Closing the print security gap

The market landscape for print security

October 2011

Today, many organisations continue to rely on printing to support business processes, particularly in the public sector, finance industry and legal profession. Networked printers and multifunction peripherals (MFPs) have evolved to become integral to the network, operating as sophisticated document processing hubs. With the ability to print, copy, scan to network destinations and send email attachments, these devices come equipped with hard disk drives and often run internal web servers. Whilst MFPs and printers have improved business productivity, they pose the same security risk as any networked device if left unprotected. With reported data breaches on the rise and growing industry and regulatory requirements around information security, businesses may suffer financial and reputational damage if they ignore the risks of unsecured printing.

Employing secure printing controls reduces risk and helps reduce costs through user authentication to minimise wasteful printing and by auditing user activity, provides organisations with better governance and accountability.

The market landscape for print security is complex with little standardisation, characterised by a mix of hardware capabilities and proprietary software from MFP manufacturers along with independent third party software products. Quocirca's research has revealed that although larger enterprises are stepping up their efforts to improve their protection, many companies have much work still to do in safeguarding their enterprise print infrastructure.

This report provides an overview of the inherent risks when operating an insecure print environment and discusses the current market landscape while recommending some best practices for adopting an integrated information and print security strategy.

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

Clive Longbottom
Quocirca Ltd
Tel : +44 118 948 3360 ext 200
Email: Clive.Longbottom@Quocirca.com

Closing the print security gap

The market landscape for print security

EXECUTIVE SUMMARY

Lack of print security can compromise an organisation.	MFPs and printers are often located in public areas, are accessible by staff, contractors and visitors, and print jobs are now originating from smartphones and tablets as well as PCs. With confidential and sensitive information regularly processed and output through MFPs, it is essential that organisations understand the important role that such devices play in the security chain.
Organisations should not be complacent to the risk of unsecured printers and MFPs.	Print security risks are varied and include potential data leaks through unauthorised access to documents in output trays, recovery of information stored on hard disks and access to print jobs in network queues. Only 15% of respondents in Quocirca's survey are concerned with data loss through MFPs and printers. However, organisations cannot afford to be complacent given the financial cost and brand damage caused by a data breach.
The print security market landscape is a complex array of products and standards.	Each printer/MFP vendor offers a portfolio that includes a mix of standard and optional hardware security features together with secure printing software products. To complicate the picture, there is no single standard for MFP security. Although many conform to the Common Criteria (ISO15408) standard, each vendor typically adopts varying levels of EAL (Evaluation Assurance Level) certification. Other certifications include the US National Institute of Standards and Technology (NIST) and the new IEEE 26000 standard.
A security assessment of the print environment is vital in uncovering vulnerabilities	There is a significant opportunity for vendors to offer professional security assessment services that would uncover potential vulnerabilities within an organisation's print infrastructure. There is certainly interest in such services with Quocirca's survey revealing that 28% of enterprises have initiated or completed a security assessment with a further 26% planning to do so in the future.
The complexity of mixed printer fleets introduces greater risk but creates opportunity for best-of-breed products	Many enterprises have complex printing needs which require a range of devices from workgroup to high-end production and are from different manufacturers. To ensure a consistent approach to security for heterogeneous printer fleets, enterprises should consider third party products which can provide a vendor-agnostic approach for user authenticated printing (or "pull-printing") and auditing.
Security and mobility are inextricably linked through the deployment of pull-printing solutions	User authenticated printing ensures documents are only released by authorised users. This not only has tangible cost-savings benefits by minimising wasteful printing but also promotes enterprise mobility. Print jobs can now be sent from a PC, laptop, smartphone or iPad and be securely released upon authentication at any device on the corporate network.
Organisations should develop a print security strategy, ideally integrated with its overall information security approach.	Depending on the level of security needed, organisations should adopt a layered approach that combines built-in hardware features such as hard disk encryption or hard disk overwrite with access control products which specify who is allowed to print, scan and copy documents, protecting the device and auditing usage. Businesses should also consider linking print security to the overall data loss prevention (DLP) platform, which can further tighten printing controls.
The expansion of the managed print services (MPS) market will drive the adoption of print security products.	Quocirca expects more MPS providers to adopt a services-based approach to security, where security is an embedded component of a broader MPS offering. Given the market complexity, vendors should include scalable security assessments customised to business size and requirement.

Conclusion

Although many organisations are still oblivious to the security vulnerabilties of MFPs and network printers, there are a range of measures that can be adopted to enhance the security of these devices. Data breaches through printing practices is an all too common occurrence. Businesses should evaluate their existing printer and MFP fleet to ensure appropriate hardware security features are enabled and should adopt pull-printing solutions that not only enhance security, but minimise waste and promote flexible printing for today's increasingly mobile enterprise.

Introduction

Recent high profile data breaches are a stark illustration of the financial, legal and reputational damage that can occur when confidential or sensitive information goes astray. Whether it is customer data, intellectual property, confidential communications or privileged information, data volumes continue to rise, making information security a priority for all enterprises. Although security remains a top concern on the IT agenda, protecting and securing the printing environment remains a gaping hole for many enterprises today.

Despite the digital age, information is still shared and reproduced among business partners and customers as well as within the enterprise using printers and multifunction peripherals (MFPs). In Quocirca's recent enterprise study, 52% of respondents indicated that printing is critical or very important to business activities with a further 24% indicating that printing plays an important, if not essential, role.

MFPs now operate as sophisticated document processing hubs with integrated functionality that include printing, copying, scanning, faxing, email, storage and even web access. Although the move to a shared MFP workgroup environment can offer advanced productivity and collaboration between employees, customers and partners, it also generates an enormous security risk.

Left unsecured, it is all too easy for printed, scanned and copied documents to end up in the wrong hands, either accidentally or intentionally. Although many enterprises have built a strong security perimeter to protect servers, network equipment and PCs, the survey reveals that many enterprises are failing to pay the same strategic priority to printers and MFPs. As a consequence, 70% of respondents indicated they have suffered one or more accidental printing-related data breaches.

