Mobile is the New Normal for Conducting Business

"One-fourth of information workers using tablets and 22% of all information workers use a file sync/share solution like Box, Dropbox, SugarSync, or YouSendIt—and 70% of employees using Dropbox—use it for work or work and personal files." [1]

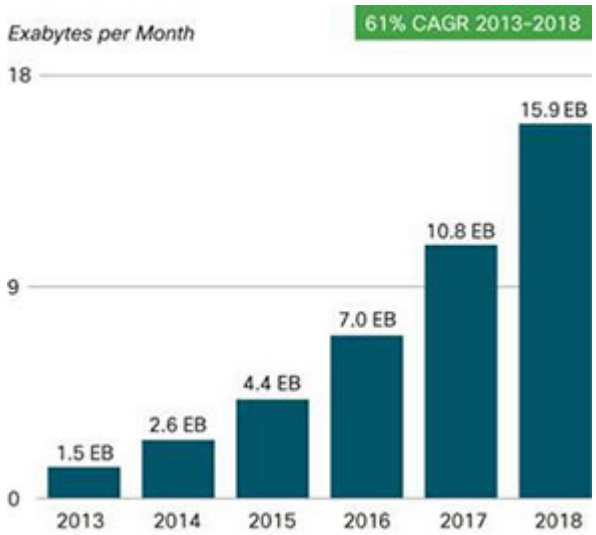
BYOD Comes of Age in the Workplace

These are trying times for IT organizations—particularly when it comes to resolving conflicting demands for security and convenience. IT organizations are being pulled in two different directions: On one side, increasing regulatory compliance and governance mandates require that businesses take great care of sensitive information, tracking and auditing its use and preventing unauthorized access. On the other side, employees, partners, and customers expect new levels of convenience and immediacy when it comes to accessing information.

Mobile is the new normal for business computing. In addition to laptops, VPN, and so on, smart phones and tablets are giving people new levels of mobile connectivity—and they expect to be able to use them for work.

"Global mobile devices and connections in 2013 grew to 7 billion, up from 6.5 billion in 2012. Smartphones accounted for 77 percent of that growth, with 406 million net additions in 2013." [2]

Cisco predicts that by the end of 2014, the number of mobile-connected devices (including machine-to-machine or "M2M") will exceed the number of people on Earth. (As shown in the chart.)



4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

80% of Smartphones Used in the Workplace are Employee Owned

"Enterprise IT was once the driving force behind consumer technology innovation and trends. In a role reversal, tech-savvy consumers are now pushing businesses to integrate personal mobile devices into the enterprise IT fabric." [2]

In June 2012, McKinsey reported[4] that 80% of smartphones used in the workplace are employee owned. Helping fuel the growth in enterprise mobility is the fact that more people have multiple devices of their own and they don't only use them for personal email. Employees want and expect to use their tablets, smart phones, and personal computers to access work applications, whether at home or on the road. This is even true in highly regulated industries like healthcare, where providers want to use mobile devices to access sensitive information.

Overall, these trends can be beneficial for businesses by improving productivity and collaboration, and by reducing costs of provisioning company-owned devices to users. However, these related trends have a major impact on IT organizations that now have to support file access for devices that are outside the enterprise networks (mobile), and/or outside of IT control.

One of the greatest challenges for the IT organization is managing the wide range of unstructured documents and files that are essential to daily processes and operations. Contracts, product plans and designs, presentations, status reports, and financial spreadsheets are just a few examples of the kinds of documents that contain intellectual property, proprietary information, or regulated data.

These are exactly the types of files that are at the heart of collaboration with partners and customers for business productivity. Employees want and need to access these files from their mobile devices. In this environment, you need a sound strategy for providing access while retaining some degree of control.

Limitations of Cloud-Based File Sharing Services

Cloud-based services like Dropbox or Google Apps make it easy to share files between devices and locations. Using these services, files are stored in the cloud-based service and synced onto users' desktops or mobile devices. These services are easy for people to use; most users have a consumer file-sharing background. But these services also have potential drawbacks for business applications:

- Realistically, most of the files you need to share are created within your enterprise, which means that you're paying to store them twice: once on internal systems and once in the cloud.
- As a business, you need to track and audit sensitive data. When the data resides in multiple locations, managing compliance with policies is near impossible.
- You may not be ready or willing to move sensitive data to the cloud. Many businesses want to keep their most sensitive data within their own enterprise network for fear of a data breach (like the one that happened to Drop Box in 2012[3]).

Ad Hoc Methods Limit Visibility and Control

Another approach is to leave it to employees to transfer the files they need, as they need them. For companies that have not actively embraced a strategy for mobile content sharing, this is the status quo, with employees using a combination of methods including:

- Sending email attachments to their personal email account or to others
- Writing files to removable media like USB devices
- Using their own, personal accounts on consumer file-sharing services

While these ad hoc methods offload the work from the IT organization, they burden the user with the effort of figuring out how to move files as they need to do their jobs. For example, some files are too large to send in email attachments.

In addition, the business as a whole loses visibility into where and how data is moving through the organization. Without this insight, there's no way to know if a data breach has occurred. The solutions used rarely meet business requirements for security. For example, email attachments are typically sent without encryption, and USB devices are easily lost or misplaced.

Employee Training and Policies Are Not Enough

Many businesses attempt to educate employees about policies for remote or mobile file access and sharing. You might try to forbid mobile access to sensitive data, for example, or create strict employee guidelines for when and how data can be moved to personal or remote devices.

