Print Security Landscape, 2024

Mitigating the print infrastructure as a threat vector

Print security trends in the US and Europe
Vendor Excerpt: Sharp
July 2024

QUOCIRCA

Executive summary

The rise of hybrid work has blurred the lines of traditional print infrastructure security. Public networks and less-controlled environments are now commonplace, demanding a more robust approach to print security. Meanwhile, the rise of AI is creating further security challenges, increasing the potential for vulnerable devices to become easier targets and be compromised as a result of weak security protocols. Print manufacturers and channel partners must adapt by offering enhanced security solutions that integrate seamlessly with existing IT infrastructure. This shift presents a significant opportunity. By becoming trusted advisors, the print channel can guide organisations towards comprehensive solutions across device, data, and document security. Prioritising the print infrastructure as a critical element of wider information security strategies will not only safeguard businesses, but also unlock new revenue streams for the print industry.

Quocirca's Print Security Landscape, 2024 study reveals that organisations face ongoing challenges in securing the print infrastructure. Employee-owned printers are viewed as a key security concern by 33% of organisations, which reflects the difficulty in controlling home printing – at both a device and document level – as documents can be exposed to unauthorised users. Despite the growing awareness of printing as a security weakness, organisations are struggling to translate this knowledge into action.

Print-related data breaches remain a significant threat, with 67% of respondents (up from 61% in 2023) reporting at least one data loss incident in the past year. This number jumps to 74% for midmarket organisations. This is leading to a decline in confidence, particularly among small and medium-sized businesses (SMBs), in the overall security of their print infrastructure.

Notably, organisations operating a standardised fleet are less likely to report one or more data losses (59%) than those operating a multivendor fleet (70%). This reflects the challenge of maintaining consistent security across mixed brands compared to proprietary security platforms that are embedded in a standardised fleet. Third-party print management solutions can help with securing printing across a mixed fleet. However, the extra workload for IT in managing a mixed fleet, along with the additional difficulties and hard costs of sourcing multiple print device drivers, integration systems, and monitoring and reporting systems, makes mixed fleets less attractive than standardised ones.

The latest research exposes a concerning gap in print security perception between chief information officers (CIOs) and chief information security officers (CISOs). While both expect increased security spending (77% of CIOs and 78% of CISOs), CISOs are significantly less confident in current print security measures than CIOs. This disconnect is further emphasised by the higher percentage of CISOs (41%, versus 34% of CIOs) who find managing print security challenges difficult. Interestingly, CIOs exhibit greater concern (52%, versus 32% of CISOs) about unsecured home printers, which highlights a potential blind spot.

This fractured view creates a key obstacle. Aligning CIO and CISO perspectives on security is essential for achieving robust information security. Bridging this gap is no longer an option – it is a necessity. Fortunately, Print Security Leaders, as defined by Quocirca's Print Security Maturity Index, are mitigating risks. Leaders are organisations that have implemented a higher number of print security measures than Followers and Laggards. Leaders report lower levels of data loss and have higher confidence in the security of their print infrastructure.

This presents a valuable opportunity for suppliers to position themselves as strategic partners and strengthen their security propositions to help customers mitigate risks associated with unsecured printing in both the home and office environments. By identifying and promoting the best practices employed by these Leaders, suppliers across the print ecosystem can play a crucial role in guiding Followers and Laggards to improve their security posture.

