Print security: An imperative in the IoT era

A market perspective on print security, 2017

January 2017

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

Bob Tarzey
Quocirca Ltd
Tel: +44 1753 855794
Email: Bob.Tarzey@Quocirca.com

Contents

EXECUTIVE SUMMARY **3**

SCOPE AND DEFINITIONS **4**

PRINT SECURITY VULNERABILITIES **5**

BUSINESSES MUST BRIDGE THE SECURITY GAP **7**

PRINT SECURITY CONCERNS 7
THE PREVALENCE OF A PRINT DATA LOSS 9

NOT ALL SECURITY ASSESSMENTS ARE EQUAL **12**

PRINT SECURITY BEST PRACTICES **13**

VENDOR PROFILE: HP **14**

QUOCIRCA OPINION 14
SECURITY OFFERINGS OVERVIEW 15

FUTURE OUTLOOK **17**

Executive summary

The evolving IoT security threat

October 2016 saw one of the worst distributed denial-of-service (DDoS) attacks in history, when a strike on DNS provider Dyn took a major part of the internet's DNS infrastructure offline – including Amazon, Twitter, Spotify, Netflix and Reddit. This attack is representative of the increasing complexity of the data security threat, and the rising number of high-profile breaches that are affecting hundreds of millions of users worldwide. Its nature also signals the evolving shape of the threat: the attackers targeted the rapidly growing network of connected devices known as the Internet of Things (IoT).

The number of IoT devices – think vending machines, thermostats, video cameras and networked printers – is estimated to reach anywhere between 20 and 50 billion by 2020. These devices are smart and connected, but they are also vulnerable. IoT devices can be remotely managed, and are able to generate, store and retrieve a wealth of data as well as initiate service or maintenance requests. For hackers and malware looking for a way into a corporate network, unsecured IoT deployments provide the perfect entry point.

IoT devices have already been used to create large-scale botnets – networks of devices infected with self-propagating malware – as well as crippling DDoS attacks. The notorious strike on Dyn leveraged the Mirai botnet, and involved a network of hardware devices including CCTV video cameras and digital video recorders.

The true impact of a data breach

The consequences of any networked device being compromised are far reaching, whether the outcome is downtime or data loss. A data breach can leave a company open to huge fines and legal penalties, and damage its reputation and customer confidence. According to PwC[1] 90% of large and 74% of small UK organisations reported suffering a data breach in 2015, while a 2016 study from the Ponemon Institute[2] reveals the average total cost of a breach to be $3 million, with the average cost per stolen record $158.

In Europe, the penalties for a data breach will become even higher when the new General Data Protection Regulation (GDPR) comes into force in 2018. Companies that handle EU citizens' data will have new obligations in a number of areas – including data subject consent, data anonymisation and breach notification – requiring major operational reform. Regulators will be authorised to issue penalties equal to €10m or 2% of a business's global gross revenue, whichever is greater, for breaches. The UK will be required to comply with the GDPR, whatever the agreed terms of its exit from the EU, as member countries will remain key trading partners.

Implementing strategies to ensure that data on endpoints is protected from theft, loss, digital intrusion or prying eyes is therefore critical to any organisation.

Protecting the weakest link: the multifunction printer (MFP)

With its advanced connectivity and capacity to store large volumes of data, the multifunction printer (MFP) has long been a 'weak link' in the IT infrastructure – one that businesses can no longer afford to be complacent about.

The MFP has brought increased convenience and improved productivity to the office environment. A smart, sophisticated device which runs its own software and services, it has evolved to become an integral document processing hub capable of handling print, copy, fax, scan and email. However, its ability to monitor usage and collect data, as well as network connectivity only increases the potential for exploitation by hackers.

With MFPs often situated in easily accessible locations, if the proper controls are not in place it is all too easy for unauthorised users to get their hands on confidential or sensitive information left in output trays – either intentionally or by accident. In Quocirca's recent survey 61% of large enterprises admitted suffering at least one data breach through insecure printing.

This security gap must be closed. Organisations need to take steps to include effective print security as part of their overall information security strategy. This should encompass a full evaluation of security risks associated with the existing print infrastructure at a hardware, user and document level, the implementation of the technology, and user engagement.

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 200 enterprises with over 1,000 employees in the UK, France, Germany and the US in April 2016. 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, Samsung, Sharp, Ricoh and Toshiba, 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 Nuance, NT-Ware (part of Canon), Pcounter, Pharos, Print Audit, Ringdale, SafeCom 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: HP, Konica Minolta, Lexmark, Ricoh and Xerox.
- Third-party ISVs: Nuance, Ringdale, NT-Ware, 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.

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.

