Why Securing Your Printers Matters for Government

Research Brief

Why Securing Your Printers Matters for Government

Imagine you walk into your agency Monday morning to find the place in utter chaos. You quickly learn that a cyberhacker has infiltrated your agency's IT systems and frozen every program and system. Access to financial systems: gone. Access to contract records: gone. Access to email: gone. Access to all of the documents and data that you need to complete your job: gone.

Essentially you've been locked out of your own agency's information systems from the inside out, taken hostage in your own backyard. And the only way to get access back? Either pay the hacker a large ransom fee, or dismantle all devices connected to the network and start from scratch.

This IT hostage situation sounds like a scene from a blockbuster film, but this was exactly what happened to Danish company Aalborg Paint and Varnish on Wednesday, January 21, 2015. All of the company's IT systems were paralyzed from an encryption ransomware that only the hacker had the password to. Aalborg employees lost access to their financial systems, customer records and mail systems for days, and had to continue business by writing everything down on paper. "There is no doubt that the situation was disastrous," said Pernille Skall, co-owner and sales and personnel manager at Aalborg Paint and Varnish.

With little help from the police or their insurance provider, the company took the only action they could: cut the wires to the old equipment. This allowed the company to purchase new devices and restore at least part of their IT environment from recent backups – something the hackers were not willing to promise even with payment of the ransom.

But how did the hacker even infiltrate their IT systems in the first place? Was it through a cloud platform? An insecure mobile device? Insider threat? No. The culprit was a network-connected label printer.

There is no question that technology is radically changing the environment we live in at an uncharted pace. In a world where new tech gadgets are deployed every day, it is easy to overlook the standard-feature technologies that still play a role in our lives. Case in point: the printer.

Today, the public sector is focused on optimizing its work for an increasingly digital world, but printers still play a major role in government work, and office life in general. The average U.S worker uses about 10,000 sheets of copy paper per year. More so, it's estimated that federal employees print on average 30 pages per day – 7,200 pages per employee, per year.

Government employees will continue to have a vast variety of printing needs. In a previous GovLoop community survey of more than 400 government respondents, 58 percent indicated that they need color printing at their agency on a regular basis. Nearly half (42 percent) said that they have high-volume printing needs of multiple and large documents, while an additional 27 percent said they need to be able to print in large paper formats. Two-thirds (67 percent) of those same respondents indicated that their ideal printer would have multifunctional capabilities, like copying, scanning and faxing in addition to printing.

Public-sector employees also utilize printers for confidential work and needs. Nearly two-thirds (64 percent) of respondents from a previous GovLoop survey indicated that they print confidential documents – like HR and financial records – to a shared or network-connected printer.

So with a platform that's so heavily utilized, and in a threat environment where cyberattacks are coming at the public sector from all sides, surely government places a priority on the cybersecurity of printers, right? Unfortunately, no. Despite using printers for classified document printing, respondents indicated that their agencies do not have stringent security policies in place to make sure these documents, and the printers, are safe. In fact, only 19.5 percent said their ideal printer would be properly secured, and 47 percent said they did not believe that printer security is an area of concern for their agency.

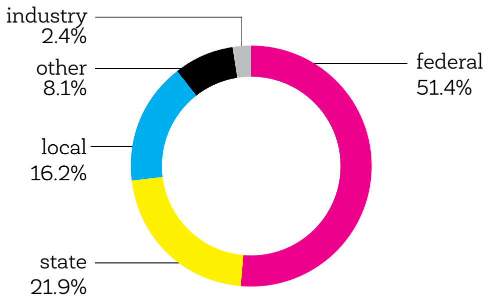
Though printers are still in such high demand, security remains lax. Only 38 percent of survey respondents indicated that their organization has a security policy regarding printers. Nineteen percent said their organization does not have a policy, and the other 43 percent were not sure.

Thus, even though printers are still widely utilized – even for confidential information – they are not properly secured throughout the public sector. There is such an intense focus on digital, mobile and cloud that oftentimes the security of end-point devices like the printer falls out of view. As we will discuss in this research brief, however, the printer should be included in your agency's overall security policy and compliance.

