Print Security Landscape, 2025

Identity, AI, and Quantum: Navigating the New Threat Landscape

Print security trends in the US and Europe
Excerpt report: Sharp
July 2025

QUOCIRCA

Executive summary

The print infrastructure continues to present a significant, evolving threat vector within corporate networks. Increasingly sophisticated and connected multifunction printers (MFPs), including those leveraging artificial intelligence (AI) and the future computational power of quantum computing, are vulnerable endpoints susceptible to advanced cyber threats.

The risks of mixed fleet environments

Organisations reliant on mixed fleets and those with older 'legacy' print devices face a range of security risks. Quocirca's research found that 59% of respondents are currently operating a multi-vendor fleet, with 41% operating a standardised, single vendor fleet. Mixed fleets require more robust management to ensure that each device is kept at the latest security patch level and that security across the fleet does not leave gaps that can be easily compromised.

Unlike modern MFPs that are engineered with advanced security features, older legacy devices lack robust embedded security, such as hardware roots of trust, secure boot functionalities, or self-healing firmware, leaving them more susceptible to low-level attacks or firmware manipulation. Legacy devices may not support advanced network security features like granular port control, complicating efforts to segment and isolate them effectively from critical network infrastructure. There are also limitations in terms of patching and updates, older models reaching end-of-life for crucial security fixes are exposed to newly discovered and unmitigable vulnerabilities. In addition, authentication mechanisms are often inadequate, offering only basic or no user verification at the device itself, which contributes to the risk of uncollected sensitive documents and unauthorised access to confidential information.

The integration of older assets into modern, centralised security management platforms is often difficult or impossible, hindering consistent policy enforcement and real-time monitoring. Quocirca's research shows that organisations operating complex, often multi-vendor print environments, face elevated risks and increased costs associated with potential data breaches. While just 19% of organisations managing a standardised print fleet are concerned about sensitive documents being printed, this compares to 34% of those with a multi-vendor fleet.

This disparity extends to the perceived threat from AI; 49% of organisations with multi-vendor fleets deem it very important that vendors employ AI to protect against AI threats, a figure that drops to 28% for those with standardised fleets. Furthermore, authentication methods often vary significantly across differing environments, exacerbating the complexity of maintaining a consistent security posture. Awareness of quantum threats is also high, with 66% of IT decision-makers (ITDMs) acknowledging the importance of printers being protected against such attacks.

Print-related data losses are falling – but are still significant

Overall data losses stemming from insecure printing practices have decreased to 56% from 67% in 2024, indicating progress. However, a significant gap persists; print security leaders, defined by the implementation of more security measures, report substantially fewer data losses (47%) compared to laggards (79%), underscoring the direct efficacy of proactive security investments. Documents on home printers constitute the top factor for data loss at 53%, followed by improper document disposal at 44%. This 'human factor' vulnerability is particularly pronounced in sectors such as retail (73% for home printers) and financial services (63% for home printers), indicating a critical need for both comprehensive user education and technological solutions to mitigate risks associated with decentralised printing. The need for print management systems that fully embrace hybrid working is clear. The average cost of a print-related data loss stands at £820,000, escalating to £937,000 for organisations managing multi-vendor fleets, while those with standardised fleets report a lower average of £630,000.

All this – the increasing sophistication of device-level threats to access the network, the ongoing human element of paper-related data loss, and the amplified risks and costs associated with multi-vendor environments, presents an urgent imperative for organisations and the print market itself. Improving print security posture

requires a multi-layered approach - prioritising standardised, secure print infrastructure, implementing robust identity and access management frameworks including mandatory authentication across all devices, and deploying solutions that prevent sensitive document printing in unsecured home environments.

AI security and quantum computing concerns on the rise

Alongside this runs the emerging promise and threat provided by AI and quantum computing. Overall, 40% of respondents are extremely or very concerned about the risks presented by AI, with 86% stating that it is either very or somewhat important that vendors use AI and machine learning (ML) in identifying and managing security risks in the print environment. 66% also state that it is either extremely or very relevant that they look to OEMs to develop quantum-resistant print devices, and that they would then want to adopt these within their print environment.

Integrating AI-driven security capabilities and preparing for quantum-safe transitions are now strategic imperatives. Addressing these areas will not only reduce the incidence and financial impact of data breaches but also strengthen overall corporate cybersecurity resilience. Those in the print supply chain that do not prepare to deal with these issues or attempt to 'AI-' or 'quantum-wash' their portfolio will struggle in the market, losing customer confidence and loyalty as the provided systems fail to live up to expectations.

