The Print Security Landscape, 2022

Securing the remote and hybrid workforce

Report Excerpt: Konica Minolta

January 2022

QUOCIRCA

Executive summary

Quocirca's Global Print Security Landscape 2022 report reveals that many organisations are struggling to keep up with print security demands in today's hybrid work environment. Home printing is creating new security concerns, exacerbated by shadow purchasing of devices. SMBs and mid-size organisations are finding it harder to keep up with print security challenges leading to a higher incidence of print-related data loss. This is leading to a lower confidence, particularly among SMBs, in the security of their print infrastructure. However, in Quocirca's Print Security Maturity Index, those organisations classed as leaders that 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. 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.

The study is based on the views of 531 IT Decision Makers (ITDMs) in the US and Europe. 23% of the respondents were from SMBs (250 to 499 employees), 29% from mid-size organisations (500 to 999 employees) and 47% from large enterprises (1,000+ employees).

Key findings

- **Remote working is here to stay and is creating an expanded threat landscape.** Pre-pandemic approaches to securing the print environment focused around a primarily static, office-based workforce now need to move to supporting workers who spend some time in the office, and some in the home environment. On average, 44% of employees are expected to work remotely as offices fully reopen. Hybrid work creates significant security challenges for IT teams to manage as the exploitable attack surface increases. The proliferation of shadow IT and unsecured home networks means that organisations need to rethink their security posture around the print environment.
- **IT security remains the top investment priority over the next 12 months.** 53% of respondents say it is one of their highest three priorities. MPS (managed print services) are second in importance (41%) followed by managed IT services (38%) and cloud services (35%). 70% of organisations expect to increase their print security spend over the next 12 months, with only 11% expecting a decrease.
- **A reliance on printing creates a need for effective print security.** Despite rapid digitisation over the course of the pandemic, many organisations remain reliant on printing. Printing will remain critical or very important for 64% of organisations in the next 12 months. 44% anticipate that office print volumes will increase, and 41% that home print volumes will do likewise. Printers and networked MFPs pose a security risk not only in terms of printed documents being accessed by unauthorised users, but also as an ingress point to the network if left unprotected.
- **Just a quarter (26%) feel completely confident that their print infrastructure will be secure when offices fully reopen.** Organisations are struggling to keep up with print security demands: more than half (53%) say it has become considerably or somewhat harder to do so. 67% of respondents are concerned about the security risks of home printing, compared to 57% who are concerned about office print security.
- **Print security is lower on the security agenda than other elements of the IT infrastructure.** Top security risks are considered to be cloud or hybrid application platforms, email, public networks and traditional endpoints. Employee-owned home printers come in as the 5th top security risk (24%) ahead of the office print environment (21%). This suggests both a lack of awareness and complacency in not fully appreciating the security vulnerabilities around printing, which remains an integral endpoint in the IT environment.
- **There are marked differences between MPS users and non-MPS users.** Organisations that use an MPS provider foresee much greater growth in print volumes and are most confident in the security of their print environment – despite having a higher awareness of the risks. They are also twice as likely to state

that keeping up with print security challenges has become somewhat or a lot easier. The visibility and control provided by an MPS appears to ease the security burden for users, increase assurance that they can ramp up print volumes if needed, and reduce complacency, therefore lowering the likelihood of being blindsided by a security incident.

- **In the past 12 months, over two thirds (68%) of organisations have experienced data losses due to unsecure printing practices.** This has led to a mean cost per data breach of £631,915. Such quantified financial losses are bad enough for organisations to manage, but they also state many other negative impacts, such as a loss of business continuity and ongoing business disruption after the breach. Customer loss is reported to be the biggest impact for SMBs. Large organisations are less likely to have suffered a print-related data loss, with 36% reporting no breaches compared to 24% of SMBs. The public sector is the most affected vertical. Vulnerabilities around home printers were cited as the top reasons for data loss – such as home workers not disposing of confidential information securely, and interception of documents stored in the home printer environment.