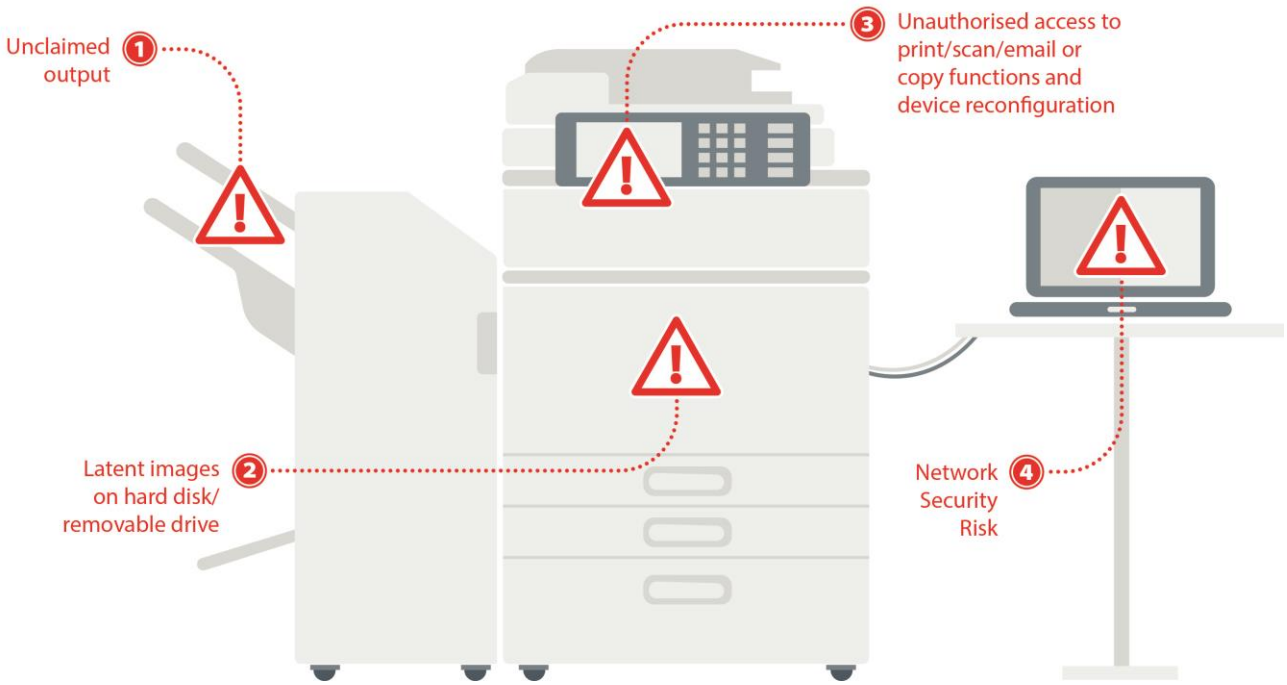

Figure 1. MFP Security Vulnerabilities

The potential risks are illustrated in Figure 1. 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 potential 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.

Printer hacking: A real threat

Hacked printers produce nationalist propaganda

In March 2016, an infamous black hat hacker admitted to hijacking 29,000 printers in several college campuses across the US to remotely print multiple copies of racist and anti-Semitic flyers. Students and staff at universities from Princeton to Washington University at St. Louis to the University of California at Berkeley reported finding the offensive flyers in the output trays of their printers and fax machines. But some individuals outside of college campuses also reported hate mail 'mysteriously' showing up on their printer.

The notorious cyber hacker Andrew Auernheimer, better known as 'Weev,' owned up to the printer attack stating it was 'a brief experiment in printing,' as well as a prank illustrating the risks with the trend towards connected devices known as the Internet of Things. Auerenheimer used a single line of code to scan the internet for unprotected printers that were connected to the web using the open port 9100. He then created a PostScript file containing a flyer advertising a white supremacist news web site. The printers were programmed to automatically print this file format out.

Auernheimer was able to access and commandeer the printers remotely because they were all hooked up to the Internet via open, unsecured connections. He identified more than a million such printers—many of which were on university campuses, which tend to have large public Internet networks—and estimates that he forced 'tens or hundreds of thousands' of them to print his flyer.

This highlights the real threat of hackers being able to host malicious scripts on vulnerable printers. Most printers require port 9100 to be open and this effectively hands over an anonymous FTP server to a hacker.

Businesses must bridge the security gap

Print security concerns

Today, most organisations recognise the risk of operating an insecure print infrastructure. Overall, 72% indicated it is a major concern, with the professional services reporting the highest level of concern (88%) compared to the industrial sector (53%) (Figure 2).