This report analyses the findings from Quocirca's Industry Survey conducted among 400 IT decision-makers involved in the print infrastructure in their organisations in May/June 2025.

Key findings

- **Print manufacturers continue to advance their security offerings.** Over the past year, most vendors have enhanced both hardware and software security. HP has advanced its leadership position, evidenced by the introduction of quantum-resistant printers which sets a new benchmark for the industry along with ongoing development of its zero trust print architecture (ZTPA), and its new Workforce Experience (WXP) platform. Xerox has a broad security offering across hardware and solutions and particularly excels in content security and advanced authentication. Additionally, its acquisition of ITsavvy boosts its IT-led security services capabilities. Canon continues to invest in an information security approach across its devices, notably, its new imageFORCE platform uses machine learning and AI-trained algorithms to recommend optimal device security settings. Lexmark stands out for its mature secure-by-design approach. Ricoh's secure-by-design approach delivers protection from endpoint to cloud, enabling secured workflows and data protection. Konica Minolta uses machine learning and automation across its bizhub i-Series MFPs, along with its Shield Guard cloud platform, and its bizhub SECURE offering. Sharp continues to deepen its IT-led cybersecurity services for SME clients, supported by a range of industry partnerships. A key differentiator for Epson is its multi-core printer/scanner system on a chip (SoC) which presents fewer potential vulnerabilities for attackers to exploit and provides robust hardware security across its MFP product portfolio.
- **Organisations expect to increase print security spend.** Overall, organisations expect to increase their print security spend by 13% in the coming year, rising to 16% amongst organisations operating a mixed fleet. Top concerns are securing home printing (28%), protecting confidential or sensitive documents from being printed (28%) and understanding the type of threats and vulnerabilities of the print infrastructure (25%). Organisations operating a mixed fleet tend to be the most concerned, because managing security across multiple vendors introduces inherent complexities and inconsistencies that can amplify risk.
- **Broader implementation of print security measures.** Top measures include secure cloud print submission (45%), reporting and analytics (43%) and operating a formal process to respond to security incidents including remediation (43%). 37% have adopted a zero trust approach for their print environment and 37% have implemented user authenticated printing (for instance using smart cards). The majority (85%), use and manage device certificate management but of these, just 19% say they actively deploy and manage these across their complete print infrastructure on an ongoing basis. This rises to 33% amongst print security leaders and drops to 10% amongst laggards. The high adoption of certificate management, contrasted with its limited comprehensive deployment, suggests that many organisations are not yet achieving the full benefits of such an approach and therefore may still have vulnerabilities.
- **User authentication methods are varied.** The most common authentication methods are Windows authentication (47%) and passwords or PINs entered directly at the print device (47%). 38% use biometric authentication and 37% use mobile authentication. The diverse range of authentication methods indicates a varied and somewhat fragmented approach to print device security. The lower adoption rates for more advanced authentication methods points to a potential security gap for many organisations and a clear opportunity for print solution providers to educate clients and offer more sophisticated, integrated authentication solutions that align with modern cybersecurity best practices.
- **Print security leaders less likely to report a data loss.** Organisations classified as print security leaders, are less likely to report a data loss – 47% compared to 79% of laggards. This highlights the effectiveness of proactive print security strategies and for vendors, reinforces the opportunity to educate clients on the benefits of comprehensive print security and to provide scalable solutions that elevate security maturity across all organisational sizes. Overall, 56% of organisations report a print-related data breach, down from 69% in 2024. This reduction is mainly due to a fewer number of UK organisations reporting a data breach – just 24% in 2025, compared to 70% in France. Notably, more small and medium-sized businesses (SMBs) (60%), report a print-related data loss compared to 53% of large enterprises.
- **Lost IT time is the top impact of a data loss.** Of those that reported a print-related data breach, 24% report that the top impact was lost IT time responding/managing the breach, rising to 27% amongst

larger enterprises, and 30% for those operating a mixed fleet environment. The top impact for SMBs was negative impact on business continuity (28%). This reflects that the true cost of a print-related data breach extends far beyond direct financial penalties. For larger enterprises and those with complex mixed print fleets, the substantial diversion of IT resources towards breach management underscores the hidden burden of inadequate print security. Meanwhile, for SMBs, the direct threat to business continuity highlights their heightened vulnerability and the critical need for solutions that minimise downtime and simplify incident response.

