quocirca

Business and IT Analysis

Global Print Security Landscape, 2019

A global market perspective on print security, 2019

REPORT EXCERPT

February 2019

The far-reaching financial, legal and reputational implications of a data loss mean that information security is a business imperative. Safeguarding the ever-increasing volumes of valuable corporate data against unauthorised access has become integral to maintaining business operations and adhering to increasingly vigorous data privacy compliance requirements.

For many organisations, their cyber-attack surface area is increasing as connected Internet of Things (IoT) endpoints proliferate. These include both legacy and the new breed of smart printers and multifunction printers (MFPs). Consequently, businesses must take a proactive approach to print security as these print devices can provide an open door to corporate networks. By taking steps to analyse the potential vulnerabilities of print environments, businesses can mitigate risks without compromising productivity.

This report discusses the risks of unsecured printing and recommends best practices for integrating print into an overall information security strategy. It also highlights some of the key offerings by print manufacturers and independent software vendors (ISVs) in the market.

Louella Fernandes
Quocirca
Tel : +44 7786 331924
Email: Louella.Fernandes@Quocirca.com

Contents

quocirca

Executive summary

Data breaches are rarely out of the headlines and compliance pressure, such as the introduction of GDPR, means security remains high on the corporate agenda. Cyber threats and data breaches are no longer the sole domain of the IT department, they must be considered at board level as the repercussions are simply too big to ignore. Businesses of all sizes are potentially exposed to reputational, legal and financial losses as the result of cyber attacks. Due to the increasing sophistication of attacks and the emergence of insider threats, businesses face a battleground to balance business productivity with the need for privacy and security. One area of the IT environment which is often overlooked is the print infrastructure. The majority of organisations rely on print to support business-critical processes, meaning it can be the gateway to valuable, confidential and sensitive information.

Quocirca's Print Security 2019 report discusses how print security is becoming a greater concern to businesses with 59% reporting a print-related data loss in the past year. With only 27% classed as print security leaders, it is imperative that businesses become more print security conscious, particularly as they look to close the paper to digital gap in their business processes. This ultimately requires print security to move higher on the C-level agenda.

In response, print manufacturers are elevating awareness of print security risks. Today most offer a diverse range of product offerings encompassing built in hardware security, print security solutions and comprehensive security and risk assessments.

HP has cemented its lead as a visionary for print security, driving industry standards and offering one of the most comprehensive hardware, software and services portfolios. Nevertheless, most competitors are hot on their heels in developing their print security propositions. Leading players are moving to a secure-by-design approach, where security is built in from the ground up on new hardware.

What is setting the leaders apart in the market is their investment in security services such as assessments, monitoring and analytics. As the threat landscape becomes more sophisticated, machine intelligence will be key in being able to respond to or predict threats. This will enable an organisation to enhance their print security posture and mitigate potential risks.

Key findings

- **Businesses remain reliant on printing.** Print will continue to play an on-going role in the business processes of most US and European organisations. 87% expect print to still be important in two years' time compared to 91% today.

- **The dependence on print creates risk.** Print is considered to be one of the top security risks to any organisation. 66% rank print in their top 5 risks, second only to cloud-based services at 69%.

- **Print security maturity varies.** Organisations vary in their capability to ensure the security of their print environment. In Quocirca's Print Security Matrix, 27% were classed as print security leaders, with 17% as laggards and the rest classed as followers. USA had the most leaders at 36%, UK the least at 18%.

- **Businesses are increasing their print security spend.** On average 11% of IT security spending goes on specific print security measures. 77% say print security spending is increasing.

- **Print related data breaches are frequent and costly.** 11% of all security incidents are print related, equating to an average of nine print-related incidents per year. 59% of these lead to data losses, costing an average of £313,000 per-annum to deal with. Other impacts include lost productivity and revenue.

- **The majority are concerned about malware attacks.** There is a perception gap where security risks are concerned. The top perceived security risk is malware, rated as the highest concern by 70%. However, when it comes to actual incidents, the most likely cause is the accidental actions of internal users, which are involved in 32% of incidents.

- **The use of a managed print service (MPS) leads to improved print security.** Overall 62% of organisations are using an MPS to gain access to print management and security skills which are often lacking in-house. This figure rises to 76% for print security leaders (as measured by Quocirca's index) compared with just 44% for the laggards.