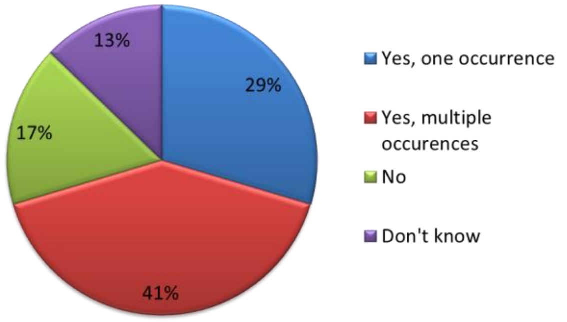

Figure 1. Accidental data breaches through printing

There is certainly some indifference to the printing security threat. Just 15% of organisations believe their printing infrastructure to be very secure and whilst 60% are most concerned with data loss through corporate email, only 15% of respondents are concerned with data loss through MFPs or printers. Larger enterprises are most likely to take print security seriously, with many operating an integrated information and print security strategy. The picture is very different for organisations with 500-1,000 employees, with over a third claiming not to have any print security strategy at all.

This report provides an overview of the inherent risks associated with printing and how these can be mitigated through a layered approach to security that encompasses built-in hardware security features and software solutions. The report also discusses why businesses should operate a fully integrated IT and print security strategy and outlines some best practices to achieve this goal.

Scope

Quocirca has included the following vendors in this study:

- Hardware vendors: Canon, HP, Konica Minolta, Lexmark, Ricoh and Xerox.
- Third party ISVs: Equitrac, Ringdale, SafeCom, NT-Ware, Pcounter

Each vendor was requested to complete a written submission detailing its strategy, capabilities and customer references to ensure key facts and figures were captured. These submissions were followed up with vendor interviews. Quocirca also conducted a survey of 125 IT managers in the UK, France, Germany and the Nordics to capture their views of print security and solutions.

Definitions

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

- **MFP:** An MFP (Multi-Function Product/ Printer/ 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. Examples of an embedded platform include Canon MEAP, Ricoh Embedded Software Architecture (ESA), Xerox EIP and HP OXP.

- **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 on-going management. MPS comes in many flavours, from entry level basic MPS packages that wrap hardware, service and supplies based on a cost per page contract to more sophisticated enterprise engagements that include document workflow solutions, change management and continuous management, based on stringent service level agreements.

The weak link in the information security chain

Printing remains an important element of business processes in an increasingly mobile and collaborative business world. In a recent Quocirca survey of 125 European enterprises (500+ employees), 76% indicated that printing was critical or important to their business activities. Yet, despite the fact that printed output often contains confidential or sensitive information there is a distinct lack of concern regarding data loss through printers or MFPs. Only 15% of respondents indicated this to be a concern compared to 57% citing corporate email as the top concern. Almost half of respondents have little or no concern regarding data loss through printing, suggesting a real lack of awareness of the security risks posed by unsecured MFPs.

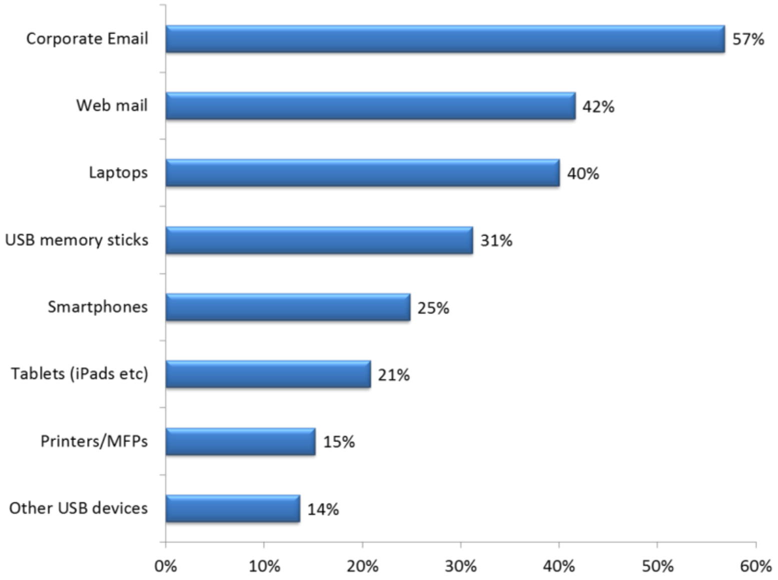

Figure 2. What is your level of concern regarding data leakage via the following? (Rated as important or very important)

Given that MFP and print security is low on the agenda, it is unsurprising to see that just 42% of businesses had placed some or significant effort into print security. Nevertheless, the survey reveals that businesses that are more dependent on printing to support their activities are most likely to have made efforts to secure printed documents. However, businesses cannot afford to be complacent - whether printing plays a critical or just supportive role, the likelihood of sensitive or confidential information passing through is high and therefore businesses must take a serious view of their potential risk exposure through an unsecured print infrastructure.

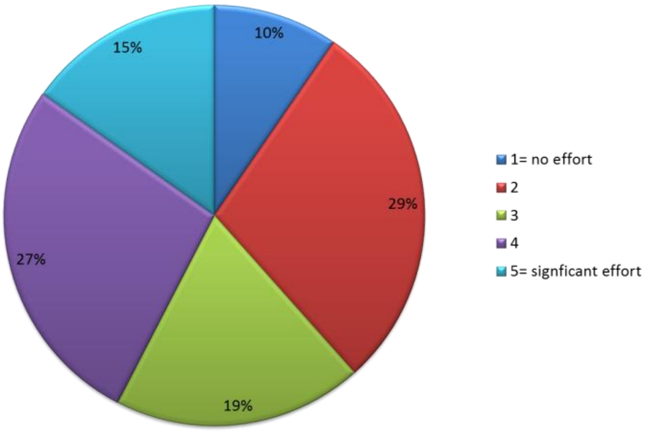

Figure 3. How much effort has the organisation put into managing the security of printed documents?

Printing security threats

Left unsecured, MFPs can pose a real security risk due to a number of vulnerability points. Not only do they store copies of thousands of possibly sensitive documents on their hard disks, but MFPs can be vulnerable to internal and external network attacks. What's more, their advanced features make it easy for sensitive information to be copied and distributed beyond the boundaries of the enterprise. With more businesses operating a shared print environment using centralised MFPs, the potential for information falling into the wrong hands is high– whether accidentally or intentionally.

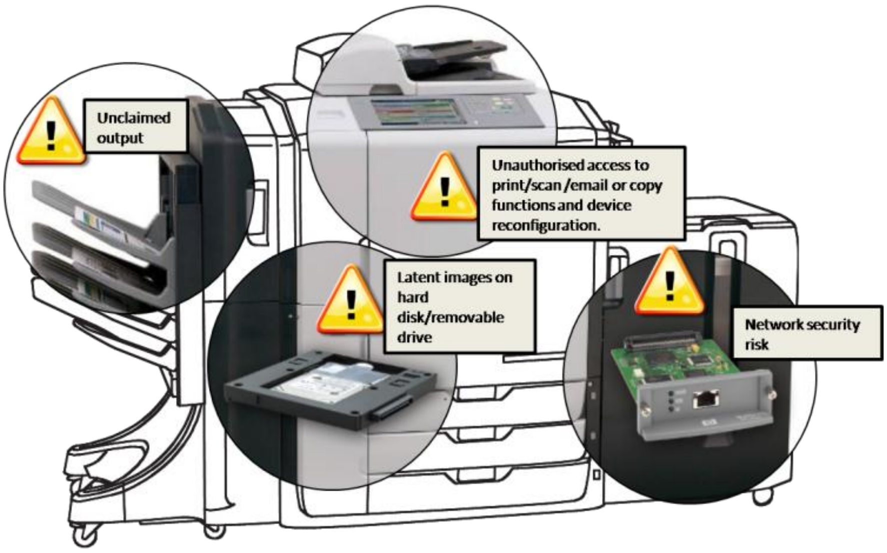
Unclaimed output
Unauthorised access to print/scan /email or copy functions and device reconfiguration.
Latent images on hard disk/removable drive
Network security risk

Figure 4: MFP security vulnerabilities ***(Source: Quocirca Report – Think Print, Think Security Feb 2010)***

Potential security threats as shown in figure 4 include:

- **Unauthorised access to the printer or MFP.** A user with unrestricted access may take confidential information left inadvertently on an output tray. Meanwhile, anyone with access to an MFP can also send information to any fax number or e-mail address, potentially without trace.
- **Hardware theft**. Documents sent to printers and MFPs will often be stored on the hard disks prior to printing. A stolen hard disk can expose these documents.
- **Unauthorised changes to settings.** If a device's settings and controls are unprotected, anyone can reroute print jobs and even access passwords and network information.
- **Network sniffing.** A "network sniffer" can read data travelling between a PC and a printer, exposing the print job and routing addresses.

Best practices for securing MFPs and networked printers

Fortunately, there are a range of measures that help guard against the potential threats of an unsecured print environment. Layered protection covers multiple points of vulnerabilities and should include built-in hardware security features together with advanced access controls and auditing tools dependent on the level of security required.

- **Control access.** Limiting access to the MFP to known users is a crucial step in safeguarding confidential or sensitive information. The most common authentication mechanisms include passwords, smartcards, and two-factor authentication, such as a combination of a password and card access. MFPs can be configured to authenticate users against the organisation's corporate directory via LDAP (Lightweight Directory Access Protocol), LDAP over Secure Sockets Layer (SSL) or Kerberos. Authentication can be implemented by either using an external authentication server, using authentication features embedded within a device, or by installing software that works with the MFP on a PC or workstation. This form of access control is also known as "pull-printing." In addition, the scan-to-email and fax functions can be limited to pre-approved addresses to prevent documents being sent to unauthorised recipients.

- **Secure the device.** In order to ensure sufficient protection of data, encryption of the MFP's hard disk drive is vital and effective. MFPs also require features to protect data both in storage and in transit. Devices should support the Advanced Encryption Standard (AES). When AES is activated, information stored on the hard disk drive is secured with 128-bit encryption. 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.

- **Secure the document.** In addition to access and device controls, document encryption 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.

- **Secure 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.

  Many MFPs are equipped with an intelligent network interface that provides a secure firewall to each MFP, preventing unauthorised access to configuration and network settings. Access can be controlled at three levels, which include IP address filtering and TCP/IP, services blocking which prevents specific communication protocols and gives administrators the ability to close vulnerable ports and disable the device's embedded home page.

  MFPs should be able to protect data transmission through common encryption protocols such as SSL or IP Sec. Many recent MFPs also support IEEE802.1X, which helps maintain a high level of security by blocking access from unauthorised devices.

- **Monitor and audit.** To ensure compliance and to trace unauthorised access, organisations need a centralised and flexible way to monitor usage across an often diverse fleet of printers and MFPs. Auditing tools should therefore be able to track usage,a 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 that provide such capabilities in a heterogeneous environment.

MFP and printer network security

- **IPv6:** IPsec (IP Security) is a standard part of IPv6, a set of protocols for securing Internet communications by encrypting and authenticating traffic between specified parties. This gives IPsec-compatible products an extremely high level of network security.
- **IEEE 802.1x:** This provides an authentication system for any devices which attempt to access the local area network (LAN) or wireless LAN. Network devices that are unable to authenticate to the 802.1x authorisation server are denied all network access.
- **SNMPv3:** The Simple Network Management Protocol (SNMP) provides a way to remotely configure MFPs. SNMPv3 security features support authentication and encryption.

Business drivers for print security

A number of factors are likely to drive business investment in print security over the coming years.

- **Protection of data and intellectual property.** A data security breach has far-reaching consequences that can lead to brand damage, financial penalties, legal costs and customer attrition. Over 70% of respondents indicated the security of personal data as a top concern that will drive print security adoption in the future (Figure 5).
- **Compliance and regulatory requirements.** Governance and compliance requirements have put additional burdens on IT groups within retailers, healthcare providers, financial services companies, and numerous other vertical industries. Evidence is now required to demonstrate proof of data controls against industry regulations such as Sarbanes-Oxley, PCI DSS, ISO 27001/2 and the Data Protection Act. In the UK, the Information Commissioner's Office (ICO) now has powers to fine companies and organisations up to £500,000 for serious breaches of data protection principles under the Data Protection Act.
- **Cost pressures.** Device consolidation and standardisation initiatives are being employed to strip down infrastructure and operating print costs. Ensuring document security becomes a top priority within a shared environment, since documents are more transient and can be shared across groups and teams. Only 34% of respondents expect cost reduction to drive print security adoption, indicating that many organisations are not aware of the tangible cost savings that can be gained from deploying pull-printing products. Ensuring documents are only released by authorised users minimises wasteful printing which leads to both financial and environmental benefits. Quocirca estimates that the use of pull-printing can reduce page volumes anywhere between 25% and 40%.
- **Increased mobility.** The growth in enterprise mobility is driving demand for employees to be able to print securely from any device (whether it is a PC or mobile device) and to any printer or MFP at any location. This will see an expansion in the use of pull-printing solutions which addresses the dual requirements of enhanced security and flexible printing across a corporate network.

