ovum

Maintaining Corporate Privacy in the Digital Age

Securing sensitive data while in motion and at rest

Introduction

Organizations large and small are investing in digital transformation programs, cloud migration projects, and enterprise mobility initiatives to grow their businesses and increase operating efficiency. However, Ovum is concerned that corporate information security management policies do not appear to be adapting quickly enough to cope with the tumultuous rate of change imposed by the rapidly evolving business and technological landscape.

Although encryption has been around for many years, it has come to the fore recently as a means of making it more difficult to gain unauthorized access to sensitive or confidential information, especially within the context of mobile devices. Ovum expects the adoption of encryption technologies to grow rapidly in the near term due to the fact that conventional approaches to information security are failing to stem the flow of data leakage incidents and privacy breaches. Eventually, all data will be encrypted at rest and/or in motion. However, for a variety of technical, practical, and legislative reasons, organizations must be diligent and meticulous in their use of this technology, with the customer and employee experience being of paramount importance.

Companies can prioritize the encryption of corporate data by carrying out a data classification exercise across their business processes and IT infrastructure. However, data classification is a resource-intensive and generally costly process. Not only is it time- and resource-consuming to implement a manual classification in the first place, but it also requires employees to be aware of changing classification policies going forward, and to potentially apply them to information and data items that they have already created and distributed.

While training can help raise the awareness of data privacy and information security management issues, organizations must first focus on the basics, which means putting in place a set of robust, reliable, and easy-to-use solutions to address the most common data-related activities that employees undertake every day. For most enterprises, this means improving email information security management and adopting a more proactive approach to the distribution and sharing of file attachments.

Going forward, the only realistic way of managing and maintaining such processes is to instantiate the organization's information security management regime through the use of automated, policy-driven implementations. And in the case of email messaging and file sharing/transfers, this means adopting solutions that are capable of securing data in motion as well as data at rest, both on-premise and in the cloud, and in a manner that is near enough invisible to the business end user.

CIOs appreciate the need and urgency to do a better job of managing information security

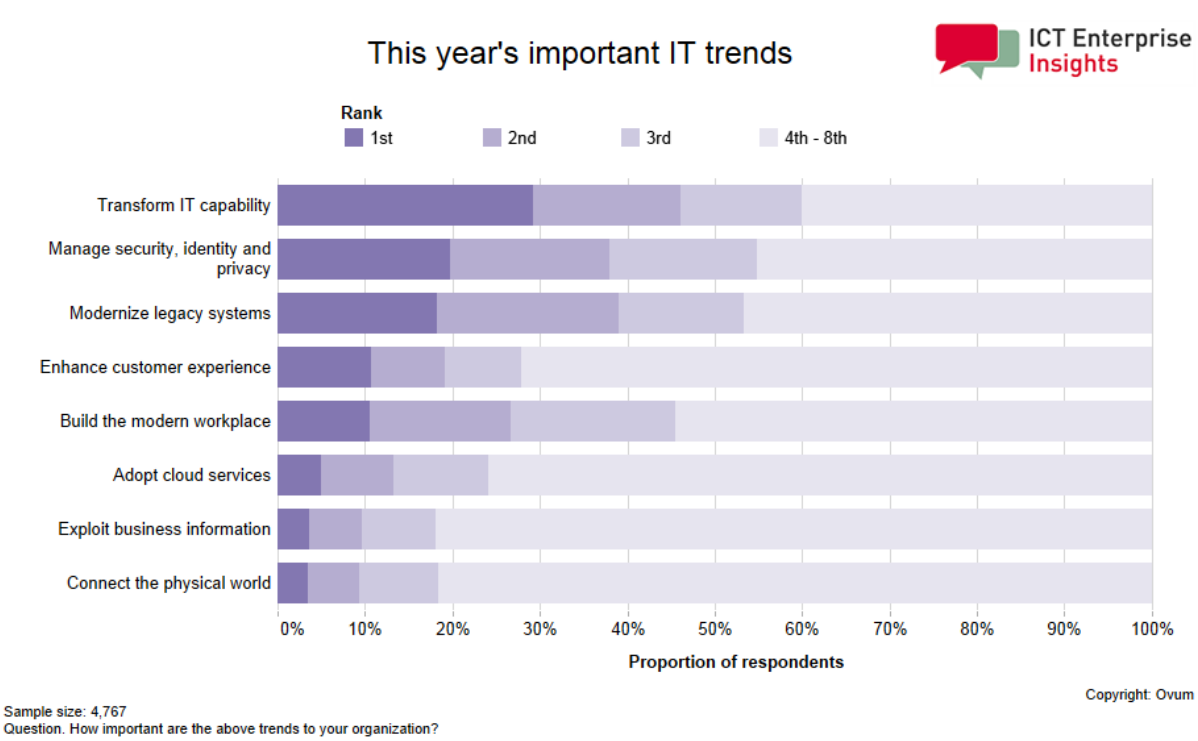
Ovum's *ICT Enterprise Insights* survey (see Figure 1) clearly illustrates that CIOs appreciate the need and urgency to do a better job of managing information security, user identity, and data privacy. But it remains to be seen if IT budget and resources will find their way to the right areas of focus. IT departments have traditionally focused on securing data at rest, but in today's highly dynamic, highly mobile world, it is now equally important to secure data that is in motion.

