IDC
Analyze the Future

I D C M A R K E T S P O T L I G H T

Securing the Print Infrastructure is Critical to Digital Transformation

December 2016

By Robert Palmer, IDC Research Director, Imaging, Printing, and Document Solutions

Sponsored by HP Inc.

An organization's IT security plan is an obvious high priority to ensure appropriate protection and response to potential threats and breaches. Print security needs to be a part of this plan, especially in the age of 3rd Platform computing (mobility, cloud, big data, and social). Part of any comprehensive plan to address the security of the organization's print environment should thus include solutions and services to address both device and data security. This paper examines the importance of securing the print and document infrastructure and the role that managed print services can play in achieving this goal.

Introduction

Issues related to security and data privacy have consistently ranked at the top of the list for CIOs and IT managers for well over a decade. IDC's own research shows that security has now become a top priority for a majority of businesses, ranking only slightly behind another key business initiative: digital transformation. While both are viewed as key business differentiators, it is important to understand how digital transformation and security are intimately linked.

Organizations face a broad range of threats when it comes to securing their IT infrastructure. Most tech-savvy organizations have made security a top priority by focusing on issues such as protecting the network from outside attacks, securing network devices, managing access to connected devices, and preventing the disclosure of confidential data.

On the surface, it is easy to see how all of these issues revolve around the need to protect the organization’s most valued assets: business information and client data. Businesses are spending billions of dollars on document management and Enterprise Content Management (ECM) software, making significant investments in systems to gain control over business-critical content. Compounding the challenge is the continued drive toward mobility and cloud computing. Today's knowledge worker demands 24/7 access to information, which means that content must move freely from both inside and outside the corporate firewall.

Interestingly, an organization’s print and document infrastructure is uniquely positioned right at the intersection of digital transformation and IT security. Nevertheless, most businesses fail to recognize the security vulnerabilities associated with their existing print and document environment. At the heart of this issue is the role of the smart MFP, which has become an intelligent business processing hub that serves as an on- and off-ramp to business information, whether it is stored in the device, on the corporate network, on paper, or in the cloud.

An Unseen and Unmanaged Threat

The connected MFP is a potential security risk as an unmanaged connected device. However, the MFP can also be leveraged as a front-line asset for securing network access, managing data security, and protecting access to information.

According to research from IDC's *User Perspectives on Print Security, 2015*, more than 30% of organizations have no security policies in place for managing access to and controlling usage rights for printers and MFPs located on the network. At the same time, over half of respondents surveyed indicate a high level of concern regarding the unauthorized use of copiers or MFPs.

There are similar inconsistencies when it comes to how businesses view their current IT security practices. According to IDC's *MaturityScape Benchmark: Print Security in the United States, 2016,* more than 70% of respondents say that print security has a high level of influence on the printers and MFPs that they buy or lease. Surprisingly, however, the number of respondents indicating that print security was "very important" was 26%, or fewer than those concerned with overall IT security.

Many security and IT managers have assumed that systems put in place to protect the network would extend to other connected peripherals. But security around the network perimeter is crumbling, and every device connected to the network is now an endpoint security risk—printers and MFPs included.

The threat is real, with potential security breaches due either to malicious attacks using a network printer or MFP as an entry point, or unintentional yet careless use of devices by employees. The print environment is unique because it is leveraged specifically to manage data, documents, and information in both digital and paper format, so business-critical content is exposed and vulnerable in a variety of ways. Neglecting to secure the print environment as part of an overall IT strategy leaves an organization as vulnerable as if it were taking no IT security action at all.

The end result of a security breach to the print and document infrastructure is the same as that of any other security lapse: extensive costs related to downtime to identify and fix a security breach, fines associated with corporate governance and regulatory compliance, lost customers, or other harmful damage done to the company's reputation.

Secure Print Services

The challenges associated with print and document security are easily identified, but developing a secure print strategy has proven difficult for many businesses. One problem relates to the various stakeholders within the organization. Device security tends to reside within the IT function, and typically includes the IT department, security manager, helpdesk, endpoint security, and network security. In addition, any discussion regarding security of printers and MFPs often involves facilities management.

Content security, on the other hand, is often viewed in conjunction with issues around regulatory compliance, and stakeholders tend to reside in corporate risk and governance. Representatives from ERP applications, database clusters, content management, and other line of business (LOB) managers can also be involved. More often than not, security for content and printers is handled separately, which leads to a lack of integration and increased vulnerability gaps. At the same time, businesses are often unaware of the various secure printing solutions and professional services that are available in the market.

This is an area where managed print services (MPS) could play an important role in advancing print and document security. While many businesses have contracted with an MPS provider to optimize their print infrastructure to drive efficiencies and reduce output costs, print and content security have gone largely overlooked in most contractual print services engagements. Today, some MPS providers have the capacity, tools, and resources to help businesses identify and prioritize current

security threats. Part of this process could include an upfront security assessment, which is vital to identifying gaps in current device and content infrastructure. Businesses can then work in partnership with the service provider to develop and deploy secure managed print services to address current vulnerabilities, harden the document infrastructure, and mitigate future security risks.

The MPS provider is also uniquely adept at gathering together various stakeholders to deliver contractual print services across departments and lines of business, which is crucial to deploying a holistic approach to device and content security. This approach is also beneficial to developing a security plan that extends with the organization's own digital transformation strategy. Secure print services can range from base-level security for safeguarding the equipment and data, to more advanced measures that are considerably more complex in their implementation and offer a higher level of device security and content protection.

Conclusion: From Reactive to Proactive

The bottom line is that the print and document infrastructure has not received the level of attention given to other threats in network and cyber security. Breaches create fear and uncertainty and the impact to operational costs, job performance, and company reputation can be severe.

Organizations must take proactive steps to address security concerns in the print and document infrastructure, and the MPS provider should be viewed as an important partner in this endeavor. When seeking out print services providers, consider those that demonstrate core competencies in threat level assessment and remediation capabilities.

In addition, choose partners with hardware and solutions built around a security ecosystem to address the following vulnerabilities in the document infrastructure:

- User authentication and authorization
- Device management
- Device malware protection
- Firmware updates and password management
- Content security, privacy, and data integrity
- Capabilities to address the human element involved in the installation, configuration, and usage of equipment

MPS solutions should also be designed to integrate with third-party document management and ECM systems to provide further protection and to aid with governance and regulatory compliance requirements.

By taking a holistic approach, businesses can begin to shore up vulnerability gaps and harden protection in the print and document environment, which is likely to be your organization's weakest security link.

ABOUT THIS PUBLICATION

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.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 **www.idc.com**

4AA7-0385EEW