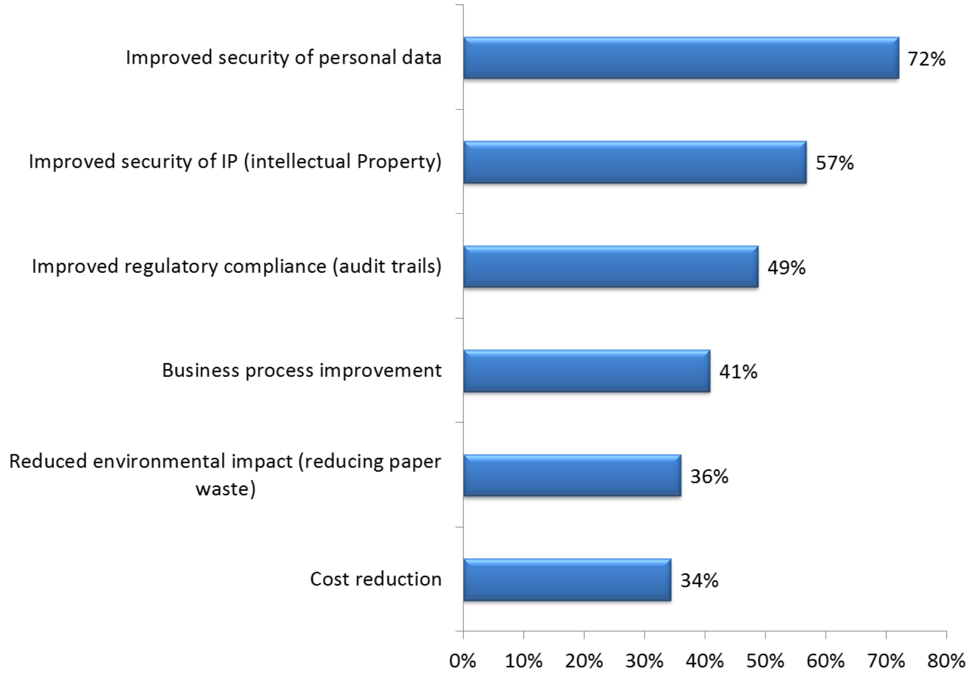

Figure 5. Which of the following concerns will drive investment in print security over the next two years?

Market Landscape

The print security market is characterised broadly as follows:

- **Hardware vendors.** All the major vendors including Canon, HP, Konica Minolta, Ricoh and Xerox offer comprehensive portfolios that include built-in hardware security features, access control software products and third party vendor-agnostic pull-printing solutions. Some vendors also offer security assessment services either independently or as part of their MPS offerings.
- **Third party solutions vendors.** A range of ISVs offer pull-printing solutions including Equitrac (part of Nuance Communications), NT-Ware (part of Canon), Pcounter, Pharos, Print Audit, Ringdale, SafeCom and YSoft.
- **Data loss prevention.** Although vendors in this space are not strictly operating in the print security market, Quocirca believes the capabilities they offer to block printing documents based on content analysis offers a higher level of security for organisations looking for a more tightly integrated information security strategy.

MFP Security Standards

The most important standards with regard to printing are:

Common Criteria certification
The Common Criteria (ISO 15408) is a standard for computer security, which can also be applied to document output devices. Some device manufacturers have certified their equipment under the Common Criteria process. But because of the process's cost and complexity, certification is often limited in scope to a subset of device functionality – such as hard disk overwrite capability.

IEEE P2600
The IEEE P2600 working group is defining a security standard for hardcopy devices, as well as recommendations for security capabilities of devices when deployed in various environments, including enterprise, high-security, small office/home office, and public spaces. The P2600 working group has broad industry participation, including Hewlett-Packard, Lexmark, Canon, Xerox, Sharp, Ricoh, IBM, Epson, Okidata, Equitrac, and Océ.

ICSA Labs NAPS certification
ICSA Labs, an independent division of Verizon Business, announced the NAPS (Network Attached Peripheral Security) certification program in September 2009. This includes rigorous testing that examines several different aspects of a networked printer and copier device and how each impacts its overall security. ICSA is also hoping to gain attention from enterprise clients concerned about device security with a NAPS assessment program that offers an evaluation and report and results of testing and recommended configuration instructions.

National Institute of Standards and Technology (NIST) Security Checklist
The National Institute of Standards and Technologies (NIST) has been tasked by U.S. legislation to develop checklists that facilitate security configuration of devices likely to be used by the U.S. Federal Government. NIST has requested IT equipment manufacturers to develop these security checklists for their products. Details of the checklist program are available at http://csrc.nist.gov/checklists

Market summary

The print industry is already characterised by lack of standards when it comes to software, consumables and hardware platforms. Unfortunately, the print security market is no different, awash with different hardware capabilities, proprietary software and independent third party solutions. Most hardware vendors offer a mix of products scalable from SMBs to large enterprises, but in the main, portfolios can appear complex and confusing. While Quocirca expects an increase in the usage of pull-printing solutions amongst larger enterprises, it is likely that the level of adoption of built-in hardware security features will be variable as this is dependent on the customer's awareness and understanding of hardware MFP security. Hardware vendors still have much work to do to simplify their messaging around print security and help customers navigate the patchwork of standards, features and solutions that each MFP or printer supports.

