ABERDEEN
STRATEGY & RESEARCH
ILLUMINATE. INSPIRE. IGNITE.

PRINT SECURITY: SEEING (AND MANAGING) YOUR MULTI-FUNCTION PRINTERS AS FULL-FLEDGED ENDPOINTS ON YOUR NETWORK

In Collaboration with SHARP

KB

PRINT SECURITY: SEEING (AND MANAGING) YOUR MULTI-FUNCTION PRINTERS AS FULL-FLEDGED ENDPOINTS ON YOUR NETWORK

July 2023

Derek E. Brink, CISSP
Vice President and Research Fellow, Cybersecurity and IT GRC

ABERDEEN
STRATEGY & RESEARCH
ILLUMINATE. INSPIRE. IGNITE.

Executive Summary

For a majority of smaller organizations (<=250 employees), **Print Security** is widely perceived as an integral part of their leading cybersecurity strategies. Given that most have already made *endpoint security* a priority, they should expand their thinking about seeing and managing "endpoints" to include their *multi-function printers* (MFPs).

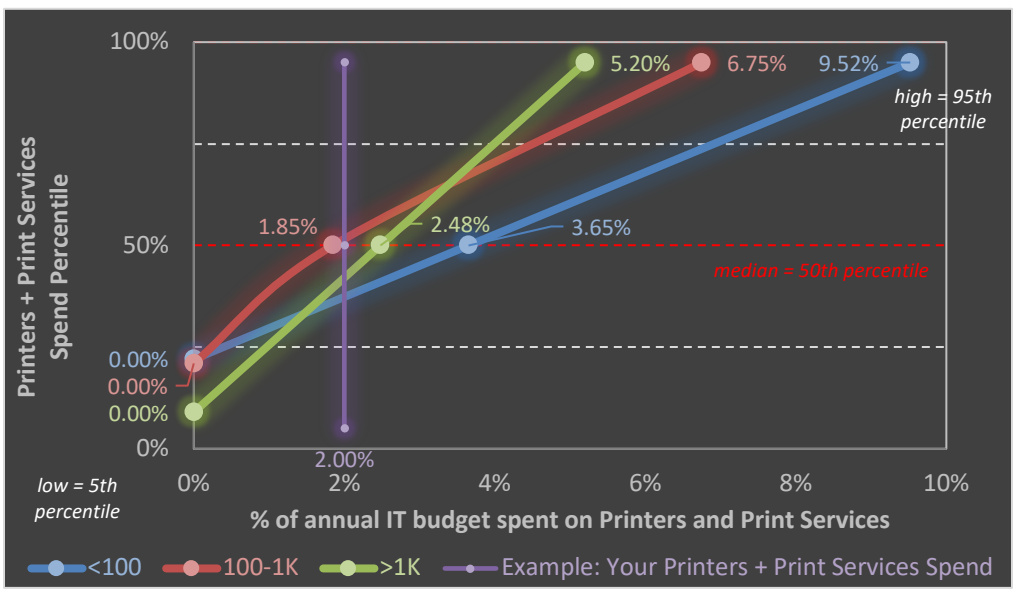
Spending on printers and print services, as a % of annual IT budgets — how does your company compare?

The Spiceworks *2022 State of IT* report provides valuable insights into the **percentage of IT budgets that are spent on printers** and **print services**. Aberdeen recently added to this dataset with a more sharply focused study on **Print Security** among smaller organizations (<=250 employees).

For example, Aberdeen's research shows that based on their total number of employees, smaller organizations are spending a higher median percentage of their IT budgets on printers and print services — and across a wider range as well, as shown in Figure 1:

- <100 employees: **0% to 9.52% (median: 3.65%)**
- 100 to 1,000 employees: **0% to 6.75% (median: 1.85%)**
- >1,000 employees: **0% to 5.20% (median: 2.48%)**

Figure 1: Based on the number of employees, a median of 1.85% to 3.65% of annual IT budgets are spent on printers and print services.



