SIGMA
SOLUTIONS

SigmaUptime

Volume 12 Number 3

YOURS, MINE & OURS

THE CHALLENGE OF COMMINGLED PERSONAL AND BUSINESS DATA IN THE AGE OF BYOD.

Administration | Maintenance

Monitoring | Troubleshooting

Sigma Managed Services and IT Operations

Sigma's portfolio of managed services enable you to transfer full lifecycle support of your IT infrastructure to Sigma's highly qualified engineers, freeing up valuable resources for strategic initiatives that are core to your business and customers. All critical components of your data center are protected and maintained including server, storage and network infrastructure, infrastructure applications, backup systems, virtualization and IP communications. Elements of our Sigma One Source Managed Services portfolio include:

Private, Public & Hybrid Cloud Integration

Industry reports are filled with headlines proclaiming most companies will rely on cloud computing in the very near future. Count on Sigma to provide the guidance and insight to help you determine the right balance of cloud-based and on-premise computing strategies.

Desktop, Mobile Computing & Collaboration

Sigma architects create custom solutions to address your needs for:

- Desktop virtualization
- Messaging and collaboration
- Wireless and mobility
- Mobile device management

Application Infrastructure Solutions

Sigma provides the systems and storage that form the foundation for "big data" solutions, including:

- Data integration
- Big data/analytics
- Industry-specific integration

Integrated Data Center Solutions

Sigma's expert engineers plan, implement and operate solutions for:

- Virtualization
- Storage
- Networking
- Information management and security

SIGMA SOLUTIONS

888-895-0495 **www.sigmasolinc.com**

Austin | Chicago | Dallas | El Paso | Houston | New Orleans | Oklahoma City | San Antonio | Tulsa

Contents

Sigma
UPTIME

Editorial Correspondence:
7360 East 38th Street, Tulsa, OK 74145
Phone (800) 726-7667 • Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

Sigma UPTIME is published bimonthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

More and more business data is stored on employees' personal mobile devices, creating privacy threats for employees and legal and regulatory challenges for businesses.

YOURS, MINE and OURS

It used to be easy to separate work from our personal lives. Most of us went to work in brick-and-mortar business locations where we were supplied with the tools we needed to do our jobs. Computing equipment was tethered to the company network by cables, and it was difficult to transfer more than a token amount of data into or out of the office.

Mobile devices have changed all that.

Today's smartphones and tablets are powerful computers capable of storing large amounts of data. They enable us to work from anywhere, blurring the line between our personal and professional lives.

The Bring Your Own Device (BYOD) trend makes the distinction even fuzzier, creating new legal and business challenges as a consequence. One of the biggest issues involves the growing volume of company data stored on personal devices, and the conflict between employee privacy and the employer's need to control and access that data.

"Workers don't want their employers examining their personal devices. But if the company becomes embroiled in litigation, it may be required to confiscate employees' phones to determine if any relevant information is stored there," said James Smith, Director of Solutions Engineering, Sigma Solutions.

continued on page 6

More than one-third of businesses surveyed by Symantec have experienced the exposure of confidential information on lost or stolen mobile devices.

"And if a device is lost or stolen, the company may need to remotely wipe the data. The employee's personal information is going to be erased along with the company data."

It's not a trivial matter. According to Symantec's 2012 State of Information Report, 31 percent of enterprise information is accessed on mobile devices, and 14 percent of it is stored there. The Symantec report does not break down these statistics in terms of personal versus company-issued devices. However, a 2013 Cisco Partner Network Study found that 92 percent of employees use their own smartphones for work at least once per week, with 62 percent doing so every day.

Legal Challenges

The drivers behind the BYOD phenomenon vary. Some companies have embraced the concept, citing increased revenue, productivity gains and reduced equipment costs as key benefits. In fact, Gartner predicts that by 2017 half of employers will require employees to supply their own devices for work purposes.

Other organizations have been more hesitant to allow BYOD but have given in to employee preferences. Workers like using the devices they are most familiar with and the convenience of accessing business applications and data from anywhere.

