UBM

Secure Enterprise File Sharing:

Striking the Right Balance Between User and IT Needs

By Michael Krieger

THE SOCIAL BUSINESS. We live in a world increasingly fueled by social interactions and social media. The benefits of a social, collaborative business environment are clear: faster decision making; better communication with customers, partners and co-workers; and a better understanding of the ever-changing marketplace.

That often requires sharing of data not only between users' desktops; increasingly mobile devices including tablets and smartphones are being used to both consume and exchange business-critical information. And since simplicity and speed are both key factors in determining whether users will adopt a new tool, many business users have turned to public cloud services rather than wait for internal IT to deliver a collaboration solution that works for them, leading to the rise of "Shadow IT." However, by circumventing IT to get this functionality on the spot, users may unintentionally compromise security and governance mandates.

WHAT'S AT STAKE?

Uncontrolled file sharing — done outside the aegis of IT management — is dangerous. First, shipping files and documents utilizing consumer or public file-sharing services can violate government regulations, including PCI, HIPAA, SOX and other U.S. regulations, not to mention the litany of European and other regulations that multinational organizations need adhere to.

Consumer-grade file sharing tools bring other risks as well. There is very little information — and less visibility into the security practices such as encryption at rest and in motion, detecting suspicious activities and antivirus measures that are employed in these data centers. Before utilizing one of these services, make sure they measure up to your standards. Pay special attention to the lack of encryption, since shared sensitive information — such as that pertaining to merger and acquisition activity — may risk exposure to the public at large or to a third party who could benefit financially from that intellectual property.

Is Mobility the Natural Enemy of Security?

Mobility goes hand-in-hand with cloud solutions. With the explosion of mobile platforms and devices, utilizing a cloud-based collaboration or Enterprise File Sync and Share (EFSS) platform offers IT a shortcut to integrating the various endpoints that users – both within and outside the organization – demand to access enterprise data and applications. But what about security? This device explosion, fueled by the Bring-Your-Own-Device phenomenon that has permeated organizations of every size, makes it increasingly difficult for internal IT teams to support every tablet and smartphone that business users demand for both data consumption and creation.

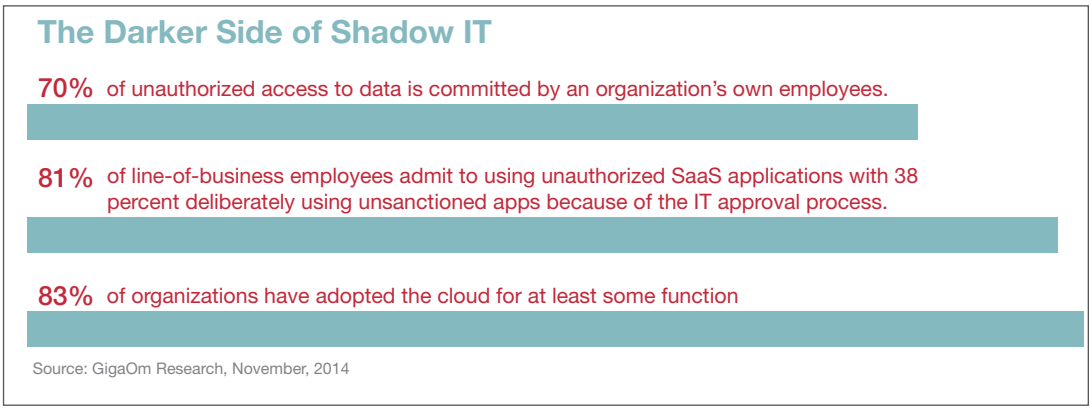
Organizations contemplating enterprise-class collaboration need to ensure that enterprise content – whether at rest or in transit – is secured and safe from prying eyes if devices are mislaid or stolen, or if an employee is terminated. Look for EFSS solutions that enable a central management capability no matter who is given access, and further ensure that access can be simply and quickly revoked to meet governance and protocol demands.

How big an impact can Shadow IT have on IT and the business? Amazingly, Shadow IT now represents more than a third of total IT expenditures worldwide. The numbers continue to climb quickly — the Q4 2014 Netskope Cloud Report stated that while the average enterprise IT professional thought there were 40 to 50 SaaS applications running in his or her enterprise, the actual average was a startling 579! And more than 88% of those cloud applications aren't enterprise-ready, which presents security and compliance holes that could lead to steep fines, data loss, and a damaged brand.

BRING SHARING OUT OF THE SHADOWS.

In our instant-app world where you can launch a SaaS application after a quick Web or app store purchase, IT must come to an understanding with the lines of business (LOB). If IT cannot provide a timely solution to collaboration or file-sharing problems, the LOB has options — and very often options that IT has good reason not to embrace. The question is: How can LOBs and IT reconcile the immediacy of users' needs versus the security and regulatory issues that keep IT up at night?

Start with education — a conversation between IT and LOB users that educates users about the potential risks of using unsanctioned applications that could lead to security data and breaches, and that also educates IT about the functionality and devices users need to more effectively carry out their jobs. By taking an educational rather than accusatory tone, IT can contain and even mainstream Shadow IT into other areas and encourage users to work in better partnership with their IT colleagues, ultimately leading to faster time to deploy new applications and functionality and thus faster time to value for the enterprise.



"You have to think of [end users] as your teammates; you don't want to create this us-versus-them mentality," says Brian Lillie, CIO of global colocation provider Equinix Inc., who is quoted in a recent article on searchconsumerization.com. Asking users was all it took to get the relationship turned around. "We could see we weren't meeting their needs, and so went to them to ask how we could help. It is more like forging a partnership than trying to impose something on them they don't want or understand," Lillie added.

