The Insecurity of Network-Connected Printers: Executive Summary

Sponsored by HP

Independently conducted by Ponemon Institute LLC

Publication Date: September 2015

The Insecurity of Network-Connected Printers

Executive Summary

Ponemon Institute, September 2015

We are pleased to present the results of our study, *The Insecurity of Network-Connected Printers,* sponsored by HP. The purpose of the research is to highlight the security risks created by insecure printers and other peripheral devices. The intention is to focus on action strategies and best practices in addressing end-point device security.

We surveyed more than 2,000 IT security practitioners in North America, EMEA, Asia-Pac and Latin America. The combined global findings are presented in this executive summary.

To ensure a quality response, we confirmed that all respondents are familiar with their organizations' approaches to securing data and have responsibility for safeguarding sensitive or confidential information. Sixty-five percent of respondents say the format of information safeguarded is mostly digital and 22 percent say it is a combination of both hardcopy and digital. Only 13 percent of respondents say they mostly secure printed information.

Key findings

Following are the most salient findings of this research organized according to the following three topics:

- People issues and printer insecurity
- Process problems and the lack of governance
- Technology challenges

People issues and printer insecurity

Lack of employee awareness creates an insider threat. A significant risk exists because 56 percent of respondents believe employees in their organizations do not see printers as an area of high security risk. This could lead to negligence when using printers and other peripheral devices that contain sensitive and confidential information.

Executive management, sales and human resources present the highest risk. Only 30 percent of respondents say their organization has a process for identifying high-risk printers. However, respondents can identify the departments or functions where the greatest printer security measures should be applied.

Based on the type of data generated and/or printed, executive management (65 percent of respondents), sales (63 percent of respondents) and human resources (57 percent) are seen areas of greatest risk in the workplace. Sales (93 percent of respondents) and human resources (76 percent of respondents) are also vulnerable to a possible data breach because these departments are most often considered to have poor printer-related security practices and lax access controls.

Process problems and lack of governance

Printer security is an overlooked security risk. Only 44 percent of respondents say their organizations' security policy includes the security of network-connected printers. Instead, 64 percent of respondents say their organization assigns a higher data risk to desktop or laptop computers than printers. As a result, most (62 percent of respondents) are pessimistic about their ability to prevent the loss of data contained in printer memory and/or printed hardcopy documents. These printers are vulnerable to unauthorized access through WiFi and open ports.

Current steps to secure printers are ineffective. Enforcing policies, training employees and office shredders in office areas are the main steps taken to secure printers and hardcopy documents (49 percent of respondents, 46 percent of respondents and 39 percent of respondents, respectively).

Why are these steps ineffective? First, the majority of respondents say their companies do not have security policies that include network-connected printers or do not know (55 percent of respondents). Second, current training programs may not be making a difference because 56 percent of respondents say employees in their organizations are not aware about the security risks associated with printers. This lack of awareness may also affect the use of shredders to dispose of sensitive and confidential information.

Organizations admit they are not succeeding at governing the use and security of printers. Only 38 percent of respondents believe information contained in printer memory is thoroughly wiped clean during the disposal or refurbishment process.

Moreover, the following tasks are not often performed well: integration of printer access and use with network intelligence and/or SIEM solution (77 percent of respondents), establish and enforce printer security policies that are consistently applied across the enterprise (66 percent of respondents), encrypt data at rest stored within printer memory and/or hard drives (63 percent of respondents), encrypt data in motion across the organization's fleet of printers (62 percent of respondents) and assign access rights to printers based on the sensitivity of document printed (56 percent of respondents).

Stopping unauthorized access to network-connected printers is often ignored. Only 34 percent of respondents say their organization has a process for restricting access to high-risk printers, including printed hardcopy documents. As a consequence, an average of 44 percent of network-connected printers within their organizations are insecure in terms of unauthorized access to data stored in printer memory and an average of 55 percent are insecure in terms of unauthorized access to printed hardcopy documents.

Technology challenges

A data-breach involving a network-connected printer has likely occurred in the organizations represented in this research. While companies may be ignoring the risk, 60 percent of respondents acknowledge that such a data breach has occurred with certainty (10 percent), very likely (24 percent), or likely (26 percent). Only 24 percent of respondents say that a data breach involving a network-connected printer did not happen. Sixty-seven percent of respondents say a data breach involving a desktop or laptop has occurred with certainty (35 percent of respondents), very likely (23 percent of respondents) or likely (9 percent of respondents).

Most respondents predict a data breach resulting from insecure network-connected printers in the next 12 months. Fifty-seven of respondents believe such a data breach will occur and 51 percent of respondents predict a data breach involving insecure desktop or laptop computers. The risk is expected to increase for both because of the expanded use of mobile technologies (65 percent of respondents), the increased rate of malware infection (61 percent of respondents), an increase in the number of remote workers (60 percent of respondents) and more network-connected devices (53 percent of respondents).

Technologies that help pinpoint high-risk printers, such as those containing malware, are critical, according to 70 percent of respondents. Sixty percent of respondents say printers and desktop or laptop computers are equally likely to be infected with malware (50 percent of respondents) or more likely than desktop or laptop computers to be infected (10 percent of

respondents). In other Ponemon Institute research it was revealed that 56 percent of companies ignore printers in their endpoint security strategy.[1]

Other critical success factors include monitoring of devices and users (64 percent of respondents), technologies that encrypt sensitive or confidential documents contained in printers (55 percent of respondents), technologies that restrict access to documents contained in printer memory (52 percent of respondents) and strict enforcement of non-compliance (50 percent of respondents).

The number one feature most important to the security of network-connected printers is the ability to spot anomalies in any given device within the fleet of printers, according to 88 percent of respondents. A list of seven features of enabling technologies for printer security were all rated as very important by the majority of respondents.

The ability to pinpoint anomalies is followed by the ability to manage security protocols for the entire fleet of printers from one centralized console (84 percent of respondents), the ability to set and monitor policies for the entire fleet of printers (73 percent of respondents), ability to configure printers to be compliant with specific corporate security policies (71 percent of respondents), ability to enable encrypted communication among devices across the fleet of printers (68 percent of respondents), ability to determine printers that are added to or removed from the network (65 percent of respondents) and ability to install and manage digital certificates across the fleet of printers (59 percent of respondents).

Conclusion

Printers are an integral and ubiquitous part of the workplace. However, as shown in this research, many companies are ignoring the security risks associated with printers and other peripheral devices. In other Ponemon Institute research, 53 percent of IT managers realize printers are vulnerable to cyber crime.[2] According to the *2014 Global Report on the Cost of Cyber Crime*, the average cost to resolve a cyber attack is $7.6 million.[3] Following are some recommendations for reducing the threat:

- Security policies and practices should include safeguards to prevent the loss of confidential and sensitive data.
- Training and awareness programs should address the appropriate handling of sensitive and confidential information when using network-connected printers and peripheral devices.
- An assessment should be conducted to determine the departments and functions that pose the greatest security risks because of the types of information generated and/or printed. In those areas, printer-related security practices and access controls should be strengthened.
- Technology solutions that would improve the ability to secure printers across the enterprise and assign access rights to printers based on the sensitivity of documents printed should be part of an overall strategy to improve printer security.

[1] Ponemon Institute, Annual Global IT Security Benchmark Tracking Study," March 2015
[2] Ibid
[3] Ponemon Institute "2014 Global Report on the Cost of Cyber Crime," sponsored by Hewlett Packard Enterprise, October 2014

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**,we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.