Business processes are increasingly digital in nature, which means that sensitive information is constantly circulating around an organization's IT systems. Transactional systems account for a great

deal of this traffic and data flow, but business exceptions and process interventions nearly always result in one thing: email. The corporate email system has long been the "go-to" system for business notifications and person-to-person interactions, and it is still the communication medium of choice for most business users when they need to collaborate on an activity or disseminate information. But most business users have never sent a digitally signed or encrypted email, even though the content of their message may warrant it. Why is this? The answer is straightforward enough: thus far, the management of digital certificates and encryption keys has been too onerous and burdensome a task for the IT department, the sender, and the recipient.

So, while website owners are racing to implement a more secure set of protocols to protect user data and privacy, organizations are potentially putting their corporate communications at risk. Ovum does not want to overplay the information security management issues associated with email, as the vast majority of corporate messages are the "flotsam and jetsam" of mundane business activities. But corporate compliance managers might think it prudent to add the following addendum to every email sent externally: **"This email address is not secure, is not encrypted, and should not be used for sensitive data."**

Figure 1: Ovum ICT Enterprise Insights Survey



Source: Ovum

Information security management underpins government, business, and commerce

The Edward Snowden revelations certainly placed a spotlight on the nature of government surveillance operations, and they served as a wake-up call for those businesses and institutions that routinely handle customer information and other sensitive business data. And yet, three years on from

the disclosures, relatively few organizations have systems in place that adequately secure and protect sensitive data at the edge of the organization, especially that which is in motion, such as email.

The threat of data interception by third parties and malicious acts by rogue actors may be of primary concern to a subset of organizations, but accidental exposure of information can just as easily result in the loss of professional and brand reputation, non-compliance fines, and even loss of business. Most business email users have, at some time or other, sent an email to the wrong person or attached the wrong file, and while the ability to retract a message may be possible when the sender and recipient(s) use the same email system, it is generally not possible to rescind messages that are sent to email addresses outside of the organization. Similarly, the ability to withdraw access rights to an email attachment is generally problematic unless proprietary information rights management technology is used.

High-profile news stories have raised the profile of data encryption, information security, and data loss prevention, especially on mobile devices. But organizations are still getting to grips with many of the concepts, challenges, and consequences of implementing this technology on a broad basis, and may be exposing their business data to risk while they do so. Ovum's advice is to pick a broadly impactful yet manageable business use case, such as corporate email and file sharing, and to then work through the issues of an end-to-end implementation with a trusted implementation partner or vendor.

Ovum's *Enterprise Security Software Forecast* (Report ID: EI0025-000018) predicts an average compound annual growth rate (CAGR) of 10.1% over the next three years, with annual global spending predicted to hit $50bn by 2019. It will be interesting to see where businesses and institutions spend their money and what they get in return. More importantly, it will be interesting to see how employees and consumers react to any change in process or interaction style, and how this impacts general business and commerce.

Enterprise IT infrastructure and end-user computing environments are going to be hybrid

Enterprise adoption of cloud-based email, communication, and collaboration services is predicted to accelerate as we head through the decade, with Microsoft and Google at the forefront of the market, along with growing competition from Amazon and others. However, Ovum predicts that hybrid configurations, where services run on-premise and in the cloud, will be common for many large organizations, and for a variety of reasons, ranging from the practical to the political. As a result, IT departments will have to think carefully about how they secure their data and where they place their trust.

