



Your Data at Risk: What Employees Don't Tell You (and How You Can Help Them)

By Frank Kenney, Vice President, Global Strategy, Ipswitch File Transfer
Report

Your Data at Risk

Ipswitch File Transfer conducts periodic surveys to better understand the needs of its market. The latest survey took place at Infosecurity Europe 2011, where we asked 100 IT professionals some confidential questions about transferring large or sensitive files. Their answers provided a graphic reminder that when company systems hinder employee productivity, it's both a security risk and bad for business. There's no way to sugarcoat the results, which in some cases were rather alarming:

- 60% of employees are using personal emails to send sensitive files. Of that, almost 50% said they relied on personal email because the files were too large to send from their work server, and 50% said they rely on personal email to hide from management what they send...
- More than 25% of employees have lost a USB drive containing confidential information...
- 65% of respondents report feeling pressure from their customers and partners to improve the way they send and receive files...
- 49% said they were unable to send a file that was critical to their job due to the file size...
- 78% of respondents have experienced a significant email slowdown due to the sending or receiving of large attachments...
- Only 15 percent of companies surveyed can guarantee that files reach their intended recipient...

There's an obvious message behind these results. Business users have a job to do (get purchase orders in, send catalog information out, etc.). They're the ones who have to work with customers and partners, and deal with the consequences if business is lost. They can't have delays, they can't have slowdowns, and they have to be able to guarantee that their files will arrive. They're not being given the tools they need to send large and confidential attachments – or the processes and technologies are so difficult to use that people are ignoring them and taking matters into their own hands.

How difficult is it? Whenever business users need to send a large file that won't fit through email, they usually have to go through a complex, time-consuming procedure with the IT department. They start by creating a help ticket requesting a user name and password, an IP address so they can send the file, and details like how long the address should be open (usually as long as it takes for the customer or partner to get to it). After 24-48 hours, someone from IT responds, advising that the requested time window is out of the question, that the limit is a day or less, and the day/time when the link will be active. Now the user has to frantically contact the recipient and make arrangements to send the file before

Your Data at Risk

the link expires. This manual one-size-fits-all approach may fulfill security requirements, it may provide corporate visibility and enforce policy, but it's a productivity killer for employees who are trying to do their jobs and help the company grow.

GOING ROGUE

Of course, if a corporate email system can't handle a large file, or if IT vetoes their service request, committed and resourceful employees don't throw up their hands and give up, they look for workarounds. Rather than deal with IT, they take the file to their Gmail, Hotmail or Yahoo account. Or else they send it through one of the free cloud services that let you upload and download files. Or they'll stick the file on a USB thumb drive or DVD, drop it in the mail, and hope it arrives. It's not just individual employees who are going rogue; teams and even entire departments discretely go outside on their own if IT can't meet their needs. The fact that free or very cheap solutions are now available makes this option even more attractive.

All these methods are simple, cheap and convenient; they're also extremely risky. Most free software tools have strings attached, with contracts that give explicit permission to examine your email and attachments. Though the content won't be read by a human or identified, it will still be used to trigger advertising – which may not seem like a big deal but doesn't give the professional image that most companies want.

Other concerns are more dangerous. Lack of visibility and control into these external services puts them outside any reasonable comfort zone when transferring sensitive files. For example, after the transfer is complete, do they erase any backups they may have of your file? Do they use information in the file to better advertise to you ala Google, Yahoo or Microsoft? Even more to the point, they're unlikely to be in compliance with SEC rules or the mandates put in place to protect consumers and businesses (FIPS 140-2, HIPAA, PCI, Basel II, etc.). By turning to these unauthorized measures, people are not only breaking corporate policy, they're probably violating the law every single day.

While many highly-publicized data breaches are caused by hackers, the ones we rarely hear about are when employees are just trying to be productive:

- When an express mail service loses a DVD containing 10,000 customer records...

Your Data at Risk

- When a USB stick with customer records and their credit card information is lost on the subway. (Let's hope nobody finds it, or if they do, they simply erase it and keep the USB stick.)...
- When a VP hurrying to catch a plane leaves his iPhone at the security gate, and it contains emails with NDA information about acquiring a publicly traded company. (Let's hope he can remote-erase it, because there are plenty of backdoors to get into an iPhone or any other device, even if the phone is password-protected.)

It's not a pretty picture when a basic part of doing business – moving information from point A to point B – ends up violating regulations, breaking laws and exposing the company and its senior management. It gets even uglier: the survey revealed that when external device with sensitive business information goes missing, **40% did not report it to the IT department**. Thus, companies are often unaware of these debacles until it's too late for anything except damage control.

DIFFERENT PERSPECTIVES, DIFFERENT PRIORITIES

All of this unauthorized maneuvering is because IT and end users have different priorities that lead them to work at cross-purposes. On one side, corporate IT is responsible for enforcing security policy to prevent exposure and protect the business. On the other: the people responsible for bringing in money and keeping the business moving – administrative assistants, sales people, marketing staff and others on the front lines. Employees are demanding that the company give them better tools to do what they need to do – and if they can't, to at least get out of the way. But as we saw above, when they plunge off on their own, the potential consequences are too dangerous to ignore.

We've seen this conflict time and again, and the IT department never wins. Ultimately they relent and put in place the technologies and capabilities that employees need in order to do their jobs – after too many breaches and too many warnings to employees that they've violated corporate policy. It's only then that it dawns on companies that it's time to change course. They finally ask themselves: *“Why are we holding our employees back? We should be giving them the tools they need to their jobs.”*

The prevailing attitude about security is that it's a zero-sum game, where either you have it or you don't and there are no shades of gray. But the reality is more nuanced. Security is really about assigning value to data: establishing the level of risk to a company and its employees if different types of data get into the wrong hands. Not all data carries the same

Your Data at Risk

risk, and it's counterproductive to make blanket rules that treat all types of data the same way. For example, a 10 GB company catalog with high resolution graphics that's public information doesn't need to be handled with the same level of security as a small spreadsheet with credit card numbers on it – but that's what companies frequently do.

Rather than fighting a losing battle, companies need to revisit their security policies and see whether the policies currently in place are appropriate for what employees are trying to accomplish. From this, IT can determine the type of technology to recommend and deploy. When risk is low or on non-existent, like for the catalog mentioned above, one of the free tools may be perfectly acceptable. However, for other data transfers, much stricter measures will be required, while also being easy to use so they will be embraced – not shunned – by the employees who need to use them.

PRODUCTIVITY WITHOUT RISK

In many cases, the solution can be found using ad-hoc, person-to-person technologies that allow non-technical users to send files of any size simply and securely to anyone at any time in a well-governed way. Some solutions, like the [Ipswitch Ad Hoc Transfer module](#), allow files to be transferred quickly and securely through Microsoft Outlook or any Web browser, eliminating the risks associated with easy-to-lose physical devices or non-compliant software. Employees get a fast, easy and convenient way to share information, while providing companies with the visibility and control they need to ensure that sensitive information is protected.

Secure file transfer takes a few simple steps, without involving the IT department. When an employee needs to send files of any size, they click the button on their Outlook ribbon to send a link to the recipient. The recipient clicks the link to download the file, after which the link is destroyed. You don't need to send a Help Me ticket, a trouble ticket or whatever it's called in a particular organization. You don't need to request that IT provision a server for you and then de-provision it when the transfer is done. All the set-up work and network handshaking happens transparently behind the scenes.

The IT department stays in control, but it wears that control lightly. IT can set global, departmental or user file transfer policies, and has complete internal and external visibility into what is being sent, to whom and by whom. Employees can move files with point and click simplicity within the parameters they have been given. They don't have to worry about

Your Data at Risk

encryption or staying up to date with the latest mandates and corporate policies – these are handled automatically by the software, with oversight by corporate IT.

THE WAR ENDS – AND THE WINNER IS...

Companies are struggling to strike the right balance between productivity and security, particularly as more employees work remotely. IT managers need to make it easier for people in the organization to move information securely. What most companies don't realize is that they no longer have to choose between the two extremes.

Options are available that let employees be as productive as they need to be, but also extend the company's governance to that productivity. Employees get a fast, convenient and familiar way to share information while the enterprise gets the visibility and control it needs to ensure security and compliance. Corporate IT and business users can end their long battle, and they both come out winners.

ABOUT IPSWITCH FILE TRANSFER

Ipswitch File Transfer is a global technology provider that builds solutions to securely move your valuable data. We enable companies and people to better manage their data interactions when visibility, management and enforcement matter. Our managed file transfer solutions deliver the control necessary to enable governance and compliance for our millions of global users – including the majority of Fortune 1000 enterprises and government agencies. These organizations trust Ipswitch File Transfer solutions to secure, manage, automate and streamline their critical and highly sensitive file transfers and data workflows. Learn more at <http://www.ipswitchft.com> or contact us at <http://www.ipswitchft.com/Company/Contact.aspx>, or on LinkedIn and Twitter.

BEHIND THE SCENES: THE SORDID DETAILS

It was revealing to take visitors aside at Infosecurity Europe 2011 after they completed the survey and ask how they sent large files that couldn't fit through email. After glancing around furtively, they whispered their secret: *"Don't tell anyone, but ..."* and explained that they use products like Gmail, Box.net or Dropbox – products that may be free but violate any number of regulations for sending company information. The irony is the people admitting that they engaged in these surreptitious operations were IT professionals concerned about security! We can only surmise that the results for regular business users would be even more alarming.