- **Home printing environment is growing source of data loss.** Overall, 53% report that documents have been accessed by unauthorised people in the home environment, rising from 43% in 2024. This rises to 57% amongst SMBs and drops to 49% among large enterprises. A further 44% state that a breach has occurred due to a document not having been disposed of correctly after use. Notably, larger enterprises are more likely to provide home printers that adhere to company security policies (43%) than SMBs (34%). This indicates that the shift to hybrid and remote work models has made the home printing environment a primary and growing source of data loss, highlighting a significant and persistent human factor vulnerability.
- **The average cost of print-related data breaches has fallen.** Compared to 2024, the average cost of a print-related data breach has fallen from over £1m to around £820k. SMBs report an average data loss of £639k, the mid-market £795k and larger enterprises £937k. For all organisations, these figures show that print-related breaches carry a significant financial penalty, reinforcing the need for security investments that align with an organisation's size and risk profile to mitigate these substantial potential losses.
- **AI security concerns loom large.** Overall, 40% are either extremely or very concerned over the bad impacts AI can have in the wrong hands when it comes to their pint infrastructure. However, 41% believe that it is very important that print vendors use machine learning) and AI to identify potential security threats and cyber-attacks, rising from 34% in 2024. This indicates that customers are increasingly looking to vendors to provide intelligent, proactive defence mechanisms against sophisticated cyber threats. For print vendors, this presents a compelling opportunity to differentiate their offerings by integrating and clearly articulating their AI/ML capabilities, transforming their role from hardware providers to essential partners in an enterprise cybersecurity strategy.
- **Familiarity with quantum computing is relatively high.** 52% of respondents state that they are either expertly or very familiar with the concept of quantum printers, and 66% of organisations say it's important that print vendors develop post-quantum or quantum-resistant print devices, indicating a strong willingness to procure and implement such technologies within their fleets. This high level of awareness and readiness for quantum-resistant print devices, even in the nascent stages of quantum computing, signals a forward-thinking approach among ITDMs. It presents a significant, long-term strategic imperative for print vendors to invest in quantum-safe cryptography research and development. The expressed willingness to procure these devices also suggests that early movers in this space could gain a substantial competitive advantage by positioning themselves as future-proof and security-conscious partners.
- **Satisfaction with print security offerings is on an upward trend.** Overall, 40% indicate they are very satisfied, with a further 54% indicating they are quite satisfied. UK respondents are the most satisfied (54% are very satisfied) compared to France (25%). Those using an MPS are most satisfied (46%), along with print security leaders (55%). There is a distinct CIO-CISO satisfaction gap when it comes to print security offerings. While 53% of CIOs report being satisfied, only 25% of CISOs share this sentiment. This suggests that current vendor offerings might not be fully addressing the granular security requirements or advanced threat concerns that CISOs prioritise. A key finding is the clear demand from organisations for more education and guidance from suppliers, particularly at a consultancy level, regarding print security. While satisfaction with print security offerings is on an upward trend, the persistent request for better education and consultancy reveals a significant opportunity for suppliers. This indicates that customers are not just seeking products, but also expertise and strategic guidance to navigate the complexities of their print environments.

Table of Contents

Vendor profile: Sharp

Quocirca opinion

Sharp is positioned as a Leader in Quocirca's 2025 Print Security Landscape assessment. It is building its capabilities as a trusted security partner by delivering a comprehensive strategy that encompasses mature hardware security, extensive cybersecurity industry partnerships, and an IT services-led approach to security training for both its channel partners and SME clients. Over the past year, Sharp has deepened its consultative security approach, assisting customers in defending, protecting, and monitoring their entire print and IT infrastructure, concurrently expanding its geographical service coverage across Europe. Bolstered by strong IT services capabilities, often built through acquisition, Sharp is well positioned to serve as a strategic security services partner for SMEs in particular, addressing the complex security requirements of both the IT and print environments.

Sharp has continued to invest in building awareness of its security offerings and consultative security approach among European SMEs, bolster its service and product offerings, and expand its geographical coverage of services. For example, Synappx Manage, its new global cloud-based device management application for print (and, in the future, display) devices, is currently being rolled out across Europe for direct customers. Sharp has also maintained a strong focus on helping businesses navigate the threat landscape by aligning with NIS2 Compliance Readiness & Monitoring and PSTI MFP product compliance and developing EU RED compliance for the 1 August 2025 release. Additionally, Sharp completed its Nordic Security Awareness Training pilot based on Nimblr services and has since been extending this service offering across its European markets.