Source: Aberdeen, July 2023

How does your organization compare?

As an illustrative example — if your organization is spending *2%* of its annual IT budget on printers and print services, this translates to the *37th percentile* if you have less than 100 employees, the *52nd percentile* if you have between 100 and 1,000 employees, and the *42nd percentile* if you have more than 1,000 employees.

If you're interested in taking a quick interactive assessment to see how your organization compares, visit the *Printers and Print Services widget*.

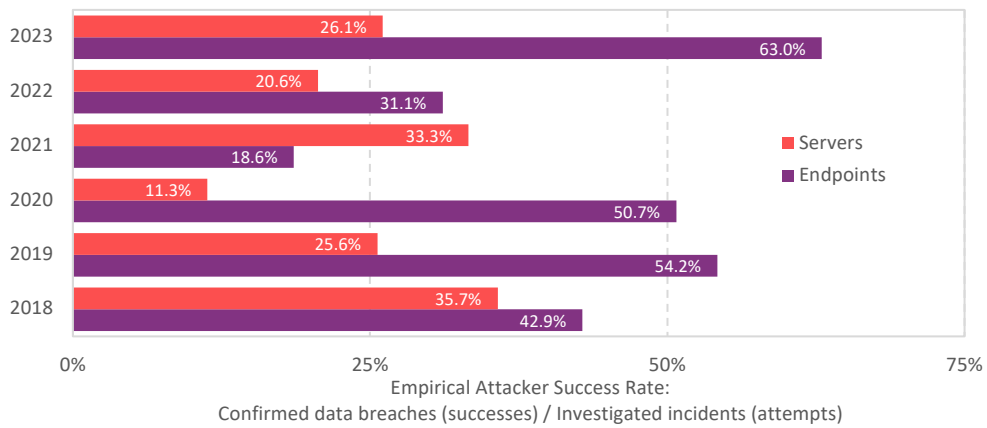
These findings suggest that larger organizations have the resources and scale to invest in printing and print services (and presumably in Print Security) in a more predictable way than smaller organizations do. That is, to the extent that there is always a "hierarchy of needs" to be met with finite IT budgets, smaller organizations are actually investing more — on a percentage basis — of their available resources to meet the basic printer and print services needs of their employees. However, this also leaves fewer resources available for investing in higher-level business objectives, such as addressing print-related cybersecurity risks.

How big are your print-related cybersecurity risks?

For several years, the annual Verizon *Data Breach Investigation Report* (DBIR) has provided fact-based insights into the likelihood of successful data breaches by asset type. Aberdeen's analysis shows that the empirical success rate for attackers — i.e., *confirmed data breaches* (successes) *as a percentage of investigated incidents* (attempts) — is as much as 4.5-times higher for **endpoints** than it is for **servers** (see Figure 2).

Given that most organizations of all sizes have already made **endpoint security** a priority, this simply means that they should expand their thinking about "endpoints" to include printers and print services. Modern **multi-function printers (MFPs)** — which routinely receive, store, send, and print your business-critical documents — are in fact full-fledged endpoints on your organization's network, with all of the usual categories for endpoint-related **security vulnerabilities and exploits** (*including network, platform, OS, applications, identities, and data*) to be monitored and managed.

Figure 2: Analysis of confirmed data breaches by asset type shows that attackers have had a much higher success rate on *endpoints* than on *servers*.



Source: Empirical data adapted from Verizon DBIR 2018 (N = 4,020 incidents; 1,530 breaches), DBIR 2019 (N = 3,667 incidents; 1,068 breaches), DBIR 2020 (N = 16,242 incidents; 2,314 breaches); DBIR 2021 (7,391 incidents; 2,284 breaches); DBIR 2022 (13,399 incidents, 2,916 breaches); DBIR 2023 (8,443 incidents, 2,382 breaches); Aberdeen, July 2023

Seeing (and managing) your multi-function printers (MFPs) as full-fledged endpoints on your organization's network

As an illustrative example — MFPs that are seen by Active Directory as merely "printers" offer very little in terms of group policy management.

