Print Security Landscape, 2024

Mitigating the print infrastructure as a threat vector

Print security trends in the US and Europe
Vendor Excerpt: Ricoh
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: Ricoh

Quocirca opinion

Quocirca positions Ricoh as a leader in its assessment of the print security market in 2024. Ricoh offers a broad, security-centric portfolio of products and services encompassing device, data, and document security. Beyond embedded hardware-security features, Ricoh has built deep expertise in cybersecurity. Depending on the region, Ricoh offers tailored cybersecurity services that provide risk and readiness assessments and help customers detect, monitor, and remediate security incidents.

Multi-layered security approach

Ricoh harnesses embedded device-level features alongside an array of solutions and services to target three fundamental aspects of the print and document infrastructure – product and application security, infrastructure security, and compliance with industry standards such as Common Criteria, NIST, and FIPS 140-2. Ricoh has enhanced the security of its solutions and services with end-to-end encryption (with PKI), TPM2.0, TLS1.3, AES 256, and robust encryption standards.

The company also prioritises zero-trust security principles. Its print and document management solutions include features such as strong authentication, security policy enforcement, micro-segmentation, automation, data classification, and protection. This comprehensive approach ensures customers benefit from a robust defence-in-depth strategy.

Real-time device monitoring

At the beginning of 2024, Ricoh USA introduced the IoT Command Center, an all-in-one device-agnostic platform that enables real-time problem detection, resolution, and actionable insights from connected devices. Key features and capabilities include device status reporting and monitoring, remote device configuration, and remote device control.

Broad IT services offerings

Ricoh's offering includes a wide range of IT services and solutions, from firewalls and pen testing to identity management, designed to facilitate seamless and secure digitalisation. The company also offers security consultancy and managed services that complement its device and solution security layers to optimise document, data, device, and information security. In the UK, for example, Ricoh's Managed Cybersecurity services offer vendor-agnostic security assessments, compliance audit, ransomware audit, and penetration testing to enable customers to understand and manage security vulnerabilities. Ricoh also offers managed security services in the US, which help monitor, protect, and remediate security threats.

Ricoh has acquired 20 IT services and cybersecurity companies in the past three years, a move that has enabled it to significantly expand its expertise in cyber and data security. This, combined with strong partnerships with industry leaders in security such as CISCO, BullWall, Microsoft, Trend Micro, VEEAM, Carbonite and SentinelOne, places the company in a strong position to address diverse market needs.

Centres of Excellence

The company has also created a growing number of Centres of Excellence in EMEA, where teams incubate new and evolving technologies such as IoT, cybersecurity, and blockchain. Additionally, Ricoh's CDP cyber AIOps capability, which can detect and respond to cyber threats regardless of whether the threat affects a single device or an entire network and features extended security capabilities, such as digital device fingerprinting and threat hunting, is a key differentiator.

In the US, Ricoh has been planning, executing, and training its internal software development and engineering teams to adopt industry-standard DevSecOps practices to improve collaboration, speed up secure software development, and standardise secure coding practices to improve the quality, time, and cost of software delivery.

Ricoh is a good choice for organisations looking to protect information across the document lifecycle, as well as those looking for a single provider that can manage security across the print and IT infrastructure. Ricoh's

offerings are somewhat fragmented by region and channel, so organisations will need to evaluate how integrated Ricoh's print security and cybersecurity service offerings are in their region.

Security offerings

Robust hardware security

Ricoh's print devices are designed and manufactured with end-to-end security protection and the latest security features, including improved privileged account control, the latest Transport Layer Security (TLS1.3), support for the latest standard of security chip TPM (TPM2.0), multifactor authentication, and integration with multiple identity providers.

Secure cloud-based solutions

Proprietary Ricoh solutions and partner offerings enable customers to leverage the agility and innovation of cloud technology while maintaining robust security throughout the print and document environment. Additionally, Ricoh provides secure print-routing options, including offline direct print, cloud secure print, client PC secure print, and edge printing with gateway integration, further enhancing security and flexibility in print management.

AI/ML analytics through Ricoh's IoT Command Center

This provides device- and vendor-agnostic monitoring, traffic data analysis, AI/ML analytics (predictive and anomaly detection) with auto-remediation, end-to-end security monitoring, automated compliance auditing, and change tracking.

Print security vulnerabilities and remediation

Ricoh offers device-agnostic offerings for print security vulnerabilities and remediation. Security specialists help customers build a comprehensive security strategy that is assessed, evaluated, and retested before disaster strikes. For example, Ricoh's Print Security Services are offered by dedicated, highly trained resources rather than shared services organisations. Its approach, based on governance, risk, and compliance best practices, quickly identifies vulnerabilities for security breaches, gaps that can result in cyberattacks, and other internal technology exposures before they impact a customer's business.

Security services

Ricoh security services cover employee training and awareness, cloud security, security filtering, end-point protection, post-breach detection and response, and back-up solutions.

@Remote enables a secure connection for devices to provide full status and service alerts, which is used as part of the Ricoh managed services to monitor devices. Ricoh's vulnerability service scans Ricoh print devices connected to @remote and the solutions installed on the servers to provide detailed reports on vulnerabilities and prevent risks to the environment. Ricoh also uses comprehensive fleet management tools – Streamline NX and CloudStream – to monitor and report on devices, including services such as automatic updates, advanced monitoring and reporting, policy enforcement, and remediation.

Strengths and opportunities

Strengths

- **Global reach.** Ricoh's global services team provides standardised, consistent end-to-end solutions in approximately 200 countries and territories around the world.
- **Comprehensive security-led offerings across the hardware and solutions portfolio.** Ricoh has a strong heritage in managing and optimising multivendor fleets for organisations with stringent security requirements. Its professional and IT services capabilities enable it to deliver robust, customised services tailored to the varied security needs of customers.
- **Mature IT services offering and expertise through acquisition.** This has enabled Ricoh to develop deep expertise in cybersecurity, which sets it apart from some traditional competitors in the market.

Opportunities

- **Articulate a cohesive security service offering.** Currently, Ricoh's security offerings are fragmented across different groups, leading to some inconsistency in approach by region. Global customers should evaluate local capabilities, as these may vary by region.
- **Develop a stronger channel-led security programme.** Ricoh relies on a strong channel network to deliver products and services to its SMB customers. Supporting channel partners with IT-centric security tools such as audits and assessments will enable channel partners to strongly differentiate themselves in the market.

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.