QUOCIRCA

Print Security Trends 2022

7 priorities for securing the remote and hybrid workplace

https://quocirca.com/print-security-2022

Foreword

The expanding threat landscape

The past year has seen a major change in how organisations operate. Quocirca's research reveals that on average 44% of an organisation's workforce are working remotely or fully from home. As the hybrid work model persists the threat landscape is set to become increasingly complex and vast. The rise of bring your own device (BYOD), cloud-based services and IoT is creating new windows of opportunity for cyber attackers to gain a foothold in company networks. And attacks are more advanced and coordinated than ever before.

Today, ransomware attacks are impacting small and large businesses alike and supply chain attacks are growing in frequency and severity due to their scalability. The recent SolarWinds, Kaseya, Hafnium and PrintNightmare attacks have exposed that inadequate security controls can wreak havoc on any company's operations. Many such attacks are attributed to sophisticated Advanced Persistent Threat (APT) actors.

Traditional cyber defences can't always protect against these attacks, leaving an organisation vulnerable if it does not put in place proactive multi-layered security measures, while adopting a Zero Trust approach. The print infrastructure is one critical element of the IT environment that must be protected.

The print security imperative

Despite the ongoing shift to digital processes, many organisations continue to rely on printing to support business activities. Quocirca's research reveals that 64% of organisations believe printing to be critical or very important to their organisations in 2022. However this reliance can create security vulnerabilities – not only through unauthorised access of documents, but as an IT endpoint which, left unsecured, can represent an access point to the company network.

Despite this reliance on printing, just 26% say they are completely confident in the security of their print infrastructure. On the IT security agenda, printing is relatively low: unauthorised or unapproved home printers is in fifth place as a top IT risk, after cloud/hybrid applications, email, cloud and traditional endpoints. In 10th place, 21% consider office printers to be a key IT risk. Notably, organisations using a managed print service (MPS) are more aware of the risks. 28% consider home printers a risk, and 32% consider office printers a risk.

The majority (68%) of organisations report some level of print related data loss in the past year. This has led to an average data breach cost of £631,915. On top of the financial repercussions, organisations cite business disruption and customer loss as major impacts of such data breaches.

7 print security priorities

In 2022 we can expect to see increased adoption of Zero Trust strategies to protect print endpoints, applications and infrastucture with a 'never trust, always verify' approach. A Zero Trust approach can help prevent malware, phishing and data exfiltration attacks. A core component is identity and access management (IAM). To enhance security, combining passwords with other authentication methods such as smart cards, three-factor authentication, and biometrics will be a top priority for many organisations.

Looking to 2022 and beyond Quocirca has highlighted 7 key priority areas that CIOs and CISOs should urgently address in order to mitigate the risks around printing in the hybrid workplace.

Quocirca's research indicates that leaders who have adopted a range of measures to increase print security resilience have the greatest confidence in their security posture and see fewer data losses. With the threat landscape only set to become more complex, with more advanced cyber attacks resulting in far reaching financial and business impacts, IT leaders cannot afford to be complacent around protecting the print infrastructure.

What the numbers tell us

19% say that the zero-day Windows print spooler vulnerability PrintNightmare impacted their business

26% cite email compromise as their top security incident

20% reported a direct printer device/IoT attack

64%

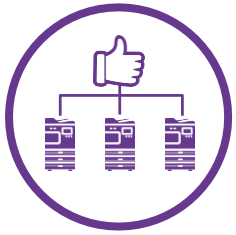
of IT decision makers say that printing is critical or very important to their business

67%

are concerned about the security risks of home printing

61%

of CIOs say it is getting harder to keep up with print security challenges and demands, compared to 44% of CISOs



26%

feel completely confident that their print infrastructure is secure

68%

of organisations report one or more print-related data losses in the past year leading to an average cost of £631,915 for a data breach

70%

plan to increase their print security spend in the next 12 months

QUOCIRCA

7 print security trends for 2022

1. A continued reliance on printing demands effective security
2. Printing risks are increasing in the expanded threat landscape
3. CIOs are finding it harder than CISOs to keep up with print security challenges
4. A managed print service (MPS) improves print security confidence
5. The majority of organisations report print related data losses
6. Data losses are costly and disruptive
7. Multi-layered print security measures help mitigate risk

Methodology

Quocirca's Print Security 2022 Study is based on the views of 531 IT Decision Makers (ITDMs) in the US and Europe. 23% of the respondents were from SMBs (250 to 499 employees), 29% from mid-size organisations (500 to 999 employees) and 47% from large enterprises (1,000+ employees). The research was conducted online in October 2021.

1 A continued reliance on printing demands effective security

Overall, 64% of respondents to Quocirca's survey indicate printing will remain critical or very important in the next 12 months, down from 71% now. Notably it is smaller organisations that expect the importance of printing to decline faster – 59% believe it will be critical or very important in the next year down from 72% now. In comparison, 65% of larger enterprises believe it will be critical or very important compared to 73% now.