Experience shows that relying on behavioral policies is simply not enough. If employees want or need to work from home or on the road, they will find a way to do so, even if it means circumventing corporate policies.

If you have no visibility into whether people have local copies of sensitive data, then you cannot understand or mitigate your risk if an employee's mobile device is stolen. And if the employee was in violation of policy when the breach occurred, they are less likely to report it. While employee training and policies are invaluable, you need to supplement them with the right technologies.

Even rocket scientists don't get it right: A report to the US House of Representatives in February 2012 revealed that "Between April 2009 and April 2011, NASA reported the loss or theft of 48 Agency mobile computing devices, some of which resulted in the unauthorized release of sensitive data including export-controlled, Personally Identifiable Information (PII), and third-party intellectual property." [5]

Combining On-Premises Control with Cloud-Based Access and Sharing

Clearly, you have to support remote and mobile file sharing, but does that mean changing the way that you currently do business or manage access to files? You may not be willing to move your critical files to cloud-based file sharing services, but you still need to provide access to employees and partners wherever they are, on whatever devices they use.

Long a leader in secure file sharing, Globalscape offers another option for handling enterprise mobility and personal devices. The company has designed a mobile file sharing solution to complement its award-winning, secure file transfer offering, EFT™ to give you another way to handle the growing trends in enterprise mobility and BYOD without sacrificing control.

Centralized Control and Mobile Access Using Globalscape's Mobile Transfer Client™ (MTC™)

Globalscape's Mobile Transfer Client™ lets businesses retain control over their information while giving employees and partners the flexibility to access the information they need, when and where they need it.

MTC provides simple and secure mobile access to files stored and managed securely within EFT. Businesses benefit from having a centralized location for secure file access on EFT, without needing to upload/sync files with cloud servers or pay for additional cloud storage.

EFT can reside in your enterprise data center or in secure, hosted facilities, depending on your deployment model. Either way, files are not transferred to a separate cloud storage service, nor are they duplicated between your file servers and the cloud. It works with files of any size, and encrypts data in transit for secure access.

MTC adds convenient mobile access to business files without compromising security and controls over file sharing. The administrator can define access policies for files in shared folders. EFT automatically applies access policies and tracks and audits all access, so you have visibility into what's happening with business data.

How MTC Works

Before anyone can use MTC to access files on EFT, the user must have an account on EFT, and mobile users must download and install the MTC app on their devices. Just as with any other EFT account, the administrator defines access policies for each MTC user or group. When the remote employee wants to use a file that is on EFT, they must first authenticate with MTC, select the appropriate containing folder, and then select the file. EFT and the MTC app create a secure pathway, immediately compressing, encrypting, and delivering the content to the remote user. The user views the file with the available apps on the mobile device. MTC does not upload files to separate servers in the cloud; the file remains on EFT, and data is SSL-encrypted in transit.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

If the user has appropriate permissions on EFT, they can upload a revised version of the file from their device back to EFT. Everyone working on the file will see the latest version, which accelerates collaboration.

Using Globalscape EFT, you retain control over files on a server that you manage, with policy-based access controls. You control where the data is stored, whether on-premises or in a hosted environment. All file access is audited and tracked, whether that access occurs within enterprise networks or from unmanaged devices from afar. You have one place to set policies, track access, and secure your files.

Summary

Not taking action is not an option in today's mobile and consumer-driven IT environment. If you ignore the need for mobile access, people will find ways around policies and potentially expose your business to unseen risks.

You don't have to be forced to use a cloud-based file storage solution. Globalscape's EFT with MTC combines the best of both on-premises server and secure moblie access. Using Globalscape, you retain control over your information assets and visibility into who accesses them. At the same time, you can satisfy employee and partner requirements for mobile and remote access to information and flexible collaboration.

Visit http://www.globalscape.com/mft/mobile-transfer-client.aspx to download a PDF of the MTC datasheet, user guide, and administration guide.

Sources:

1. Schedler, Ted. "2013 Mobile Workforce Adoption Trends." Forrester. 4 February 2013. https://www.vmware.com/files/pdf/Forrester_2013_Mobile_Workforce_Adoption_Trends_Feb2013.pdf
2. Cisco Visual Networking Index. "Global Mobile Data Traffic Forecast Update, 2013-2018." 5 February 2014. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html
3. Information Age. "Dropbox Confirms Security Breach." 1 August 2012. http://www.information-age.com/technology/security/2114488/dropbox-confirms-security-breach
4. McKinsey & Company, Inc. "BYOD: From company-issued to employee-owned devices." June 2012. http://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/High Tech/PDFs/BYOD_means_so_long_to_company-issued_devices_March_2012.ashx
5. Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology. "NASA Cybersecurity: An Examination of the Agency's Information Security: Statement of Paul K. Martin, Inspector General, NASA." 29 February 2012. http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf

About Globalscape

Globalscape ensures the reliability of mission-critical operations by securing sensitive data and intellectual property. Globalscape's suite of solutions features Enhanced File Transfer™, the industry-leading enterprise file transfer platform that delivers military-grade security and a customizable solution for achieving best-in-class control and visibility of data in motion or at rest, across multiple locations. Founded in 1996, Globalscape is a leading enterprise solution provider of secure information exchange software and services to thousands of customers, including global enterprises, governments, and small businesses.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)