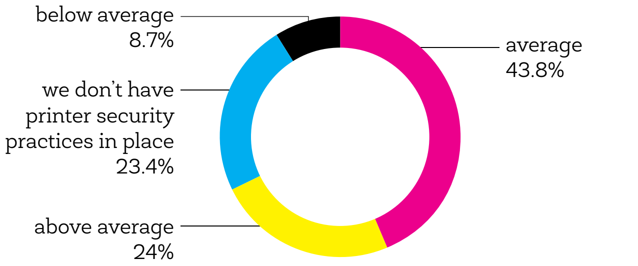
This research brief:

- **Reveals findings** from a GovLoop community survey of 365 public-sector respondents about their agencies' printer security practices and policies;
- **Shares insights** from HP Inc.'s Chief Security Advisor and Practice Manager Michael Howard about why securing your agency's network-connected printers is of utmost importance;
- **Explores why** printers are often left out of agency-wide security policies, and the risks of not securing printers;
- And **provides methods** for improving printer security at your agency.

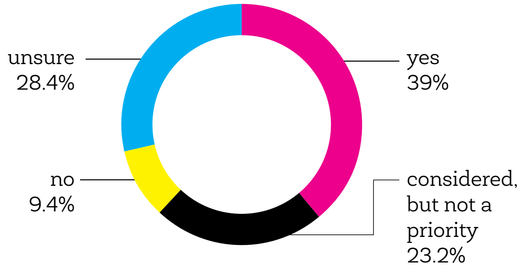
Which level of government do you work for?



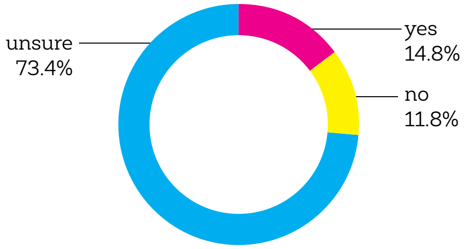
How would you describe your organization's printer security practices?



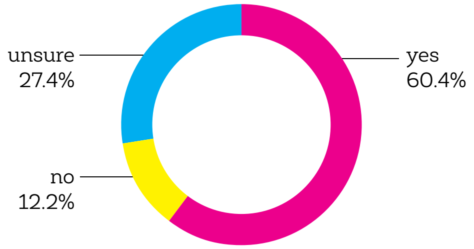
Does your organization consider security of printers and printer end points a priority?



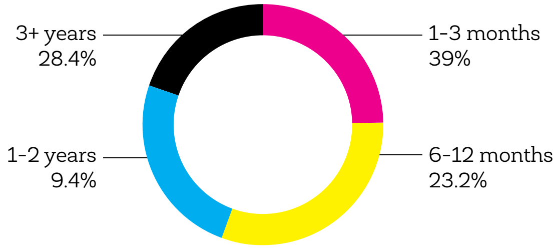
Is your organization considering updating its printer security policies & compliances?



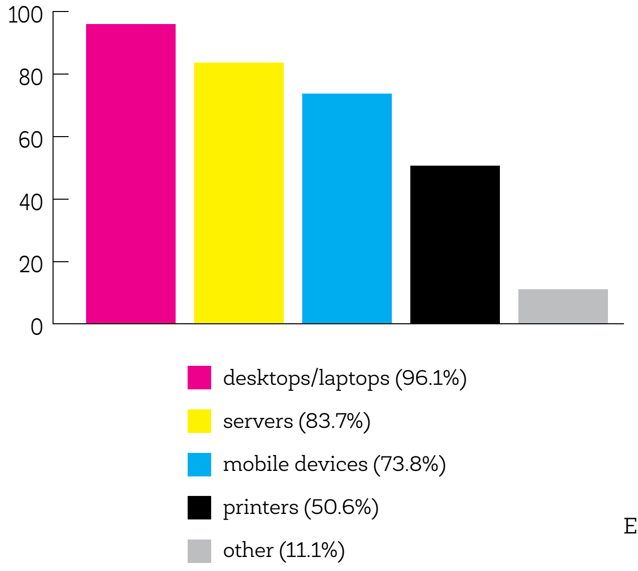
Does your organization assign a higher security risk to desktop or laptop computers than printers?



If yes, in what timeframe will those security policies be implemented?



For which of the following endpoints does your organization have IT security practices? Select all that apply.



Do you...

	YES	NO	UNSURE
Educate users about the safe and secure use of printers and control of documents?	41.9%	42.2%	16.4%
Assign access rights to printers based on the sensitivity of data printed?	33.1%	43.5%	23.7%
Deploy digital certificates and encryption when printing across network devices?	27.8%	34.9%	37.7%
Ensure data is encrypted on printer hard drives/mass storage?	28.5%	29.8%	42%
Have monitoring procedures to track the use and physical access to printers?	41.5%	27.7%	31.4%
Scan your printing infrastructure for vulnerabilities and remediate those vulnerabilities?	19.9%	29.3%	52%
Enable your printer logs and review periodically to check for anomalies or security incidents?	27.4%	28%	44.9%

The Printer: A Security Afterthought

It's clear that the printer is still a cornerstone machine for government. But with the prevalence of new devices and rapidly changing technologies, there is a critical aspect of printing needs, however, that tends to be ignored: security.