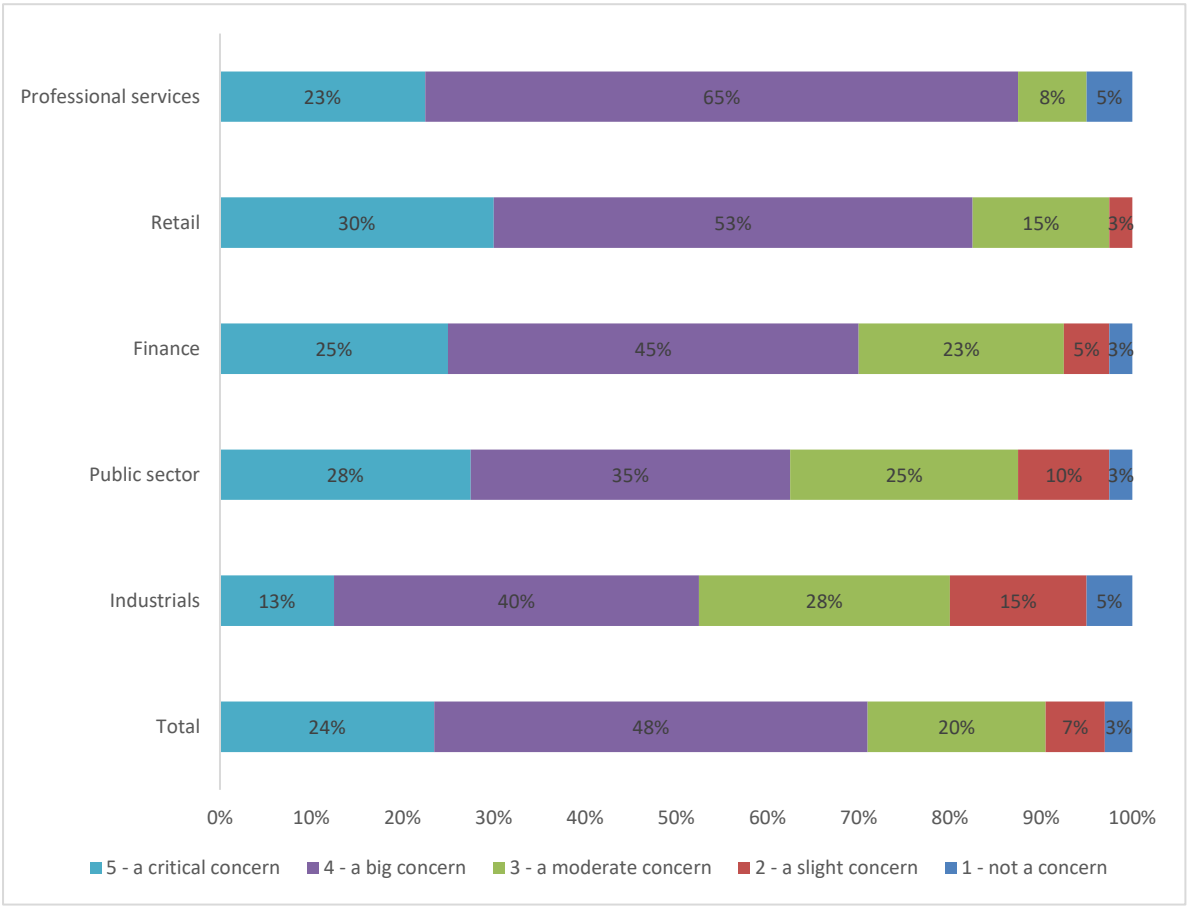

Figure 2. How concerned is your organisation about a data breach, where confidential or sensitive information is compromised through insecure printing practices within your organisation?

Although the majority are concerned across all elements of printing, access to the network via an unsecured MFP was the top concern for 67% of respondents (Figure 3). This reinforces the growing awareness of printers and MFPs as network connected devices and the associated security vulnerability this represents.

The public and industrial sectors are least concerned about MFPs being an entry point to the network (60%) whilst retail and professional services are most concerned (73%).

The retail sector also show a high level of concern around documents being accessed by unauthorised users and 80% cited a lack of audit trails on usage as a top concern. Retail organisations often operate a disparate and distributed print environment. This can make it more challenging to protect and secure, from both a technology and user access perspective.

