IPSWITCH
FILE TRANSFER

Are Employees Putting Your Company's Data at Risk?

Survey Results Exposing Risky Person-to-Person File Sharing Practices

An eBook Report

ARE EMPLOYEES PUTTING YOUR COMPANY'S DATA AT RISK?

Ipswitch File Transfer conducted a survey of over 200 IT leaders and practitioners with security responsibilities about person-to-person file-sharing practices. And the results should alarm IT and security professionals.

Findings show that employees are circumventing IT staff by sending confidential and highly sensitive company files via means that are insecure and lack auditability. The results serve as 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 of the survey:

84% **of employees are using personal emails to send sensitive files,** often because the file size exceeds corporate mailbox quotas, or because they want to use documents at their next place of employment without the company's knowledge

MORE THAN 50% **of respondents expose company files or data** by uploading to a cloud-based service such as Dropbox or YouSendIt

MORE THAN 30% **of employees have lost a USB drive** containing confidential information

over half **of IT managers lack any visibility into file and data transfer** within their organizations

Many respondents also reported feeling pressure from their customers and partners to improve the way they send and receive files.

Are Employees Putting Your Company's Data at Risk? provides a detailed look at:

- **How and why sensitive data and files are being handled and exchanged**
- **Employee awareness of and adherence to data security policies**
- **IT visibility into file and data movement**

In this eBook, we highlight statistics associated with the key findings and offer recommendations for safeguarding sensitive corporate data while enabling users to get their job done. We hope this helps you benchmark your own data security efforts and inspires you to take steps to balance data governance with user empowerment!

Read on to learn more.

MAJOR FINDINGS IN 5 KEY AREAS

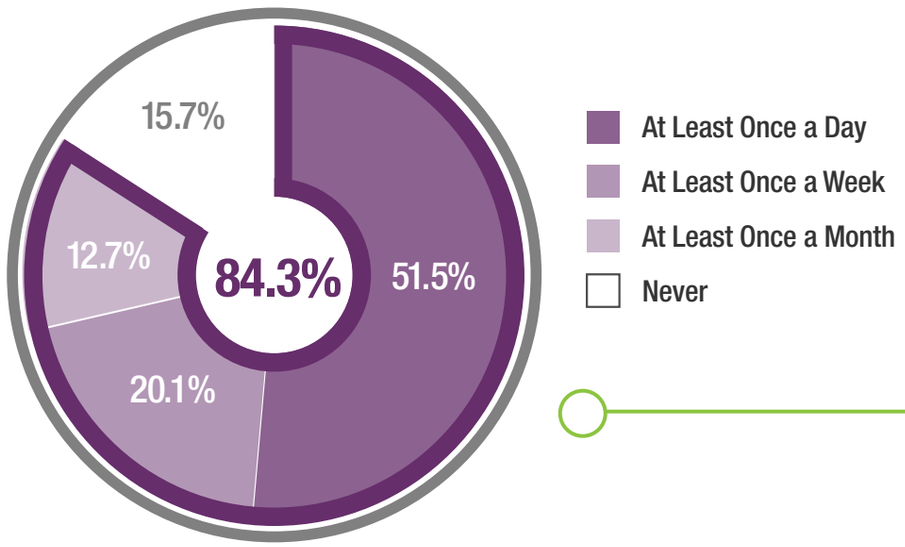
IT is Losing Control Over Data: IT and User Concerns and Priorities are at Odds

Are Employees Putting Your Company's Data at Risk? is the third annual report about data security based on Ipswitch File Transfer's confidential surveys of IT professionals. This year's survey surfaced many of the same issues and trends that we uncovered in 2011. Specifically, the study results revealed insights in five key areas.

1. Insecure Means Are Used To Send Confidential Files

A vast majority (84%) of the respondents send classified or confidential information as email attachments. Of that majority, 72% do this at least once per week, and 52% do this at least once per day.

How Often Do You Use Email To Send Classified Or Confidential Information – Payroll, Customer Data, Financial Information, Business Plans, etc.



Employees are circumventing IT protocols and turning to unsanctioned tools in record numbers, resulting in a lack of visibility and control for IT and exposing organizations to security and compliance risks

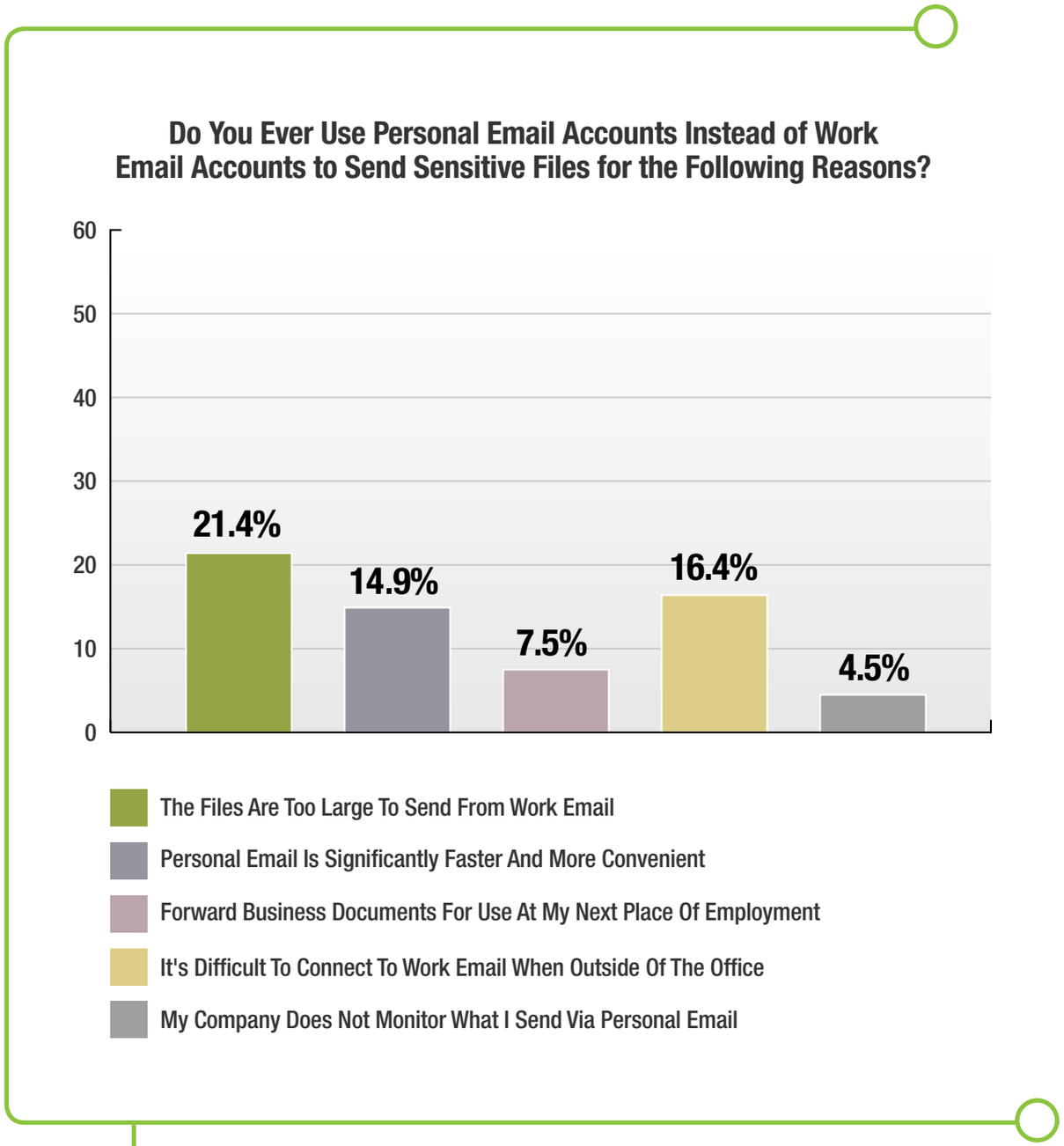
If your organization maintains policies and measures to ensure the security of files sent as email attachments, you may have no reason for concern. However, if employees in your organization are following the suit of others who responded to our survey, the following findings should serve as a wake-up call.

2. Many Use Personal Email to Send Company Documents and Data

Nearly half of the respondents use personal email to send company documents and data. And they do so for a variety of reasons:

- **To circumvent file-size limits prescribed for work email**
- **They find it faster and more convenient than using corporate email tools**
- **For use in their next place of employment**
- **They find it difficult to connect to work email when outside of the office**
- **IT doesn't monitor what they're sending via personal email**

Hackers are always on the lookout for ways to steal sensitive data, and they are just as aware as the rest of us about the growing use of personal email accounts by those on the job. It's no surprise that we hear stories such as the one about a group of hackers posting online the user names and passwords to more than 400,000 personal email accounts.[1]



Business users resort to personal email accounts to overcome file size or connectivity restrictions. Another common reason is to gain access to documents once they're at their next place of employment.

2. Many Use Personal Email to Send Company Documents and Data (cont.)

Business users are sending a clear message with their responses to our study: they have jobs to do – for example, sharing product information with customers or sending purchase orders to partners – and don't want to deal with the consequences of not getting their work done. They can't afford the delays or slowdowns associated with jumping through perceived hoops to send out information and files that keep business humming along. And if IT doesn't provide the tools they need to send large and confidential attachments – or if the processes and technologies are too difficult to use – users will take matters into their own hands.

As someone in IT, you may be shaking your head, thinking these reasons don't justify the renegade user behavior. But consider what business users typically must go through to transfer a file deemed too large to send via corporate email. They often have to submit to a complex, time-consuming procedure to send the file via a sanctioned file-sharing site. It starts with creating a help ticket indicating the amount of time the link should remain active and requesting a user name, password, and IP address. After 24-48 hours or longer, someone from IT responds, advising that the requested time window is out of the question, that the limit is a day or less. Now the business user is put into a frantic mode, contacting the recipient to make arrangements for sending the file before the link expires.

This manual one-size-fits-all approach may fulfill security requirements, and provide corporate visibility into – and enforce policies around – file sharing. But it's a productivity killer for employees who are trying to do their jobs and help the company grow.

Business users are sending a clear message. If IT doesn't provide the tools they need to send large and confidential attachments – or if the processes and technologies are too difficult to use – users will take matters into their own hands.

IPSWITCH FILE TRANSFER

3. Employees are Using Consumer-Grade File Transfer Services for Business Purposes

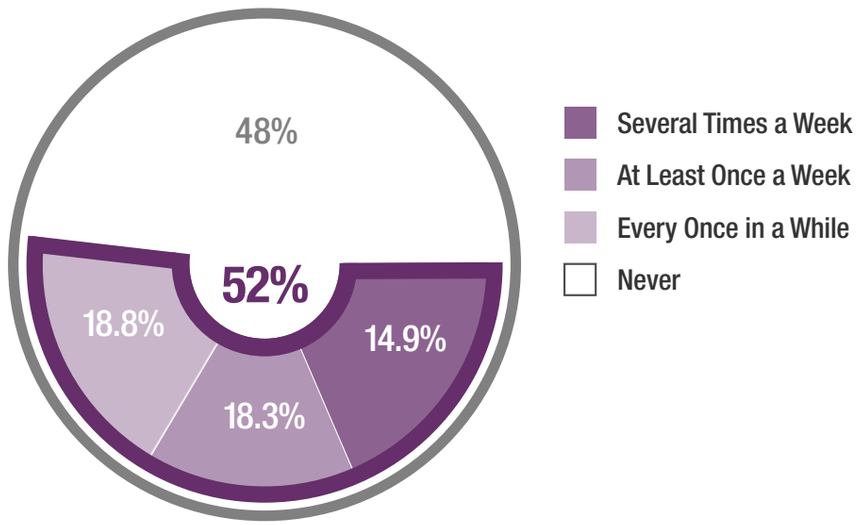
If the corporate email system limits the size of file attachments or if IT vetoes their service request, committed and resourceful employees don't just throw up their hands in resignation: **they look for workarounds.**

And the growing prevalence and popularity of file transfer sites and cloud services aimed at consumers is making it easier for business users to sidestep IT restrictions. After all, it's becoming more commonplace for business users to turn to the services they're using in their personal lives as a way to get work done. And it's all the more appealing to do so when the services are readily available and free to use. Moreover, it's not just individual employees who are going rogue: teams and even entire departments discretely bypass sanctioned means if it results in getting work done quickly and efficiently. In fact, more than half of the respondents say they use file transfer sites or cloud services to share or back up work-related files, and 34% say they use them weekly.

Of course, this behavior – and others – makes it harder for IT to stay in control of sensitive files and data leaving the corporate walls.

More than half of the respondents step around IT policy and use consumer file transfer sites or cloud services to share or back up work-related files.

Do You Ever Use a File Sharing Website or Cloud Service to Share or Backup Work-related Files? (Such as Dropbox or YouSendIt)

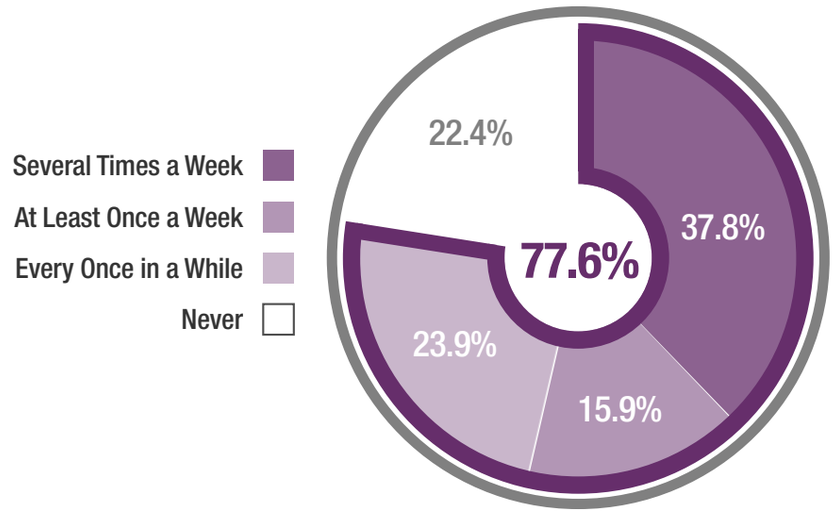


4. Risk of Data Theft is High

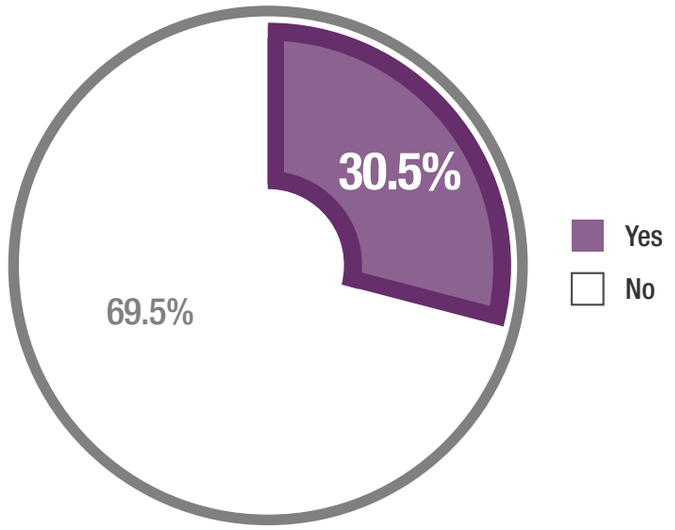
When business users aren't turning to personal email accounts or free file-sharing services to send business information, they're often sticking files on a USB thumb drive, smartphone, or other external device. **More than two-thirds (78%) of respondents to our survey say they are using such means to move or back up work-related files.**

These methods are simple, cheap and convenient – and also extremely risky. Consider that 31% of respondents have lost an external device containing sensitive business or personal information.