Although office closures have severely impacted office print volumes over the past year, 44% expect these to increase over the next 12 months, while 41% expect home print volumes to increase. Notably, CISOs are more bullish with 53% and 58% respectively expecting a rise in office and home print volumes, compared to 42% and 40% of CIOs.

This ongoing dependence on printing, particularly in large organisations that are managing a hybrid workforce, will demand more effective and integrated print security measures that protect and manage devices, documents and the network.

> "Smaller organisations expect the importance of printing to decline faster than larger organisations"

Figure 1. How important is printing to your business?

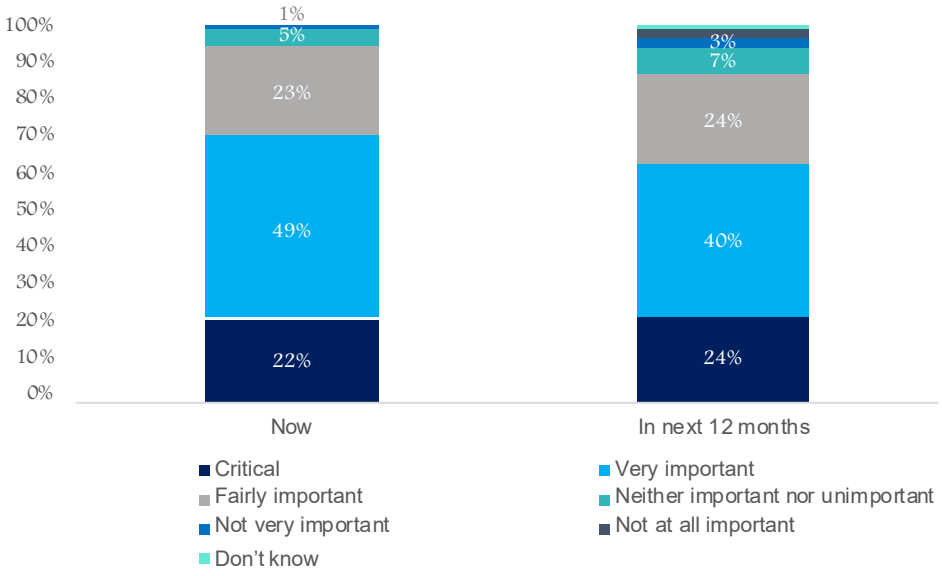
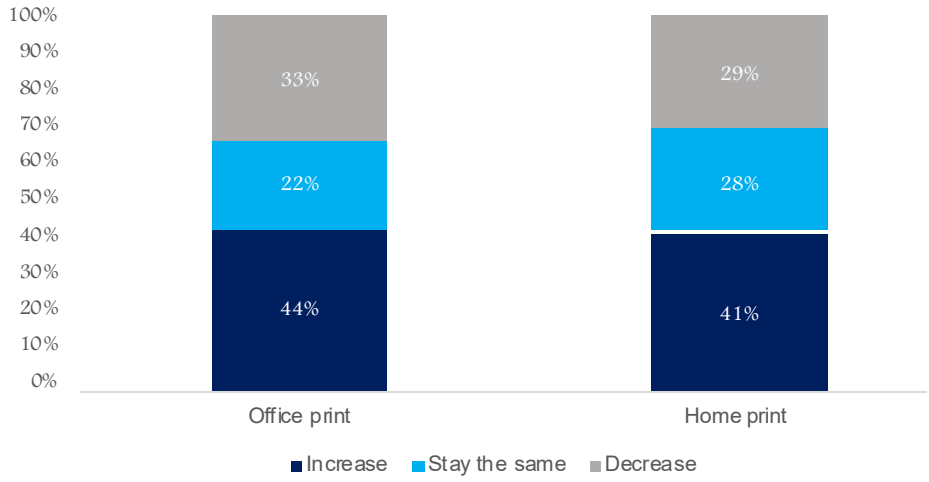


Figure 2. Over the next 12 months, how do you expect your organisation's print volumes to change?



2 Printing risks are increasing in the expanded threat landscape

> “shadow purchasing has a major impact on the overall threat landscape”

The move to hybrid working means that more devices are being used – many of them not provided, managed or controlled by the organisation. Bring Your Own Device (BYOD) has expanded to become Bring Your Own Office (BYOO), with desktop/laptop computers being used alongside tablets, mobile phones, printers and other devices. This shadow purchasing has a major impact on the overall threat landscape that an organisation has to monitor and manage. This requires a greater focus on endpoint management, data encryption and Zero Trust models that encompass authentication such as identity access and management (IAM).