Lack of security certification standards
The lack of security certification standards, which includes Common Criteria, IEEE P2600 and National Institute of Standards and Technology (NIST) Security Checklist, fosters further confusion. Where Common Criteria Certification is concerned, each manufacturer typically chooses which security features it considers to be important and certifies only those features. The IEEE P2600 standard seeks to overcome this by requiring vendors to certify a device rather than a feature. In the meantime, businesses should evaluate standard and optional security mechanisms on devices such as image overwrite, authenticate, removable hard drive, hard drive erasure and basic access authentication as well as considering third party secure printing solutions. Quocirca research indicates that awareness of such standards is highest in the US with 64% of organisations believing MFP security certification to be important or very important compared to 40% of organisations in the UK and France. Just 12% of US respondents are unaware of MFP security certification compared to an average of 25% in Europe.

Third party pull-printing solutions suit enterprise diverse fleets
According to Quocirca's research, around 35% of enterprises are using some form of print access control, and it is most prevalent in enterprises above 1,000 employees. While smaller enterprises should look for standardised solutions from their suppliers, larger enterprises operating a diverse printer fleet will need to look beyond proprietary vendor solutions to vendor-agnostic third products, which can offer a standardised approach for user authentication, monitoring and reporting.

Quocirca expects the deployment of pull-printing solutions to be partly hampered by the level of investment needed for external authentication hardware devices for each MFP or printer. This can be overcome by using embedded software which is integrated directly with the MFP, or using software based release products that can be installed on a local PC or workstation. Software only products, which do not require a separate server, are the most cost-effective as do not require server license fees and are usually based on a per device cost. Vendors that use this approach include Pcounter with EveryonePrint and Print Audit's latest Print Audit Secure product.

Vendors should expand security assessment services
The sweet spot for print security lies within the large enterprise space. These businesses have complex printing needs, often operating a mixed fleet environment, and are most likely to be relying on printing to support business critical processes in some form. This represents a strong opportunity for vendors with such enterprises to offer print security assessment services either as part of existing MPS engagements or independently. There is some indication in Quocirca's survey that enterprises prefer to purchase secure printing solutions separate from MPS contracts, but given the cost reduction opportunities using such products. MPS providers should look for innovative ways to incorporate them in wider MPS contracts. Equally, growth in the general Managed Security Services (MSS) market also presents an opportunity for printer vendors to work with such independent providers to create broader awareness of the print security threat.

Quocirca perspective: Hardware vendors

The following section provides a highlight of the print security strategy for each vendor. More details are available in a full competitive analysis report (see Appendix).

Canon

Canon offers a wide range of built-in and optional hardware features, along with software, to address print security requirements of businesses of all sizes. Its flexible and scalable print management tool uniFLOW sits at the heart of Canon's security proposition and offers capabilities such as user authentication, usage auditing and reporting. Notably, through keyword recognition using optical character recognition (OCR), uniFLOW can prevent print, copy, fax or scan jobs across both Canon and third party devices. For maximum security, jobs can be held and checked for restricted content before they are printed or sent to their scan destination. Currently, uniFLOW is the only integrated print and scan management product to offer this feature.

Canon is focusing on integrating its security solutions with existing enterprise data loss prevention (DLP) systems. For instance, uniFLOW Secure Audit Manager (iWSAM) module is an optional security product that captures and archives all copy, scan, print, fax and send jobs. It indexes and stores for future searching and auditing, the full image of the document, any embedded images, text, job log, and attribute information such as user name, IP Address, device names, and time/date stamp. In the event that a data breach occurs, iWSAM can be used to help trace it, but only if it was processed on a Canon MFP.

Canon is particularly targeting chief information security officers (CISOs) to raise awareness about how print security should be integrated with broader information security measures. In Europe, Canon is an active participant in many information security forums and events, such as the ISF Annual World Congress. Although Canon's DLP approach is currently only a European initiative, it is promoting uniFLOW as the architecture for a multilayered enterprise document security platform on a global basis. Quocirca believes that Canon's strong relationships with the CISO community in Europe will serve to raise awareness for enterprises to adopt an integrated print and information security platform.

HP

HP has built a strong portfolio to help businesses manage risk and secure their enterprise print infrastructure. HP's Imaging and Printing Security Framework approach has been established for over 10 years and is based on four pillars – secure data, secure devices, protect printed documents, and monitoring and managing the printing fleet. HP has augmented the framework to add risk management and compliance considerations. HP's security portfolio includes the HP Access Control Printing Solutions suite, which is a modular set of software products that encompasses authentication, rules-based printing, job accounting and secure pull printing. This modularity offers customers the flexibility to choose the level of security they need.

Security is a fundamental part of HP's managed print services (MPS) strategy, and according to HP, the take up rate for direct enterprise MPS contracts that include one or more of HP's security offerings is growing across all regions. Through a wide range of industry-specific security products, HP is particularly well positioned to deliver customised solutions that address specific vertical markets, particularly for target markets such as financial services and insurance, manufacturing and distribution, healthcare, communications/media/entertainment and public sector.

HP is one of the few vendors to offer a self-assessment checklist tool - the HP Security Action Plan, which enables businesses to analyse and determine their print security needs (http://www.hp.com/go/secureprinting). Probably more comprehensive and therefore suited to larger enterprises is HP's security assessment service, which is offered as part of HP's Managed Print Service. HP is also building the channel route-to-market for security, management and workflow solutions for SMB and enterprise accounts not served directly by HP offerings. HP has recognised that security and mobility are inextricably linked, and is currently one of the few hardware vendors to address the security challenges of mobile printing as part of its overall print security strategy.

However, HP has a large and complex portfolio and must ensure that it brings its professional services, domain expertise and channel partners into play to ensure that this mix of own-brand and partner products and services is well understood by its enterprise and SMB customers and prospects.

Konica Minolta

Security is a key element of Konica Minolta's overall strategy, supporting its marketing efforts in its main target markets of finance, government/ public sector, healthcare and legal, which require security components in their business. Konica Minolta has a comprehensive range of print and document security features, many of which are standard features for their bizhub range of devices. Rather than certifying optional security kits, Konica Minolta claims to have the widest range of ISO15408 fully certified MFPs in the market. Security is a key component of its MPS offering, Optimized Print Services (OPS), with Konica Minolta estimating that currently over 50% of its MPS engagements are driven by secure printing requirements. Konica Minolta's desire to focus on particular vertical markets including finance, healthcare, legal, education and government means it addresses the specific print security requirements on a sector-by-sector basis.