Whatever the impetus behind BYOD, it is exacerbating a number of business challenges related to data access and protection. One such issue is e-discovery. In the very likely event that a company becomes involved in litigation, it is required to produce all evidence related to the case — including any data that might be stored on employees' smartphones.

Email, text messages … any amount of information could be relevant, and the company has an obligation to produce it no matter where it's stored. That raises tricky privacy questions, with rules varying from state to state.

Nearly one-third of all respondents to Fulbright's 9th Annual Litigation Trends Survey encountered issues involving privacy and/or data protection in disputes or investigations in 2012. Rates were particularly high among larger companies, as well as among the engineering, financial services, healthcare, insurance and tech sectors. Issues arose most frequently in the context of collecting data from company equipment and from employees' personal equipment.

Experts say that company data usually exists in multiple places so it's relatively rare that an employee's smartphone would have to be confiscated for e-discovery. Still, the company would have to disclose the fact

BYOD Policies on the Rise but Gaps Remain

As the Bring Your Own Device (BYOD) trend continues unabated, organizations are attempting to close legal gaps by informing workers of their rights and establishing policies and rules governing BYOD programs. According to research by Ovum, 30.6 percent of U.S. employees who use their own devices at work report having signed a corporate policy governing BYOD.

However, Ovum warns that too much BYOD activity is still going unmanaged. Of those survey respondents who bring their own devices to work, 17.7 percent claim that the IT department doesn't know and 28.4 say their IT department actively ignores that BYOD is happening.

"Unmanaged BYOD creates a great data security risk, and the implications of losing sensitive data via a personally owned device can be dire from financial, reputational and legal perspectives," said Richard Absalom, consumer impact IT analyst at Ovum. "Every business must understand the behavior of its own employees … and manage it according to its risk profile."

that the information is stored on the smartphone. The device could be implicated in an evidentiary challenge.

Regulatory Risk

Regulatory compliance is a closely related issue. Organizations face an increasing number of government and industry regulations mandating the protection of sensitive data and tracking of information access. BYOD threatens regulatory compliance due to increased security risks.

Mobile devices can easily be lost or stolen yet few employees encrypt data or even protect the device with a strong password or passcode. As a result, more than one-third of businesses surveyed by Symantec have experienced the exposure of confidential information on lost or stolen mobile devices.

A new study by the Ponemon Institute suggests that companies aren't doing enough to reduce the risk of BYOD. More than 60 percent of the privacy and compliance professionals surveyed admitted that they don't require or were unsure if they required mobile devices to be tested for security before allowing them to connect to the company network. Only 44 percent said their companies effectively ensured that only authorized individuals accessed corporate systems.

"This is a huge gap, particularly for companies in the healthcare and financial services sectors," said Elias Khnaser, Chief Technology Officer, Sigma Solutions. "It can also impact companies that must comply with the Payment Card Industry Data Security Standard if cardholder data is stored on devices outside the company's control."

Further complicating matters is employee privacy. While organizations can monitor employee behavior on company-owned devices and networks, monitoring employee-owned devices can raise privacy concerns. And an organization could face liability for wiping personal data from a device that is lost or stolen unless the employee has agreed to it. Gartner recommends that employers obtain express, written consent to delete data from personal devices.

"Organizations with BYOD programs need to be aware of the legal and regulatory issues raised by employee-owned devices," Smith said. "Companies need to protect and access business data yet be sensitive to employee privacy. It's a difficult balance to strike."

Making the Switch to IPv6

It's not exactly like the Mayan Apocalypse, or even Y2K. No tick of the clock is going to signal the end of the IPv4 Internet addressing system. But network administrators worldwide are facing the task of transitioning to IPv6, a project that requires careful planning to avoid business disruption.

The move to IPv6 is inevitable. IPv4's 32-bit addressing allows for about 4.3 billion unique IP addresses. That's simply not enough to accommodate all of the Internet-connected devices in use today. In fact, the pool of IPv4 addresses managed by the Internet Assigned Numbers Authority dried up in 2011, although a few regional Internet registries still have some IPv4 addresses available.