- **Most organisations have conducted a print security assessment.** Overall, 70% have carried out an assessment, although only 18% have conducted these in-house. For the rest they are conducted by third parties such as MPS providers or managed security service providers (MSSP).

- **The use of print-specific security measures varies.** Overall, 51% have a formal print security policy, 48% apply regular firmware updates, 40% use pull printing, 37% use secure mobile printing and 36% third-party device testing.

quocirca

Scope and definitions

This paper examines the security challenges of operating an unmanaged and insecure print infrastructure. It draws on research carried out by Quocirca amongst 250 enterprises in the UK, France, Germany and the US in December 2018. Alongside the primary research, key vendors in the market participated to provide details of their security offerings.

The print security market is characterised broadly as follows:

- **Hardware vendors.** All the major vendors, including Canon, HP, Kyocera, Konica Minolta, Lexmark, Ricoh, Sharp and Xerox offer comprehensive portfolios that include built-in hardware security features, access control software and third-party vendor agnostic pull-printing. Some vendors also offer security assessment services either independently or as part of their MPS offerings.
- **Third-party ISVs.** A range of ISVs offer secure print solutions including (but not limited to) Nuance, EveryonePrint, Papercut, Pharos, Print Audit, Ringdale and Y Soft.
- **Data loss prevention**. Although vendors in this space are not strictly operating in the print security market, Quocirca believes the capabilities they offer to printing documents based on content analysis offers a higher level of security.

The following vendors participated in this study:

- Hardware vendors: Brother, Canon, HP, Lexmark, Ricoh and Xerox.
- Third-party ISVs: EveryonePrint, Ringdale, Y Soft.

Each vendor was requested to complete a written submission detailing its strategy, capabilities and customer references to capture key facts and figures.

The following definitions are used through the course of this report:

- **MFP:** an MFP (multi-function printer, or sometimes product or peripheral), multifunctional, all-in-one (AIO), or multifunction device (MFD) combines print, copy, scan and fax functionality. MFPs offer advanced features such as scan-to-email, scan-to-network destinations and are often based on an embedded software platform. This allows software developers to build integrated solutions for MFP devices.
- **Pull Printing:** pull printing functionality allows a document to be released only upon user authentication using methods such as proximity/magnetic/smart cards or biometric recognition. Users submit jobs to designated pull-printing queues and jobs are moved from the pull-printing queue to the dedicated print queue. Requiring the user's presence at the printer in order to collect print jobs reduces print waste without imposing accounting limits.
- **Managed Print Service (MPS):** This is the outsourcing of the print infrastructure through a process of assessment, optimisation and ongoing management. MPS comes in many forms, from entry level packages that wrap hardware, service and supplies based on a cost-per-page contract to more sophisticated enterprise engagements that include document workflow, change and continuous management, based on stringent service level agreements.

The print security threat

The continuing digitisation of business processes may prompt expectations of the demise of paper and printing in the workplace. Such views are misplaced. Quocirca's research consistently shows that businesses remain dependent on print to support business activities. However, the way print is being used, managed and integrated into business processes is changing. Alongside this are growing concerns about the security threats that arise from continued reliance on printing. There are two broad areas of threats: those posed by the documents that print devices produce; and the vulnerability of the print infrastructure itself.

Paper output from printers often includes confidential documents, which can end up in the wrong hands at any point during their lifecycle, for example early on - if left in output trays, or later - if disposed of carelessly. Documents are also a privacy and compliance problem. Instances of documents being sent to the wrong recipient are all too common, especially in sectors like healthcare, where there is still plenty of paper correspondence. Documents destined for printing are also a risk before ink and paper ever meet, as most print devices contain local disk drives to store and queue output.