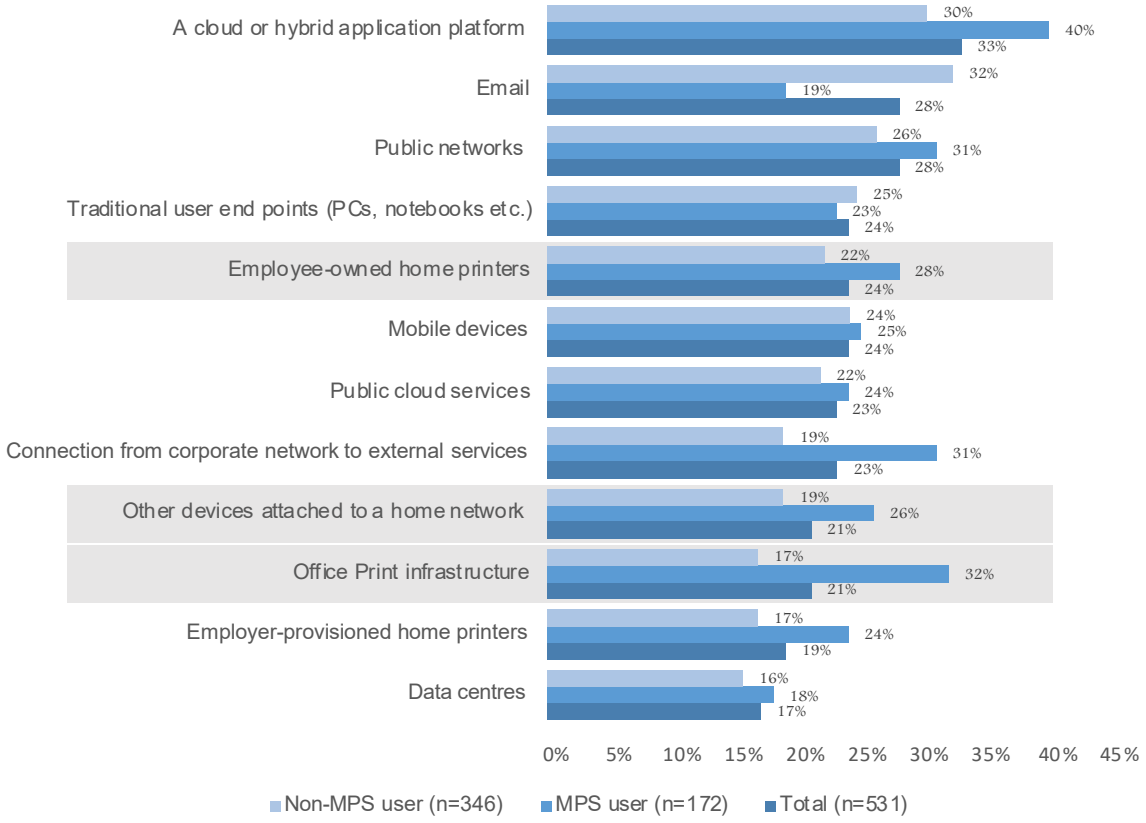
Organisations using a managed print service (MPS) are more cognisant of print security risks

Despite the continued prevalence of printing across both the home and office environments, printing is lower on the security agenda than other elements of the IT infrastructure (Figure 3).

Overall, 24% of ITDMs view employee-owned home printers as a top security risk, with 21% citing that the office print infrastructure poses a top risk. This compares to 33% that cite cloud or hybrid platforms, email (28%), public networks (28%) and traditional endpoints (24%) as presenting a high risk.

There are distinct variations in the perceived risks around printing depending on whether the organisation is using an MPS. In most cases – apart from email and traditional user endpoints – MPS users are far more wary of the threats posed by each area, which may be because they are also far more likely to have visibility of their print environment. All organisations should be implementing measures to mitigate risks around both home and office printing.

Figure 3: Which areas do you consider to pose the greatest security breach risk?



3 CIOs are finding it harder than CISOs to keep up with print security challenges

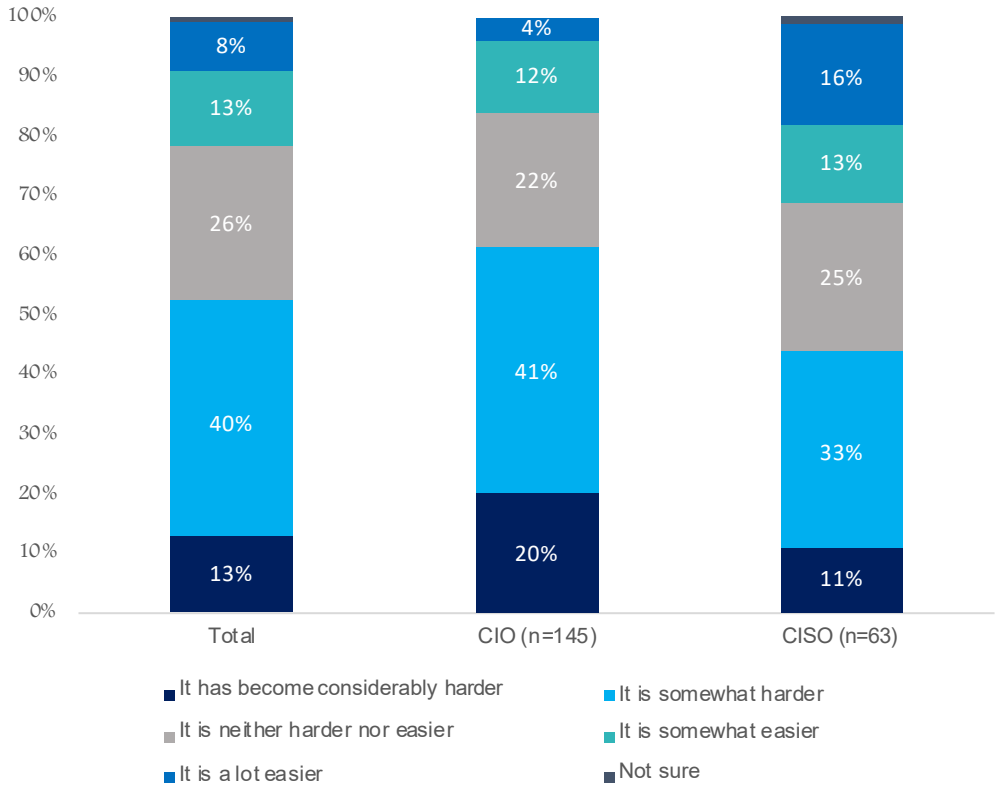
The shift to remote working has made it more difficult for many organisations to keep up with print security challenges (Figure 4), with more than half (53%) overall stating that it was either considerably or somewhat harder. This rises to 55% amongst SMBs.

CIOs seem to be finding it harder to keep up with challenges - 61% stated that they were finding it considerably or somewhat harder, compared to only 44% of CISOs, 29% of which stated that they were finding it somewhat or a lot easier.

As organisations have accelerated their digital initiatives over the past year, migrating to the cloud to better support remote working, the CIO and CISO roles have needed to become more aligned. While the CIO will be focused on delivering business value through technology, CISOs are focused on risk mitigation.

As the exploitable attack surface expands, these leaders must work collaboratively to ensure that a technology roadmap for the print infrastructure is resilient and secure while supporting business efficiency.

Figure 4: How do you feel about keeping up with print security challenges and demands?



4 A managed print service (MPS) improves print security confidence

Overall, 26% of respondents say they are completely confident that their print infrastructure is secure, and a further 34% are mostly confident (Figure 5). US respondents are the most confident, with 37% reporting they are completely confident compared to just 16% in the UK, 17% in Germany and 22% in France. Industrials is the most confident sector (31% say they are completely confident), dropping to 21% in the finance sector. Mid-size organisations report the highest confidence (33%) compared to 20% of smaller organisations.

Notably, organisations using a managed print service (MPS) have the most confidence in their print security. 84% of MPS users are completely (37%) or mostly confident (47%) in their security compared to only 49% of non-MPS users (22% and 27% respectively).

This demonstrates how MPS can help organisations mitigate risk and instil confidence in their security posture. MPS can deliver proactive security measures such as remote monitoring and remediation and in-depth security assessments that are fundamental in understanding security vulnerabilities across the hybrid work environment. Indeed, organisations using an MPS have far higher satisfaction levels with their suppliers' capabilities (42% being very satisfied) than those without an MPS (20%) (Figure 6).

> "26% of respondents say they are completely confident that their print infrastructure is secure"

Figure 5: How confident are you that your organisation's print infrastructure (office and remote workplace) was/is protected from security breaches and data loss?

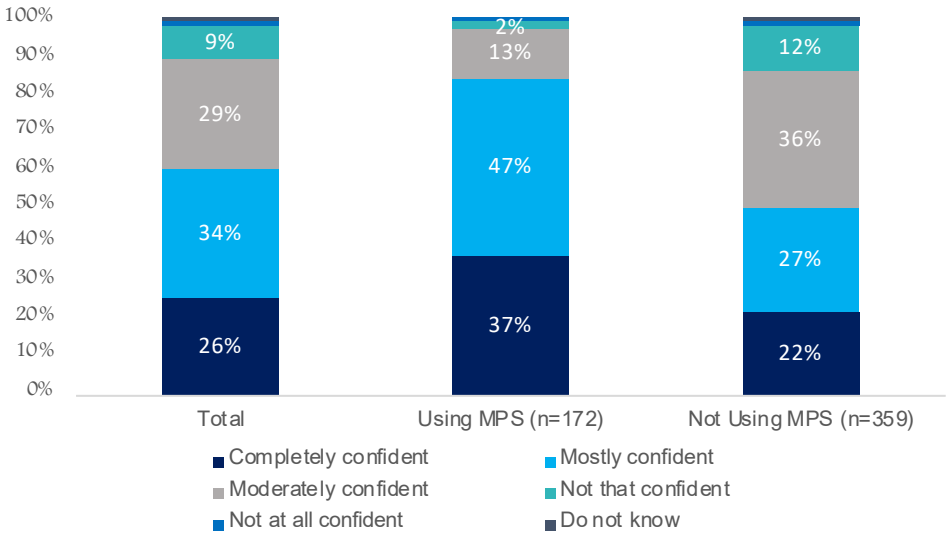
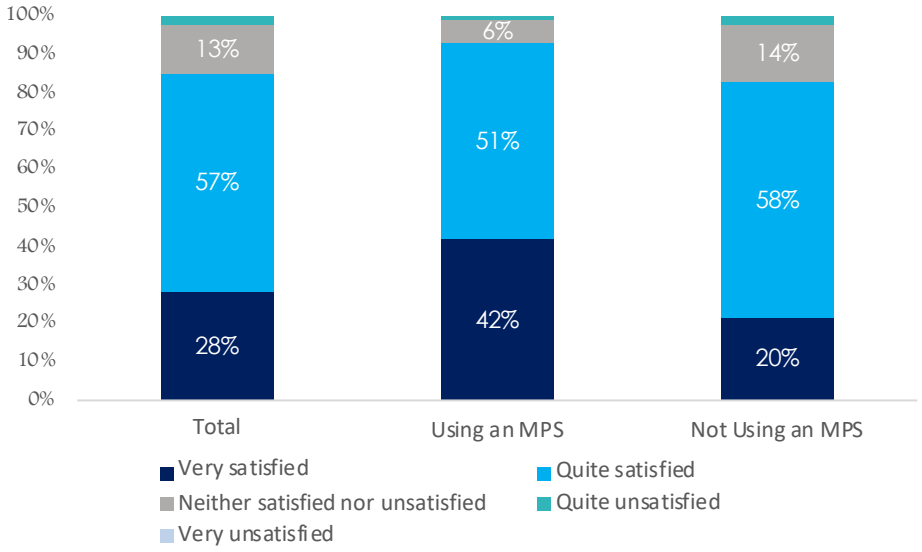


Figure 6: How satisfied are you with your print supplier's capabilities when it comes to securing your print infrastructure?



5 The majority of organisations report print related data losses

68% of organisations report experiencing at least one print related data loss over the past 12 months (Figure 7), rising to 72% in the US and 77% in mid-sized organisations, and dropping to 59% amongst large organisations. Public sector organisations were most likely to have experienced a data loss during the period (77%), while industrials reported the fewest data breaches (62%).

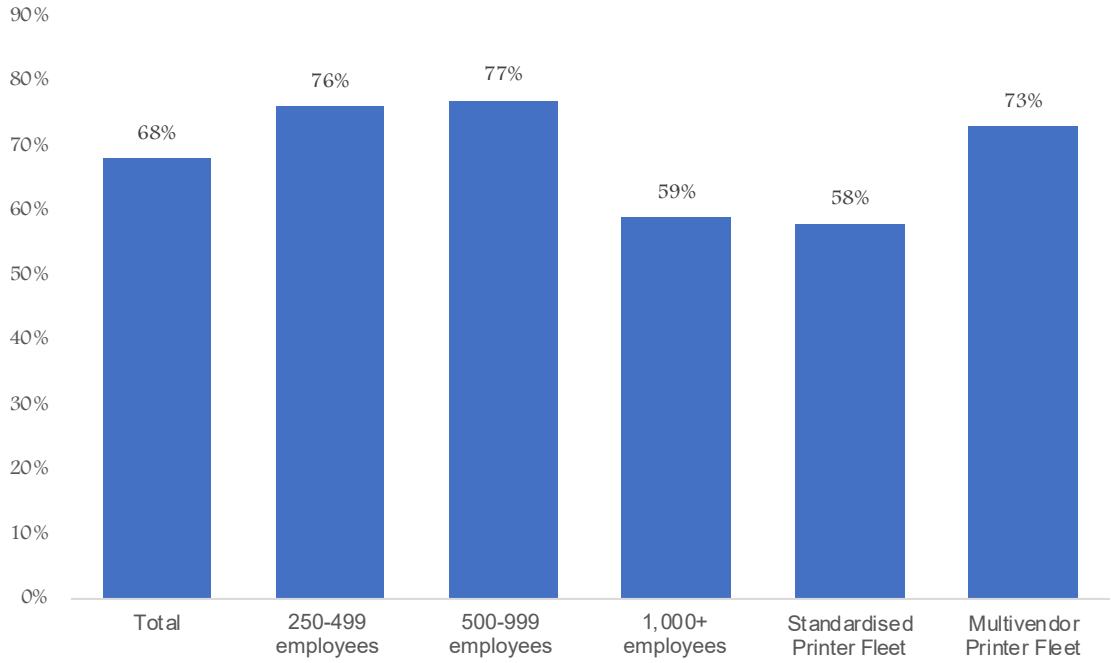
With mid-sized organisations stating the highest confidence levels in the security of their print platforms, yet also disclosing the highest number of data breaches, there is an obvious disconnect between perception and reality. Unlike smaller organisations, larger organisations are most likely to have an MPS in place backed by proactive monitoring and remediation. However MPS providers are increasingly offering security audits for SMBs which can help identify vulnerabilities and create a more resilient roadmap for print security.

In our study, 66% of organisations are operating a mixed fleet environment which can create security blind spots. Indeed, 73% of those operating a mixed fleet of printers reported data breaches - while 58% of those with a standardised fleet did.

Transitioning to a standardised fleet can help mitigate risks around the challenges of managing and securing a heterogenous environment. While third party print security solutions can enable a diverse fleet to be managed, organisations should carefully evaluate platforms to ensure that robust security can be applied across all printers in a hybrid work environment – covering device, document and network security.

> “66% of organisations are operating a mixed fleet environment which can create security blind spots”

Figure 7: One or more print-related data loss over the past 12 months



6 Data losses are costly and disruptive

Print related data losses are costing organisations an estimated average of £632,000 per breach.

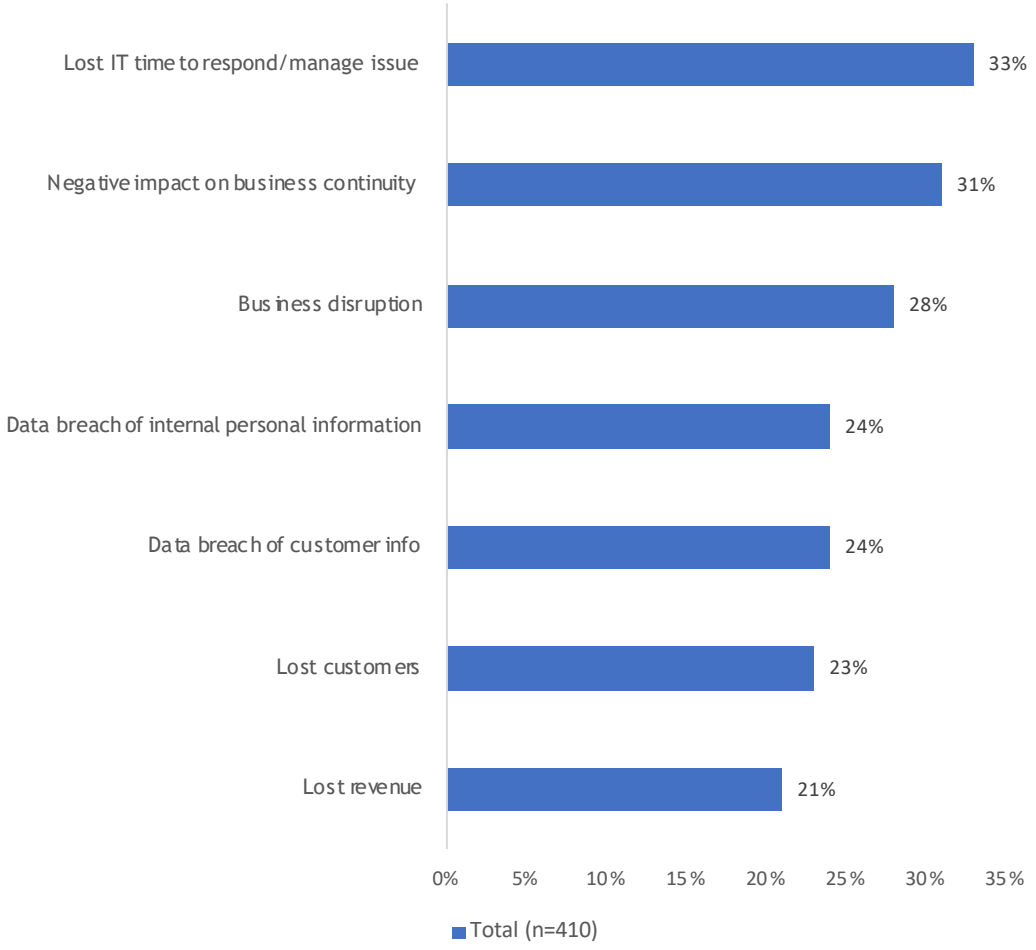
Beyond the simple direct costs of a data breach, organisations also report a range of other impacts (Figure 8). The highest impact overall is on the amount of time it takes the IT team to respond to and manage the issue (33%).

Although SMBs find this less of a problem, with only 23% stating it as a major impact, 30% report that the data loss had led to lost customers. This compares to just 18% of mid-size businesses. The impact of lost customers on any SMB cannot be underestimated.

Smaller companies need to understand the consequences of a data breach in order to assess risk. Many often mistakenly believe that they are too small to be a target, or underestimate the vulnerabilities around their print environment – creating weaknesses for cyber attackers to exploit.

> “Smaller companies need to understand the consequences of a data breach in order to assess risk.”

Figure 8: What were the major impacts of these data losses? (Top 7 shown)



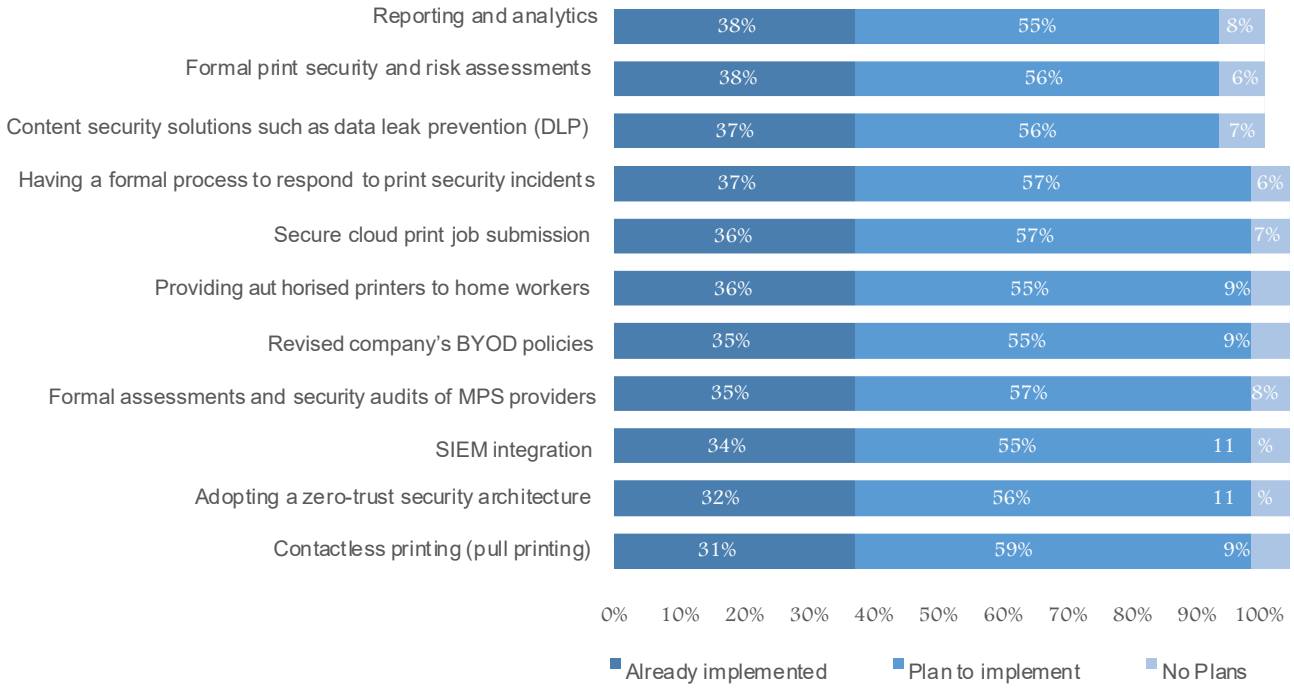
7 Multi-layered print security measures help mitigate risk

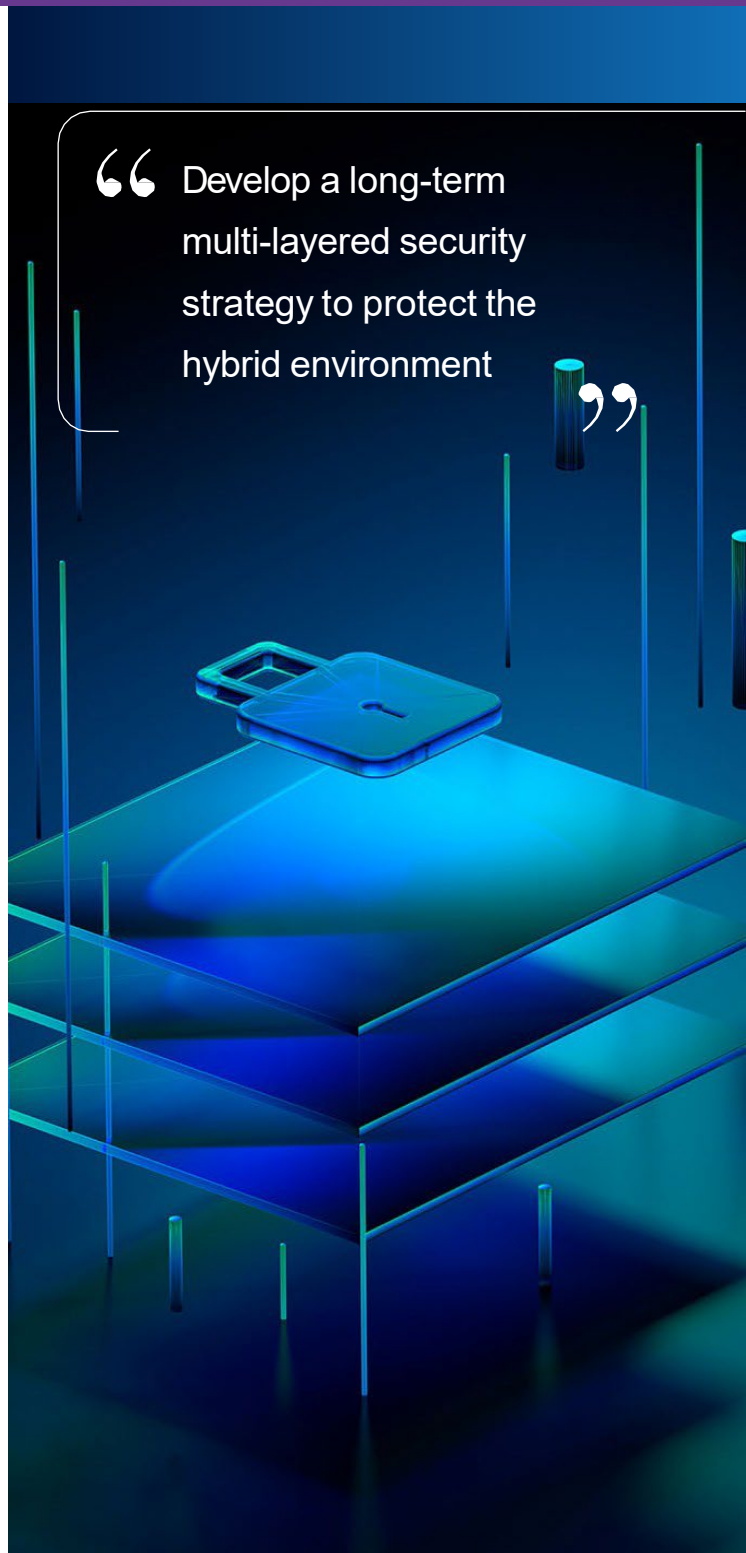
With such marked differences between respondents' confidence in the security of their print environments, and the problems they have encountered due to a lack of adequate print security, organisations must now take the steps required to create a long-term strategic approach to information security, moving to embrace the change to hybrid working and the use of a more disparate printer fleet.

A multi-layered approach to print security that addresses an organisation's specific needs can take account of a range of measures (Figure 9). The use of reporting and analytics (38%) along with formal assessments (38%) is the most widely implemented approach. This rises to 41% and 45% respectively in large organisations, which are also far more likely to implement many of the other measures.

SMBs show lower adoption in areas such as implementing formal print security and risk assessments (30%) and revising security/BYOD policies to cover home printers (23%). Currently, 32% of organisations have adopted a Zero Trust security model.

Figure 9: Has your organisation implemented any of the following print security measures?





Buyer recommendations

Because the hybrid work environment expands the exploitable attack surface, numerous layers of security are required to protect it from external and internal threats.

In addition to investing in security awareness and training for employees, IT leaders should consider the following:

1. Conduct in-depth risk assessments.

Organisations must ensure that the print infrastructure is fit for purpose across device, document and network security. This can be carried out internally, or by third parties such as managed security service providers (MSSPs) or managed print service (MPS) providers. New assessments must fit in with broader IT security and risk assessments.

2. Adopt Zero Trust principles.

Zero Trust operates on the basis of 'never trust, always verify', assuming that an environment will be compromised and no device should ever be fully trusted. Organisations have started to implement Zero Trust environments, but mainly within the constraints of their IT environment. This now needs to be extended to printing across the wider hybrid workplace.

3. Provide authorised printers for home workers.

To avoid the security risks associated with shadow purchasing, organisations should ensure that remote workers are using approved or authorised printers. Newer devices are more likely to include the latest security features. By including them in existing MPS contracts, organisations will be able to track, secure and manage printing in the remote environment.

4. Revise BYOD policies to include employee printers.

For many organisations, supplying and provisioning printers to all employees working from home may not be practical. Existing bring your own device (BYOD) policies must now be updated to cover the home environment – moving to a BYOO (bring your own office) approach, with policies covering desktop/laptop PCs, tablets, mobile devices, desk phones and print devices.

5. Evaluate content security solutions.

Content management systems based around document metadata, where documents are classified in accordance with their sensitivity, allow specific policies to be set - such as 'this document cannot be printed' or 'this document can only be printed on an approved printer'. This enables home-based employees to use their own printers for routine jobs without the risk of restricted documents ending up in wastebins.

6. Implement pull printing.

Requiring PIN/smartcard or biometric authentication is vital to ensuring confidential or sensitive information is not accessed by unauthorised users. Pull printing is most useful in shared access and distributed print environments. It can also be applied to allow home users to submit print jobs securely via the cloud to office printers, or even their own printer – enabling them to be tracked at a central level.

7. Continuously monitor through reporting and analytics.

Risk assessments, tuning content security and configuring SIEM (security information and event management) systems all require insight provided by gathering reports from across an organisation's network, including its extension into employees' homes. SIEM systems themselves can often provide this information, as can other log management tools.

For Quocirca's full analysis of the Print Security Market, please visit https://quocirca.com/print-security-2022

About Quocirca

Quocirca is a global market insight and research firm specialising in analysing the convergence of print and digital technologies in the future workplace.

Since 2006, Quocirca has played an influential role in advising clients on major shifts in the market. Our consulting and research is at the forefront of the rapidly evolving print services and solutions market, trusted by clients who are seeking new strategies to address disruptive technologies.

Quocirca has pioneered research in many emerging market areas. More than 10 years ago we were the first to analyse the competitive global market landscape for managed print services (MPS), followed by the first global competitive review of the print security market. More recently Quocirca reinforced its leading and unique approach in the market, publishing the first study looking at the smart, connected future of print in the digital workplace. The Global Print 2025 study provides unparalleled insight into the impact of digital disruption, from both an industry executive and end-user perspective.

For more information, visit www.quocirca.com

QUOCIRCA