How Often Do You Use a USB Drive, Smartphone, Tablet or Other External Device to Move or Back Up Work-related Files?



Have You Ever Lost a USB Device, Smartphone, or Other External Device Containing Sensitive Business or Personal Information?



The risk of using external devices to transfer information: 31% of respondents have lost an external device containing sensitive business or personal information.

4. Risk of Data Theft is High (cont.)

In July 2012, a USB drive with data on 14,000 patients and about 200 staff was stolen from the home of an employee of Oregon Health & Science University (OHSU) during a home invasion.[2] This is just one example of the dangers of allowing data to be stored and moved using USB drives versus a secure transfer method.

Plus findings from a survey conducted by Ponemon Institute highlight a related risk. The survey found that 55% of information lost on USB flash drives is likely due to malware-infected devices that introduced malicious code onto corporate networks.[3]

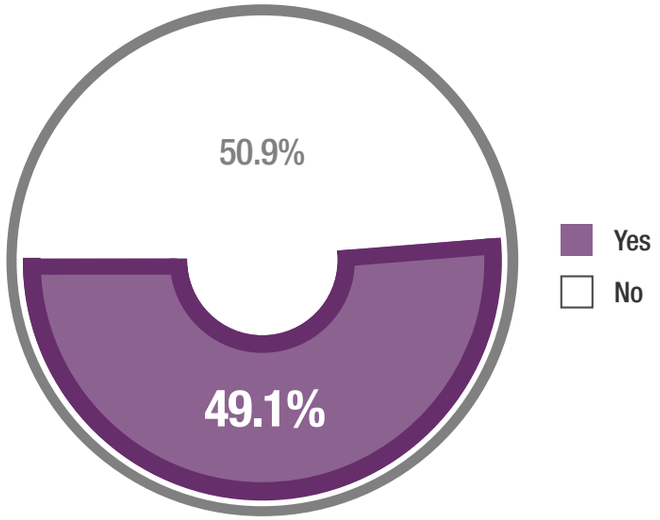
Lack of visibility and control into these external devices puts them outside any reasonable IT comfort zone when files are being transferred. By turning to these unauthorized methods of moving files, employees are not only violating corporate policy, they're at risk of violating national regulations …every single day. If nothing else, you're likely to be out of compliance with SEC rules or the mandates put in place to protect consumers and businesses when it comes to sharing information, such as HIPAA, GLBA, SOX, FERC, and those associated with state data breaches, to name a few. (For a list of publicly recorded data privacy breaches, visit http://www.privacyrights.org/data-breach).

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 to possible litigation. It gets even uglier: the survey revealed that when respondents lost external devices with sensitive business information, 49% did not report it to the IT department. That means companies are often unaware of these debacles until it's too late for anything except damage control. In other words, they can't place a legal hold on data, or find data during eDiscovery, and may be at risk of data spoliation.

Survey Says Your Data is in Danger

- 78% of respondents are using USB thumb drives, smartphones or other external devices to move or back up work-related files
- 49% did not report a lost external device containing sensitive business or personal information to the IT department

If So, Did You Report the Lost Device to the IT Department?