- **Quocirca's Print Security Maturity Index reveals that only 18% of the organisations can be classed as Print Security Leaders**, meaning they have implemented six or more security measures. The number of leaders rises to 22% in the US and falls to 12% in France, which also has the highest number of laggards (37%). Print Security Leaders are likely to spend a higher amount on print security, experience fewer data losses, and report higher levels of confidence in the security of their print environment. When compared by vertical, finance has the largest percentage of leaders (23%).

- **Less than a third (28%) of ITDMs are very satisfied with their print supplier's security capabilities.** This drops to 20% in the public sector. US organisations are most satisfied, with those in Germany least happy. ITDMs who use an MPS have far higher satisfaction levels (42% are very satisfied) than those who don't (20%).

- **Most ITDMs turn to managed security service providers (MSSPs) for print security advice.** MSSPs are the primary source of security guidance for 35% of organisations overall, rising to 40% in the US. Just 18% of ITDMs overall would turn to an MPS provider for print security guidance, while 21% would consult a print manufacturer. This points to an opportunity for MPS providers and channel partners to collaborate more closely with MSSPs.

- **CIOs and CISOs differ in their views on the future of print, and their handling of security challenges relating to the hybrid print environment.** CISOs are more bullish, with 53% and 58% respectively expecting a rise in office and home print volumes, compared to 42% and 40% of CIOs. Notably, CIOs (32%) and CISOs (33%) show the most concern around home printing compared to other IT respondents, ranking it as their second top security risk. CIOs also seem to be finding it harder than CISOs to keep up with print security challenges – 61% stated that they were finding it considerably or somewhat harder, compared to only 44% of CISOs, where 29% also stated that they were finding it somewhat or a lot easier.

Vendor Profile: Konica Minolta

Quocirca opinion

Security is integral to Konica Minolta's Intelligent Connected Workplace portfolio, which encompasses a range of solutions to address the digital transformation needs of businesses of all sizes. Comprehensive security offerings extend beyond embedded device security to encompass document, data and network security. It claims to have a wider range of Common Criteria/ISO 15408 EAL3 standard certified MFPs than any other OEM, and offers standard document protection measures including data encryption, secure deletion, watermark copy protection and PDF signatures. In addition to its hardware-centric focus on security, Konica Minolta has forged global partnerships with HPE, Sophos and Microsoft, to deliver best in class hardware, security and IT solutions via its Workplace Hub business IT solution.

Of particular note are its custom-tailored security services – bizhub SECURE - which have been available since 2011, and additional security layers offered by its bizhub SECURE Platinum and bizhub SECURE Ultimate options. In addition, over the past year, Konica Minolta has been actively shifting its customers to its cloud based secure print management platform. This provides flexible options depending on whether a customer is looking for a fully cloud hosted, hybrid cloud and on-premise infrastructure. The platforms are available both locally and globally.

Notably, this is complemented by one of the broadest ranges of IT services offered by a print manufacturer. With the acquisition of All Covered in 2010, Konica Minolta set the bar high on the integration of managed IT services into a traditional print-centric portfolio. Its broad approach delivers a complete service across cybersecurity, helping businesses to identify, contain and analyse network penetration, including attacks by malware, ransomware or hackers. In the US Konica Minolta provides cyber security assessments. For example, its US cyber security practice provides HIPAA assessments to meet healthcare sector privacy requirements as well as financial assessments for community banks to satisfy PCI compliance requirements.

Quocirca believes that beyond its traditional print security offerings, Konica Minolta's deep expertise across IT services strongly sets it apart from some of its key competitors, particularly in the SME market. An opportunity is for Konica Minolta to build integrated cybersecurity professional services that encompass printing and include in-depth security assessments across a multivendor fleet environment (across home and office devices). By leveraging its mature managed IT services capabilities and IT expertise, Konica Minolta could potentially offer one of the broadest cybersecurity service offerings in the print market.

Key security highlights

Comprehensive hardware security
Konica Minolta devices adhere to a range of security certifications and have undergone penetration testing. For instance, Konica Minolta's bizhub i-Series passed the penetration testing by NTT DATA, an internationally respected IT services provider, and the security division of NTT Ltd. No vulnerabilities were found during the tests performed on the devices. Further, Konica Minolta bizhub multifunctional devices include embedded security features which are enhanced with bizhub SECURE, which provides an extra layer of comprehensive protection.

