

Defending Your Business Infrastructure with Print Security

An IDC InfoBrief, Sponsored by Brother International Corporation | **August 2018**

By Keith Kmetz, Program Vice President, Imaging, Printing & Document Solutions

IDC ANALYZE THE FUTURE

Executive Summary

The evolution towards a 24/7 accessibility platform for business information has heightened the need for increased security diligence across all IT technologies.

Organizations are more susceptible to harmful breaches if steps to secure the IT environment are not taken. The average total monetary cost to the organization for an average security breach is over $815,000.

Security programs need to address the unique characteristics of print environments as an ongoing, mission-critical business information function. Print security includes addressing vulnerabilities at the device, data/document and network levels to achieve the desired results. There are several key security features already available to address these areas of vulnerability, but most organizations typically do not implement them.

Organizations desire a strong security plan, but face many substantial challenges in the process. These concerns can be addressed with the right set of solutions from their technology providers.

The security feature set for print technology has a strong influence on the buying decision. Nearly two-thirds of respondents to a recent IDC survey indicate that the security feature set has a high influence on the buying decision.

The benefits of implementing a robust print security plan are considerable and offer bottom-line impact. The most noted benefits of reducing print-related cost, as well as reducing/eliminating risk and gaining efficiencies by effectively managing print, can all be applied to the bottom line.

The average total monetary cost to the organization for an average security breach is over $815,000.

Market Education Needed: Closing the Security Gap in Printing

Cloud, mobile, and other advanced computing technologies are driving "anytime, anywhere" access to business information. Some of this content could be particularly sensitive or even harmful if it falls into the wrong hands. Such a scenario has heightened the need for overall IT security, but what about unique technologies like print?

An effective overall IT security strategy requires continued diligence—you are as vulnerable as your weakest point. Certain document-intensive industries have market-specific regulatory compliance standards that mandate certain levels of security regarding how information is accessed, distributed, and managed—e.g., HIPAA in healthcare, Sarbanes-Oxley in financial, FERPA in education.

The consequences of a breach can be substantial and not just limited to financial penalties or fines, but can have longer-lasting negative impact (e.g., costs to correct the breach, harm to the organization's reputation). Security can help an organization run more cost-effectively and enhance IT productivity.

All of the above has heightened the need for overall IT security, but what about unique technologies like print? Print has unique characteristics that need specific attention in order to maximize overall IT security across the organization, as this technology is involved in paper-based processes (printing, copying, faxing) as well as electronic-based processes (scanning to various digital repositories).

Security can help an organization run more cost-effectively and enhance IT productivity.

Printer and MFP Document Functionality Is Used Extensively as Part of a Business' Core Operations

Printing, copying, faxing and scanning are fundamental to the document processing requirements across business of all sizes. IDC estimates that over 1 trillion pages are printed in the U.S. every year.

Printers and multifunction printers (MFPs) of all types are used throughout companies, from personal, desktop devices to networked, workgroup and departmental devices. Printer functionality is used extensively throughout a business's operations—in many different types of environments and for various applications.

It's a daunting task to manage and ensure security with all the necessary printing, copying, faxing and scanning taking place within a company. Companies need to partner with technology providers that can expertly assist in the management of these essential and highly-used, mission-critical functions for a business' success.

IDC estimates that over 1 trillion pages are printed in the U.S. every year.

What Is Print Security?

DEVICE-LEVEL

- A print device is a system. It has a display screen or user interface, memory, hard drive, communication ports, and network ports. Thus, there are many attractive points-of-access available that could come under attack.
- Steps should be taken to ensure authorization/authentication of users to print equipment. Organizations do this for employees' personal technology devices (PCs, phones, tablets), but not always with personal or departmental printing devices. They should.
- The breach potential for print is huge with so many entry points, and a successful attack only needs one small hole, like a mouse in the house. Once malware is in, it's hard to get rid of.

What Is Print Security?

DOCUMENT-LEVEL

- Documents and the information in them are susceptible to security breaches in the following ways:
  - Prints/copies/faxes left in a tray for undetermined time with sensitive information
  - Interception of unencrypted documents in motion (scans, faxes)
- Access to specialty media used for unique applications in markets such as printing checks in banks or prescription media in hospitals or clinics.
- Should all staff have access to such media?

Source: Brother, 2018

What Is Print Security?

NETWORK-LEVEL

- Ensure that all citizens of the network are equipped and familiar with security tools and processes specific to print technology.
- Print includes both digital and paper business processes. As a result, single-function and multifunction printers (MFPs) are hubs for considerable document activity—not just printing and copying, but a wide range of document traffic that must be monitored and secured.
- Should all staff have carte blanche access to all device features, such as the ability to scan and fax certain information outside the organization?

Source: Brother, 2018

Quantifying the Cost of a Breach

One breach is one too many

IN A RECENT IDC SURVEY:

24% of all respondents indicated that their company had a significant IT security breach in the last 12 months that required remediation.

Average total monetary cost to the organization was over $815,000.

Over 16% of these breaches involved print.