By embracing — rather than preventing — Shadow IT, the enterprise can deploy a collaboration platform that delivers on LOB needs and meets the rigorous security and governance standards that businesses need to succeed. Those qualities are all embodied in a new class of sharing application referred to as Enterprise File Sync and Share (EFSS).

HOW TO CHOOSE A FILE SYNC AND SHARE SOLUTION.

What should IT and security teams consider when evaluating an EFSS solution? First and foremost, an EFSS solution shouldn't sacrifice user convenience and ease-of-use to gain necessary security and controls.

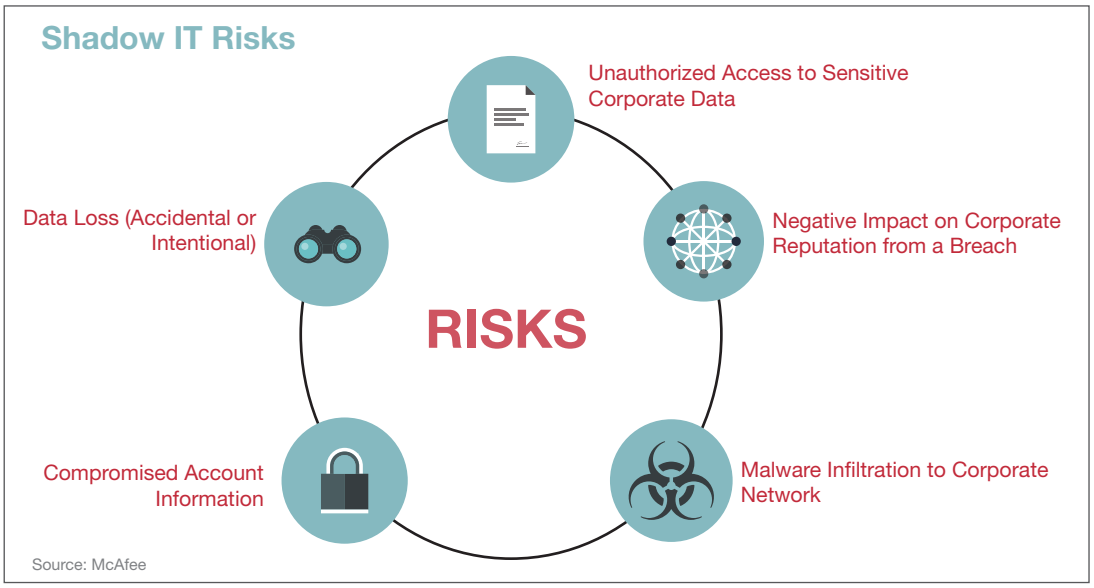
Next, enterprises should ensure the solution they choose is secure, open and hybrid. What does this mean?

- **Secure:** Security should encompass user permissions, encryption at rest and in transit, the ability to remotely wipe devices that are lost or stolen, and provide file-level digital rights management. LoB users should not need to add complexity to protect their intellectual property, and IT should be able to use existing directory and authentication rather than requiring yet another sign-on.

- **Open:** Look for solutions that avoid vendor lock-in and fit into native OS environments, enabling the use of any productivity application, any device, or any cloud or storage environment, whether public or private. Whether users depend on Microsoft Office, Google Apps, Salesforce.com or any other software, a collaboration tool should work with all of your users, applications and devices, regardless of Internet connectivity.

- **Hybrid:** An EFSS solution should give IT the ability to use a single pane of glass to manage all shared files and folders, whether stored on premises or at a cloud provider. This strengthens security and gives the transparency needed for auditors and regulators to

You have to think of [end users] as your teammates; you don't want to create this us-versus-them mentality.
-Brian Lillie,
CIO, Equinix Inc.



ensure compliance. An additional benefit of a hybrid approach is the ability to move files to the storage location that is closest to users to ensure the best performance for files that are sensitive to latency. This way, all files — whether noncritical marketing information that can be freely shared and stored in the cloud, or sensitive customer files or financial records that must be stored on premises to meet security and governance mandates — can be managed from a single console that can monitor what activity, and by whom, is being performed on any file in the EFSS environment. An added benefit is the resource optimization that can be gained by moving some files to the cloud, freeing up space on more expensive high-performance on-premises storage for the most demanding workloads.

By adopting a secure, open and hybrid EFSS approach, IT gains unified visibility, centralized control, and the flexibility to support any device, application, storage or cloud. LOB users gain a single, common platform for all users — internal or external — that offers simple control of permissions across multiple domains as well as the flexibility to collaborate, share and synchronize files and folders from anywhere, using any device or productivity applications with any other authorized users.

NEXT STEPS. Where are you on your journey to simple, secure enterprise collaboration and file sharing? To find out what EFSS strategy is right for you, contact the experts at Egnyte by visiting www.egnyte.com or calling US: 1-877-734-6983 / International: +44 (0)845-528-0588.

About Egnyte

Egnyte transforms business through smarter content allowing organizations to connect, protect and unlock value from all their content. Our Content Intelligence platform delivers smart content collaboration and governance in the cloud or on-premises to thousands of businesses around the world, even the most regulated industries. Founded in 2007, Egnyte is privately held and headquartered in Mountain View, CA. Investors include venture capital firms, such as Google Ventures and Kleiner Perkins Caufield & Byers, as well as technology partners, such as CenturyLink and Seagate Technology. Please visit **www.egnyte.com** or call 1-877-7EGNYTE for more information.

EGNYTE