The devices landscape will also continue to change in the years ahead, so email and data protection solutions must span a variety of platforms, operating systems, and architectures. New messaging architectures, protocols, and standards are also likely to emerge as the industry considers how best to move forward into the digital age. Consumer messaging apps, such as WhatsApp, Facebook Messenger, iMessage, and WeChat provide an insight into the future of modern communications, so organizations should start to consider how future messages and files flowing through their organizations might be protected and managed.

Email will continue to be an important medium for the communication and transfer of information, both internally within an organization and externally with third parties. But as enterprises of all sizes

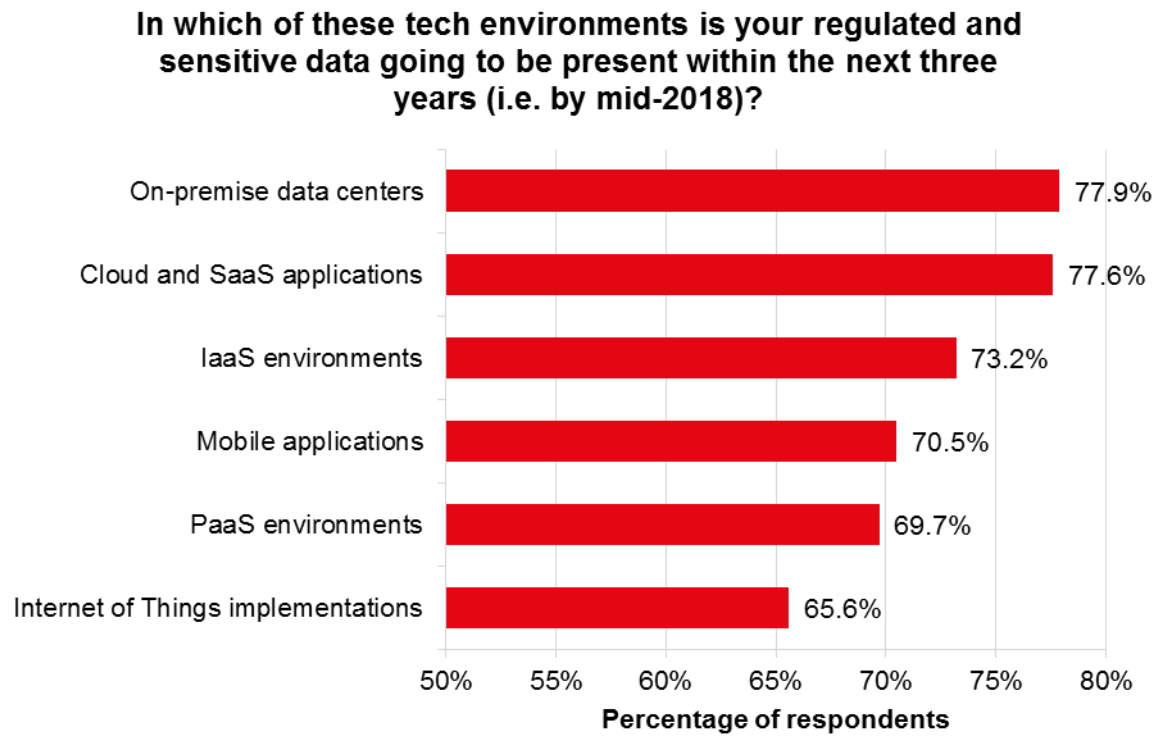
transition to hybrid email, content management, and collaboration environments, strategic attention must be focused on the situation before the complexity and management overhead of these systems gets out of hand. Organizations need to focus on running the business, not wrestling with data security challenges, so a well-architected, easy-to-use, and easy-to-manage approach to data privacy and security is required.

The long-term protection of customer and corporate privacy presents a significant challenge

Cloud computing is fueling productivity in modern business. It connects the entire workforce, bridges relationships between organizations, business partners, and customers, and connects everyone socially. It has transformed how we communicate and deal with information, radically changing the world's most established companies and how IT budgets are managed. Recent Ovum research found that on average, one-sixth of an organization's overall IT budget is already typically spent on software-as-a-service (SaaS).

Around 80% of enterprises are now using, or planning to use, cloud computing across deployment (private, public, and hybrid) and service (infrastructure-as-a-service [IaaS], platform-as-a-service [PaaS], and SaaS) models. This figure is up from two-thirds at the start of 2014. However, discussions with CIOs and IT professionals do expose a variety of issues relating to the long-term preservation of data and information, especially from the perspective of cloud-based email platforms and document management systems.

