CANON SOLUTIONS AMERICA

CANON SEE IMPOSSIBLE

DATA BREACH PREVENTION: WHAT HAVE WE LEARNED?

By Patrick Henry

The message to managers of in-plants and enterprise MFP (multifunction printer) fleets in a four-part series of articles preceding this one was blunt: data breaches are a clear and present danger to every print-providing organization that handles information it is responsible for keeping confidential. The in-plant or fleet without a formal breach prevention program is at special risk, because the news on this front just keeps getting worse.

According to the Identity Theft Resource Center (ITRC) and the data security firm CyberScout, 791 data breaches took place in the U.S. in the first half of 2017, setting a new mid-year benchmark. ITRC data from 2005 through July 25, 2017 spans 7,756 data breaches that involved 904,368,414 records containing personal identifying information. Adam Levin, chairman and founder of CyberScout, says numbers like these warn us that “breaches are the third certainty in life and we are all living in a constant state of cyber insecurity.”

While not every in-plant and fleet is destined for a data breach, too many will suffer the losses that these incidents inflict. This is because the circumstances in which data breaches can take place are universal—so universal, in fact, that the 2017 Cost of Data Breach Study from IBM and the Ponemon Institute estimates that organizations have a 27.7% average probability of experiencing a material data breach in the next 24 months.

Odds like that, combined with an average cost of $7.6 million per data breach incident (according to IBM-Ponemon survey findings), are a call to action that no conscientious in-plant or fleet manager should ignore.

A data breach occurs when records that link people’s names to other identifying pieces of information—for example, Social Security, telephone, and credit card numbers—go missing or are diverted into the wrong hands. In breaches suffered by organizations surveyed for the IBM-Ponemon report, anywhere from 2,600 to 100,000 records became compromised.

As noted, the dollar cost of losses occurring on this scale is high. First comes the immediate post-incident cost of finding and repairing the breach. Time spent undoing the damage is time that the in-plant or the fleet has to subtract from performing its primary mission—another drain on cost-efficient operation.

If the parent organization is subject to mandates governing data security, add financial penalties to the list of potential costs. But the highest cost of all could come in the form of lost business opportunity as adverse publicity and lawsuits drive current and potential customers away. Financial pain for the parent organization will be pain shared, in one way or another, by its in-plant and fleet.

It’s true that the most widely publicized data breaches have had nothing to do with the way the affected organizations were running their captive printing operations. For example, a notorious hack involving the personal and credit card information of 70 million customers of a retail chain began with the theft of credentials from one of the retailer’s external contractors—a provider of heating, ventilating, and air conditioning services.

Nevertheless, in-plants and fleets have vulnerabilities of their own that need to be addressed. The fact is that while most organizations go all out when it comes to ensuring general IT security, many of them don’t place the same emphasis on upholding the security of their printing systems.

This can lead to serious gaps on the print side. For example, in a 2015 survey of more than 2,000 IT professionals from around the world, the Ponemon Institute found that on average, 55% of devices were insecure in terms of access to data stored in printed hard copy. Close to half (44%) of devices were insecure in terms of access to data contained in the devices’ mass storage.

Potential risks abound in MFP devices commonly used in in-plant and fleet environments: easy-to-discover default usernames, passwords, and port settings; open output trays; unsecured hard drives; unencrypted connections to networks; and exposure to unauthorized mobile printing applications. Plugging these holes helps protect data both from theft and from being altered either accidentally or maliciously.

But, the response can’t be to simply slam the door shut. The goal of practical breach prevention is to maintain confidentiality and integrity while assuring that data and devices remain accessible to legitimate users.

Although there is no such thing as a one-size-fits-all breach prevention program, effective ones have the following features in common:

Device security. Hard drives are tamper-proofed against data theft and may be physically secured (locked) within the device.

User authentication. Only users who can confirm their IDs with passwords, smart cards, or other means can print from in-plant and fleet devices.

Access control. Each authenticated user is authorized to perform a specific set of tasks on a given device—only those that the user needs in order to carry out individual job responsibilities.

