pull Printing is implemented, users must walk up to the device, authenticate and then release the print job. In addition to contributing to a secure environment, this helps provide worker productivity, efficiency and cost saving benefits.

Any print management solution worth its weight in salt should provide a centralized management platform to help you monitor device utilization and user behavior, which can help business leaders with strategic planning in terms of new technology acquisition and copier fleet logistics. If you do not have a comprehensive print management solution and you are evaluating your options, a solution that provides real-time and historical auditing of devices should be at the top of your consideration criteria. In the event of an insider breach or an audit by a regulatory agency it will help you to gather information to respond accordingly.

With the recent WannaCry and Goldeneye/Petya ransomware attacks affecting many enterprise organizations that have what would be considered sophisticated IT infrastructures, end-point protection has never been more paramount.

Among best practices would be routine vulnerability checks on your network of fleet devices. There are freeware and relatively inexpensive tools such as Qualys and Tenable that you can use to find out how exposed you are and identify the types of hardening that you need to do. Keep in mind that these types of solutions are typically device OEM agnostic and thus may report false positives in some areas of vulnerability on certain devices. Managing the fleet and the print center is a lot of daily heavy lifting so you may want to consider lobbying your parent organization to invest in a third-party provider.

Managing worker risk behavior essentially comes down to education and internal marketing. Not all internal breaches at the hands of users are malicious. They may not be cognizant of the potential risk of the volatile information within documents or the way that they use MFPs to distribute documents.

A successful awareness campaign should be continuous and widespread. Some ideas:

- Wall mount a poster at every MFP with an infographic showing the risk potential.
- Conduct seminars and start a collaborative dialog with employees.
- Include C-level executives to get top-down buy-in and support.
- Create training workshops and follow up with experiential exercises. As an example, after a workshop on preventing phishing attacks, send a simulated phishing attack to attendees' emails and take them through the experience. Nothing is stickier than real world experience.

If these activities are beyond your scope or ability, consider working with management to enlist a third-party provider.

At the end of the day the technology that enables us to grow and prosper also puts us at risk. The times dictate that, like it or not, managing risk puts another task in the manager task list. You don't have to go it alone. Talk with your vendors and seek their help. After all, today a good vendor partner is not just about toner and clicks. So can a data breach sink your fleet? Being proactive about protecting your domain can float all boats. ***IPG***