Top Security Concerns—Print Is Prominent

79% of companies surveyed by IDC say that print security is very important to them.

TOP 3 CONCERNS:

65%
Phishing attacks to trick employees into providing information that could compromise security

58%
Poor/weak passwords used by employees

55%
Printing, scanning, copying and faxing of inappropriate documents

Security Drives Buying Decisions

It is essential to work with providers who offer a robust set of print security features

67% of companies say print security spending priority is high.

Only 10% say it's a low priority.

34% of respondents anticipate print security spending will increase in the next 12 months.

Less than 2% indicate a decrease in print security spending.

However, only 52% of RFPs include language for print security.

Over 43% of RFPs do not include language for print security.

66% of respondents say security features have a high influence on the acquisition of printers, copiers, and MFPs.

Bottom-Line Impact of Print Security

Print security initiatives not only help the organization run more securely, but also offer bottom-line cost and operational efficiencies.

TOP 5 BENEFITS

35%
Reduce print-related costs.

34%
Reduce/mitigate the risk of a security breach.

31%
Efficiencies gained by more effectively managing print equipment.

29%
Extend organizational security practices to documents that are printed/scanned/faxed/copied at employee homes, customer/partner locations and hot spots.

28%
Reduce help desk inquiries on print equipment

Why Aren't More Companies Addressing Print Security Needs?

Some companies are making the mistake of not specifically addressing the unique characteristics of securing their print infrastructure. Why...

TOP 3 RESPONSES TO WHY PRINT SECURITY NEEDS GO UNMET:

44%
don't see the need for a printer security policy.

44%
think their printers are safe behind the network firewall.

37%
think security risks associated with printers are too small to justify the cost to fix.

Why Print Security Is Imperative

Each assumption on the prior page shows faulty logic. Here are the facts:

There is a need for a printer security policy due to the unique characteristics of the technology's involvement in all document processing (paper and digital) taking place in organizations.

Being behind a firewall does NOT ensure security. Attackers love to hear this kind of attitude, as it makes the breach much easier to achieve with this false sense of security in place.

For a fraction of the cost of a breach, investing in security will lessen the chance of an occurrence.

While no security program can be completely foolproof, having a comprehensive plan that includes print will help to keep incidents at a minimum and lower their severity.

Top 10 Most Important Security Features

...But often neglected in print environments

These security features are rated by companies as "highly important," but then actual usage or awareness of them is dangerously low.

Security Feature	Highly Important (%)	Actual Usage (%)
Device malware protection	68%	30%
Security policies and governance involving installation, configuration & usage	67%	28%
Administrative passwords	66%	27%
User authentication	66%	29%
Bios, operating system and firmware updates	66%	26%
Security policies and governance involving remote usage & mobile printing	64%	25%
Securing the device hard drive and removable storage media	62%	23%
Secured device ports (e.g., network connections, fax lines)	62%	26%
Automatic logoff for printers/copiers/MFPs after a set period of inactivity	61%	25%
Device management and discovery tools	61%	24%

Essential Guidance

- Recognize that an organization's IT infrastructure is susceptible to attack and the consequences can be severe. Take measures to lessen the incidence and severity of attacks and possible breaches.
- Understand that no security plan is 100% foolproof, but the implementation of a comprehensive IT and print security program will allow organizations to quickly recognize security threats and incidents.
- More importantly, the program will enable companies with a security program to respond quickly, rectify the situation, and thus minimize the impact of a security breach.
- Prepare for challenges around time and effort to implement, as well as getting executive buy-in.
- Work with suppliers who can act on your organization's security initiatives and provide products and services that align with the plan's goals
- Implement an end-of-life plan for printers and MFPs that will be replaced in the organization, so that any resident data in these machines is appropriately addressed.
- Ensure that all new devices installed are covered under the security plan.

Questions to Answer

What is the liability your business would have if customer data/information were compromised?

What is your biggest security concern? How are you addressing it?

What types of data does your organization create, store, and transmit?

How secure is your data input and output infrastructure?

How does your organization protect its confidential and proprietary information? How do you secure your company's most sensitive data?

Source: Brother, 2018

A Message from Brother

Security and compliance remain top priorities for Brother

To address the common print security threats businesses are facing today, the Brother Workhorse Series of mono and color laser printers, MFPs and scanners offer a number of advanced security features typically found in higher priced models – right out of the box.

These built-in security features help protect against print security threats and maintain compliance by:

- Controlling who has access to the device
- Protecting print and scan data
- Securing the device on the network

Brother's business-class products offer three lines of defense – one at every critical level:

Network Security: Eliminate outside threats while supporting the latest protocols and enabling device sharing

Device Security: Limit device access at the group, individual and activity level

» **No internal hard drive:** Many enterprise-level network printers use internal hard drives to store and prioritize print jobs – Brother products do not. This eliminates the risk of sensitive documents remaining on the printer's hard drive when the device is discarded

Document Security: Enable users to protect sensitive or confidential data sent over networks

Visit https://www.brother-usa.com/solutions/device-management-security for more information on Brother's security offerings.