In contrast, MFPs that can be seen and managed within Active Directory as end-user devices (like any PC) can significantly reduce the frequency dimension of print-related security risks.

Aberdeen's recent research underscores that investments in broader cybersecurity strategies are driven primarily by **risk** (i.e., **cost avoidance**). Among the top five drivers for current investments, three were related to the **frequency** aspect of risk (increasingly sophisticated *cyber threats*, increasingly *cloud-based applications and data*, and an increasingly *remote / hybrid workforce*) — and two were related to the **business impact** side of risk (*compliance requirements*, and *valuable / sensitive / regulated data)*.

From a traditional technical point of view, a strong focus on reducing risk (both *frequency*, and *impact*) makes perfect sense. Over the previous year:

- More than **1 in 5 (21%)** respondents experienced one or more **data breaches**
- About **1 in 3 (32%)** respondents experienced one or more security-related incidents that resulted in **unplanned downtime**
- More than **1 in 7 (15%)** of respondents experienced one or more material **non-compliance issues**

From a traditional technical point of view, a strong focus on **reducing risk** (both *frequency*, and *impact)* makes perfect sense. Over the previous 12 months:

- More than **1 in 5 (21%)** respondents in Aberdeen's study experienced one or more **data breaches**
- About *1 in 3 (32%)* respondents experienced one or more security-related incidents that resulted in **unplanned downtime**
- More than **1 in 7 (15%)** of respondents experienced one or more material **non-compliance issues**

What are the current perceptions of Print Security, in the context of your broader cybersecurity initiatives?

Aberdeen's research found that for a majority of smaller organizations (<=250 employees), Print Security is widely perceived as an integral part of their leading cybersecurity strategies — but *funding* for Print Security is generally lagging these perceptions. Perception and funding are strongly correlated: The more strongly Print Security is perceived as integral to broader cybersecurity strategies, the more likely it is to be funded (see Figure 3).

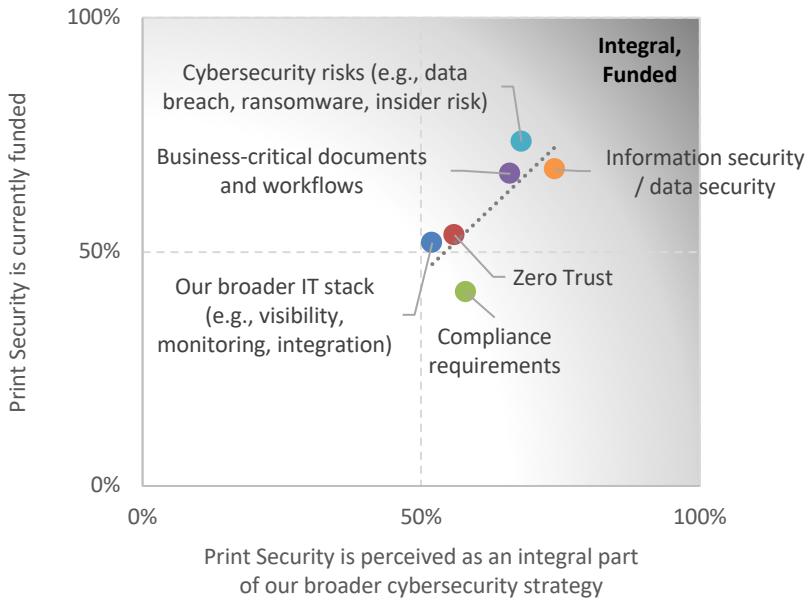
Cybersecurity strategies that drive the most funding for Print Security include:

- Information security / data security
- Cybersecurity risks (e.g., data breach, ransomware, insider risk)
- Business-critical documents and workflows

Cybersecurity strategies where funding for Print Security is most lagging:

- Zero Trust
- Compliance requirements
- Integration with the broader IT stack (e.g., visibility, monitoring, integration)

Figure 3: Print Security is widely perceived as an integral part of leading cybersecurity strategies — but *funding* for it is generally lagging.