The company's focus on hardware security ensures devices are secure from the moment they are delivered and throughout their operational life. Sharp's MFPs and printers have an extensive range of built-in security features, including document control mechanisms to prevent unauthorised access, remote firmware management, multi-factor authentication, and SSL encryption to protect data during transmission. Additionally, Bitdefender advanced anti-malware technology scans all data and files processed on Sharp MFPs, providing protection against known and unknown malware, including viruses, trojans, worms, ransomware, advanced persistent threats, zero-day threats, spyware, and more.

Sharp offers a Complete Print Security service that encompasses not only hardware security but also comprehensive solutions for document and data protection. This includes secure print release, user authentication, and audit trails to ensure sensitive information is protected at all stages of the print process. Sharp's consultative approach helps SMEs implement robust security measures tailored to their specific needs, ensuring a secure and efficient print environment.

Sharp has further strengthened its security awareness training in the past year. In November 2024, it launched a new cloud-based Security Awareness Training service that provides businesses with guidance on best practices regarding cyber security and data protection. It also established a global cross-product cybersecurity centre of excellence staffed by regional operations and HQ product development, added central deployment and management of its Security Awareness Training and Cyber Essentials services, and created a dedicated NoC team for 24/7 monitoring and remediation. It plans to expand its Security Operations Centre (SoC) capability to include managed XDR within its European Technology Support Centre in Warsaw.

Sharp has adopted Bitdefender's anti-malware SDK, using an AI-based AV engine and multiple ML models for malware detections.

Security strategy

Awareness and education

Sharp's strategy is to be perceived as the right partner to solve SMEs' cybersecurity-related issues and provides strong consultancy services together with a growing security portfolio that incorporates print security products and solutions and educational services. It focuses on building awareness and education of the continuously evolving threat landscape, associated vulnerabilities, regulations, and business and employee impact across end-user organisations and its reseller channels.

Capabilities in IT

Sharp particularly stands out for its capabilities in IT, expertise it gained with the acquisition of two IT services companies, Complete I.T. in the UK and IT Point in Switzerland. The December 2024 acquisition of Apsia, a French-based company specialising in digital transformation and cloud integration, will enable Sharp to further extend and expand its IT services footprint and offering.

Of particular note is its print security-as-a-service offering, Complete Print Security, which, at launch, was unique in the market, and its Complete Security Audit service offering, which was developed in the UK and will soon be available through Sharp Business Systems France, Apsia (France), and IT Point (Switzerland). In addition, its Microsoft Copilot Readiness Assessment service, which helps businesses deploy Copilot smoothly, efficiently, productively, and securely, further extends Sharp's comprehensive approach to cybersecurity alongside print and other security services.

Partnerships

Partnerships with companies including Bitdefender, enabling the integration of Bitdefender anti-malware technology into Sharp's Future Workplace A3 multifunction printers; ConnectWise (remote monitoring/access services and Security Operations Centre); Sentinel One (managed detection and response); SkyKick (cloud [M365] migration and backup service), Microsoft, and CyberSmart, a provider of cybersecurity regulatory compliance services including UK Cyber Essentials and NIS2, are integral to Sharp's security strategy.

Product and software security

Hardware security features

Sharp MFPs and printers have an extensive range of built-in security features. These include:

- **Trusted Platform Module provides an added layer of protection to safeguard data.** This is an industry-standard computer chip that uses cryptoprocessor technology to protect hardware such as harddisk drives and solid-state drives inside MFPs and printers. When a Sharp MFP is installed with a data security kit or TPM, the TPM chip initiates a cryptographic key that cannot be accessed by software. A matching cryptographic key is encoded during the boot-up process. If the two keys do not match, access to the device is denied.
- **Real-time intrusion detection detects abnormal connection requests and denies access.** Intrusion detection provides the next level of protection and safeguards the device against any suspicious network-access attempts.
- **BIOS integrity check at startup helps protect system files from malware attacks.** BIOS is firmware used to provide runtime services for operating systems and programs and perform hardware initialisation during the booting process. If errors are found, the device is prevented from starting.
- **Application whitelisting prevents unauthorised applications and firmware from being loaded.** This automatically monitors access attempts and only grants access to applications and operating firmware that are on an approved whitelist. Any other external applications are instantly blocked, logged, and reported.
- **Bitdefender anti-virus provides comprehensive protection from malware attacks.** Sharp MFPs integrate with broader security strategies through SIEM, enabling password policies to be remotely controlled, and include anti-malware support using Bitdefender, making it much easier for IT teams to keep data, devices, and networks secure.
- **End-of-lease data erase can protect privacy.** Sharp devices offer standard end-of-lease features to ensure all confidential data is overwritten before the device leaves the facility or customer environment. Once executed, the data is overwritten up to 10 times. If a DSK is installed or standard MFP security feature is enabled, the data is overwritten with random numbers.