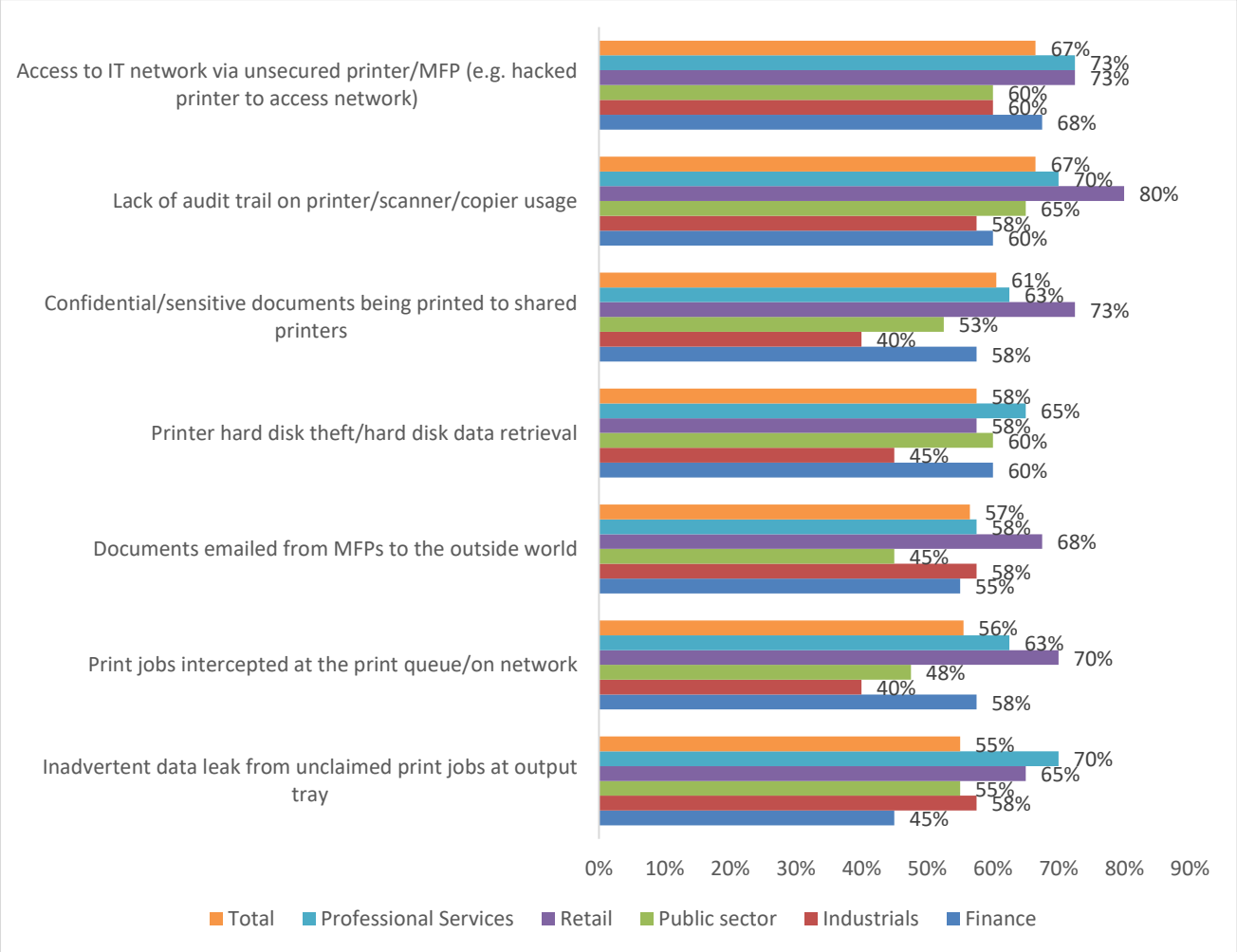

Figure 3. How much of a concern are each of the following threats to print security in your organisation? (Very or extremely concerned)

The prevalence of a print data loss

Data loss through printing is prevalent, even amongst organisations that operate a managed print service. Overall 61% reported at least one data loss in the past year, 51% in organisations with more than 3,000 employees and 68% in organisations with 1,000 – 3,000 employees. For those organisations not using an MPS it is likely that the proportion of breaches is even higher (Figure 4). In fact, in many cases organisations may not be aware of all data loss incidents, meaning that potential data loss could be even higher than what is reported.

Figure 4. Data loss by organisation size (organisations using a managed print service)

Those organisations that are operating a centralised model based on shared MFPs are less likely to have experienced data loss – 38% indicated no data losses compared to 18% of those operating a distributed model of workgroup printers (Figure 5).

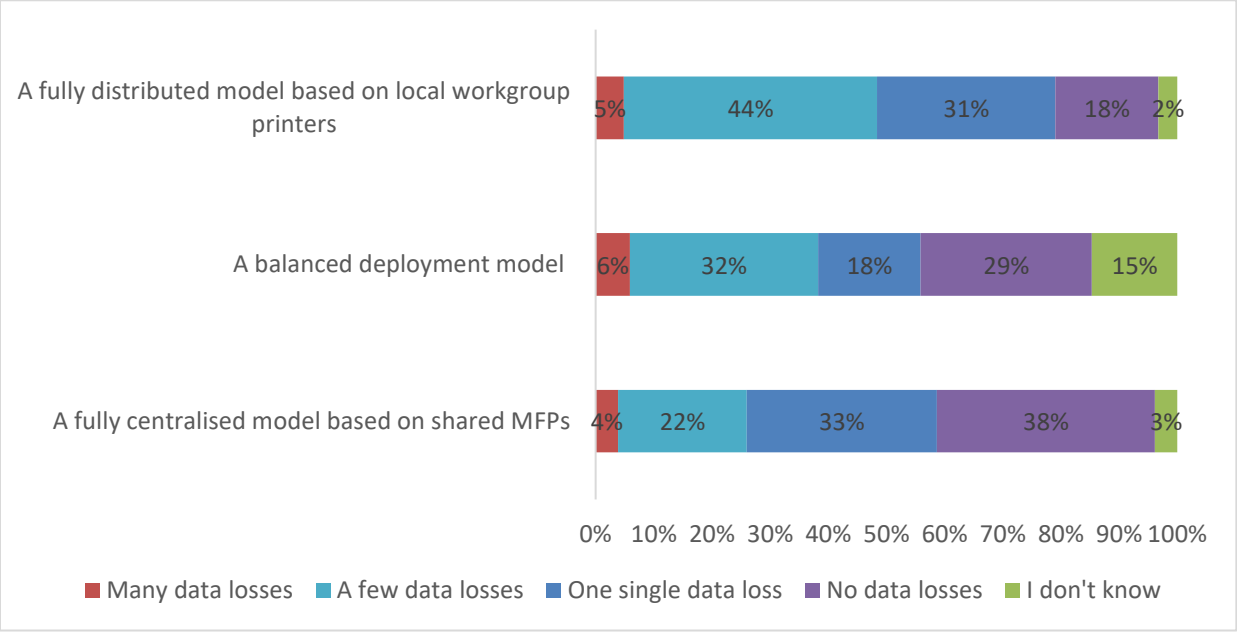

Figure 5. Data loss by print infrastructure model

While 67% of those operating a multivendor fleet reported at least one data loss, this dropped to 41% for those that were operating a standardised fleet (Figure 6).

A standardised environment is always going to be easier to control given that security functionality and tools can be applied consistently to all equipment. And normally, these organisations are further along in their MPS engagements and will have benefited from security assessments. This reflects the benefits – from an IT management and user perspective – of a consistent approach to security that is possible with a single hardware brand.

However, in many organisations, it is typical to find a patchwork of devices from different vendors which in turn require different tools and software platforms. Although a best of breed tool can be used across a mixed fleet to enable secure printing (such as pull printing), there remains a challenge in protecting the vulnerabilities of older or legacy devices which may be more exposed than newer devices with built-in security features against today's threats.

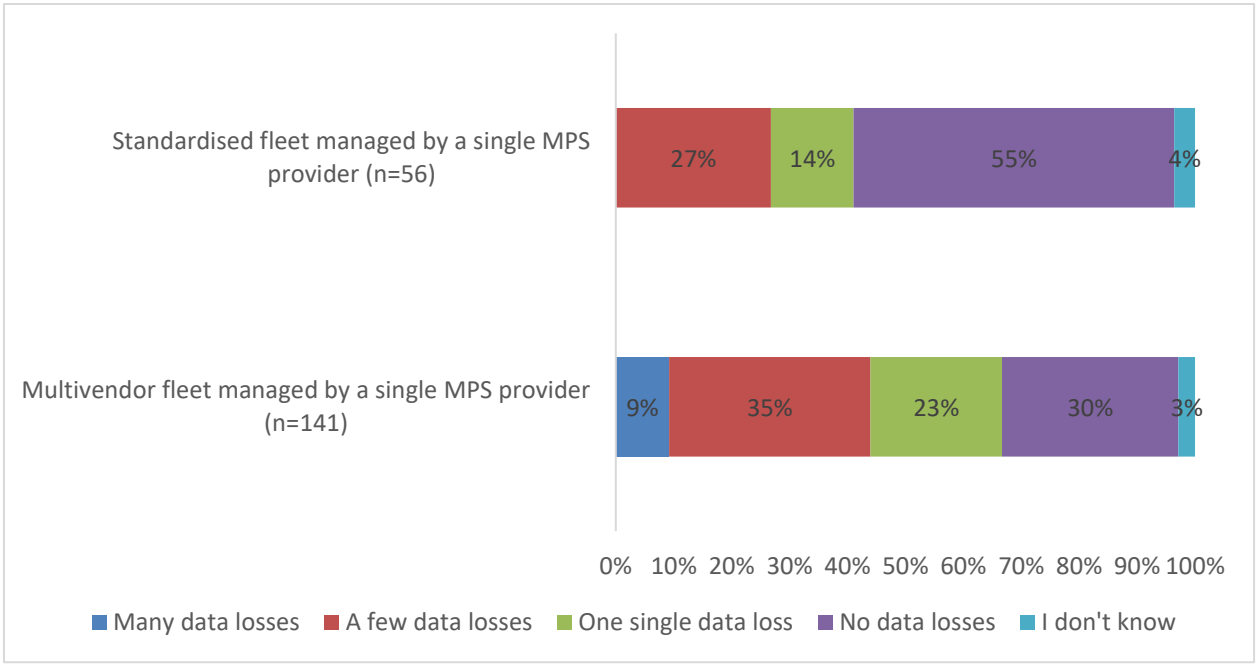

Figure 6. Data loss by fleet type

So, what is the nature of the data loss from a print perspective?

Notably although access to the network was a top concern amongst the majority of respondents, these concerns may be unfounded. Only 18% reported that an unsecured MFP has led to unauthorised access to the network. However, almost half reported that network interception, hard disk theft and unauthorised access of unclaimed output were factors (Figure 7)

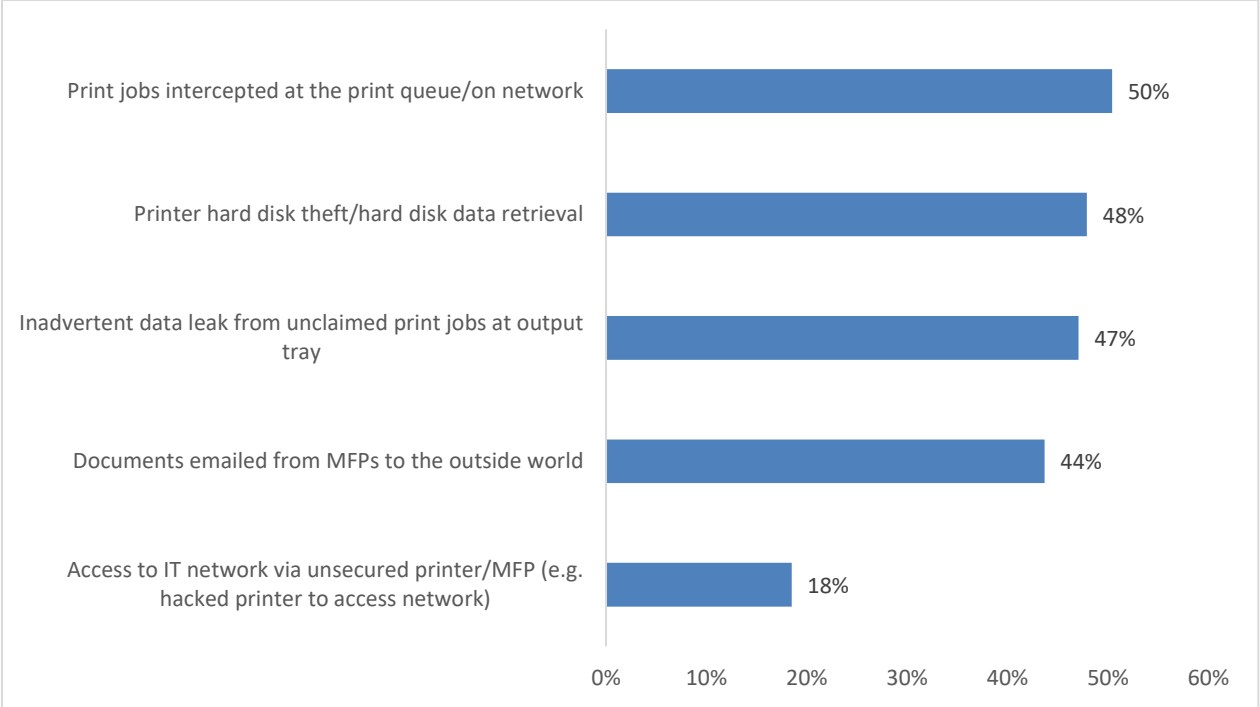

Figure 7. Reasons for data loss

Closing the gap in print security clearly requires a range of measures. Most manufacturers offer a combination of built-in security features – both hardware and proprietary and third-party software tools. The following section outlines suggested best practices dependent on business needs and highlights the offerings from key manufacturers and ISVs in the industry.

Not all security assessments are equal

After cost, security is the second top driver for adoption of a managed print service, indicated by 81% of respondents in Quocirca's recent MPS survey. Consequently many are taking up security assessments as part of their MPS process. Amongst organisations using MPS, the majority have started or completed a security assessment of their print infrastructure (Figure 8). This is more prevalent in the professional services sector where over half (55%) of organisations reported that they completed a security assessment compared to just 20% of public sector respondents.

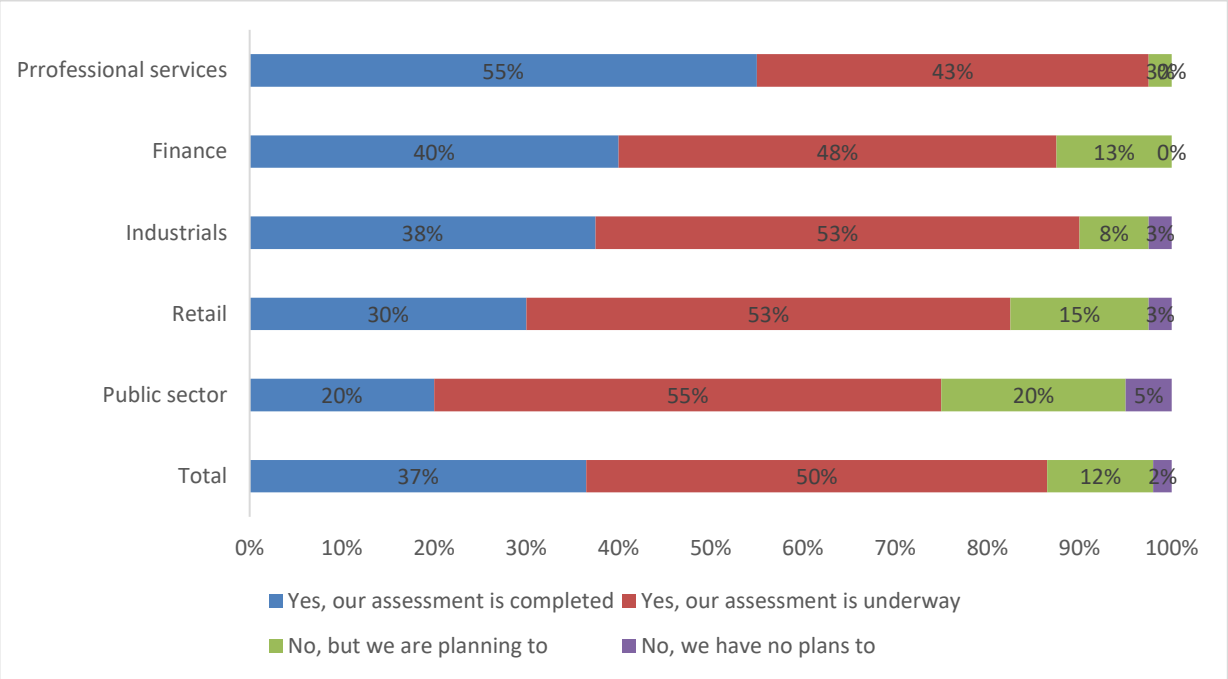

Figure 8. Adoption of security assessment services

Security assessments need to take evaluation across the device, data and the document. Businesses need to ensure that the level of security assessment matches their specific security needs and is conducted by professionals with both print and IT security expertise.

Currently, security assessments are often offered as an optional extension to traditional document assessments. However, Quocirca believes that these should become a standard part of the assessment process and MPS providers should develop KPI security metrics to ensure the effectiveness of security controls. This ultimately requires a diligent and comprehensive security assessment which can typically take several days to complete depending on the size of the infrastructure. However, this time is well spent if it identifies gaps or flaws in print security - ultimately as with any security measures the best defence is a good offence.

Print security best practices

Given the multiple points of vulnerability in the print infrastructure, businesses must employ a layered approach to print security. This requires a combination of activating built-in hardware security features, implementing software tools such as pull printing and educating users on responsible and secure printing practices.