Michael Howard, Chief Security Advisor and Practice Manager at HP, said it is critical for agencies to consider all of the devices that are connected to their network when considering security policies and practices.

"With the rapidly growing Internet of Things and the changing way that security professionals are actually doing security today," he said, "it becomes really important that agencies take a look at everything that's touching their network, including printers. They also need to make sure that they have appropriate security policies touching it."

Printers, however, are not often included in security compliance plans with other devices. In the GovLoop community survey of 365 government employees, only 38 percent of respondents said that their organization considers printer security a priority.

Furthermore, only half of respondents from the survey stated that their organization has a security policy surrounding printers. The survey shows further evidence of the lack of security measures regarding printers:

- Only **one-third** (33 percent) of respondents indicated that they assign access rights to printers based on the sensitivity of data printed, while the other two-thirds are unsure or do not assign access rights at all.
- Just over **a quarter** (29 percent) of respondents ensure that data is encrypted on printer hard drives and other storage devices.
- Only **one out of five** respondents (20 percent) said that they scan their printer infrastructure for vulnerabilities in order to remediate security risks; similarly, only a quarter (26 percent) enable their printer logs to regularly check for hiccups and any security incidents.

Ponemon Institute – a private organization that conducts research on privacy, data protection and information security – recently worked with HP to look further into printer security throughout the public sector. The results of their survey of IT security practitioners from around the world is consistent with these findings.¬¬

In fact, Ponemon found that 65 percent of respondents indicated that their organization mostly only protects information in digital formats, disregarding printed documents and printer devices. Only 34 percent of respondents said that their organization has a process for restricting access to high-risk printers.

As a result of faulty security practices, respondents of Ponemon's survey estimate that roughly 44 percent of printers are insecure in terms of restricting access to high-risk devices, and 55 percent are insecure in terms of unauthorized access to hard copy documents.

Howard believes that printer insecurity is a result of the rapidly changing device technologies/capabilities and evolving cybercrime strategies such as Advanced Persistent Threats. It is insufficient that agencies are still using traditional ways of securing devices.

"Agencies are still looking back at the traditional way that we secure IT; we have network switches and computers, we have all of those things that we generally lock down, but printers were something that just didn't need to be secured. Now it's a matter of catching up, where people have to understand that everything out there is at risk."

> "Agencies are still looking back at the traditional way that we secure IT; we have network switches and computers, we have all of those things that we generally lock down, but printers were something that just didn't need to be secured. Now it's a matter of catching up, where people have to understand that everything out there is at risk."
>
> Michael Howard
> Chief Security Advisor & Practice Manager, HP

Challenges to and Misconceptions About Printer Security

Not many organizations have stringent printing policies, and most do not see much reason to change that. In fact, only **15 percent** of GovLoop survey respondents indicated that their organization plans on updating their printer security policies and compliances.

The main reason that many agencies don't have strong measures for securing their printers? There is a gaping lack of education surrounding printers, as well as a number of misconceptions that lead public-sector employees to believe that they do not need to enhance their printer security practices and policies.

1 **The first misconception is that the printer is a "dumb" device and doesn't need the same level of treatment as a desktop or PC.** In fact, six out of 10 respondents indicated that their organization assigns a higher security risk to desktop and laptop computers than printers. Additionally, when asked which devices or endpoints for which their organization has IT security practices, nearly all (96 percent) respondents said desktops and laptops, and 82 percent said servers. Printers ranked last out of this list, with only 49 percent of respondents saying their agency has a printer security practice.

But the reality is that the printer is, in fact, a computer itself. Though often thought to be simple devices that merely sit on desks, printers today have similar computing technologies as an average laptop or desktop computer.

"What has changed over the years is these devices have become much more sophisticated," Howard said. "They truly are a computer that you're putting on your network today."

Thus, printers should be treated with the same amount of security as these other devices.

This advance in computing power also means, unfortunately, that they can be hacked just like a computer. As already mentioned, a Danish company was recently hacked via one of its label printers. The hacker then put ransomware on the data, which encrypted the data and forced the company to pay a ransom in order to get its information and access to its environment back from the intruder – essentially locking the company out from the inside.

"What we're seeing is that attacks are becoming much more vicious, and they're becoming much more costly to organizations," Howard said. "So having those security procedures in place and locking those devices down becomes much more critical."