- **Firmware attack prevention checks for abnormal firmware and can restore an original from backup.** Sharp devices include an innovative self-healing feature. A master copy of the MFP settings is backed up and can be used to safely recover the device if there is a problem.
- **Active Directory integration.** Can join a network domain as a trusted device and use single sign-on.

Authentication and access control

Sharps printers and MFPs include a suite of advanced security information and event management features designed to protect information and document assets from a multitude of physical and cyber security threats, including the most sustained and determined attacks.

They also help compliance with increasingly stringent legal and regulatory requirements, such as the GDPR.

Sharp provides tools to control and manage print security policies and securely access confidential information however it is being captured, stored, printed, or shared over a network. This includes:

- Secure user authentication before a device can be used – via ID card, Active Directory with SSO, LDAP, or print policy authentication.
- Serverless print release enables users to securely print and release jobs from up to five other devices on the same network.
- Automatic encryption occurs for any documents stored on or emailed from the device.
- Audit trail and job log features provide a comprehensive review of all user activity.

Proactive access control

To prevent any unauthorised use, Sharp's MFPs include pre-installed root certificates. They also automatically monitor access attempts and only grant access to applications and operating firmware that are on an approved whitelist. Any other external applications are instantly blocked, logged, and reported. Intrusion detection safeguards the device against any suspicious network access attempts.

Complete Print Security

Designed for SMEs, Sharp's turnkey IT security subscription service ensures MFPs are secure once they are delivered and throughout their operational life. The service combines several existing services and solutions with 24x7x365 security event monitoring to maximise the capability of security features built into the MFPs. Security alerts generated by the SIEM service are monitored by the SOC, with any suspicious activity alerted to Sharp's Warsaw-based, 24/7, multilingual European Technology Solutions Centre, which then investigates and takes the appropriate action to secure the MFP.

AI/Copilot Readiness Assessment

Sharp's AI/Copilot Readiness Assessment service is designed to help customers unlock the full of potential of Microsoft 365 and Copilot while maintaining security and productivity. The assessment has five components: a current environment that analyses the technical infrastructure to determine Copilot's impact; user workshops that identify key user profiles and best use cases for AI; a data review to assess data storage, security, and access permissions; security and compliance to ensure data protection measures align with business goals; and expert advice on optimising AI deployment.

Security Awareness Training

Sharp provides cloud-based Security Awareness Training through micro-training sessions and simulation exercises, aiming to test employees on how they should react to potential cyber-attacks. The training focuses on employees' responses to phishing emails – social engineering links – to ensure security and privacy regulations are upheld. The training is provided on an ongoing basis, rather than the traditional annual course or refresh session, maintaining a threshold of security awareness across the workforce that can be regularly adapted according to needs. This model allows businesses to monitor employee progress around their response to threats, with a dashboard highlighting user activity and results to inform on suggested further training strategies.

Sharp Services Platform

The Sharp Services Platform (SSP) is a powerful cloud platform hosted in a MS Azure datacentre in Germany for GDPR compliance. This platform enables Sharp to deploy and deliver new solutions and services to customers at scale, speed, and geographic reach. Key features include one point of administration for all SSP solutions and services, analytics, and insights; a notification gateway for enrolment, system updates, automated creation, and management of secure customer tenants that is fully integrated with License Manager; and secure connectivity between applications and services using industry-leading identity management services.

Synappx Cloud Print

Synappx Cloud Print is zero trust by design. All print jobs remain on the local network, protected by a firewall, and data is encrypted both transit and at rest. The solution is fully integrated with Entra ID and Google Workspace, preventing unauthorised users from accessing sensitive business documents or data, and security settings include two-factor authentication, administrator-selectable PIN lengths, and unsuccessful login attempts. Synappx Cloud Print also offers secure pull-printing to protect sensitive data and built-in print-auditing capabilities that enable customers to monitor usage patterns. It maintains a comprehensive print audit trail, facilitating compliance with data management regulations. Additionally, the new guest print functionality allows external users to securely print to the organisation’s devices.

Strengths and opportunities

Strengths

- **Advanced hardware security.** Sharp's MFPs and printers come with an extensive range of built-in security features, including document control mechanisms, remote firmware management, multi-factor authentication, and SSL encryption. These features ensure that devices are secure throughout their operational life.
- **Complete Print Security Service.** Sharp offers a comprehensive print security service that includes secure print release, user authentication, and audit trails. This service ensures sensitive information is protected at all stages of the print process, providing SMEs with a secure and efficient print environment.
- **Global Cybersecurity Center of Excellence.** Sharp has established a global cross-product cybersecurity center of excellence staffed by regional operations and HQ product development. This center includes a dedicated NoC team for 24/7 monitoring and remediation and a Security Operations Centre (SoC) capability expanded to include managed XDR within its European Technology Support Centre in Warsaw.
- **Strong IT expertise.** Sharp particularly stands out for its capabilities in IT. It has carved out a strong IT services offering that positions it well to offer integrated security offices for the print and IT infrastructure.
- **Integrated security services for SMEs.** Sharp continues to enhance its security portfolio, which includes specific print security products and solutions and educational services, combined with strong consultancy services tailored for SMEs.

Opportunities

- **Content workflow security.** While Sharp has made significant strides in print and IT security, it has room for improvement in integrating content workflow security solutions to provide a more holistic approach to document and data protection.
- **Multi-vendor support.** Sharp's reliance on partnerships with companies such as Bitdefender, ConnectWise, Sentinel One, SkyKick, Microsoft, and CyberSmart is a strength, but it also means Sharp must continuously manage and integrate these multi-vendor solutions to ensure seamless security across its devices.
- **Geographical coverage.** Although Sharp has expanded its geographical coverage of services, there are still regions where its security offerings are not as widely available. This limits the company's ability to provide consistent security solutions to clients in those areas.

Future outlook and recommendations

Quocirca's Print Security Study 2025 strongly suggests that print security is no longer a niche concern but a critical component of an organisation's overall cybersecurity strategy. Organisations that embrace a proactive, comprehensive approach, often through MPS, are significantly more satisfied with their security posture and better protected against the growing threat of print-related data breaches. Suppliers have a clear mandate to guide and enable all organisations towards a print security leader position, emphasising the tangible benefits of robust print security.

It is also apparent from the research that print laggards in particular, have a much lower visibility of what is happening across their print environment. Although they report lower numbers of data breaches and lower costs for any that do happen, this will be down to a lack of actual capability to monitor, measure and account for what is happening. Laggards are far more likely to fail when a breach happens – through the loss of business capability and customer loyalty, combined with the direct and indirect financial losses involved.

Supplier recommendations

Those in the print market must ensure that they can help in the provision, implementation and maintenance of measures to address customers' security needs. This report has covered a list of measures commonly used by those seen to be leaders in the print security environment. Suppliers must look to ensuring that these are provided in an integrated and easy to use manner. Alongside these measures, suppliers should also look to additional value-add capabilities that can play to a customer's needs.

- **Fully integrated systems.** Print security can no longer be viewed in isolation. It must be integrated into an organisation's wider security systems, including identity management and SIEM systems.
- **Security that covers inputs and outputs.** Modern MFPs are increasingly being seen as digitisation devices, with scan capabilities ramping up in usage. Suppliers must look to how data scanned in and extracted is then secured in the rest of its journey.
- **Data security from digitisation to end-of-life.** The security of information cannot end with what happens at the device – either as information is scanned in or printed out. Data that continues to be held on a device must be secured (for example, via encryption), and must be capable of being securely deleted based on security policies and profiles.
- **Helping customers create suitable security policies and procedures.** This cannot just be carried out based on technical viewpoints, nor just via a focus on print. Suppliers must be able to work across boundaries in the technical and business environments, helping customers to understand their security needs and then creating the right environment that can ensure their needs are met.
- **AI needs to be better managed.** AI is still in its early stages, but it is rapidly morphing and maturing into something that offers both great promise and great threat. Suppliers must now be actively leveraging AI to provide customers with greater business value not only through printing and scanning itself, but also through improved security capabilities, as well as in other areas such as device manageability and sustainability. The capability for the print environment to work in harmony with the wider IT security environment to better identify and deal with malicious AI activity must be better addressed through strategic partnerships with others in adjacent security areas.
- **Plan to deal with future issues now.** For some in the supply chain, AI came and hit them when they were unprepared. This has led to a degree of responsive activity, with AI tools and protections being bolted on to existing devices and software, often with variable results. With quantum computing on the horizon, now is the time for OEMs in particular, but in conjunction with ISVs and MSPs, to ensure that they are fully ready for when quantum computing does become more generally available.
- **Create new revenue streams through helping with end-user education.** Quocirca's research shows that respondents need help in gaining a better understanding of the fast-moving security environment. Doing so should be fairly easy for suppliers and could create strong new revenue streams.

