The Print Security Landscape, 2023

Securing the print infrastructure amidst a growing threat landscape

Print security trends in the US and Europe

May 2023

QUOCIRCA

Executive summary

Quocirca's Global Print Security Landscape 2023 report reveals that organisations face ongoing challenges in securing print infrastructure. Home printing continues to cause security concerns, with employee shadow purchasing making it harder to control document security. Print-related data breaches remain prevalent, with 61% of respondents reporting at least one data loss in the last 12 months, rising to 67% amongst midmarket organisations. This is leading to lower confidence, particularly among SMBs, in the security of print infrastructure.

Notably, the research reveals a strong disconnect between the perceptions and attitudes to print security amongst chief information officers (CIOs) and chief information security officers (CISOs). Expectations for security spend growth in the coming 12 months are similar, with 84% of CIOs and 81% of CISOs expecting their print security spend to increase. Only 28% of CISOs believe it has become harder to keep up with print security challenges, compared to 50% of CIOs. Similarly, only 45% of CISOs are very or somewhat concerned about the risks of unsecured printers, compared to 72% of CIOs. This chasm between CIOs and CISOs means the two individuals responsible for the overall technical security of the print environment when serving the business are not seeing things in the same light – and this has ramifications for the business itself.

Fortunately, print security leaders are mitigating risks. As shown by Quocirca's Print Security Maturity Index, organisations classed as leaders, which have implemented a range of technology and policy measures, are seeing lower levels of data loss and have higher confidence in the security of their print infrastructure. For print manufacturers, MPS providers, and the rest of the print channel, bridging this gap between the two security camps is a must. However, this cannot be done simply – it will require a two-pronged approach to bring the two parties closer together, as well as ensuring the business itself is more aware of the security issues around print.

Therefore, print manufacturers and channel partners must strengthen their security propositions for organisations of all sizes to help customers mitigate risk in the new era of hybrid work. Becoming a trusted advisor and provider of print security solutions that fit with an organisation's existing security environment is key. Ensuring data and information flow, along with device and output security, will create new revenue capabilities for the print channel.

The Global Print Security Landscape 2023 study is based on the views of 507 IT decision-makers (ITDMs) in the US and Europe. Respondents include 20% from the UK, 20% from France, 20% from Germany, and 40% from the US. In terms of organisation size, 24% represent small and medium-sized businesses (SMBs) (250 to 499 employees), 26% are from mid-size organisations (500 to 999 employees), and 50% are from large enterprises (1,000+ employees). Respondents are drawn from a range of verticals, including business and professional services, finance, industrials, public sector, and retail.

The study also includes the print security vendor landscape, which features Quocirca's assessment of service offerings from major print manufacturers.

The following vendors participated in this study: Brother, Canon, Epson, HP, Kyocera, Konica Minolta, Lexmark, Ricoh, and Xerox.

Key findings

- **Cybersecurity incidents continue to rise.** Overall, 42% of organisations report an IT security breach in the past year, rising to 55% among mid-market organisations and dropping to 36% amongst large enterprises, along with 51% in the finance sector, dropping to 32% in the public sector. The highest incidence across all organisations is malware, with phishing highest in the mid-market. Security breaches increased for 61% of organisations in the past year, rising to 70% in the US and 66% in business and professional services. On average, 27% of IT security incidents were related to paper documents.
- **Reliance on printing creates a need for effective print security.** Despite rapid digitisation over the course of the pandemic, 70% remain dependent on print today, rising to 72% in large organisations. A majority (80%) have changed the composition of their printer fleet over the last two years, rising to 88% in the mid-market. Overall, 79% expect to increase their print security spend in the next year, rising to 86% in the US and 85% in business and professional services and retail.
- **Print security is lower on the security agenda than other elements of IT infrastructure.** Cloud or hybrid application platforms, email, public networks, and traditional end points are seen as top security risks. Employer-owned home printers come in as the seventh top security risk (21%), ahead of the office print environment (20%). Notably, there is a disparity between CIOs and CISOs. Just 18% of CIOs consider office printing a key security risk compared to 30% of CISOs.
- **Organisations are taking different approaches to managing the security of their print infrastructure.** While 31% indicate they use an MPS provider, over half (54%) indicate that they use a managed security services provider (MSSP) to manage both print and IT security. This rises to 58% amongst smaller organisations (249–499 employees).
- **Organisations are finding it harder to keep up with print security demands.** Overall, 39% say it is becoming harder, rising to 50% in the midmarket (500–999 employees). The top challenge is keeping print management software up to date (35%), protecting sensitive and confidential documents from being printed (34%), and securing printing in the remote/home environment (31%). Hardware security is a key concern for SMBs (29%), and highest in the finance and industrial sectors (31%) and for CISO respondents (38%).
- **Organisations using MPS or that are classified as print security leaders are more confident in the security of their print infrastructure.** The visibility and control provided by an MPS appears to ease the security burden for users. While overall, only 19% of respondents are completely confident in the security of their print infrastructure, this rises to 26% amongst organisations using MPS. Overall, a further 50% say they are mostly confident. This reflects the growing complexity and challenges associated with securing both devices and documents across a hybrid workplace.
- **In the past 12 months, 61% of organisations have experienced data losses due to unsecure printing practices.** This is a fall from 68% in our 2022 study. Mid-market organisations are more likely to report one or more data losses (67%) than large organisations (57%) and the public sector (49%). On average, the cost of a print-related data breach is £743K. Beyond the financial loss, the top impact of a data breach is the lost time in addressing the breach and the impact on business continuity (30%). Vulnerabilities around home printing, such as home workers not disposing of confidential information securely, was cited as a top factor contributing to data losses.
- **Quocirca's Print Security Maturity Index reveals that only 27% of the organisations studied can be classed as Print Security Leaders**, meaning they have implemented six or more security measures. The number of leaders rises to 31% in the US and falls to 18% in Germany, which also has the highest number of laggards (29%). Print Security 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. When compared by vertical, business and professional services have the largest percentage of leaders (37%), with the public sector having the least (18%).
- **Less than one-third (32%) are very satisfied with their print supplier's security capabilities.** This rises to 50% amongst US organisations and drops to 17% in Germany. Those using an MPS have far higher satisfaction levels (39% are very satisfied) than those not currently using an MPS or with no plans to use one (23%). Print security leaders – those that have adopted a range of measures, including security assessments, pull printing, and formal print security policies, are most likely to report higher satisfaction levels – 53% of leaders are very satisfied, compared to 27% of followers and only 15% of laggards.

Table of Contents

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 2023, 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.