In the US, Konica Minolta also offers bizhub SECURE, a professional security service that will provide lock down protection on bizhub MFPs. With this initiative, Konica Minolta provides a consultancy service to match security features to the customer's environment. Quocirca believes that such services will appeal to many enterprises given the complex mix of MFP hardware and software security features that businesses must navigate. Konica Minolta plans to launch this service in Europe in April 2012. Such a service would help raise the visibility of Konica Minolta's print security offerings beyond its standard hardware features, helping it to support its OPS-led approach.

Lexmark

Lexmark's increased focus on enterprise customers has boosted its MPS business, which grew by 34% in 2011. It is also benefiting from the $280 million purchase of Perceptive Software Inc. last year, which helped broaden its customer base. Lexmark estimates that take up of its security offerings has increased by over 45% in the past year, with over 80% of its MPS engagements now including security products. Lexmark has a particularly strong presence in retail and financial services markets.

Lexmark leads with the message of "Print Less, Save More," which addresses the business need to save money in the current economic climate. In March 2011, Lexmark released a three-in-one document output management product/service comprising Print Release, My e-Task and Lexmark Accounting. This includes pull-printing, device personalisation and activity tracking and reporting across both Lexmark and third party devices. A key benefit is the ability for users to authenticate at any device across locations, for example different branch or country offices, and to be presented with a personalised device configuration. Users of the Lexmark Print Release solution and Lexmark Managed Print Services report up to a 40% reduction in pages printed.

By virtue of developing and owning all of its core technologies, Lexmark is able to deliver a strong set of innovative solutions for a secure and cost-effective print infrastructure. This also strengthens Lexmark's abilities to tailor its offerings. For instance, Lexmark provided 'PrintHere' for German public sector organisations where MFP touch screens were customised to offer confidential printing and copying using the Lexmark Print Release solution.

Quocirca believes Lexmark has a clear vision and strategy for addressing enterprise print security requirements. Its strong performance in the MPS market is testament to a well-integrated portfolio of hardware, software and a service that is further enhanced with the launch of Print Release.

Ricoh

In January 2011, Ricoh announced its plans to invest $300 million over three years in its global Managed Document Services (MDS) infrastructure. Ricoh has made significant strides in the development of its MDS portfolio, focusing its efforts on senior to board level decision makers. Security is integrated into Ricoh's hardware, software and services portfolio and it estimates that in 2011, revenue for security software products will grow by 30% in Europe. Ricoh takes a multi-layered approach to security through its long established Document Security Framework, which is available globally. The framework is underpinned by physical and network authentication, along with auditing and document workflow security, to ensure the confidentiality, integrity, and availability of documents.

Ricoh has taken a consistent and global approach to secure information – both for customers and internally. In 2004, Ricoh gained and has since maintained the ISO 27001 worldwide certification for Information Security Management for their head office and manufacturing sites. This has been subsequently extended to all individual sites.

In May 2011, Ricoh announced that a number of its products were the first globally available products to obtain the Common Criteria certification conforming to IEEE 2600.1, an international standard for IT security products. Ricoh has a set of standard built-in security features for its latest MFPs such as its Data Overwrite Security System (DOSS), which secures the hard drives and makes all confidential data unrecoverable by overwriting latent digital images after all copy, scan and print jobs. In addition, Ricoh provides a comprehensive range of advanced security solutions including authentication, secure server-less pull-printing from up to four devices (right up to multi-premises pull-printing), document management and audit and reporting features.

MFP security remains a complex topic and Ricoh is wisely focusing on assessing business security needs rather than presenting a complex array of hardware and software product features. Quocirca believes that Ricoh will further strengthen its proposition around security as it continues to develop the document process governance theme that underpins its MDS strategy.

Xerox

The development, implementation and delivery of all Xerox products, services and technologies are guided by the Xerox Security Development Lifecycle (XSDL). This focuses on network security, document security, data security and authentication. Security is managed throughout the entire device life cycle from requirements analysis, design, development, manufacturing, deployment, and disposal. Xerox builds a comprehensive range of features into its devices to help safeguard customer information, including hard drive removal, fax/network separation, image overwrite, network authentication and authorisation, encryption and secure print. Xerox is one of the few MFP vendors with an active security patch program, monitoring vulnerabilities on MFPs and posting security bulletins. Customers can sign up for an RSS feed and be alerted immediately when a new bulletin and downloadable patch is posted.

Xerox supports the Common Criteria for IT Security Evaluation (ISO/IEC 15408), which helps Xerox's customers meet the high-level security requirements and increasing regulations in the government, military, health care, legal and financial sectors. Xerox, along with other vendors, works with ISVs such as Equitrac, SafeCom, Ringdale and YSoft to enhance its security offerings. Xerox anticipates continued growth in the need for secure printing that also supports mobile workers. Security is now a key element of many of its MPS engagements, but its adoption is sometimes held back by the perceived cost implications. With security likely to play a wider role in MPS engagements, Xerox should drive awareness to the scalability of its security solutions offered through its MPS portfolio.

Quocirca perspective: Independent Software Vendors (ISVs)

Equitrac (part of Nuance Communications)

Equitrac's cost-recovery and print management products continue to see growth across its primary verticals, which include legal, education healthcare and financial services. A particular strength of the Equitrac product range is its integration with enterprise applications. For instance, Equitrac has integrated its software with more than 50 financial and accounting applications used particularly in the legal profession, but also in other industries. Equitrac products are available as embedded versions for a range of MFPs as well as through its TouchPoint Console external terminal.

The acquisition of Equitrac by Nuance in May 2011 expands the reach of Equitrac through Nuance's large channel network across North America, EMEA and Asia. The strong and established presence of Equitrac's product portfolio in the print management market positions it well to address the growth in MPS engagements that have expanded beyond device consolidation. Quocirca believes that although Equitrac will now have access to a wider channel network through Nuance, it will also need to forge closer relationships with MPS providers - both hardware vendors and independent providers. These suppliers can add real value to MPS engagements by providing a unified and centrally managed print management platform that can control the costs and risks associated with unmanaged and often heterogeneous print environments. Quocirca believes that Equitrac products will appeal mainly to enterprises that require a comprehensive platform for secure printing, cost recovery, monitoring and reporting.