Buyer recommendations

For organisations looking to invest in effective print security, navigating the rapidly evolving threat landscape is an increasingly complex and demanding challenge. It is important to build up a better understanding of what the current state of security in the world is, and what is likely to be required in the future. Only from this can a flexible and robust environment be put in place that can help protect against current and future threats. This is highly likely to require bringing in external skills – and these should be found within the leading suppliers in the print environment.

- **Prioritise print security.** Organisations, especially print security followers and laggards, must recognise that printers are network endpoints and potential entry points for cyber-attacks. Print security needs to be elevated on the IT security agenda, moving beyond an afterthought.
- **Invest in comprehensive measures.** Within this report, Quocirca has reported on the measures taken by print security leaders in order to create a stronger security posture. Followers and laggards should aim to implement a wide range of these measures as well as embracing:
    - **Managed print services.** To gain visibility, control and expert management of their print infrastructure, leading to increased confidence and reduced data loss.
    - **Secure print release/pull-printing.** To prevent sensitive documents from sitting unattended and open to unauthorised access.
    - **Strong user authentication.** To ensure only authorised personnel can access specific print functions.
    - **Data encryption.** For data at rest on printer hard drives, and in transit for print and scan job content.
    - **Regular firmware and software updates.** To patch vulnerabilities and gain access to additional functionality and capabilities. Wherever possible, these should be automated to ensure defence against zero-day attacks.
    - **Network segmentation.** To isolate printers from critical network segments, providing an additional layer of security.
    - **Continuous monitoring and auditing.** To detect suspicious activity, with automated actions being taken to remediate or isolate such actions, and notifications being provided to systems and security administrators so that they know what is happening and can take further steps if required.
    - **Employee training.** To foster a security-aware culture around printing. However, user training must be viewed as a minor, first level defence mechanism, users forget things easily, struggle to understand areas where technical descriptions may be required, and it is difficult to maintain levels of education current enough to deal with the changing landscape of the security environment.
- **Proactively assess and address vulnerabilities**. Organisations should conduct regular print security audits to identify weaknesses and then implement solutions to close any gaps. This will require the creation and maintenance of policies and procedures that must be followed to carry out such audits, along with what steps need to be taken to remediate any issues found. These policies and procedures must also cover what needs to happen if a breach occurs.
- **Consider the total cost of poor security.** The cost of a data breach (financial, reputational, operational) far outweighs the investment in proactive print security measures. Organisations need to view print security as a strategic investment, not just an IT expense. However, a full understanding of each individual organisation's security posture needs to be gained.
- **Leverage supplier expertise**. For organisations lacking in-house print and IT security expertise, partnering with suppliers who offer comprehensive security offerings and MPS is essential. This allows them to benefit from specialised knowledge and solutions.
- **AI is already here, and quantum computing is just over the horizon.** Although AI is not the ultimate answer that many thought it would be, it is proving itself to be an effective aid in many areas of business processes. Organisations need to be aware of the darker side of AI, however, particularly when it comes to security, and must question suppliers strongly as to how they are working to counter AI threats. This

must then also be extended to quantum computing - the speed with which AI has moved from advanced rule-based pattern matching through to generative AI systems, points to quantum possibly appearing faster than many think.

About Quocirca

Quocirca is a global market insight and research firm specialising in 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 are at the forefront of the rapidly evolving print services and solutions market, trusted by clients 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.

For more information, visit www.quocirca.com.

Usage rights
Permission is required for quoting any information in this report. Please see Quocirca's Citation Policy for further details.