Using 128-bit addressing, IPv6 theoretically allows the creation of more than 340 trillion trillion trillion possible unique addresses. That's about a billion-trillion times larger than the total pool of IPv4 addresses, enough to give every human on the planet trillions of addresses of their own.

Although it has been available for a decade, IPv6 has been slow to catch on while IPv4 addresses were still available. Techniques such as network address translation (NAT), in which many of an organization's devices are hidden behind a single public IP address, have extended the life of IPv4. However, organizations need to make their networks compatible with the increasing number of IPv6 addresses. And if their websites and other web-based applications cannot be reached through IPv6, they are not accessible across the entire Internet.

Planning Ahead

The transition to IPv6 is not simply a matter of flipping a switch. IPv4 and IPv6 are different protocols and are not directly compatible, so programs and systems designed to one standard cannot communicate with those designed to the other. Techniques such as NAT further complicate the transition to the new protocol.

This doesn't necessarily signal the impending death of IPv4, however. Dual stack IPv4/IPv6 devices and software can help ease the transition by running both protocols simultaneously. Other strategies for making the transition include performing IPv6-to-IPv4 translation, tunneling, and using proxy servers to facilitate a migration to the new address space as software allows.

The latest versions of most enterprise-class network components and systems are already IPv6-capable. Still, most organizations have legacy equipment and applications that do not support IPv6 — a fact they must bear in mind as they plan future IT purchases. Experts also say firewall and security policies should be reviewed to determine how IPv6 will affect them, and in-house software should be upgraded to ensure compatibility. IPv6 should be tested in an internal lab to certify software, develop operational and support practices, and support transition planning.

Perhaps the biggest impediment to the IPv6 transition is the learning curve involved. Network engineers who are well versed in IPv4 shouldn't have much trouble learning IPv6. Nonetheless, IPv6 involves new concepts and functions in a very different way than its predecessor. Organizations should invest in training so that network administrators can become familiar with deploying and configuring the new protocol.

Great Potential

While network future-proofing and infrastructure management are the key reasons for transitioning to IPv6, businesses will be able to leverage the new protocol in a number of ways. At the most basic level, it supplies the additional IP addresses needed to accommodate the many smartphones and other Internet-connected devices flowing into the workplace.

There is also huge potential for new applications and devices that are IPv6-enabled. IPv6 will enable devices to multicast, which is the ability to send information and establish unique links to multiple devices without resending the same data to each device. That will make it easier to stream live video to multiple locations at once.

IPv6 also offers built-in security and enhanced support for streaming media and other Web 2.0 applications. In addition, the QoS features built directly into IPv6 can help improve the quality of encrypted Voice over IP calls.

The depletion of IPv4 address is not some impending doomsday. As IPv6 continues to gain momentum, however, organizations that fail to plan ahead risk finding themselves at a competitive disadvantage. Even if organizations don't have immediate plans to implement IPv6, preparing for the inevitable transition now as opposed to later will only decrease the burden on IT administrators.

IPv6 will open up a pool of Internet addresses that is virtually inexhaustible for the foreseeable future. Making the switch to this new protocol doesn't have to be daunting if a thoughtful approach is taken.

IBM®

The powerful IBM System x servers. Built for business-critical solutions.

Your business is poised to take advantage of the next big opportunity. But is your IT environment ready to help you meet your goals? IBM System x advancements in scalability, reliability and performance can help you take your business where you want it to go. IBM provides the technology that will help your business innovate and thrive. Contact your Sigma representative and let us show you how IBM System x can drive your business today and provide a platform for continued innovation tomorrow.

SIGMA
SOLUTIONS

888.895.0495
www.sigmasol.com

File Sharing in the Cloud

Online file-sharing solutions allow organizations to reap the benefits of easy file sharing and collaboration in the cloud.

Online file sharing represents yet another consumer technology that is taking hold at the corporate level. Online file sharing solutions are Internet-based services that enable users to store, access, share and collaborate on documents and other files in the cloud. These services have become popular in recent years as people look for ways to access their documents from multiple devices, including traditional PCs, tablets and smartphones.