2 **Another misconception is that if the organization's other devices – like desktop computers – are behind a firewall, then printers are protected, too.**

"I think we have a false sense of security in most organizations where we think that we're protected because we're behind the firewall, or that if we have VPNs running, that we're encrypting data. And the reality is, in most organizations, the security teams don't have time to reach out and look at every aspect of what's going on," said Howard.

Assuming that printers are protected is like leaving an open window for hackers to come right in and take sensitive data. Better security around printers is especially critical since many government employees print sensitive data. Thus, the printer can be a direct path to an organization's critical records and private data if left unchecked. Unfortunately, it's not just a question of "if" but "when" an attack will occur if agencies don't beef up their printer security.

3 **A third misconception is that security is just about technological security solutions.** Printer security is not only about the technology, however, it's also about the people. For example, 42 percent of GovLoop respondents indicated that their organization doesn't educate users about the safe and secure use of printers and control of documents.

Consider the fact that a majority of government employees is in fact printing confidential documents from shared printers, and this becomes a real problem. Many of these documents may be left to sit on the printer for hours – or maybe even indefinitely – out there for anyone who walks by to snatch them up. Also, employees are likely not aware of password-protection capabilities available on printers and how to effectively utilize these features.

Public agencies need to keep their employees in mind when developing security policies, and not only try to handle things from the IT perspective, Howard said. "I think it is a matter of education, and a matter of helping them understand the value of those documents at the user level, and not just the IT level.

4 **A final misconception is that printer security is not worth the time and money,** especially given the strict budgetary restrictions that public organizations face today. Even out of the 15 percent of GovLoop survey respondents who indicated their organization is planning on updating their printer security policies, three-quarters of them said that this update won't happen for at least another six months.

Many are concerned with the amount of time and resources it takes to update printer security. For example, manually installing and updating security protocols on printers – like password protection and enabling auditing logs to track what's being printed from which devices – can take upward of 15 minutes per device, and many government IT departments are already stretched to their limits.

"When you have an organization that might have 1,000, 2,000 or even up to 30,000 devices, it appears very time-consuming," said Howard. "So, we what we hear today is that securing printers is something you have to push back and say, 'We're just going to take a chance with that risk.'"

Investing in printer security, however, can actually save your agency valuable time and money. Fleet management tools and services like those provided by HP's printer-security programs can build automated security protections into your IT environment and help your agency tighten its systems without breaking the bank or burdening IT personnel. And as we've discussed, securing your printer isn't just a "nice to have," it's a must in today's cyberthreat landscape.

Step-by-Step: Improving Your Agency's Printer Security Practices

Updating security practices can be daunting, especially when faced with the reality of incorporating hundreds or maybe thousands of printers into existing policies and protocols. The journey to securing your agency's printers, however, begins with a thorough assessment of your agency's current security situation.

Many organizations do not have time to take regular stock of how many devices are connected to their network, what security policies currently exist and how secure their printers are already. But this information is important to assessing your agency's current security level. It is also crucial to understand how users interact with the printers, like what kinds of documents they are printing and who has access to devices.

To jumpstart the journey to tighter security, here's a list of questions that can help paint a picture of the state of printers in your agency:

- **How** many devices – printers and MFPs in particular – are connected to your agency's network?
- **Who** uses these devices? How are they authenticated to access your printers and the data stored on them?
- **What** is being printed on your printers? Sensitive and confidential documents? Documents subject to controls based on compliance requirements? Documents on anti-fraud secure media (i.e. check stock)?
- **Is** there an auditing system in place to track who prints what, when?
- **Are** the printers admin password-protected?
- **Is** data encrypted to and from printers as well as at rest on the printer hard disks?
- **Is** your printer firmware up-to-date with the latest security patches?
- **Are** your printers monitored for anomalies or potential security incidents?
- **How** else are your printers currently protected, or are they not protected at all?

These questions will not only provide an accurate snapshot of where your agency stands in regard to printer security, but it will also highlight the holes that need to be filled in order to properly secure all of your network-connected devices.

The next phase is to implement adequate security policies for these devices. Howard described implementing a printer security policy as a series of three steps: setting up devices, enacting policies and then layering solutions on top of these policies that take user behaviors into account.

When agencies first bring printing devices into their existing security systems, it is important to make sure that they are **compatible.** For example, agencies need to make sure they have up-to-date firmware, admin passwords set, and they can monitor the devices for any forms of malware and security risks including integration with existing Security Information & Event Management systems.