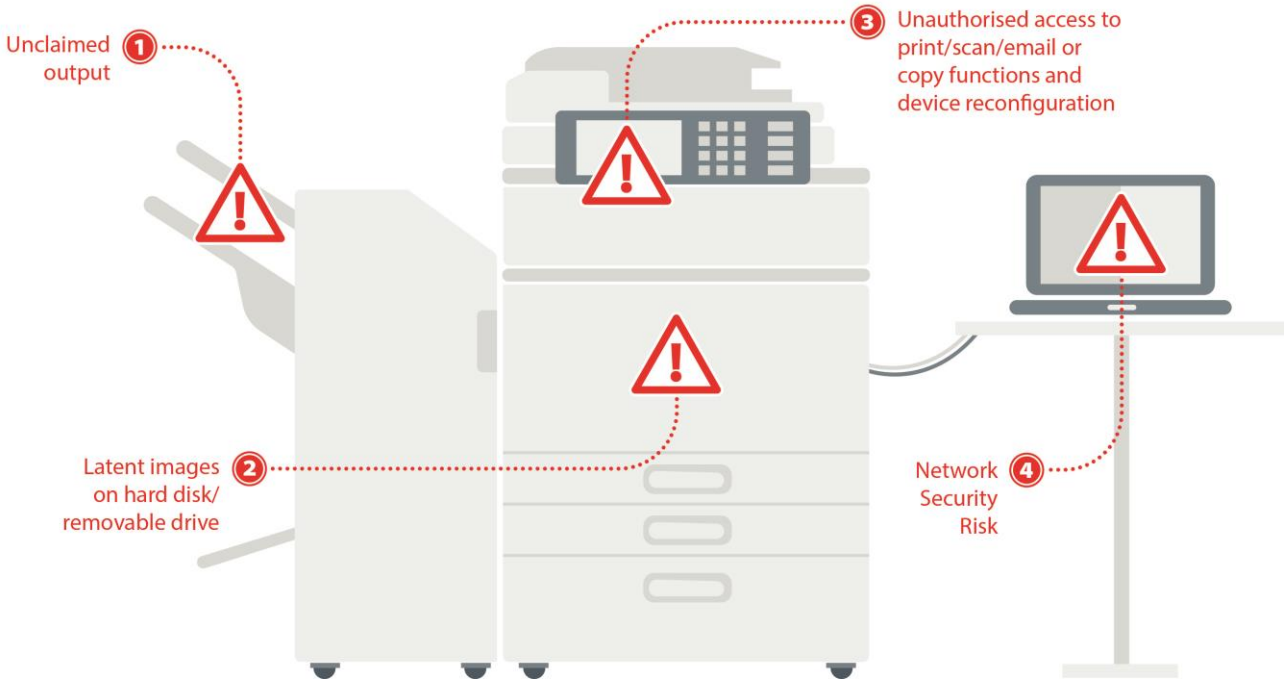
Although such stored output is one temptation for print infrastructure hackers, it is unlikely to be the primary target. The security threat from print devices is like that of any network-attached device, all of which are increasingly referred to as IoT (Internet of Things) devices. There are three main IoT related threats:

1. The device may be used as a network ingress point. In many cases printers may be poorly secured, firmware does not get updated and access credentials are easily compromised, for example because defaults are never changed or because access is shared between multiple administrators.
2. Second, sabotaging IoT devices may be an easy way to target and disrupt an organisation's business processes.
3. Thirdly, IoT devices, including printers, may be recruited to botnets which are then used to perpetrate distributed-denial-of-service (DDOS) and other attacks that can benefit from access to lots of *free* processing power.

Quocirca's Print Security 2019 market report reveals the key market trends impacting print security in today's ever-expanding threat landscape. It highlights the concerns and levels of confidence around print security and the ways these are being addressed. The report covers both European and US-based businesses ranging in size from 250 employees to many tens of thousands across a range of sectors (see appendix 1).

Print security vulnerabilities

Despite the move to digital communications, many businesses still rely on printing to support key business processes. MFPs are prevalent across businesses of all sizes and as such they are a critical network endpoint that must also be secured. Even behind a firewall, an MFP can be a front door to the network leading to the potential for compromising corporate or customer data.