Although online file sharing has its roots in consumer cloud services, it is beginning to transform the way businesses and people work. Collaboration can be greatly improved by allowing document access from anywhere, and employees find that online file sharing is much more convenient than traditional access methods. IT departments also get numerous benefits by switching to online file sharing.

According to a survey of nearly 500 IT professionals at small, medium and large organizations by Enterprise Strategy Group (ESG), 28 percent of organizations have already established corporate accounts for online storage and file-sharing services. That number is expected to grow to 50 percent during 2013.

"By now, many, if not most, knowledge workers have been exposed to some form of consumer online file storage service such as Dropbox or Box," said Terri McClure, ESG Senior Analyst and co-author of the report. "However, the fact that these services have been rapidly adopted by consumers on a personal basis, often via their smartphone's app store, has led to a situation in which companies are increasingly looking to standardize their employees' use of these services through company-owned and -managed accounts. Our research validates that IT and business professionals are serious about making online file sharing services a company-wide resource for their employees."

Business Collaboration Benefits

Keeping documents up-to-date and distributing the right copy has always been a challenge. Many companies are finding that switching to online file sharing is increasing collaboration and saving lots of money. As more and more documents are stored electronically, collaboration among workers using these documents stored online is greatly improved because the Internet never closes — workers can quickly refer back to a document when an idea appears. With an online file sharing solution, knowledge workers and their colleagues will always be on the same page (literally) and business planning, strategy and brainstorming can focus on the work.

The increasing use of smartphones and tablets by employees is a key driver behind the adoption of online file sharing services at the corporate level. The ESG survey found that 41 percent of organizations that are experiencing significant growth in smartphone and tablet usage already have a corporate online file sharing account in place, and another 27 percent expect to set up a corporate online file sharing account in the next year.

"The preponderance of smart phones and tablets in the workplace has driven many companies to sign up for and deploy a corporate account with an online file sharing service," said McClure. "Among organizations experiencing growth in these devices, the purpose for deploying a corporate online file sharing account is often to enable access to files from mobile devices."

Organizations turning to file sharing in the cloud to facilitate employees accessing files and collaboration from endpoint devices are discovering that these online services can also displace in-house file servers and the associated management complexity. Cloud file services can reduce the costs associated with virtual private networks (VPNs).

IT Department Benefits

In a typical company, the IT department is tasked with maintaining multiple servers (and their environments) for file sharing. Ensuring that these files are backed up and recoverable adds to the workload and a significant portion of the IT department's operating budget. With online file sharing, the cloud handles the task of storing and serving files.

However, concern over potential security vulnerabilities — such as data loss, theft or risk of regulatory compliance violations — is the top reason organizations are not deploying online file sharing. In addition, employees are placing corporate files in free cloud storage sites, creating serious security and compliance risks for their organizations.

ESG found that organizations are struggling to control unauthorized online file sharing account usage. According to ESG research, 83 percent of organizations are actively monitoring employees' devices and activity to uncover rogue online file sharing accounts. Yet 16 percent simply rely on an honor system, trusting that employees are not using unauthorized online file sharing services.

"Honor systems don't go far enough in mitigating the risks created by rogue online file sharing accounts," said McClure. "It's not just potentially malicious employees who could expose their organization to a data breach. Even well-intentioned employees may decide to use personal online file sharing accounts to get their jobs done faster, not understanding the security vulnerabilities this creates for their organizations."

Online file sharing is also a challenge for IT groups because they have to manage more data stored outside the data center, including on smartphones and tablets. Still, online file sharing adopters say collaborating through the cloud instead of on VPNs makes sense from a management as well as financial standpoint.

Enabling TRANSFORMATION through IT as a service

Sigma has been providing industry-leading data center solutions since 1992. Our consultative approach amplifies our engineering and integration skills, helping you to reduce costs and risks while maximizing the business benefits of your technology investments.

Sigma delivers value through an agile IT environment that responds to changing business objectives and market conditions. We can help you meet all of today's business technology challenges, including:

- Cloud Computing
- On-Demand IT
- Consumerization/BYOD
- Collaboration
- Big Data
- Mobile Device Management

SIGMA
SOLUTIONS

888.895.0495
www.sigmasol.com