The second aspect is selecting the **proper security settings** for printers. Many printing devices come with over 200 available security settings, so it is crucial to decide which of these are important to your agency and must be enabled. For example, enabling advanced authentication to use printing devices allows you to monitor and audit what users are doing on these devices and then set rules and roles.

Another way to approach it is by **extending existing governance practices** for devices like desktop computers, laptops and mobile devices into your printing landscape. Many organizations have compliance regulations they must meet when securing these existing devices, and the same can be done with printers.

The final step for ensuring secure printing practices is to **continually monitor user behavior and educate users** on proper printing protocols. As our survey revealed, only 42 percent of respondents indicated that their agency educates users about the safe and secure use of printers and control of documents. Every agency needs to be educating its users, and making sure that they know how to navigate the security protocols that are in place. This can be done by utilizing user behavior patterns to tailor the security features to how employees use the printing devices, and modifying them to meet business needs throughout the organization. Overall, making the security features fit usage practices will make users more compliant and less likely to risk information via printing devices.

As Howard said, ensuring your printers are safe is about taking small steps and building off the security practices already in place at your agency – like those for desktop computers or laptops – and then tailoring those to fit organizational printing needs.

“I think it all starts with securing the infrastructure and bringing in devices that have the capabilities to be secured at the level that your agency wants,” he said. “The second part is then creating that policy and understanding [which security settings are necessary for your organization]. And then on top of that, it’s starting to [tailor] solutions to help them enable those devices for the [organization’s business processes].”

Print Security Offerings from HP

One of the major challenges that Howard sees with government agencies' printer security is that many of them don't have the time and resources to go in on this process alone.

"Everybody is cutting back, including the government," said Howard. "You come into a lot of these agencies and the security team says, 'We're already working 12-hour days' ... They just don't have the time to develop these secure practices and monitor everything." Moreover, the demand for the cybersecurity workforce is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million.

Thus, for many agencies, the best option is to partner with a third-party vendor that can provide the tools and guidance necessary to secure their printing devices. And when it comes to printer security, HP has some unique technologies, products & services.

HP is the only company that has an entire security practice built around printers with credentialed security advisors that can help companies develop specific security policies and a roadmap to improve printer security.

Some of HP's printer security solutions include:

Access Control Secure Authentication

offers a variety of authentication options — including HP proximity card readers, and PIC/PIN codes — to protect your devices and prevent unauthorized use.

HP Access Control Secure Pull Printing

reduces unclaimed prints and increases efficiency. Users can print to a secure network, authenticate with ease and retrieve jobs when necessary — even on the go.

HP Access Control Intelligent Management

solutions help you control device usage, modify behavior, reduce costs and enforce security goals.

HP Access Control Job Accounting

makes it easy to accurately track and gather data, analyze the results and then create and send reports.

HP JetAdvantage Security Manager

the industry's only policy-based printer security compliance solution, lets IT establish and automate the maintenance of printer security settings to a security policy.

In addition, HP recently released a line of Enterprise printers, enabled with the world's most secure settings and technologies. These printers have the ability to monitor in-device memory for malicious attacks and self heal when an anomaly is detected restoring the BIOs and Firmware if impacted.

"If you were to call our competition and ask them to come in and do an assessment, and to sit down with you and help you build a clear roadmap for where you're going with security, they don't have that," said Howard. "And our hardware, with the new features that we built in this year, just puts us heads and shoulders above the competition."

Conclusion

The printer is a critical network endpoint that agencies must ensure is secure. Leaving printers insecure is like leaving a window open for online criminals and hackers, as printers often house sensitive agency data.

Today, printers have similar computing power as a desktop or laptop computer, and should be treated the same when it comes to security practices. Agencies should start with taking a critical snapshot of their network-connected devices, build upon existing security policies for other devices, and then continually monitor user behaviors and educate users on the proper printer protocols.

In a world where public-sector organizations look to digital solutions to increase safety and efficiency, securing enterprise printers can not only save your agency time and money, but protect your agency's critical information.

About HP Inc.

HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. With the broadest technology portfolio spanning printing, personal systems, software, services and IT infrastructure, HP delivers solutions for customers' most complex challenges in every region of the world.

More information about HP (NYSE: HPQ) is available at http://www.hp.com

Disclaimer: This article contains expressed opinions of the HP employee during an interview with GovLoop and HP does not necessarily share the same views.

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please email us at: info@govloop.com

www.govloop.com | @GovLoop

govloop

1152 15th St NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 Fax: (202) 407-7501

www.govloop.com | @GovLoop