Key findings

- **Printer and MFP manufacturers continue to enhance and deepen their security focus.** HP has advanced its position because of ongoing innovation across its hardware portfolio and establishing a zero-trust print architecture (ZTPA) framework and stronger alignment of HP Wolf Security across its print and PC offerings. Xerox has a comprehensive security offering across hardware and solutions, particularly with respect to its workflow and content security portfolio. Canon offers a globally consistent security offering, supported by its mature uniFLOW platform. Other vendors in the leadership category include Lexmark with a mature secure-by-design approach across its hardware range, Ricoh which stands out for its cybersecurity services, and Konica Minolta with its bizHUB secure offerings. Sharp has made strong investments in security over the past year, exemplified by a multi-layered security approach and partnership with Bitdefender. Major players include Epson, Brother, Kyocera, and Toshiba.
- **Print security has climbed the security agenda compared to 2023.** While public networks are seen as posing the top IT security risk (35%), this is closely followed by employee-owned home printers (33%), up from 21% in 2023. This potentially reflects the growth in 'shadow printing' caused by increased home working and the use of printers outside corporate controls. Office printing is in third position (29%), up from eighth in 2023 (20%).
- **Organisations are making progress in addressing print security challenges.** Overall, 30% say it is very or somewhat difficult to keep up with print security demands, down from 39% in 2023. The top print security challenge is protecting sensitive and confidential documents from being printed (28%), rising to 34% in the US. Notably, organisations operating a multivendor print environment are more likely to cite this as a challenge (30%), compared to 24% of those using a standardised fleet.
- **In the past 12 months, 67% of organisations have experienced data losses due to unsecure printing practices, up from 61% in 2023.** As in 2023, midmarket organisations are more likely to report one or more data losses (70%) than large organisations (63%), with business and professional services suffering the greatest volume of breaches at 71%, followed by the public sector (70%). On average, the cost of a print-related data breach is over £1m, compared to £743,000 in 2023.
- **Quocirca's Print Security Maturity Index reveals that only 20% of organisations are classed as Leaders.** Leaders are those organisations that have implemented six or more security measures. The number of Leaders rises to 25% in the US and falls to 14% in France, which also has the highest number of Laggards (23%). Leaders are likely to spend more on print security, experience fewer data losses, and report higher levels of confidence in the security of their print environment.
- **Artificial intelligence (AI) is creating further concerns around security risks.** Overall, 62% report that they are extremely or moderately concerned about AI creating more IT security risks. Overall, 83% of respondents state that it is very (34%) or somewhat important (49%) that vendors use AI or machine learning (ML) to identify print security threats. These findings suggest a promising opportunity for print vendors to develop and deliver innovative solutions using ML and AI for print security – whether this involves on-device AI security or AI-based remote monitoring solutions.
- **Over a third (36%, up from 32% in 2023) are very satisfied with their print supplier's security capabilities.** This rises to 47% among US organisations and drops to 19% in Germany. Those using an MPS have far higher satisfaction levels (43% are very satisfied) than those not currently using an MPS or with no plans to use one (23%).

Table of Contents

Buyer recommendations

The increased move from simple print devices to intelligent MFPs, which have multiple vectors for attack, presents an increasingly weak link in IT security. This can be mitigated with a range of measures based on an organisation's security posture.

Buyers should consider the following actions:

- **Start by conducting in-depth print security and risk assessments.** With awareness of print security issues growing, organisations still appear to be doing little to plug the gaps. Where in-house skills are lacking, organisations need to look to providers that can offer in-depth assessments of the print environment. Security audits can uncover potential security vulnerabilities across device and document security, and this can help devise means of dealing with them. For organisations operating a mixed fleet, such an audit may also provide the value proposition required for a move to a more standardised fleet, with which a consistent and cohesive approach to security can be taken.
- **Treat print security as a strategic priority – but not in isolation.** Print and IT security must be integrated and considered a higher business priority. The importance of securing the print infrastructure must be elevated to both CIO and CISO stakeholders so they are aligned on understanding the risks to the IT platform and business. Focus must be placed on how measures can be implemented to mitigate the risks of unsecured printing, as well as monitoring and managing the flow of information created by the increasing use of digitised workflows.
- **Evaluate AI security.** Vendors should be looking to embrace and integrate AI in both the device and software to provide advanced security benefits. Real-time analytics of data on the device can help prevent the use of the device as a direct attack vector. However, maintaining the AI capabilities at a hardware level in such a rapidly evolving market may be problematic. Using AI with software provides a good means of enabling a more flexible level. Overall, a multi-level approach of hardware plus software should be used to provide the greatest security capabilities possible.
- **Include remote and home workers in the managed print environment.** Consumer-grade printers may not conform to corporate security standards, but MPS may be able to provide the controls around such printers to ensure content and information security are in place. Security guidelines need to be developed and enforced on whether and how these printers can be used.
- **Build a cohesive print security architecture.** Piecemeal security solutions rarely deliver consistent and robust security, particularly across a hybrid work environment. Consider an integrated security platform that can support capabilities such as pull printing, remote monitoring, and reporting across the full fleet. Extend print security to content and workflow through the use of content security and data loss prevention (DLP) tools at the application level. Carefully evaluate vendor zero-trust claims and ensure integration with multifactor authentication platforms already used in the organisation. Evaluate whether secure print management solutions can operate in a micro-segmented network.
- **Create, formalise, and continuously review processes to respond to print security incidents.** Organisations must ensure that they are prepared for what are essentially inevitable security incidents and have the right processes in place to deal with the technical, legal, and reputational fallout from such incidents. This requires the organisation to work together to create an embracing set of policies.
- **Continuously monitor, analyse, and report.** A lack of cohesive monitoring and reporting will lead to breaches that are unseen, with longer-term impacts and costs greater than if the incident had been seen and managed earlier. Ensure that print data is integrated with other data from existing security devices, such as security information and event management (SIEM) devices, and analysed to show what has been happening, what is happening now, and what may happen in the future. Ensure that such systems cover as much of the overall platform as possible, and use the insights gained to work on plugging holes in your organisation's security on an ongoing basis.

Vendor profile: Sharp

Quocirca opinion

Sharp is positioned as a leader in Quocirca's assessment of the print security market in 2024. The company has developed a strong print security proposition across its hardware and services portfolio, supported by a rigorous approach to compliance and ongoing partnership with Bitdefender.

Over the last year, Sharp has been building awareness of its consultative security approach and layered security offering, which aligns with the NIST Framework, among European SMBs. The company continues to support businesses in navigating the threat landscape by aligning with the NIS2 Directive, which came into force in 2023. NIS2 builds on an existing legal framework to keep up with digitisation and the evolving cybersecurity threat landscape by setting a minimum standard of service for security, regardless of business.

Sharp has a global partnership with Bitdefender, integrating Bitdefender's anti-malware technology into its latest A3 and A4 business MFPs. This protects against known and unknown malware, including viruses, trojans, worms, ransomware, advanced persistent threats, zero-day threats, spyware, and more. The Bitdefender anti-malware engine performs real-time scanning of all input and output data from the devices, alerting users, IT, or security teams when threats are detected.

Sharp has also invested in delivering training packages to its internal direct sales and resellers on the topic of security and its new security offerings via a new online training platform. Other initiatives in this area include piloting cloud-based cybersecurity training as a service from European cybersecurity training organisation Nimblr with its Nordics team. This will be rolled out across Europe during 2024.

Sharp was also the first OEM to build a native Microsoft Teams connector for its latest MFPs, which enables users to securely access, share, scan, and print data from Microsoft Teams, Google, and SharePoint channels – without any additional software. Single sign-on also provides secure access to public cloud services from the device's control panel. Sharp also offers secure cloud print management. Synappx Cloud Print, its cloud print management solution, is also secure by design and supports zero-trust environments.

Across its IT services offering, Sharp provides a range of cybersecurity services, including user awareness training, incident response, and data recovery, designed to help protect customers' systems and sensitive data. Other services include a security audit, end-point security, cyber essentials accreditation, back-up, and disaster recovery.

Sharp particularly stands out for its strong credentials in the IT security space. Sharp UK is in the top 1% of Microsoft partners globally and has achieved both ISO 27001 and Cyber Essentials Plus Certifications. Sharp has achieved the latter in the UK, UK, Benelux, Nordics, Spain, Italy and Switzerland. Sharp views independent verification of its commitment to and capabilities in security as a priority, and its continued investment in information security is a key differentiator.

Of particular note is Sharp's capabilities in IT – particularly within the SMB market. The company gained decades of experience in providing IT support with the acquisition of two IT services companies – Complete I.T. in the UK and IT Point in Switzerland. This places it in a strong position to capture new revenue opportunities within its direct business, as well as support its channel partners in building their expertise in security.

Leveraging this acquired expertise and building on its heritage in delivering security-centric MPS engagements, Sharp launched a new turnkey IT security subscription service called Complete Print Security (CPS) in late 2023. At launch, this print security-as-a-service approach was a unique proposition in the market. The move positions Sharp to become a leader in print security for SMBs and opens up new revenue potential within its direct arm and the potential to extend the offering to its channel partners.

Security offerings

Robust embedded security features

New product launches in the past 12 months have included security enhancements such as the integration of wireless LAN connectivity to ensure secure wireless usage without compromising security protocols, as well as remote firmware management. A Trusted Platform Module (TPM), standard for some models and optional for others, provides a more secure experience for users by storing hard drive encryption keys on a separate piece

of hardware. SSL Certificate Validation automatically checks that all third-party servers communicating with devices are safe to prevent any unauthorised attempts to access information.

Advanced SIEM integration

Sharp printers and MFPs include a suite of advanced Security Information and Event Management (SIEM) features designed to protect information and documents from physical and cybersecurity threats. In addition to Bitdefender anti-malware monitoring, access control, intrusion detection, and self-healing firmware are standard features across the range, and security updates are provided automatically from the cloud.

Enhanced security services

Sharp's Smart Security Service, available individually or as part of the CPS service, is designed to help customers understand threats and benefit from on-device protection tailored to their individual needs. This offering ensures that Sharp MFPs are preconfigured and delivered secure 'out of the box'. After assessing a customer's environment, Sharp security experts develop a unique security configuration for all devices that match an organisation's exact requirements by activating any number of over 200 security settings.

The new security-as-a-service CPS offering is a fully managed service that combines remote device security monitoring, auditing, and management with a secure pull-print capability. Sharp monitors a customer's MFP fleet 24x7x365 using a SIEM system, enabling it to immediately identify and mitigate attempts at unauthorised access, system changes or other security events.

The CPS offering aligns with the NIST cybersecurity principles of Identify, Protect, Detect, Respond, Recover. It combines a number of its existing services and solutions, such as Smart Security, Sharp Remote Device Manager (SRDM), and Sharp Job Accounting II (JAII) with ConnectWise 24x7x365 SIEM monitoring to detect any potential cyber threats.

Strengths and opportunities

Strengths

- **Scalable offerings for the SMB market.** Sharp has a mature presence in the SMB sector, and its offerings have been customised specifically, with flexible packaged offerings, to meet the varying needs of this diverse market.
- **Robust hardware-security features.** Sharp MFPs and printers have an extensive range of built-in security features, with optional integration with Bitdefender malware technology.
- **Enhanced channel enablement through CPS.** As the channel is a key route to market for Sharp, extending its security services offering to its channel partners is key to helping them develop differentiated security-led propositions.
- **Strong IT services credentials.** In the UK in particular, Sharp has carved out a strong IT services offering that positions it well to offer integrated security offices for both the print and IT infrastructure.

Opportunities

- **Develop globally consistent messaging.** Building on its established brand recognition, Sharp can solidify its position as a leader in IT security. The company's proven track record across many European countries demonstrates a deep understanding of the current threat landscape and the ability to deliver robust security solutions. By sharing this expertise across other regions, Sharp can create more globally consistent messaging and propositions around security.

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. 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.

Usage rights

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