NT-Ware

uniFLOW, developed by NT-Ware (owned by Canon), is Canon's long-standing flagship print management platform, which provides an extensive range of cost control, cost recovery, document routing and security features. uniFLOW is a modular product making it appealing to both large and small businesses. Its capabilities range from basic print auditing and cost accounting to sophisticated enterprise features such as server clustering and print-room job submission. Although uniFLOW supports third party hardware, it offers stronger integration with Canon and Océ MFPs and has been particularly successful across Canon's global major accounts that require one print management platform across multiple geographic locations.

With the recent release of uniFLOW 5 at the end of 2010, Quocirca believes uniFLOW offers the most expansive set of secure printing features in a single platform although it is ultimately most suited to a Canon/Océ environment. In addition to restricting access to MFPs through pull printing capabilities and tracking capabilities for all copy, print, scan and fax jobs, uniFLOW now also offers keyword recognition. Using embedded I.R.I.S OCR software and rules management capabilities, uniFLOW can monitor the content of every print, copy, fax or scan job carried out on a Canon MFP. For maximum security, jobs can be held and checked for restricted content before they are printed or sent to their scan destination. This is a unique differentiator for Canon, and enables it to offer its customers an advanced level of security if required.

Pcounter

Established in 2002, Pcounter Europe is a supplier of accounting, secure print and mobile print solutions for both academic and corporate markets. Its route to market is through the indirect channel with sales and support via local integration partners and Pan-European distribution partners such as Konica Minolta. Its product range includes the Pcounter and EveryonePrint product. Pcounter is a comprehensive cost recovery and print accounting application whilst EveryonePrint is a secure print application, based on private cloud technology.

Designed for businesses of all sizes, EveryonePrint provides a low cost solution for secure printing – from PCs, laptops or mobile devices. Authentication is performed via the MFP, a web browser or via a card reader. EveryonePrint provides full end-to-end encryption and documents can be printed using the EveryonePrint web interface, through a universal driver, or by sending documents as email attachments. A multivendor solution, EveryonePrint is currently available with browser support for Konica Minolta, Canon, Sharp, Toshiba and Xerox devices with support planned for many other manufacturers. EveryonePrint currently has over 600 installations in Europe and is currently being promoted as one of Konica Minolta's tier 1 solutions for secure and mobile printing.

EveryonePrint can be installed as a standalone solution or as an add-on to print accounting applications. The locally installed solution provides a low cost entry level approach as it does not require connection to the Internet and third party servers. With a price of less than €200 per device, it eliminates the need for embedded terminals and a server license which can often be a barrier to the investment in pull-printing solutions. Nevertheless, for those businesses that require integration with a wider cost recovery/ print accounting platform, Pcounter does offer a server based version of EveryonePrint. Cost is often a limiting factor in the adoption of secure print solutions, particularly in the SMB and midmarket. As such Quocirca believes that EveryonePrint effectively addresses the need for a low cost, multivendor secure print solution that supports printing from the desktop or mobile device. However, organisations that need a more comprehensive product that includes accounting and auditing support across other functions such as copying and scanning, should look to invest in third party products that provide this level of functionality.

Ringdale

Ringdale's FollowMe solution has been around for over 13 years, pioneering the "follow-me" approach to secure printing. FollowMe's capabilities are extensive – including dual-authentication, policy and rules-based printing, accounting for all throughput and centralised storage of data for reporting, auditing and expense billing. FollowMe provides full control and management of all MFP services including printing, copying, emailing, faxing and scanning and effectively provides a single platform for businesses of all sizes to secure, manage and monitor devices in a multivendor environment. FollowMe is offered as either an external hardware component allowing compatibility with a wide range of printers and MFPs, or as an embedded version fully integrated with printers and MFP interfaces from vendors including HP, Konica Minolta, Kyocera Mita, Lexmark, Océ, OKI, Ricoh, Sharp, Toshiba and Xerox. Additionally, Ringdale's FollowMe PrintSpot product offers a cloud-based driverless printing environment, enabling mobile printing from any device supporting a web browser or able to send e-mail.

A notable feature of Ringdale's FollowMe is its integrated Business Intelligence engine which offers policy-based controls and customisable intelligent rules-based printing to address each particular customer's ever changing business needs e.g. dynamically converting e-mails to black and white, or re-routing large print jobs to the higher end output devices. Although Ringdale works with most of the major printer/copier manufacturers, it has particularly developed a strong relationship with Lexmark. The companies have worked together to deliver customised MPS-based security solutions world-wide. Ringdale's FollowMe solution portfolio is well suited to the midmarket and is scalable from around 40 devices upwards.

Given the maturity of Ringdale's FollowMe system, together with its extensive and scalable feature-set, Quocirca believes it to be a leading product amongst the third party secure print solutions, offering a wide range of embedded support. Although hardware manufacturers are beginning to develop and expand their own secure access print solutions, third party products such as

Ringdale will continue to have the edge in functionality when deployed across a multivendor fleet or when advanced functionality such as customised rules-based printing is required.

SafeCom

SafeCom has a mature product portfolio and due to the modularity and scalability of the SafeCom system, along with its flexible multi server licensing structure, it is well positioned to address the needs of smaller businesses as well as those operating across multiple, geographically diverse offices. SafeCom's product development has primarily been driven by major enterprise customers, in the financial services and education markets, who have over time expanded their SafeCom deployments from small installations to global deployments – a testament to the robustness and scalability of the SafeCom platform.

Given its product maturity in the enterprise market, SafeCom is now furthering its product development by creating a standardised version for the SMB market, focusing on ease of use and flexibility along with fast installation and implementation time. With the adoption of secure print solutions sometimes hindered by cost and complexity, SafeCom is focusing on addressing both cost control and automation of print security.

Although HP has historically been SafeCom's major alliance partner, SafeCom now also works closely with Ricoh and Xerox. The majority of SafeCom's sales through such partners are driven by managed print services contracts. SafeCom estimates that around 20% of its product sales are associated with an MPS engagement and expects this to rise to 40% by 2013. Third party products such as SafeCom remain the most popular choice for the many organisations that need a consistent secure printing approach that offers authentication and reporting across a mixed device fleet. Quocirca believes SafeCom is well positioned to expand its deployments in the enterprise space as it continues to deepen its partnerships with MPS providers. In particular, it should expand awareness of its capabilities to protect documents in virtualised environments as this continues to be a hotspot in the enterprise space. With more competitive entry-level secure printing products now available, SafeCom will need to ensure that it broadens awareness of its forthcoming product for the SMB market.