MFP Security Vulnerabilities

The potential risks are illustrated in the diagram above. These include:

1. **Unclaimed output.** Confidential or sensitive information can be collected inadvertently or intentionally by an unauthorised recipient.
2. **Latent images on hard disk.** All documents whether they are printed, copied, scanned, faxed or stored are processed within the hard disk drive. This can present a risk not only if the device is hacked, but also at the end of life when potentially hard disk data could be recovered.
3. **Unauthorised access to MFP functions.** If MFP settings and controls are not secure, it is possible to alter and reroute print jobs, open saved copies of documents, or reset the printer to its factory defaults. Potential hackers could also attack print devices to either intercept or download copies of scanned-in documents, emails and user access credentials.
4. **Network security risk.** Jobs sent to the MFP for printing typically sit unprotected on the server queue. At this stage, the printing queue can be paused and files copied and the queue restarted. In the worst case, a user from the outside can obtain confidential information, or place malware on the device. Open network ports also present a security risk enabling the MFP to be hacked remotely via an internet connection. Printers can therefore be prime targets of denial-of-service (DoS) attacks. Further, if data transmitted to a printer is unencrypted, hackers are potentially able to access this data.

Print reliance provokes security concerns

Asked to consider the importance of print 91% of respondents indicated it is important today (2018). This only drops to 87% when asked to consider the position in two years' time (2020). There was some variation: 94% of public sector organisations believe print will still be important in 2020, whilst only 84% of industrial organisations say this will be the case; 93% of larger businesses agree, compared to 80% of smaller ones. In no country or sector did the figure drop below 80% either for today or in two years' time.

At one level businesses recognise the ongoing need for print, but at another they reveal concerns about the risks associated with this dependence on print. When asked to consider the risks that may lead to security problems and data breaches in general, the print infrastructure ranks second behind public cloud services (Figure 1), with 66% ranking it in their top five risks compared to 69% for the latter. In professional services, finance and retail, print is the top concern; this is also the case in France and the USA. Whatever the reality of the risks, the perception that print is a security problem has always needed to be addressed and this will remain the case. However, whilst most are aware of the risks associated with print infrastructure, there is plenty of scope for increasing the confidence that these risks can be mitigated.

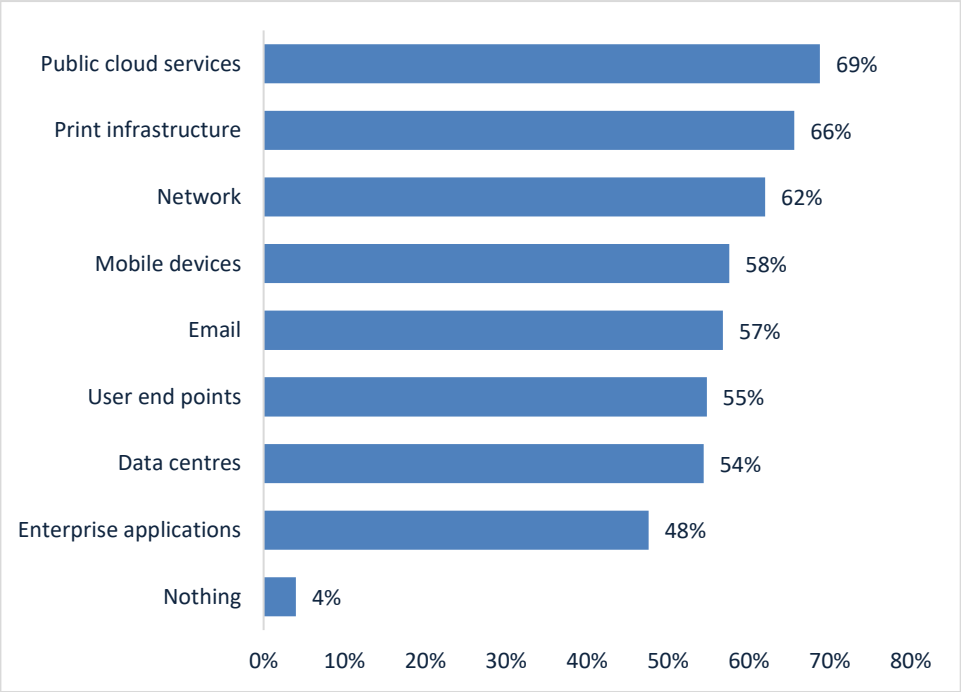


Figure 1: Rating of IT risks that may lead to security breaches (% ranking as a top 5 concern)

Note: Full report with detailed research findings is available from Quocirca. Please contact Louella.Fernandes@quocirca.com for further details.