Source: Aberdeen, July 2023

Aberdeen also asked smaller organizations about their current interest / priority for about a dozen selected Print Security capabilities. Several of the highest-ranked capabilities look a lot like simply wanting to know "what's going on" with respect to cybersecurity for printers and print services, e.g.:

- **Network security** (e.g., *monitoring*, *intrusion detection*)
- **Management of user credentials** (e.g., *passwords*, *other*) used to gain access to MFPs and print services
- **Protection of the MFP platform** (e.g., *TPM-based protection* against firmware attacks, *secure credential stores*, *secure boot*, *software validation*)
- **Data protection for digital documents sent to MFPs** (e.g., *authenticated users*, *encrypted storage*)

From an operational perspective, the very natural desire to know "what's going on" can be addressed by a couple of high-level approaches — e.g., by **integrating printing-related logs and events with other sources and feeds** (e.g., in an existing SIEM), or by **using managed monitoring, detection, and response for MFPs** (e.g., from a third-party service provider). These were commonly known as "Build vs. Buy," back in the day.

Of these two, the managed approach to these aspects of Print Security is ranked higher by the respondents in Aberdeen's study. This also makes

For the small businesses in Aberdeen's study, **the managed approach to the monitoring, detection, and response aspects of Print Security** (e.g., from a third-party service provider) is ranked higher than integrating printer-related logs and events with other sources and feeds (e.g., in an existing SIEM).

sense, given the resource constraints discussed above — which are typically manifested in terms of your IT budgets, the available bandwidth of your technical staff, or both.

Said another way: Given the practical financial realities, smaller organizations are increasingly *seeking the most cost-effective means* to obtain the Print Security capabilities they need, to *help them achieve the strategic ends* of data protection and risk reduction they want for printers and print services.

Summary and Key Takeaways

- Aberdeen's research shows that based on their total number of employees, **smaller organizations are spending a higher median percentage of their IT budgets on printers and print services** — and across a wider range.
- Empirically, the success rate for attackers — i.e., *confirmed data breaches* (successes) *as a % of investigated incidents* (attempts) — is as much as 4.5-times higher for **endpoints** than it is for **servers**. Given that most organizations have already made endpoint security a priority, this simply means that they should **expand their thinking about seeing and managing "endpoints" to include their multi-function printers and print services**.
- Investments in broader cybersecurity strategies are driven primarily by **risk**. Over the previous 12 months, more than **1 in 5 (21%)** respondents experienced one or more **data breaches; a**bout **1 in 3 (32%)** experienced one or more security-related incidents that resulted in **unplanned downtime**; and more than **1 in 7 (15%)** of respondents experienced one or more material **non-compliance issues.**
- For a majority of smaller organizations (<=250 employees), **Print Security is widely perceived as an integral part of their leading cybersecurity strategies** — but *funding* for Print Security is generally lagging these perceptions. The more strongly Print Security is perceived as integral to broader cybersecurity strategies, the more likely it is to be funded.
- For the smaller organizations in Aberdeen's study, **the managed approach to the monitoring, detection, and response aspects of Print Security (e.g., from a third-party service provider)** is ranked higher than integrating printer-related logs and events with other sources and feeds (e.g., in an existing SIEM).

Given that most organizations have already made endpoint security a priority, this simply means that they should expand their thinking about seeing and managing "endpoints" to include printers and print services. Modern multi-function printers (MFPs) are in fact full-fledged endpoints on your organization's network.

About Aberdeen Strategy & Research

Aberdeen Strategy & Research (a division of Spiceworks Ziff Davis), with over three decades of experience in independent, credible market research, helps **illuminate** market realities and inform business strategies. Our fact-based, unbiased, and outcome-centric research approach provides insights on technology, customer management, and business operations, to **inspire** critical thinking and **ignite** data-driven business actions.

18619