Figure 2: Tech environments where regulated and sensitive data is expected to be present



Source: Ovum

Sensitive content needs to remain secure, but at the same time it needs to be accessible at all times for business use and potentially for discovery requests. Data secured in an encrypted format must be decrypted each time using the appropriate digital key before it can be used. As we have already witnessed, encryption technology changes over time, which means that encrypted content stored over long periods must be actively managed to ensure that it remains accessible to those who need it. Retention periods for regulatory and compliance purposes may sometimes be decades long, so organizations must consider the business overheads associated with the longer-term management of encryption keys and digital certificates.

A major issue for organizations using encryption technology, especially where cloud-based services are concerned, is key management. This can be especially problematic during technology and solutions transitions. Today, most cloud-based solutions use encryption keys that are under the control of the vendor or service provider. But over time, organizations are likely to transition to a model where they manage all encryption keys, whether held on-premise or in the cloud, even if they do not have a burning desire to do so. Large organizations will need help and assistance managing this complexity, while smaller organizations will need help managing all aspects of the technology, from selection and implementation to upgrade and replacement.

Email has become woven into the fabric of IT systems and line-of-business applications

Even if encryption solutions have been deployed for employee-generated email, it is easy to forget that many emails are generated from enterprise applications and line-of-business systems. Such systems often send out sensitive information in batch processes or on demand, and although these may be encrypted, it is not always straightforward or easy for the recipient to decrypt them on their PC or mobile device. Indeed, consumer-related use of this technology has never caught on for this very reason, resulting in various work-arounds and mechanisms to address the issue.

Content of a sensitive nature is routinely stored in line-of-business applications, such as HR, CRM, and ERP, so not only are organizations at risk of security breaches by not encrypting this data, but they are also leaving themselves exposed to hackers every time data from these systems is sent via email internally or externally. At the same time, there is the risk that employees may inadvertently gain access to information they are not authorized to view. A recent study by Sophos noted that while there is widespread recognition of the importance of protecting customer data with encryption, this does not always extend to other sensitive information. For example, a third of 1,700 IT decision-makers surveyed admitted that they do not encrypt employee bank details, while 43% leave sensitive HR files in plain text.

Organizations clearly need a solution that maintains the privacy of emails that are sent from applications without the need to make any changes to the underlying applications. S/MIME (secure/multipurpose internet mail extensions) and PGP (pretty good privacy) are two major encryption standards that are used by some email applications, but even the creator of PGP, Phil Zimmermann, admits that using the technology across all devices is a technical challenge. Passing the all-important usability test is crucial for any product or technology adoption, and most of the offerings available thus far have clearly failed to clear the bar.

Mobile devices are often treated as second-class citizens where email encryption is concerned

Smartphones and tablet computers have extended the reach and range of digital business processes, but maintaining data privacy and information security on these devices continues to present challenges to corporate IT departments, with many still grappling with mobile device management (MDM) platforms and enterprise mobility management (EMM) solutions. It is somewhat ironic that the primary requirement for such investments continues to be driven by the need to protect and secure corporate email, a challenge that was for the most part solved by BlackBerry over a decade ago. Some organizations have adopted "closed" mobile email software solutions, but these often lack the features and functionality that consumer-minded employees are looking for or wish to use.

The fact that MDM/EMM products exist at all is testament to the fact that developing easy-to-use, easy-to-manage, secure online communication solutions is a difficult thing to get right for all interested parties. Over the years, a reasonable set of products have been developed for personal computers running Microsoft Windows, but choice is more constrained for macOS and Linux users. Choice and functionality are constrained even further on mobile devices running Apple iOS or Android, which presents a real challenge for those organizations wishing to transmit information more securely, whether using digital signatures, email encryption, or information rights management technology.

Enterprise MDM products often include device encryption capabilities and information security management elements, but these solutions generally only protect part of the communication and collaboration exchange when engaging with external organizations and third parties. Moreover, if MDM inhibits the workflow, efficiency, and effectiveness of the workforce, then a different set of compliance and security problems are likely to arise as employees look for work-arounds and alternative communication mediums.