With this service, Konica Minolta offers a security consultancy service that focuses on the secure integration of their MFPs into the customer's infrastructure. This means that this service includes, on the one hand, the more secure configuration of the MFPs and printers compared to the predefined configuration. Konica Minolta looks at the respective customer environment individually and checks how their devices can be integrated in the existing customer structure (e.g. email server, protocols used) in the best possible way and configures the devices according to the best possible security standards. On the other hand, Konica Minolta also makes a recommendation for a secure environment at the same time (e.g. recommendation for a more secure protocol). In addition, security monitoring for compliance with the defined standards takes place on a permanent basis.

bizhub SECURE helps end-users establish enhanced password protection and hardware security measures. The bizhub SECURE service can be activated on any Konica Minolta bizhub multifunctional device, either on-premises or prior to delivery. Features include encryption of entire HDD/SSD contents, lock down of HDD/SSD and temporary data overwrite and automatic job deletion of any material in electronic folders. bizhub SECURE Platinum and SECURE Ultimate offer further layers of security such as audit logs and periodic device scanning.

bizhub SECURE Ultimate includes BitDefender technology. The optional BitDefender anti-virus extension automatically scans all transmitted and received data for potential malware and viruses in real-time, so it remains protected from external threats. The anti-virus extension notifies the user whenever the MFP faces a potential risk, reports that a virus has been detected and blocks the activated job. In addition to real-time scanning, manual scanning for virus detection can be started as required and scheduled virus scanning enabled according to individual presets. Importantly, this protective functionality works regardless of the application the job is coming from. It also includes connections to cloud or USB and doesn't impact on the MFP's processing power or performance.

Konica Minolta also offers the bizhub SECURE Notifier, ensuring that settings stay as they are and the device remains in a secure state. In the event of an incident, the application sends out a notification and countermeasures can be taken.

Security driven cloud print services

The Konica Minolta Cloud Print Service Portfolio includes multiple options to support and increase customers' security. Data and document security is assured through encryption and use of certified data centres, follow-me authentication, roles-based access controls as well as controlled guest access. To address common concerns around data protection and privacy Konica Minolta minimises data sharing. Only data and metadata which are necessary for the execution of a service are collected and processed by the system and secured with appropriate technologies. The use of TLS technology ensures that data in transit is secure and ISO 27001 accreditation provides independent assurance that systems are designed and operated with cloud-first security principles and that robust processes are in place to build resilience and help avoid potential data security issues.

Advanced remote monitoring services

Konica Minolta Remote Monitoring and Management Services (RMM) offer centralised monitoring and management of the IT infrastructure, including server hardware, storage, Konica Minolta provisioned applications, operating systems and associated network infrastructure. This covers areas such as Back-up and antivirus services; real-time server and application monitoring; End-to-end audit trail for issues identified and any Konica Minolta interventions; Management services and periodic server- and application-specific monitoring services.

Locally in some countries, but globally for its Global Business Sales customers, Konica Minolta offers printer and MFP fleet assessments via device monitoring tools that scan any third-party device that supports the standard printer MIB. The most common global platform in use is SiteAudit by Netaphor. The SiteAudit Security monitor scans network settings and provides a dashboard showing at risk devices based on a network vulnerability scoring system. Real time ratings are based on antiquated settings such as SNMP v1/v2, outdated and deprecated SSL and TLS settings, FTP, SMBv1 etc. Based on the network vulnerability report Konica Minolta provides device hardening recommendations and services to clients. Recommendations include port setting changes, protocol setting changes as well as SNMP configuration updates.

Usually, organisations require security assessments for their entire network and the devices within it – not only for printers. With Konica Minolta's services like Endpoint Protection, Threat Detection and MIDR, Konica Minolta already offers this in some countries and also plans to expand to more countries.

Security products and services portfolio

Hardware

All Konica Minolta Office and Production devices conform to ISO 15408. Products are certified to the latest modern, global Common Criteria standard – The Hardcopy Protection Profile v1.0 - Sponsored by NIST/NIAP in the US, and JISEC/IPA in Japan.