Future outlook

Print security needs to be a strategic board-level issue, moving beyond the domain of the IT manager to the CISO and CIO. The continued high level of print-related data breaches demonstrates that businesses need to do more to protect their devices, network and data. An organisation's information security strategy can only be as strong as its weakest link. The expanding IoT security threat landscape means that the challenge of print security is moving beyond protecting the printed page. As IoT devices, smart MFPs are susceptible to the growing threat of DDoS attacks as well as providing an open gateway to the corporate network.

The threat to the print environment can be mitigated, but only a minority of organisations are currently succeeding. Those that are doing best, achieving the highest print security maturity scores, are some of the most prolific users of print. However, the threats exist for all organisations and print security laggards and followers can learn from the leaders.

Manufacturers must embed security into the architecture and interfaces of their products, in order to protect the lifecycle of devices, from inception to retirement. This means future proofing devices as they become more powerful, store more data and increase in functionality. MFPs should have the ability to run security updates automatically, validate new software and lock features where appropriate.

Devices should have the intelligence to identify a security event and communicate such events and remediate as appropriate. This means that print management functionality must be integrated in broader IT security management tools to provide remote warning notifications for errors or unusual activity.

Ultimately, print security demands a comprehensive approach that includes education, policy and technology. In today's compliance-driven environment, where the cost of a single data breach can run into millions, organisations must proactively embrace this challenge. By using the appropriate level of security for their business needs, an organisation can ensure that its most valuable asset – corporate and customer data – is protected. Managed Print Service providers are well positioned to provide the support and guidance needed. There is no room for complacency, given the far-reaching repercussions – legal, financial and reputational - of print related data losses.

Recommendations for IT decision makers

With businesses continuing to remain reliant on print for the foreseeable future, effective print security that forms an intrinsic part of an overall IT security plan enables the safe deployment of print infrastructure which addresses business objectives while protecting its assets. Print security needs to be firmly on the board agenda, with the risks understood by the CIO as well as the CISO.
Business leaders should consider the following when building a print security strategy:

1. A complete security ecosystem
Given networked MFPs and printers are as connected as any other IT endpoint, and not only process confidential and sensitive information but also generate this as output, print security must be treated as a fundamental element of the broader security strategy. There are multiple layers to print security – encompassing the device, network and the documents/information they produce. This demands a comprehensive risk assessment.

2. Conduct a comprehensive security assessment
The first step is to evaluate the existing fleet to discover potential security vulnerabilities, particularly when a mix of legacy and new devices have been deployed. Such insights provide organisations with visibility into their print environment and can set a foundation for ongoing monitoring of devices once the fleet is optimised and secured. Security assessments can vary widely from basic discovery to full assessments and are offered by most MPS providers.

3. Print security starts with procurement
Devices must be procured with security and remote management in mind. For the most effective control, devices should be based on common interfaces and standardised management tools. Evaluate devices that have built-in security such as intrusion detection, white-listing and syslog data collection with links to established SIEM tools.

4. Strengthen the processes for access credentials and vulnerability management
One key security challenge is the ability to easily upgrade firmware and patch devices as soon as vulnerability is publicised. Older devices that are not patchable are a particular security risk. Consider automating the deployment of firmware updates.

Access credentials are a weak point for print devices, for example default admin accounts are often left in place. Once installed, default passwords should be changed to unique, complex, strong passwords, as advised by the National Institute of Standards and Technology.

5. Protect sensitive or private jobs while in motion
End-to-end encryption of network traffic ensures secure transfer of print jobs to printers, however, as most printers cache content, locally stored data should also be encrypted. Many regulations require this, for example PCI DSS.

6. Continuously monitor the print environment and make use of analytics
Knowing the current status of devices provides a secure view of the entire print environment. Consider using network monitoring and alerting tools such as ICMP, SNP and Syslog to regularly track devices and fix issues. MFPs generate a wealth of data, for example on authentication and usage. This can be used to identify potential security events and enable fast responses to attacks. If using an MPS provider check if it offers regular compliance reports, which should include data breach monitoring and reporting.

7. User education and training
With many data loss incidents being caused unintentionally by internal users (32% of print security incidents involved the accidental actions of users in the current survey), it is vital that businesses have security training in place to educate employees on the importance of protecting sensitive information and raise awareness of relevant malicious threats. All organisations must better educate and train end users on the potential security risks associated with printing, many MPS providers will offer help with training needs.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With worldwide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

For more information, visit www.quocirca.com.

quocirca