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

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.

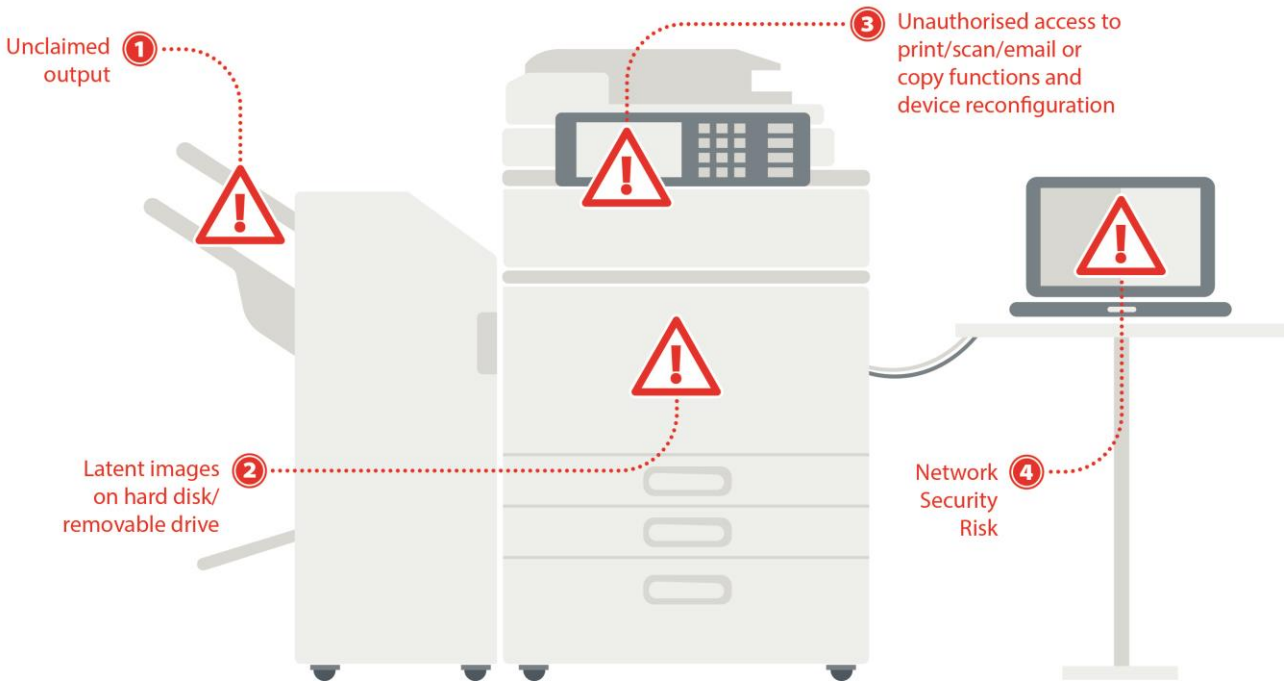

Figure 1. MFP Security Vulnerabilities

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).