Conclusion

An organisation's information security strategy can only be as strong as its weakest link and given the continued reliance on printing amongst many businesses, print security is no longer something they can choose to ignore. Print security demands a comprehensive approach that includes education, policy, and technology.

As shared printing environments become more common as a result of device consolidation, the risk of documents falling into the wrong hands is heightened. Market complexity means that organisations should adopt a multi-layered approach depending on their security requirements. A print security strategy must control access to MFPs, secure data that resides on the MFP and whilst in transmission, and must provide monitoring and auditing capabilities to track usage by device and user.

In today's compliance driven environment where the cost of a single data breach can run into millions, organisations must proactively embrace this challenge. In doing so, organisations will reap the benefits of stronger compliance with regulatory policies and greater protection for valuable intellectual assets.

Appendix A: Hardware vendors competitive matrix

Key: ● Standard feature on all devices ◖ Available on certain products ○ Available with third party solution/option

Please note this table is provided for guidance only. Due to the variance in capabilities across each vendor's product range, please refer to the manufacturer for precise details on standard and optional security features.

Company	Canon	HP [1]	Konica Minolta [2]	Lexmark	Ricoh	Xerox
Hard Disk Security						
Hard Disk Overwrite	●	●	●	●	●	●
Hard Disk Encryption	●	●	●	●	●	●
Printer lockout	●	●	●	●	●	●
Removable hard drive	◖	●	●	●	◖	●
Authentication						
User PIN	●	●	●	●	●	●
LDAP	●	●	●	●	●	●
Card	●	○	●	●	●	●
Biometric	●	○	●	○	○	○
Network security						
IP filtering/firewall	●	●	●	●	●	●
IPSec	●	●	●	●	●	●
802.1x	●	●	●	●	●	●
SNMPv3	●	●	●	●	●	●
IPv6	●	●	●	●	●	●
S/MIME for Scan to Email	●	●	◖	◖	●	●
Audit logs and Reporting						
Job accounting	●	●	●	●	●	●
Rules based printing	●	●	●	●	●	●
Customisable reports	●	●	●	●	●	●
Audit log	●	●	●	●	●	●
Document security						
Encrypted pdf	●	●	●	●	●	●
Encrypted email	●	●	●	●	●	●
Secure Encrypted Print	●	●	●	●	●	●
Secure watermark	●	○	●	●	●	●
Compliance						
ISO 15408	●	●	●	●	●	●
IEEE 2600	●	●	●	●	●	●
Firmware						
Digitally signed firmware updates	●	●	●	●	●	●

[1] Capabilities available on HP FutureSmart enabled devices, with some variance on other HP and HP-managed multivendor devices.

[2] All Konica Minolta bizhub products include security features as standard.

Note: A full competitive analysis report is available. Please contact Louella.Fernandes@quocirca.com

Appendix B: ISV competitive matrix

Key: ● Feature available ○ Not Available/ Requires third party option

Product name (s)	Equitrac Office, Equitrac Express, Equitrac Professional	Ringdale FollowMe	PCounter	SafeCom Smart Printing	uniFLOW	YSoft SafeQ
Licensing model	Client/Server/Device	Client/Server	Client/Server	Device/ Functionality	Client/Server	Server/ Device
Embedded solutions	Canon, Ricoh, Xerox, Fuji Xerox, Sharp, Konica Minolta, Océ, HP, Kyocera Mita	HP, Konica Minolta, Kyocera Mita, Lexmark, Océ, OKI, Ricoh, Sharp, Toshiba, Xerox	Ricoh, Xerox, Sharp, Konica Minolta, HP, Canon, Lexmark, Oce, Kyocera Mita, Toshiba	Canon, Fuji Xerox, HP, Konica Minolta, Kyocera, Lexmark, Océ, Ricoh, Samsung, Sharp, Xerox	Canon MEAP, Canon embedded firmware on Canon MFP devices, Xerox EIP, HP OXPD	Konica Minolta, Xerox, Ricoh, Sharp, Océ
Number of MFPs supported per server	Unlimited (depends on licence)	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Maximum number of users supported	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
			Accounting/Cost Recovery capabilities			
Tracks print output pages	●	●	●	●	●	●
Tracks copy output pages	●	●	●	●	●	●
Tracks fax output pages	●	●	●	●	●	●
Tracks scan output pages	●	●	●	●	●	●
Tracks colour and mono pages in single document	●	●	●	●	●	●
Account limit enforcement by user/department	●	●	●	●	●	●
Account limit warnings	●	●	●	●	●	●
Restricts printing by application type	●	●	●	○	●	●
Rules and routing	●	●	●	●	●	●
Job re-direction	●	●	●	●	●	●
Multiple routing rules per printer	●	●	●	●	●	●
Rules by application (e.g. print emails in black and white/ print large jobs duplex)	●	●	○	●	●	●
Universal driver	○	○	○	○	●	○
Customisable reports	●	●	●	●	●	●
LDAP authentication	●	●	●	●	●	●
Authentication via PIN	●	●	●	●	●	●
Authentication via access card	●	●	●	●	●	●
Magnetic stripe	●	●	●	●	●	●
Biometric/Fingerprint	●	●	●	○	●	●

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, 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.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures for demonstrable business value in any implementation. The capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver 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.

Details of Quocirca's work and the services it offers can be found at http://www.quocirca.com

Report Note

This report has been written independently by Quocirca Ltd. Quocirca has obtained information from multiple sources in putting together this analysis. These sources include, but are not constrained to, the vendors themselves. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in information received in this manner.

Therefore, Quocirca expressly disclaims all warranties and claims as to the validity of the data presented here, including any and all consequential losses incurred by any organisation or individual taking any action based on such data.

All brand and product names are trademarks or service marks of their respective holders and do not imply an endorsement by Quocirca of the trademark owner, or vice-versa, or that the trademark owner has authorised Quocirca to promote its products, services, or content.