Key features include:

- **Run-time intrusion detection**
    - Bitdefender: to detect and prevent malware intrusion
    - Firmware manipulation prevention: to detect and stop firmware being manipulated
    - SIEM: to analyse/notify intrusion occurring
    - bizhub SECURE Notifier: to detect security policy violation by unauthorised access (Soon with ShieldGuard)
- **Device monitoring.** Fleet RMM: Fleet monitoring and management for a wide range of network and security aspects of devices. The tool provides a device template distribution function, across the fleet. The Fleet RMM tool provides a Scan and Reset function. The system monitors device settings and if it detects that a device does not match the template then it will provide an option to reset it and return it to the original template settings.
- **Secure printing via user authentication.** Devices support password, ID card authentication as well as a biometric finger vein scanner.
- **Account tracking.** Usage can be monitored across the fleet and data applied to ensure compliance and to trace unauthorised access.
- **Access control and security functions.** Offer greater security against threats and can also be used to facilitate better governance and enhanced accountability.
- **Log information.** Enables immediate detection of security breaches, it also supports accounting and cost allocation by user and department.
- **Job Log Utility.** Provides comprehensive electronic tracking logs of user activity.
- **Auto delete function.** Erases data stored on the hard disk after a set period.
- **Password protection of internal HDD.** The read-out of data on the hard disk requires password entry after HDD removal. The password is linked to the device, meaning data is not accessible after the HDD is removed.
- **Content security.** Copy Guard is a copy protection function that prints concealed security watermarks such as "Private" or a date in the background to prevent unauthorised copying and embeds a copy restriction pattern on all printed sheets. If an attempt is made using a device that supports the copy guard function to copy a sheet that has been copy protected, a copy guard pattern is scanned, the copying process is cancelled, and the job is deleted. External print management applications can be programmed to block transmission if the scanned or printed document contains sensitive or confidential information.
- **bizhub.** The *bizhub SECURE* service can be activated on any *Konica Minolta bizhub* multifunctional device, either on-premises or prior to delivery.
- **bizhub SECURE:**
    - Change of admin password
    - Encryption of entire HDD/SSD contents
    - Lock down of HDD/SSD
    - Temporary Data Overwrite
    - Automatic job deletion
- **bizhub SECURE Platinum:**
    - Change the Administrator password
    - Encrypt the entire contents of bizhub hard drive
    - Create a secure alphanumeric password to lock down bizhub hard drive
    - Time bizhub multifunctional device to autodelete any material located in electronic folders
    - Disable non-secure and unwanted services, protocols and ports
    - Enable SSL on the bizhub (self-signed certificate)

  - Enable Network User Authentication and User/ Administrator Account Auto Log Off
  - Enable Audit Logs
- **bizhub SECURE Ultimate:**
  - Change the Administrator password
  - Encrypt the entire contents of bizhub hard drive
  - Create a secure alphanumeric password to lock down bizhub hard drive
  - Time bizhub multifunctional device to autodelete any material located in electronic folders
  - Disable non-secure and unwanted services, protocols and ports
  - Enable SSL on the bizhub (self-signed certificate)
  - Enable Network User Authentication and User/ Administrator Account Auto Log Off
  - Enable Audit Logs
  - Enable real time scanning
  - Set up periodic scanning times

About Quocirca

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

Disclaimer:
This report has been written independently by Quocirca. During the preparation of this report, Quocirca has spoken to a number of suppliers involved in the areas covered. We are grateful for their time and insights.

Quocirca has obtained information from multiple sources in putting together this analysis. These sources include, but are not limited to, the vendors themselves. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in any information supplied.

Although Quocirca has taken what steps it can to ensure that the information provided in this report is true and reflects real market conditions, Quocirca cannot take any responsibility for the ultimate reliability of the details presented. Therefore, Quocirca expressly disclaims all warranties and claims as to the validity of the data presented here, including any and all consequential losses incurred by any organisation or individual taking any action based on such data.

All brand and product names are trademarks or service marks of their respective holders.