Quocirca recommends that the following measures are taken:

1. **Ensure print devices are part of an overall information security strategy.** Printers are no longer dumb peripherals and must be integrated into an organisation's security policies and procedures.
2. **Adopt a security policy for the entire printer fleet.** Ultimately, in the event of a data breach, an organisation must be able to demonstrate that it has taken measures to protect all networked devices. It only takes one rogue or unsecured device to break an organisation's defences. Many organisations offer a multitude of devices across locations. An organisation should be able to monitor, manage and report on the entire fleet, regardless of model, age or brand.
3. **Secure access to the network.** Like other networked devices, MFPs require controls that limit network access, manage the use of network protocols and ports, and prevent potential viruses and malware. Transmitted data should be encrypted.
4. **Secure the device.** Activate hard disk encryption and data overwrite functionality. Hard disk encryption adds an additional layer of security securing stored data be it actively in use by the device, sitting idle on a device, and/or used by the device in a previous job. To avoid the risk of data being recovered when the MFP is moved or disposed of, data overwrite kits should be employed to remove all scan, print, copy and fax data stored in the hard disk drive.
5. **Secure access.** Implement user authentication to eliminate the risk of unclaimed output being left in printer trays. User authentication, also known as pull printing, ensures documents are only released to the authorised recipient. Authentication through smartcards or biometrics is required before access permission to the printer is given and can be enabled across an enterprise-wide device fleet, a specified printer, or an external authentication server such as Microsoft's Active Directory.
6. **Secure the document.** In addition to access and device controls, digital rights management capabilities can further discourage unauthorised copying or transmission of sensitive or confidential information. This can be achieved by enabling features such as secure watermarking, digital signatures or PDF encryption. Secure watermarking embeds user-defined text only visible when a document is copied; encrypted PDFs can only be accessed by users with correct passwords; and digital signatures help verify a PDF's source and authenticity. Some devices also have enhanced features to detect the type of document or even the content and determine if the user has permission to print.
7. **Ongoing monitoring and management.** To ensure compliance and to trace unauthorised access, organisations need a centralised and flexible way to monitor usage across all print devices. Auditing tools should therefore be able to track usage at the document and user level. This can be achieved by either using MFP audit log data or third-party tools, which provide a full audit trail that logs the identity of each user, the time of use and details of the specific functions that were performed. Businesses operating a diverse mixed-brand fleet should consider vendor-agnostic tools to provide these capabilities. Furthermore, as security threats are constantly evolving, continuous monitoring is essential to establish ongoing governance of the print infrastructure.
8. **Seek expert guidance**. Manufacturers and MPS providers continue to develop and enhance their security offerings. Take advantage of security assessment services which evaluate potential vulnerabilities in the print infrastructure. Note that not all assessments are equal. Ensure that the assessment provider demonstrates the credentials to fully evaluate the security risks across device, data and users. There are also a range of security certifications that are published by the National Institute for Standards and Technology.

Vendor profile: HP

Quocirca opinion

Testament to its long-term investment in print security, HP has the broadest and deepest portfolio of security solutions and services in market. It has created a compelling and scalable proposition that provides a layered security approach for businesses of all sizes. Its strong network and IT heritage has given it access to proven IT security expertise which it has fully leveraged in building its global print security team.

HP is one of the few manufacturers to bring security to the forefront of its print strategy. Security is now tightly integrated with its MPS strategy, encompassing services and solutions that cover basic device security to advanced solutions that address people, process and compliance requirements. HP continues to grow and invest in HP Secure MPS, its security led MPS programme which was launched in 2016.

The major components of HP Secure MPS include HP's enterprise printer portfolio, security software solutions and security services. HP boldly claims that its latest range of Laserjet enterprise printers are "the industry's most secure printers". The unique capabilities offer three technologies designed to thwart an attempted attack and self heal. This includes HP Sure Start which validates the integrity of the BIOS on booting up; white listing which ensures that only authentic and untampered HP code is loaded into memory and run-time intrusion detection which checks for anomalies during complex firmware and memory operations.

After a reboot occurs, HP JetAdvantage Security Manager, a policy-based printer security compliance solution, automatically assesses and, if necessary, remediates device security settings automatically to bring devices into compliance with the organisation's policy. JetAdvantage Security Manager enables IT to establish and maintain security settings such as closing ports, disabling access protocols, auto-erase files and more.

Administrators can be notified of any suspicious print activity via security information and event management (SIEM) tools such as HPE ArcSight or Splunk integration. Notably, HP the only printer manufacturer to offer integration of printer event data with major with such SIEM tools. This is a key competitive advantage for HP, particularly as it brings print security within reach of the traditional IT security tools.

A further differentiator for HP is the depth of its multivendor security services. These include a robust security assessment of the print infrastructure followed by the development and deployment of a robust security plan that spans device, data and document workflows. HP reports that it has already conducted security assessments for 60 customers on a global scale. These services are delivered by credentialed print security advisors and then maintained within a Secure MPS programme. HP is now extending these services to include a new retainer service that provides ongoing monitoring of a security plan; new implementation services and a new governance and compliance service.