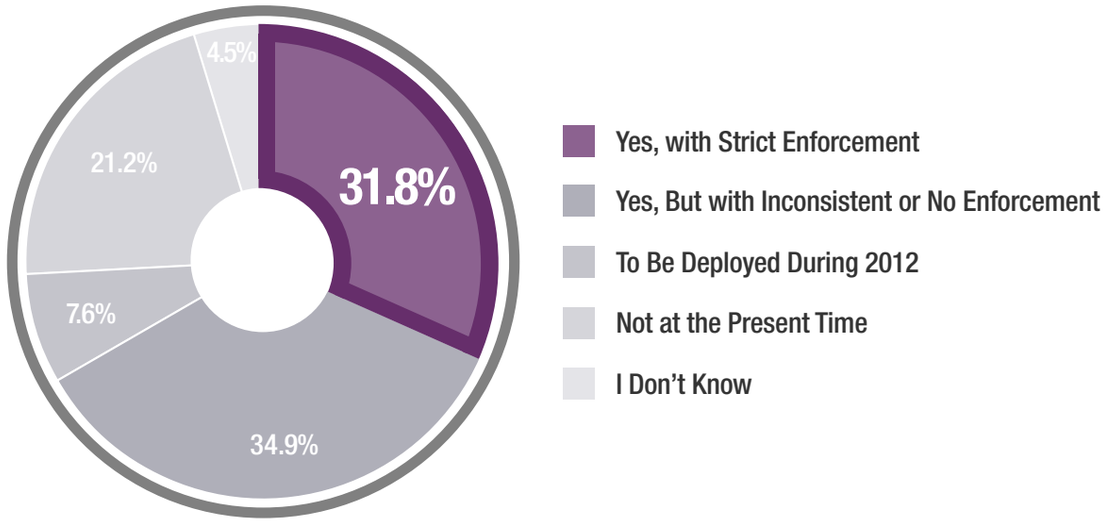
5. IT Management Visibility into Data Movement is Low

Most companies create and maintain company policies that mandate the use of approved tools for moving and sharing information. In fact, nearly 67% of respondents to our survey said they have such policies. However, **fewer than 32% of those with policies in place strictly enforce the policies**, making these mandates largely meaningless.

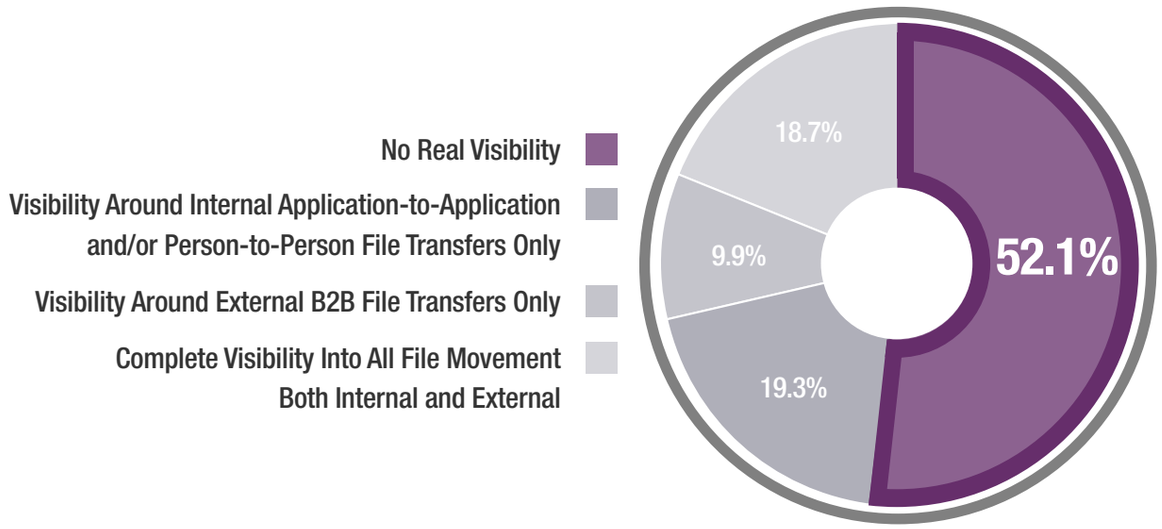
One reason these policies may not be strictly and consistently enforced is that IT can't track the files entering and leaving the company. According to our survey, 52% of IT management lacks any visibility into file and data movement. And this puts organizations at tremendous risk. After all, no visibility means no governance, and no governance means no compliance with internal policies and external regulations and laws.

Lack of IT visibility into file and date movement puts organizations at tremendous risk. No visibility correlates to lack of governance and compliance.