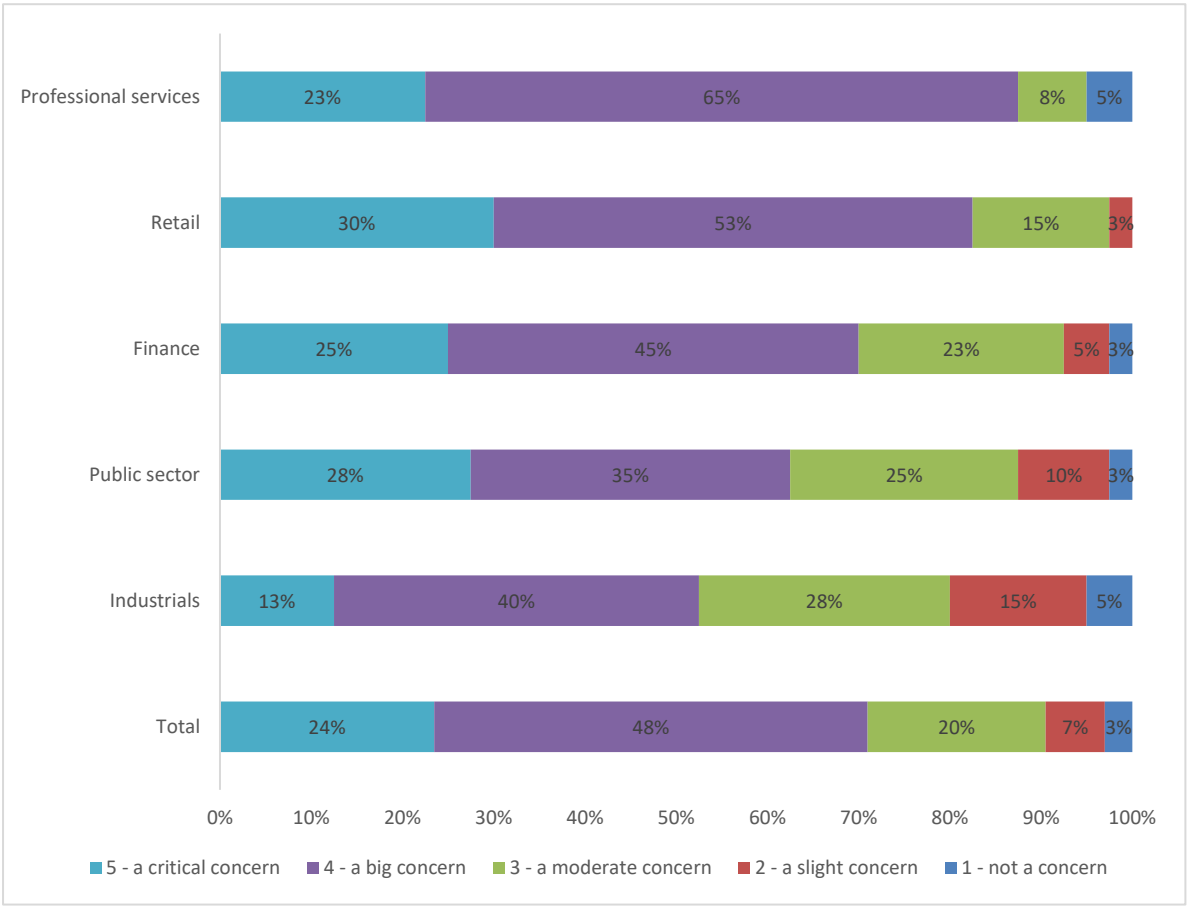

Figure 2. How concerned is your organisation about a data breach, where confidential or sensitive information is compromised through insecure printing practices within your organisation?

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.

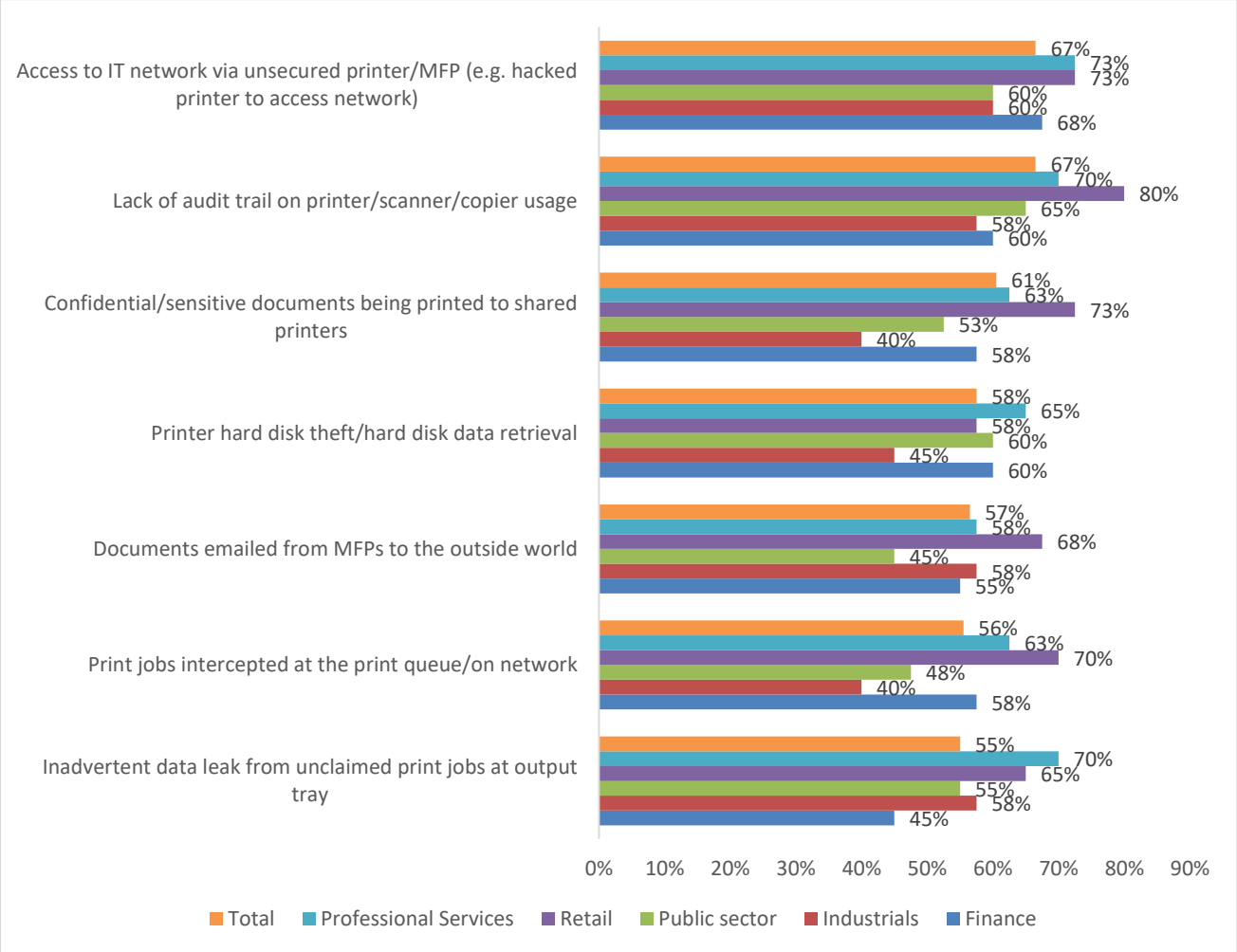

Figure 3. How much of a concern are each of the following threats to print security in your organisation? (Very or extremely concerned)

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).

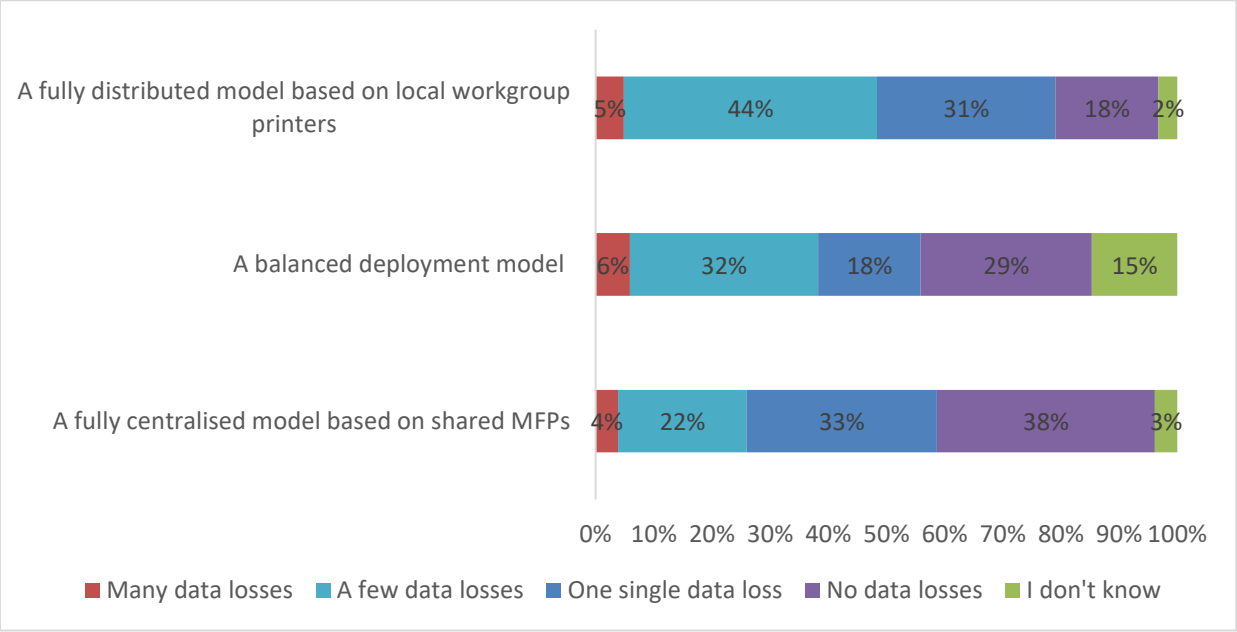

Figure 5. Data loss by print infrastructure model

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.

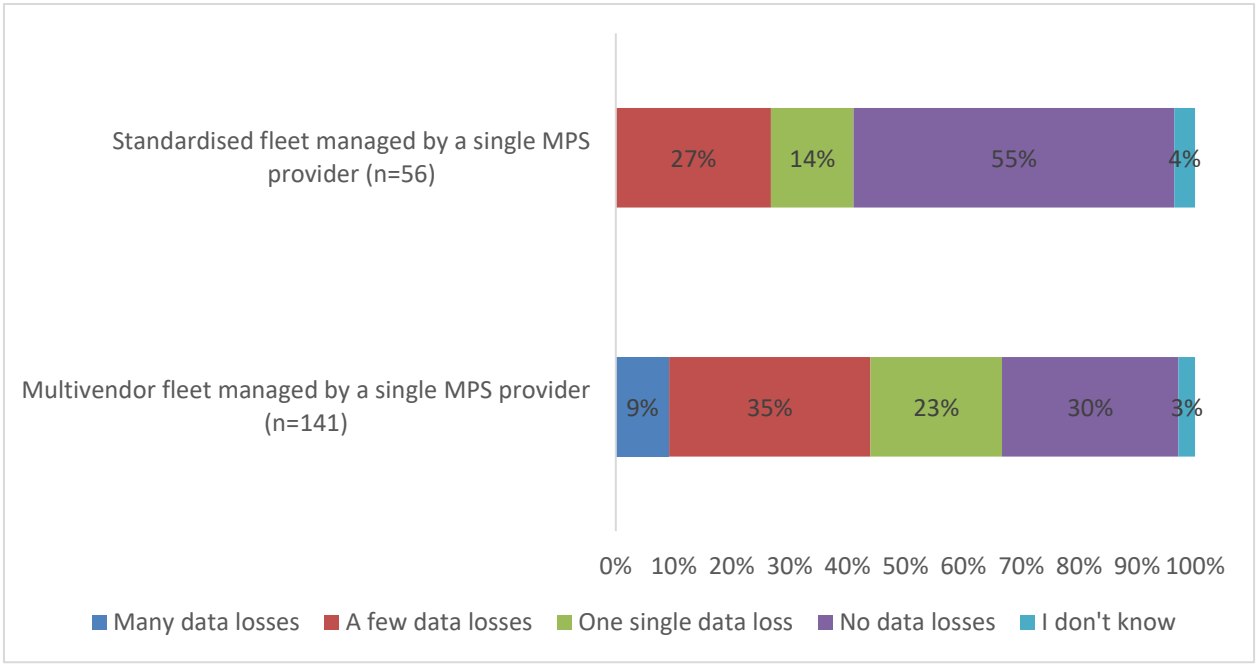

Figure 6. Data loss by fleet type

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)

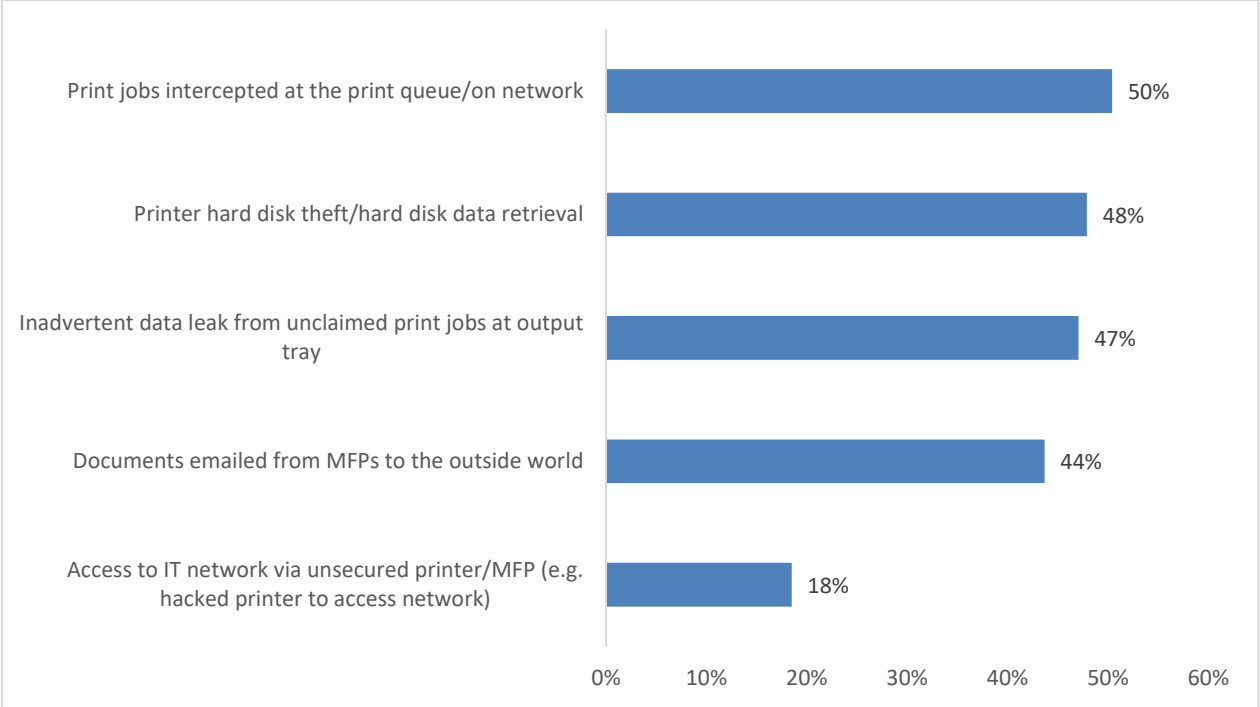

Figure 7. Reasons for data loss

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.

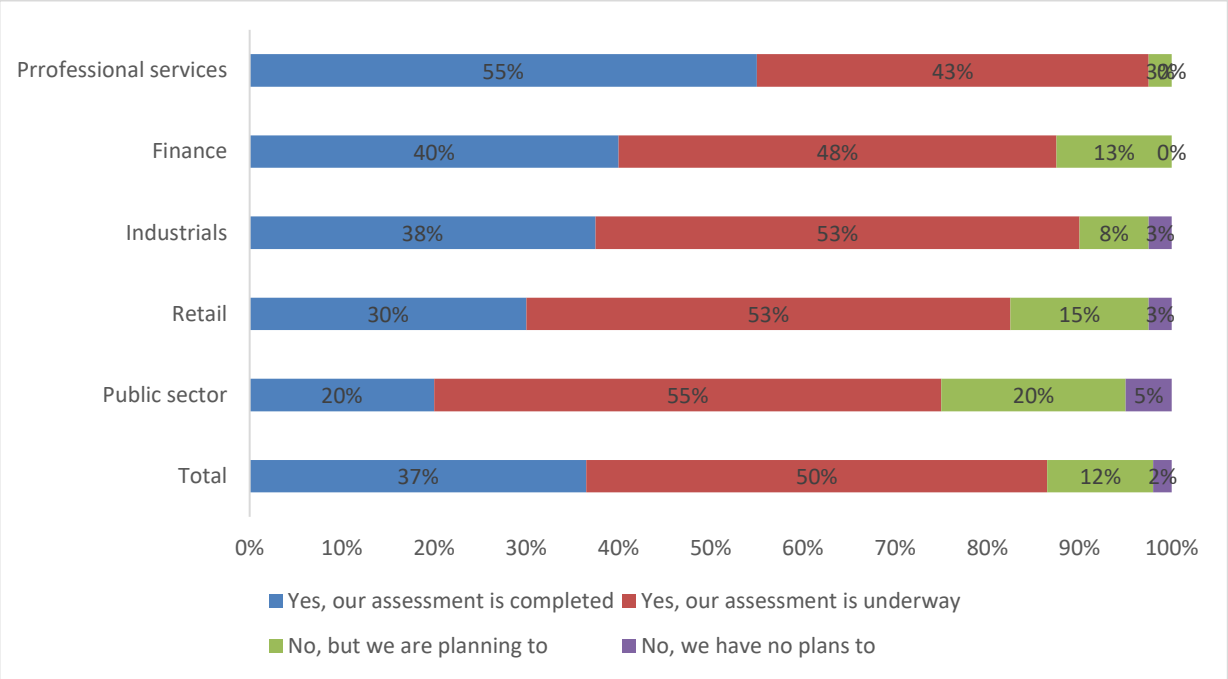

Figure 8. Adoption of security assessment services

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 summary

Manufacturers

HP

Testament to its long-term investment in print security, HP has the broadest and deepest portfolio of security solutions and services in the 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.

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

Konica Minolta

Integrated MFP security technology has been a long-term focus of Konica Minolta and is central to Konica Minolta's Optimized Print Services (OPS) strategy. Konica Minolta devices are certified almost without exception in accordance with the Common Criteria/ISO 15408 EAL3 standard. Rather than certifying optional security kits, Konica Minolta claims to have the widest range of ISO 15408 fully certified MFPs in the market.

Konica Minolta offers a comprehensive range of solutions across access control, data security, network security and scanning security, with functionality varying across device. It also offers a range of document protection measures, such as data encryption, secure deletion, watermark copy protection and PDF signatures.

Responding to the growing concerns around print security, Konica Minolta offers bizhub SECURE which is part of its OPS offering. Targeted at businesses of all sizes, this professional service offers a range of device security options and assists end-users with the setup of enhanced password protection and hardware security measures. Konica Minolta also works with third-party ISVs such as Y Soft SafeQ to provide access control and job tracking.

In addition to Konica Minolta's strong security proposition around its hardware devices, it also has an established IT-Security Competence Centre (CC) that is able to provide a range of IT-Security consultancy to customers, including in relation to its OPS offering. Services include auditing, evaluation, implementation, training and support. The range of services on offer may be particularly beneficial when managing and reporting on the security risks of third-party devices at the initial stages of an engagement where Konica Minolta may often be managing a multivendor fleet.

Konica Minolta should certainly look to leverage its growing capabilities in the IT services space as this will also provide further opportunities for offering integrated print and IT security services. In the US, All Covered already offers a comprehensive suite of managed security services. This is a key differentiator against traditional competitors who do not have a dedicated IT professional services that can potentially take a holistic security-led view of the IT and print infrastructure.

Lexmark

Lexmark takes a holistic approach that focuses on secure remote management, secure network interfaces, secure access, secure data and secure solutions. This includes a range of device, network and user security features. Lexmark provides a broad range of assessments to Enterprise and middle-market customers worldwide. This includes full document, business process, security needs, document security and environmental assessments. Its security and document security assessments provide recommendations on ways to make their output environment more secure with a focus on areas such as secure management, document security, secure user access, data protection, and secure routing.

As part of its MPS engagements, Lexmark offers two types of security assessments – security needs and document security assessments. The security needs assessment provides an evaluation of the customer environment with a specific focus on security and threats associated with malicious user, malware/virus, and remote and local access. The assessment allows Lexmark to develop recommendations to tailor security to meet specific customer needs that carefully balances security requirements without the disruptions to end-user productivity.

Lexmark also offers document security assessments which provide an analysis of how documents are being used with a focus on reducing misuse or theft of information. The assessment includes an in-depth examination of how documents, data and content is being used by individuals so that recommendations can be developed for the implementation of solutions to reduce/eliminate the misuse, loss, and/or theft of information that may be sensitive in nature.

Security is a key consideration in the ongoing monitoring of Lexmark's MPS fleets. Its MPS tools and systems continuously monitor a deployed fleet, providing both security policy control and visibility and alerts to events affecting the fleet.

Ricoh

Ricoh has a strong focus on information security, carrying the global ISO 27001 certificate for information security management. Ricoh works proactively with customers to address security concerns around Information Capital. Information security and governance is integral to its Managed Document Services (MDS) strategy. Its core solutions cover device, user and network security, including user authorisation, systems configuration, network protection and monitoring and auditing.

Print Security Optimisation assessments are included in an MDS engagement, based on customer requirements. These assessments are being enhanced with a new approach to create an optimal state of security around a hardcopy device by understanding threats and vulnerabilities to customers' information assets. This standardised approach encompasses the analysis, optimisation and governance of the state of print security for customers' most valuable information assets. It applies the same model for total cost of ownership (TCO) and sustainability optimisation and is based on the same fundamentals of its MDS strategy - understand, improve, transform, govern and optimise. Ricoh audits the current print environment to create a baseline print security risk which is addressed through Ricoh's

hardware and software portfolio. Through ongoing optimisation, Ricoh ensures the optimised state of security is maintained. The end result is the optimised print infrastructure harmonized with customers' office environment and security policies.

This phased approach also includes its dedicated data cleansing service, launched in 2015. This removes, beyond recovery, any residual information contained on end-of-contract devices and is supported across multiple brands. This turnkey service can be integrated into an organisation's device lifecycle management policy and provides a certified and auditable approach to prove that data has been disposed of securely.

Ricoh's overall information management security proposition is enhanced by its adjacent IT infrastructure and business process services practices. Ricoh offers a range of services within the Managed IT Services space including cloud services, security services and networking services. Ricoh can potentially leverage these services to managed security services and develop a flexible security proposition for the SMB market that covers both the IT and print infrastructure.

Samsung

Security is a key focus for Samsung both in current implementation and future product design. Samsung SmartUX MFPs have all received Common Criteria Certification to level EAL2+ and conform to Samsung's built-in five layer Security Framework, defined as User, Data, Network and Fax, Document and Management Security.

The SmartUX itself has full customisation capability at the user level, enabling features to be hidden or removed for specific user profiles. This capability is also linked to the secure authentication and card reader capability meaning any of Samsung's own or partner secure authentication solutions can enable advanced customisation of the UI.

User security concentrates on protecting the MFP from unauthorised user access through authentication and authorisation control whilst secure data is delivered by built-in functions such as HDD Encryption (AES-256), HDD Image overwrite (up to 9 times) and automatic encryption of scanned and printed data. Network security is ensured by the implementation of mandatory industry standard protocols and these can be opened/closed depending on user preferences. On a hardware level, documents can be secured before print using a driver level pin code as well as being watermarked or stamped with user related data. Usage can be logged to deliver further levels of management security.

As a future development, Samsung will deliver a Smart Security Manager Application. This will offer device protection to a higher level. It will offer LKMA (Load-time Kernel Module Authentication) to prevent modification to OS modules, IMA (Integrity Management Architecture) to stop unauthorised modification of system and executable files and self-testing to detect and notify any anomalies during start-up. These will work in conjunction with Secure Boot, a mechanism that will prevent unauthorised boot loaders and kernels during start-up. This includes the TPM (Trusted Platform Module), a secure dedicated microprocessor designed to secure hardware by the integration of cryptographic keys into devices.

On an application basis, Samsung offers internally developed secure print and scan solutions alongside partnerships with industry leading ISVs. Samsung offers a range of secure print solutions as part of its Business Core 2.01 suite, a flexible portfolio of five device-based and hence 'serverless' solutions aimed at SMBs, supporting up to 10 compatible devices and accommodating up to 500 users.

This includes a range of modules including Secure Login Core Module which supports a variety of authentication types, including ID cards, passwords, proximity cards and personal ID numbers; Printing Security Core which prevents unauthorised access or retrieval of confidential documents; Document WorkFlow Core which delivers document scanning and storage with full audit trail; Cloud Connector Core which delivers secure document storage and retrieval to cloud-based location (SharePoint 365, One Drive etc.) and Usage Tracker which enables IT Management to track device usage and each activity performed on it to provide full non repudiation against any activity.

In addition to the above, Samsung Fleet Admin Pro has the capability to have standard configuration sets defined for each device or device type on the network. The settings on each device are then monitored in real time and any changes reported back to the network administrator. This is used by clients to ensure that key network settings, user access rights and application controls are maintained at all times. Fleet Admin Pro is also used to manage firmware

deployment and features a full capability to deploy only approved firmware and drivers to each device or queue from a common library.