HP is certainly ahead of its traditional print competitors with its deep focus on print security, but like its competitors faces the challenges of bringing print security to the attention of the Chief Information Security Officer (CISO). However, by virtue of its dominance and maturity in both the print and IT space HP is uniquely positioned to drive industry standardisation and raise awareness of the risks of operating an unsecured print infrastructure. HP can also leverage its strong consumer brand to communicate the importance of print security in the Internet of Things landscape.

Although it does have a broad portfolio, there are some further opportunities for development. So far, HP has particularly focused on device, data and network security. Although it does partner with TROY to offer high levels of document security for fraud protection, content security is one area where HP lacks broader solutions. To further enhance its print security strategy, HP should seek partnerships not only with traditional information security vendors but also those in the IoT space. This will be particularly important as the IoT permeates the enterprise. With the core services of MPS becoming more commoditised, security solutions and services promise to be a key enabler for building more value in MPS engagements.

HP has now built an extensive set of security services and to avoid complexity will need to develop a modular and flexible approach. This will enable organisations to take a phased approach whilst addressing any concerns about employee productivity being hindered by sophisticated print security measures.

Security offerings overview

FutureSmart technology

HP's enterprise printers are equipped with FutureSmart technology which provides a robust range of hardware security features. This includes:

- **HP Sure Start.** To prevent an attack at the point of start-up, HP is implementing BIOS-level security. This applies the same BIOS security protecting HP's Elite line of PCs since 2013 to new HP LaserJet Enterprise printers. In the event of a compromised BIOS, a hardware protected "golden copy" of the BIOS is loaded to self-heal the device to a secure state.
- **Whitelisting.** This ensures that only HP authentic code and firmware can be installed and loaded onto devices.
- **Run-time Intrusion Detection.** This protects the printer by continuously monitoring memory to identify, detect and highlight potential attacks to Security Information and Event Management (SIEM) tools like ArcSight. The device will automatically reboot flushing memory and bringing it back to a safe state. This technology was developed in partnership with Red Balloon Security, a US based embedded device security company.

HP's latest enterprise printers can also be used with HP's Jet Advantage Security Manager which checks and resets device security settings to maintain compliance with security policies.

To ensure support for older device fleets, HP will retro fit legacy devices, allowing customers to benefit from these security features for devices from 2011. According to HP, with a firmware update, all three features can be enabled on the HP LaserJet Enterprise printers delivered since April 2015. For HP LaserJet Enterprise printers launched since 2011, two of the features, whitelisting and Run-time Intrusion Detection, can be enabled through an HP FutureSmart service pack update.

Solutions and services

- **HP Access Control (HP AC):** This is a server software solution for authentication, authorisation and secure print capabilities. This broad suite of solutions includes secure pull printing, secure authentication, mobile release, job accounting, intelligent print management and intelligent rights management. HP offers a scalable approach comprising HP AC Express, a lower cost solution for HP and selected Xerox, Ricoh and Lexmark devices; and HP AC Enterprise which provides a full suite of HP AC solutions.
- **HP Capture and Route:** A server software solution that enables scanned content to be controlled and tracked.
- **HP's JetAdvantage Security Manager**: HP JetAdvantage Security Manager is a policy-based compliance solution that automates security monitoring and management. Instant-on Security will automatically validate the security settings after a reboot or establish the settings when any new devices are added to the fleet. This includes policy creation and editing features to develop and apply a single corporate security policy across an entire fleet of HP devices. The solution also automates the application of device certificates and automatically restores printers to the company's security policies to new printers added to the network or after a re-boot. HP also offers a modular range of secure print solutions through its HP Access Control portfolio to add layers of authentication, support compliant document workflows (i.e. pull printing), job accounting and add controls on device usage and feature access (i.e. default duplex printing). HP enhanced its global JetAdvantage Security Advisory Services for MPS customers, and continues to apply broader HP security capabilities into MPS-related industry workflow solutions.
- **HP Secure Print Analysis:** a free online tool that allows a client to self-evaluate their print security practices. The tool generates a private checklist of fundamental and advanced printer security actions in five focus areas: device, network data, access control and authentication, monitoring and management, and documents.
- **HP Printing Security Advisory Service:** HP also offers a comprehensive Printing Security Advisory Service, which evaluates an enterprise's current print security position and recommends solutions to address an organisation's print security risk exposure. HP credentialed print security advisors conduct a multi-day workshop with a client's IT and Security staff to evaluate their current end-point security strategies, identify gaps and build a security & compliance plan based on standards and best practices for their industry. New services announced in December 2016 include:
    - A new retainer service that delivers on-going monitoring of an agreed security plan

  - New implementation services using industry best practices
  - New governance and compliance services, which includes device monitoring, remediation and proof of compliance
- **HP and TROY document protection:** HP and TROY document protection uses a host of security solutions and features to protect high-value documents. It offers high levels of security for localised, distributed, and light production workgroup applications. Organisations can capture the full value of secure, distributed, on-demand printing of high-value documents while also lowering costs and maintaining tighter security and control. Designed for government, healthcare, education, legal, and enterprise customers, organizations can use HP and TROY document protection to help them

Future outlook

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.

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 automatic 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.

References

[1] 2015 Information Security Breaches Survey, PwC UK
[2] 2016 Ponemon Cost of Data Breach Study

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.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium-sized vendors, service providers and more specialist firms.

For more information, visit www.quocirca.com.

quocirca