Do Existing Company Policies Mandate the Use of Approved Tools for Moving and Sharing Information?



What Level Of Visibility Do You Have Into Files And Data Moving Inside and Outside Of Your Organization? (Includes Files Sent By People, Servers And Systems)



RECOMMENDATIONS

Companies are struggling to strike the right balance between productivity and security, particularly as more employees work remotely. Employees want simplicity and convenience, while IT managers require visibility, security and control. IT leaders and practitioners need to understand the benefits, risks, and consequences associated with the proliferation of personal file transfer and file sharing tools.

A prevailing attitude about security is that it's a zero-sum game: you either have it or you don't and there are no shades of gray. But the reality in the business world is more nuanced. In the end, security is 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. After all, not all data carries the same risk, and it's counterproductive to apply blanket rules that treat all data the same.

IT managers need to make it easier for people in the organization to move information securely. What most companies don't yet realize is that they no longer have to choose between the two extremes.

Rather than fighting a losing battle, companies should revisit their security policies and gauge whether they are appropriate for what employees are trying to accomplish. Based on this, IT can determine the type of technology to recommend and deploy for moving and protecting data. When risk to data is low or non-existent, a free, consumer-grade tool may be perfectly acceptable. But for data transfers requiring stricter security measures, IT should provide easy-to-use, secure tools that employees will embrace.

IT managers need to make it easier for people in the organization to move information securely. What most companies don't yet realize is that they no longer have to choose between the two extremes.

SUMMARY

It's easy to chalk up these findings to the convergence of consumer-grade online services and the BYOD movement. And while those trends set the stage for behaviors that put corporate data at risk, the real culprit and reason for all this unauthorized maneuvering is the age-old conflict between IT and end users. On one side is the IT group responsible for enforcing security policies to prevent exposure and protect the business. On the other are the people responsible for bringing in money and moving business forward: support staff, sales reps, 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 that can't be done, to at least get out of the way. But **as the evidence shows, when they go out on their own, end users take steps that can lead to dangerous consequences for the company.**

We've seen this friction time and again, and the IT department never wins. Sure, IT often tries for some period of time to rein in rogue employees by issuing warnings about policy violations. But ultimately, after one breach too many, IT relents and puts in place the technologies and capabilities that employees need in order to do their jobs. Only then does it dawn on companies that it's time to change tactics or tools. They finally ask themselves: "Why are we holding our employees back when we could be giving them the tools to do their jobs?"

One popular answer is to **provide IT-sanctioned methods and tools that protect data while making it easy for business users to get their jobs done**. In many cases, the solution can be found using ad-hoc, person-to-person file transfer 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.

This represents a win-win for IT and the business, provided that these file transfer solutions:

1. Are as easy to use as the consumer-focused tools business users have opted for
2. Enable IT to be in full control of how and where information is shared
3. Can adapt to address changing regulatory and compliance requirements

> As employees continue to go around IT and use their own tools to send and share files in the workplace, IT must balance the need for end-user simplicity with the governance and control required by the organization.

IPSWITCH FILE TRANSFER

RESEARCH DETAILS

Are Employees Putting Your Company's Data at Risk? was produced by Ipswitch File Transfer based on its survey of more than 200 IT professionals and practitioners.

About Ipswitch File Transfer

Ipswitch File Transfer is a global provider of managed file transfer solutions that deliver the control necessary to enable governance and compliance with the ease-of-use that supports broad end-user adoption. Millions of global users - including the majority of Fortune 1000 enterprises and government agencies rely on Ipswitch for their file transfer needs and data workflow needs.

1- *The New York Times, Yahoo Breach Extends Beyond Yahoo to Gmail, Hotmail, AOL Users,* July 12, 2012
2 - *SC Magazine, Thumb drive with data on 14k hospital patients stolen,* August 3, 2012
3 - I*nformationWeek, How USB Sticks Cause Data Breach, Malware Woes,* August 8, 2011

Learn more at www.ipswitchft.com.

IPSWITCH
FILE TRANSFER