BYOD and mobile device proliferation present significant challenges to corporate IT policies

Some organizations try to constrain their information security management boundaries by restricting employees to a limited set of computing devices and standard operating environments. However, the appeal and flexibility afforded by the bring your own device (BYOD) movement have served to turn many corporate IT polices on their head, piling extra burden onto the beleaguered IT department as a result. Those organizations wishing to implement or accommodate BYOD want to do so in the most efficient and cost-effective way possible, which means finding a set of products and solutions that suit the "everything-is-hybrid" enterprise IT architecture model.

Many enterprises are using flexible device strategies to mobilize the workforce and reengineer business processes. Used in conjunction with smartphones and tablet computers, apps, cameras, and data capture peripherals are being used by field agents to capture, consume, and transmit content. Some of this content will be of a sensitive nature and needs to be protected in transit as well as at rest on the device, and IT departments would ideally like to implement a single solution that does this across all device types, operating systems, and relevant applications.

Developed and licensed by Microsoft, Exchange ActiveSync (EAS) has become the de facto standard for synchronizing mobile devices with messaging servers, providing access to email, calendar,

contacts, notes, and tasks. EAS has evolved to support a broad range of mobile device policies and also facilitates the use of S/MIME email encryption. EAS is supported by Android, iOS, Windows Phone, and BlackBerry, so sending and editing encrypted emails on mobile devices is now much easier than it once was. The implementation of EAS can present a few challenges for organizations that do not have a significant investment in Microsoft products, and for those that do, migration to the cloud and Exchange Online brings with it a different set of encryption options (Office 365 Message Encryption, S/MIME, and Information Rights Management) that need to be considered and understood. There are, of course, alternatives to EAS, and there are also products available that are enabled by EAS that do not require Office 365 Message Encryption (OME).

The expectations of business IT users are set by their personal use of consumer IT

The vast majority of employees owning a smartphone or computer will have a personal email account, yet only a tiny minority will have any understanding of S/MIME, encryption, or digital signatures. As with the web, people just use what they have been given and do not seek to complicate matters further. This means that the biggest risk for organizations today from an information security management perspective is ignorance.

Most employees are generally unaware of the technical aspects of the computer and communication equipment that they use on a daily basis. Employees use the tools they are given and expect the "experts" to make it work in the manner required. Providing employees with the facility to digitally sign and send encrypted emails is a good starting point, but it does require training and education to drive adoption. And even then, many users will not bother using the capability if it complicates their workflow or hinders their ability to work smoothly with partners, customers, and clients.

Simply put, end users do not expect to have to take additional steps to send business emails, and many already think that their communications are secure and private because they are using "enterprise products." After all, this is business email. And then there is the question of which emails to encrypt and which ones to leave as-is. These are the kind of decisions that are best handled by policy-based IT solutions, not business professionals trying to get work done.

Restrictions on large email file attachments are driving business users toward shadow IT

The proliferation of corporate email has resulted in huge storage requirements for on-premise email servers. To address this almost exponential growth, IT managers have implemented mailbox quotas and file attachment size restrictions. Alas, this tactic is driving many business users toward file transfer products that are not sanctioned by the business, with consumer-oriented file sharing products being used as the primary work-around.

The Ovum report *Employee Mobility Survey 2015/16: Task and Application Usage Trends* shows that 32.5% of the 4,502 employees who were surveyed use a file sync and share product that they found themselves. This demonstrates that if organizations do not supply access to systems for employees to transfer and share data, they will provision their own solutions, and these solutions might not provide

the necessary level of security, audit, and control that the data warrants, thus once again putting sensitive data at risk.

Most of the vendors offering freemium, consumer-based file sync and share products now offer premium products for business use. But these are not the versions being used, because when employees self-select these tools they spare little, if any, thought to the management of the content being stored within the repository. They are just trying to get work done.

Cloud services give rise to data sovereignty issues

Even before Edward Snowden's revelations showed the full extent of the US National Security Agency's (NSA) electronic surveillance, data privacy was becoming a global issue. Government snooping, combined with massive data leaks over the last few years, has forced national governments to recognize that privacy laws have outlived the paper-based age, and need to catch up to the realities of the digital economy. The result has been an unprecedented wave of new legislation designed to govern how certain sensitive data can be gathered, stored, processed, and shared.