Close partnerships with Nuance, Y Soft and Ubiquitech enable Samsung to deliver enterprise level industry standard print and workflow management solutions on a global basis. For other referenced ISV solutions, Samsung operates a robust validation and verification process so that end-users can be assured that solutions conform to the Security Framework set down by Samsung and will not introduce security vulnerabilities.

To date, Samsung does not offer a formal security assessment service as part of its MPS offerings. However, it does deliver an analysis of the print security issues as part of the wider fleet design at the point of MPS implementation planning.

Xerox

Xerox offers a comprehensive approach to security across its hardware, software and services portfolio. Xerox endorses the ISO 15408 Common Criteria for Information Technology Security Evaluation and has validated approximately 150 devices to this standard. Specific product security features (that vary by device) include image overwrite, data encryption, user authorisation and secure print, removable hard disk drive kits and network security features to protect devices from unauthorised remote access and 'data in motion'.

Beyond its hardware security features, Xerox's 'Secure and Integrate' phase is an established element of its managed print services (MPS) strategy. This phase focuses on securing and integrating the recommended print environment, encompassing security, mobile printing and print server and print queue management. Xerox offers a robust set of tools to control and secure a customer's print environment and has also established key partnerships with Y Soft (security), EFI (public printing), Elatec (card readers), CA (print server monitoring), and Cisco (Energy Management), as well as Atos (print server management).

In 2016, Xerox expanded its security services through the Xerox Print Security Audit Service and its Secure Print Manager suite of solutions (both Xerox and partner solutions), which offer analytics, secure printing and control and reporting. The Print Security Audit service aims to help organisations manage security across their entire printer fleet. Xerox software scans the network and performs an automated audit. It compares current device security settings against a predefined IT configuration and security policy. The information gathered identifies devices that are compliant with the client policy as well as non-compliant devices that require remediation.

Its Secure Print Manager Suite is based on both Xerox and partner technologies, this solution offers 6 modules – user authentication, user analytics, secure document release, job tracking, chargeback and accounting, and rules-based printing. A flexible and modular usage-based pricing model means that a customer can adopt a layered approach to document security, implementing the functionality required and adapting, as business needs change. This provides a scalable and low-cost option for SMBs that do not need a full range of security features.

Notably, Xerox provides a comprehensive portal for all its security information, bulletins and advisory responses. Xerox is the only manufacturer, at time of writing, that has publicly reported the potential impact of the recent Distributed Denial of Service (DDoS) attack that targeted Internet of Things (IoT) devices. Xerox studied the Mirai botnet source code that was responsible for the attack and reported that it cannot successfully attack any Xerox device as the two services the botnet uses, telnet and SSH, to open a command line are not supported. Xerox should certainly expand awareness of this resource as it demonstrates one of the more mature and proactive approaches to print security in the market.

Perhaps the strongest element in Xerox's security strategy is its implementation of McAfee and Cisco technology across its ConnectKey MFPs. Xerox and the partnership with Cisco allows complete visibility into network and policy management including user identification, provisioning and audit logs.

The use of McAfee's whitelisting technology provides a high level of malware protection on ConnectKey devices. McAfee's whitelisting technology detects unauthorised attempts to read, write or add to protected files and directories and sends alerts if they occur. Integrity control functionality also prevents files from being executed from any location by untrusted means. In addition, McAfee's ePolicy Orchestrator (ePO), a security management software tool, presents the users drag-and-drop dashboards that provide security intelligence across endpoints — data, mobile and networks.

Xerox should certainly leverage these technologies fully, as it offers an opportunity to integrate the management of IT and print security. Xerox may need to consider building more IT security expertise consulting (either independently or with partners) within its broader MPS engagements. As the security threat landscape evolves, the need for broader security assessments which encompass risk analysis and ongoing security optimisation of the print environment will be key to competitive advantage.

Vendor profile: Y Soft

Y Soft

Quocirca Opinion

Despite being a relatively young company, Y Soft, privately founded in 2000 and headquartered in the Czech Republic is making strong inroads in the print management and secure printing market. It has successfully moved beyond its traditional strong hold in the Eastern Europe, now operating globally in 16 countries with 14,000 customers in 120 countries. While Europe and Central Europe provide 58 percent of the company's fiscal year 2016 revenue (31 and 27 percent respectively), the remaining revenue is split evenly, 15 percent each, between North America/Latin America and the Asia Pacific Region whilst the Middle East/Africa revenue represents 12 percent.

Y Soft has established partnerships with many major OEMs, including Konica Minolta, Ricoh, Sharp and Xerox to offer its YSoft SafeQ Workflow Solutions Platform, a print management and workflow solution which enables organisations to manage and optimise their printing, copying and scanning. The majority of YSoft SafeQ sales are part of a broader MPS engagement, and Y Soft supports its channel partners throughout the implementation lifecycle through a standardised Global Operational Excellence (GOE) Framework™.

In May 2016, Xerox announced that it had selected YSoft SafeQ as the solution for perpetual and flexible subscriptions in the Xerox Secure Print Manager Suite. As with any best of breed tool, the YSoft SafeQ software solution can be utilised with optional, complementary hardware and software solutions. As a fully turnkey solution, businesses benefit from an integrated hardware and software solution rather than building a solution from disparate systems and vendors that require different pricing, support and service contracts, leading to an inconsistent user experience.

Y Soft today is the only ISV that has expanded into the 3D printer market. In 2014 it acquired a 51% stake of Czech 3D print manufacturer be3D, for $2 million and have fulling integrated them into Y Soft. YSoft's BE3D EDEE printer is specifically targeted at the education market and is the first 3D printer with print management features and a comprehensive accounting system to manage and recover 3D printing costs.

In 2014, it established Y Soft Ventures, its in-house investment arm, and in 2016 it established YSoft Labs to drive R&D across new and emerging technologies. The YSoft SafeQ platform is proving an attractive proposition for organisations, particularly SMBs that want a low cost and modular approach to print management and security. Channel partners also benefit from a multi-tenancy approach where they do not pay for the same module twice if they are sharing the infrastructure between multiple customers. Meanwhile, its ownership of its own 3D print technology means that Y Soft is uniquely positioned to address the emerging need to manage 3D printing.

Product Overview

The YSoft SafeQ platform addresses three key areas, print management for traditional printers and networked MFPs, 3D print management and document capture. A server application connects MFPs and networked printers to the corporate directory, enabling the implementation of pull printing, print governance policies as well as workflows for the capture, processing and distribution of digital content.

Modules include:

- **Authentication.** Protects against unauthorised users by securing access to MFPs, until the user authenticates via a card reader/PIN, username/password or combination.
- **Rules-based engine.** Enforces print governance with a library of pre-defined rules for cost savings such as colour to black and white, single to double-sided and send to most economical device, or create customised rules. Enables notifications to inform users of cost consequences which leads to better print usage, often reduced usage and notifications if the user does not comply to cost savings policies help enforce print governance
- **Print roaming/client based print roaming.** Secure printing from any MFP without needing additional print drivers, scalable from one office to multiple locations. Jobs print only when user authenticates eliminating sensitive documents in output tray. The use of a centralised server reduces the need for costly servers by handling complex print tasks on client workstation

- **Mobile print.** YSoft Wireless Print for Mac and IOS mobile devices (Apple AirPrint functionality) enables secure printers, either via the web or email to the MPF. Mobile print supports both iOS and Android devices, supports anonymous guest printing and provides automatic conversion across formats including JPG, PDF, DOC, PPT, XLS and PNG.
- **Managed Workflows/Core and Advanced Workflows.** One-click secure scanning to pre-defined document libraries (such as Microsoft SharePoint and Dropbox). Utilises an OCR engine to enable image cleanup, append or prepend pages and blank page removal.
- **Credit and Billing.** Supports price lists, cost centres, billing codes and usage quotas for cost allocations. Ability to set up pay-to-print accounts and virtual accounts.
- **Reporting**. Predefined custom management reports for usage audits, including sustainability reports. Pre-defined or custom reports can be accessed and displayed via the web or an MS excel document.

In addition to the standard features of pull printing, secure document capture features include:

- Access to scan features is based on authentication and authorization of user.
- Document and metadata are encrypted end-to-end.
- PDFs can be password protected.
- Audit reports track activity by individual or groups of individuals
- Sensitive documents can be redacted during the processing stage
- Processing captured data with OCR can be extended and fed into additional existing workflow systems that look for specific patterns (i.e. personal information, sensitive client details)
- Automatic purging of unprinted documents based on pre-defined time periods eliminates unwanted prints

YSoft SafeQ also offers the following capabilities for securing 3D printing.

- 3D printer uses authentication and authorization as described above to prohibit unauthorized access
- 3D printer door locks during and after print is finished and unlockable only by job owner to prevent printout theft
- Reporting tracks who and what was printed in order to recover costs and avoid risk of losing overview of who prints what
- Files sent for printing are stored securely on a server side, utilizing existing security measures.

Partnerships

Y Soft has strategic partnerships with a number of major OEMS. Globally this includes Konica Minolta and Xerox/Fuji Xerox. In Europe, Y Soft partners with Sharp and Ricoh. Other partnerships include: Samsung, HP, Epson, OKI, Develop, MJ Flood, Toshiba, Philips, UniData, HID.

Billing Model

YSoft SafeQ is sold on a per-device basis, regardless of the number of users. YSoft SafeQ is offered through license purchase as well as a subscription service.

Professional Services

Y Soft's standardised Global Operational Excellence (GOE) Framework is designed to provide support across the design, delivery and utilisation of the YSoft SafeQ suite of solutions.

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

Disclaimer:

This report has been written independently by Quocirca Ltd. During the preparation of this report, Quocirca may have used a number of sources for the information and views provided. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in information received in this manner.

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 and advice.