

Print Security Landscape, 2024

Mitigating the print infrastructure as a threat vector



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

Executive summary 2

Key findings 3

Buyer recommendations 5

Vendor profile: Lexmark..... 6

About Quocirca 9

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: Lexmark

Quocirca opinion

Lexmark is positioned as a leader in Quocirca's assessment of the Print Security Landscape in 2024. Over the past year, it has enhanced its security-led hardware portfolio, with its new flagship A3 platform supporting extensive built-in security features. In June 2023, Lexmark refreshed the global messaging around its secure-by-design approach, creating a fresh narrative around its robust security story to educate and inform. The company also expanded its approach to include four pillars – products, solutions, services, and standards – and created an updated security guide and new assets and articles, which are accessible on a dedicated web page.

Secure by design

Lexmark's long-established secure-by-design approach ensures security is embedded in all its products. This encompasses core device security, device and data hardening, and security solutions and services to build in features designed to fit customers' varied security risk profiles. All Lexmark hardware, software, and firmware are designed using the security principles outlined in its Secure Software Development Lifecycle (SSDL). Additionally, devices can track security-related events and device setting changes and be configured to export the Security Audit Log information to a SIEM (Security Information and Event Management), such as Splunk, using industry-standard syslog protocols.

Enhanced security services

Recent developments include a new Security Services programme launched in January 2023 in North America and EMEA and November 2023 in Australia and New Zealand, with other geographies to follow. This provides a comprehensive approach to device security, vulnerability remediation, and a security-focused device management service. Its assessment practice is implemented by a team of security experts who use a variety of internally developed, industry-standard tools. Additionally, the company has partnered with IT security firms to provide a more complete and comprehensive security consulting service. It plans to further expand this service to deliver full IT and network assessment services that extend beyond the print environment.

Customisation through technology ownership

A strong differentiator for Lexmark is technology ownership across hardware, firmware, and software, which enables it to quickly assess and address customer-specific security needs. Lexmark's advanced device management and conformance tools, on-device runtime and firmware protections, and security assessments and analytics services support zero-trust architectures.

Lexmark was the first print vendor to secure ISO 20243 supply chain security certification for the entire printing device, including cartridges, supplies, and integrated solutions. The company was also the first OEM to certify devices to the new Common Criteria HCD cPP. All products released from early 2023 comply with the standard's new requirements.

Expanded partnerships

Lexmark has continued to enhance its print security posture through partnerships with companies including Elatec, HID Global, innerActiv, Upland, Tungsten Automation (previously Kofax), Vasion, Pharos, and Ringdale.

Lexmark's broad security-centric hardware and solutions portfolio is a good fit for organisations using managed print services (MPS) that are looking to drive further transformation around the security of their print infrastructure. In particular, organisations that are looking to standardise their print environment across both A4 and A3 devices and move to secure cloud print management should evaluate Lexmark.

Lexmark's strong credentials in secure cloud print infrastructure management, along with content security and secure capture solutions, can also help organisations mitigate wider risks associated with paper dependencies. Lexmark's security services may vary by region, so customers need to assess the availability of the more advanced services in their market.

Security offerings

Secure-by-design products

Lexmark printers and MFPs include several out-of-the-box secure features such as secure OS start-up and verification, Trusted Platform Module, memory and storage protections, firmware protections, fax and network separation, and TLS 1.3 encryption. Other configurable security features include role-based authentication, Active Directory, card authentication, out-of-service erase, device and settings access, audit logs, and certificate management.

PrintCryption

The Lexmark PrintCryption solution protects sensitive information as the print job is encrypted at the workstation and decrypted on the network print device. It is ideal for businesses handling highly confidential information. This level of printing security enables better compliance and supports multiple levels of AES encryption.

Secure fleet management

Lexmark security management solutions allow administrators to manage fleets quickly and easily while ensuring devices remain in compliance with the organisation's security posture. Device remote management security features allow authorised personnel to configure the device for network access to keep unauthorised users from altering the device's configuration.

Markvision Enterprise

Markvision Enterprise is a key component of Lexmark's secure-by-design approach, engineered to ensure optimum security for every print device on the network. With Markvision Enterprise, businesses can manage both device configuration and security policies in a single, easy-to-use solution. Markvision Enterprise itself can also be monitored by a SIEM solution.

Security services

Lexmark security services are designed to identify, categorise, and mitigate security risk in MPS engagements through three service components – security consulting, assessment, and configuration management. Security consulting helps customers identify and address general print security, and security assessments identify risks, vulnerabilities, and security improvements specific to Lexmark devices. With its configuration management service, Lexmark implements customer-approved recommendations generated during the security assessment. Using a broad set of cloud and premise-based device management capabilities, Lexmark support teams deploy firmware updates, monitor and enforce secure device configurations, and report on conformance levels and activity.

Lexmark Cloud Fleet Management (CFM)

Lexmark devices with embedded connections to CFM communicate securely to the cloud, requiring no local software to be installed and no ports or firewall exceptions to be made. CFM allows device firmware to be easily updated and customers' unique security policies to be easily applied to every device in the fleet.

Strengths and opportunities

Strengths

- **Secure-by-design approach.** Security is an integral design and engineering goal embedded in all Lexmark products and services. Its holistic, systematic approach to security encompasses the device, the fleet, and the whole network infrastructure.
- **Technology ownership.** Lexmark owns its core technology across services, solutions, software, hardware, and firmware, reducing the risk of security holes between different platforms and technologies.
- **Proven industry expertise.** Lexmark has an established presence in regulated industry, meeting stringent government and industry standards and certifications including Common Criteria and FIPS.
- **Security-centric cloud services.** LCS removes infrastructure from the physical environment to the cloud, and delivers scalability while maintaining the same levels of security, control, and performance.

- **Data Loss Prevention (DLP) capabilities.** Lexmark Secure Document Monitor (LSDM), available worldwide, captures user data and content from every document that is printed, scanned, or faxed directly from the device for better, more immediate end-point monitoring.

Opportunities

- **Expand IT-centric partnerships.** Broadening its security consulting services with IT partners would enable Lexmark to deliver full IT and network security assessment services beyond the print environment scope.
- **Enhance channel propositions.** Lexmark's new channel security propositions and training will enable it to build further channel engagement. Flexible and simple channel-led security packaged services will help its channel partners expand their security-led offerings.

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.

Disclaimer:

© Copyright 2024, Quocirca. All rights reserved. No part of this document may be reproduced, distributed in any form, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission from Quocirca. The information contained in this report is for general guidance on matters of interest only. Please note, due to rounding, numbers presented throughout this report may not add up precisely to the totals provided and percentages may not precisely reflect the absolute figures. The information in this report is provided with the understanding that the authors and publishers are not engaged in rendering legal or other professional advice and services. Quocirca is not responsible for any errors, omissions or inaccuracies, or for the results obtained from the use of this report. All information in this report is provided 'as is', with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this report, and without warranty of any kind, express or implied. In no event will Quocirca, its related partnerships or corporations, or its partners, agents or employees be liable to you or anyone else for any decision made or action taken in reliance on this report or for any consequential, special or similar damages, even if advised of the possibility of such damages. Your access and use of this publication are governed by our terms and conditions. Permission is required for quoting any information in this report. Please see our [Citation Policy](#) for further details.