"Pull" printing. Jobs are sent to the device but held in queue until the user commences printing by first verifying his or her ID.

Encryption. Secure Socket Layer (SSL) and/or other encryption protocols protect stored and shared data at all times, throughout the entire network.

Centralized administration. With automated and centralized record-keeping, in-plant and fleet managers can track utilization, monitor compliance, update software, and troubleshoot system problems across multiple devices, simultaneously.

Taking steps towards security in printing environments pays off in ways that can be measured. International Data Corporation (IDC) reported that after 16 organizations it interviewed tightened their printer security procedures, they saw their average annual number of breaches decline from 9.9 to 1.5. Because what IDC calls a "significant" printer-related security breach can take hundreds of employee hours and hundreds of thousands of dollars to repair, preventing even one of them yields major savings.

For positive reinforcement, there are the potential savings that stem from efficiencies gained when "pull" printing and other security procedures are in place. Organizations where people print only what they need, when they need it, consume less toner, ink, and paper than organizations without controls. People who spend less time lining up at copiers and have more time to concentrate on their primary tasks.

The preceding articles in this series offer good advice for setting up a breach prevention program or strengthening an existing one. The core elements of what they recommend for breach prevention in in-plants and fleets are as follows:

Recognize the risk. No in-plant or fleet is immune to data breaches. Because the nature and the variety of the threats change constantly, periodic print security audits are important.

Raise awareness through education. Employees engaging in breach-prone activities probably don't realize that they're doing anything wrong. Train them to spot potential problems and to adjust their behavior accordingly.

Parental guidance advised. This means working cooperatively on security with the IT department and other responsible groups within the parent organization. If there ever was a corporate quest in which everyone needed to be on the same page, data breach prevention surely is it.

Tap vendor expertise. Suppliers of printing systems to enterprise fleets and in-plants understand that support for data security must be an inherent capability of the equipment they sell into these environments. The vendors have both hardware with security features and software solutions to help address the breach-related issues raised in this series. They are eager to share them.

Because printing technologies never stop evolving, preventing the kinds of data breaches associated with document production will always be a moving target. Even now, cloud computing applications and the rising use of print-capable mobile devices are complicating the task of data security for managers of in-plants and fleets.

But, the good news is that remedies are emerging at the same pace. For managers ready to embrace them, the threat of printing-related data loss need never become a what-keeps-you-up-at-night concern.

RECOMMENDED READING

The preceding article concludes a series of reports on data breach prevention and cyber safe production for managers of in-plants and enterprise fleets. The author of the series is Aaron Hale, a Senior Advisor for Canon Solutions America's Enterprise Services & Solutions division.

All are available at the In-plant Graphics website (**www.inplantgraphics.com**)

Success Can Be Fleeting *April 2017*
Can a Data Breach Sink Your Fleet - *Part 1 June 2017*
Can a Data Breach Sink Your Fleet - *Part 2 July 2017*
Cyber Safe Production Workflow *August 2017*
Are You Certifiable? *November 2017*

ABOUT THE AUTHOR

Patrick Henry
Senior editor, Printing & Packaging Publishing Group, NAPCO Media
1-917-647-0590

Patrick Henry is a journalist, an editor, and an educator who has covered the graphic communications industry for more than 30 years. He has written for most of the industry's principal trade media and has been chief editor of several of its leading publications. Henry holds numerous awards for editorial excellence and has been recognized for exceptional service to the industry, particularly in education.

This analysis was commissioned by Canon Solutions America and NAPCO Media to help printers better understand how today's technology can optimize their production and how they can benefit by adopting these solutions.

Canon Solutions America, Inc., a Canon U.S.A. Company, provides enterprise, production print and large format solutions, supported by exceptional professional service offerings. www.csa.canon.com.

Canon

CANON SOLUTIONS AMERICA

For more information, call or visit
1-800-815-4000 CSA.CANON.COM

Canon is a registered trademark of Canon Inc. in the United States and elsewhere.
All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged.
©2017 Canon Solutions America, Inc. All rights reserved.
11/17-415-1838