Countries as diverse as Brazil, Singapore, and Russia are tightening regulations, and the EU is nearing the end of a lengthy process of revising legislation in this field, which will affect any organization operating in its member countries. These restrictions are being imposed because organizations are becoming borderless and employees more mobile, which along with a migration to cloud-based IT systems can cause conflict with new laws. The compliance obligations arising from legislation are becoming more complicated, particularly for organizations that operate across different jurisdictions, and particularly in the context of how legislation applies to data that is stored by cloud-based service providers.

Global organizations need to adopt an orchestrated approach to data sovereignty and information security management that covers people, processes, and technology, but this is easier said than done. Ovum recently surveyed 366 IT decision-makers from around the world, representing different industry sectors and organizational sizes. When asked about investment strategies, 55% said they are planning to provide new training for employees, 51% said they will amend and adapt policies, and 53% said they will prepare by adopting new technologies. However, most organizations are not effectively using even their current technology to address data privacy concerns. According to the survey results, only 44% of respondents monitor user activities and provide alerts to data policy violations, and only 53% classify information to align with access controls. Almost half (47%) have no policies or controls that govern access to consumer cloud storage and file-sharing systems such as Dropbox.

The decision-making challenge is exacerbated by a patchwork of contradictory and conflicting global privacy regulations, and organizations therefore need technology options to address all eventualities. Another complicating factor is trust in the provider market, with the Ovum survey identifying a "Snowden effect" that seems very real. The US is ranked as the least trusted country and the most likely to gain unauthorized access to sensitive information among 20 industrialized economies, with China coming in second, and Russia third. New regulations will put US companies at an even greater disadvantage, with 63% of respondents believing that the proposed EU GDPR regulations will make it harder for US companies to compete, and 70% thinking that the new legislation will favor European-based businesses.

Summary

Compliance and regulation have been driving the corporate email management agenda for many years, but evidence suggests that information security management, with a particular emphasis on privacy, is now starting to drive investments for proactive organizations. In addition, high-profile news stories involving encryption technology and mobile devices have pushed the topic of email management and the protection of data in motion onto the executive agenda. For European businesses and institutions, governance and data sovereignty have become key areas of concern where cloud-based email services are concerned, especially where the service is delivered by a US company.

From an industry perspective, the base-level security afforded by email's underlying protocols is being closely scrutinized, as comparisons are made to modern chat-based systems and consumer messaging applications such as WhatsApp. But while improvements in message transport security are welcome, organizations must still consider the need for end-to-end encryption in their business process and customer interactions, especially where mobile devices and connections to public networks are concerned.

Solutions for email encryption, secure managed file transfer, and secure mobile communication are available from a range of vendors, and using these solutions ensures that online communication with partners and customers remains confidential, reliable, and efficient. However, product choice begins to narrow when device- and location-independence are factored into the selection process.

Totemo, a Swiss software company, can address these requirements through its patented, FIPS 140-2-validated security platform, which can be integrated into almost any existing IT infrastructure. Totemo's customers include major organizations from across a range of industries, including financial services, pharmaceutical, automotive, telecommunications, healthcare, manufacturing, government, application service providers (ASP), outsourcing providers, and professional services. Totemo was founded in 2001 and is based in Küsnacht, Switzerland.

Appendix

Methodology

This white paper was sponsored by Totemo and draws on Ovum's research and analysis of the enterprise end-user computing and information security management markets. The paper also references Ovum's proprietary tools and databases. The views expressed in this white paper are based on Ovum's ongoing research into the technology and services markets, including conversations with IT vendors, system integrators, service outsourcers, and enterprise clients.

Further reading

Data Privacy Legislation Impact on Enterprises, IT0018-001493 (April 2016)

Enterprise Security Software Forecast, EI0025-000018 (October 2015)

Aligning Mobility Strategies with Data Privacy and Tax Regulations, IT0021-000094 (August 2015)

The Impact of EU Data Privacy Legislation on the Enterprise File Sync and Share Market, IT0021-000080 (April 2015)

"Government can't afford not to manage BYOD," IT0007-000788 (November 2014)

Office 365: Email Migration, Coexistence, and Adoption, IT0021-000035 (October 2014)

Authors

Richard Edwards, Principal Research Analyst, Enterprise Mobility & Productivity

richard.edwards@ovum.com

Alan Rodger, Senior Analyst, IT Infrastructure Solutions

alan.rodger@ovum.com

Sue Clarke, Senior Analyst, Information Management

sue.clarke@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

CONTACT US

www.ovum.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo