FORTRA

**WHITE PAPER** (Globalscape)

# Dangerous File-Sharing

## Certain File-Sharing Practices Put Sensitive Corporate Data At Risk

To the shock of many, **the greatest threat to data security** today is not targeted cyber attacks or fraudulent hackers, it's the carelessness of corporate employees. In fact, according to a 2013 Ponemon Institute report, almost two-thirds of data breaches can be attributed to negligence, human error, and system glitches.

While most CIOs and CSOs are actively working to slow this trend, doing so gets harder every year. At the heart of the issue is a rapidly evolving expectation around the speed at which information is shared and consumed. Today's workforce expects instant access to information, and the ability to send and receive data at the press of a button. When corporate technology and tools come up short, employees are forced to find a workaround.

Most often, that workaround is a consumer-grade file sharing tool, such as personal email, consumer file-sharing sites, remote devices, and cloud storage services, all of which present unique and significant security and compliance risks to organizations.

To uncover the breadth of this issue, Globalscape asked more than 530 U.S. professional employees about their informationsharing habits.

**This report covers:**

1. The unsanctioned tools that employees use to share sensitive company information
2. The security, compliance, and governance risks to enterprises
3. Why most IT policies and company-provided tools come up short
4. Steps for reigning in the risky information-sharing practices of employees

## Survey Demographics

Total respondents:

**532**
**Employees**

## Demographics:

14.8%
Financial management or accounting

34.8%
Marketing, sales, publication relations or legal role

50.0%
Management, administrative, human resources or project-management role

0.40%
Other

## Could Consumer File-Sharing Tools Be The Biggest Threat To Your Corporate IP?

In the last 12 months, **63 percent of employees** have used personal email to send sensitive work documents. Perhaps more surprisingly, **74 percent** of those employees believe that their companies approve of this type of file-sharing behavior.

Employees' reliance on personal email is a major red flag for IT, especially considering the **breach of millions of Gmail and Yahoo** accounts in December 2013.

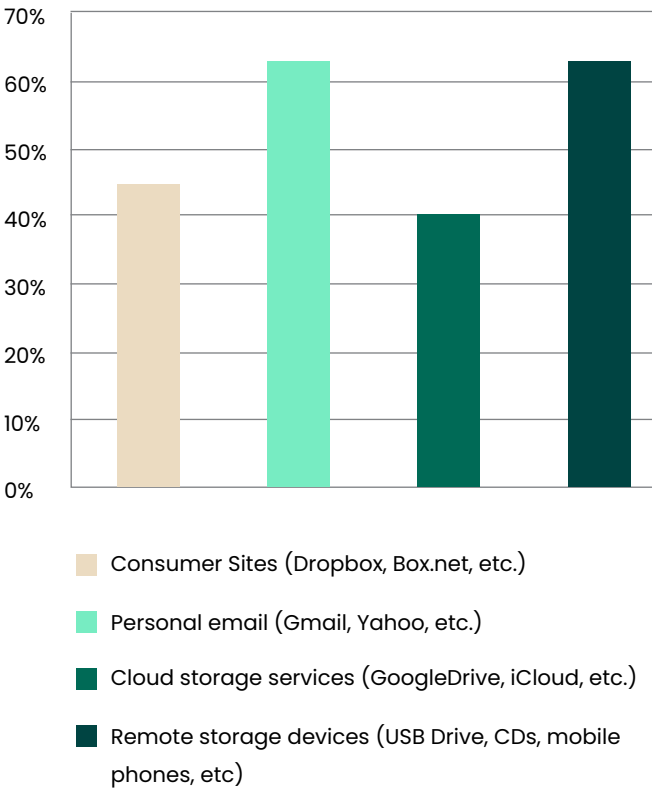
But personal email isn't the only third-party tool that IT needs to be concerned about.

**63%** of employees have used remote storage devices like USB drives and mobile phones to transfer confidential work files.

**45%** of employees have leveraged consumer sites like DropBox and Box.net to send sensitive work information. Could Consumer File-Sharing Tools be the Biggest Threat to Your Corporate IP?

**30%** of employees have turned to cloud storage services to move work-related files.


## In the past 12 months, which of the following have you used to send or move sensitive work documents?
(check all that apply)



## While these tools make it fast and easy to send and receive data, they create real problems for IT. When employees leverage these tools:

- Security goes out the window, and business information becomes more accessible to fraudsters
- Companies aren't in compliance with key regulations including FIPS, FSA, HIPAA, SOX, and others
- Visibility into the flow of information is lost (i.e., which files were sent, by whom, and to whom)

Employees' reliance on consumer-grade tools to transfer work-related files is not an isolated problem. Nearly half of all employees surveyed transfer work files through unsecured channels (remote storage, personal email, cloud storage, and consumer file-transfer sites) several times a week.

Personal email presents the biggest problem: 80 percent of employees that use personal email to transfer sensitive work files do so at least once a month. Even scarier, of that group, nearly a third have had their personal email hacked at least once, yet they continue to put company information at risk.

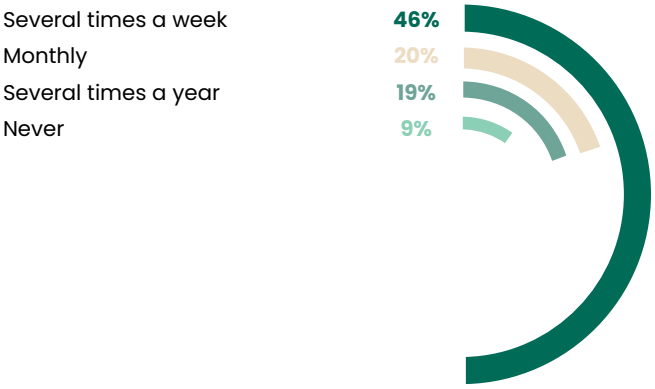
The reliance on consumer-grade cloud solutions is even riskier when password behavior is considered. Fifty-two percent of employees surveyed use the same password for all or most of their personal accounts, which could trigger a massive chain reaction of account takeover should one channel suffer a breach.

## The Blame Game: Employees Or It?

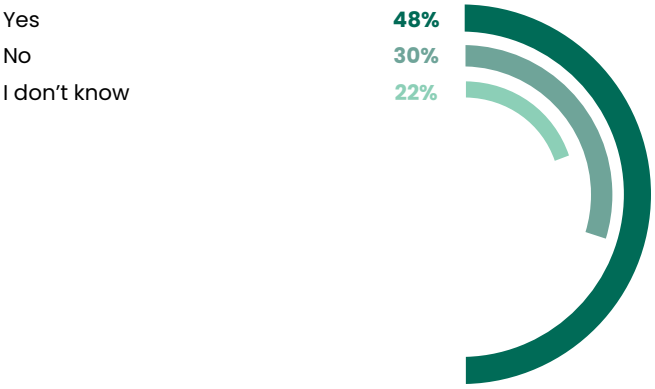
The first step toward better management of employee behavior is to create effective policies and clearly communicate them. That sounds simple enough, but it's actually a major struggle for most IT departments. In fact, there is a blatant lack of understanding amongst today's workers, not just in regard to the details of their company's IT policies, but to whether their company has a policy at all.

- Only 48% of employees said that their companies have policies for sending sensitive files
- 30% said that their companies don't have policies in place
- 22% weren't sure whether a policy existed

## How often do you use the above methods for sending or moving sensitive work documents?




## How often do you use the above methods for sending or moving sensitive work documents?



Policy enforcement is also lacking. Of those employees at companies that have policies for sending files, **62 percent** still use remote devices, **54 percent** still use personal email, **39 percent** use consumer sites, and **27 percent** upload company data to cloud storage services.

## Secure File Transfer Starts With Understanding Employees

When an employee's action puts information at risk or compromises compliance, more often than not, there is no malicious intent. Rather, it's a case of employees doing everything possible to remain productive, and losing sight of security and compliance in the process.

If organizations want to ensure that employees follow policies and adopt the secure and managed tools that they provide, IT teams need to truly understand the business needs of employees.

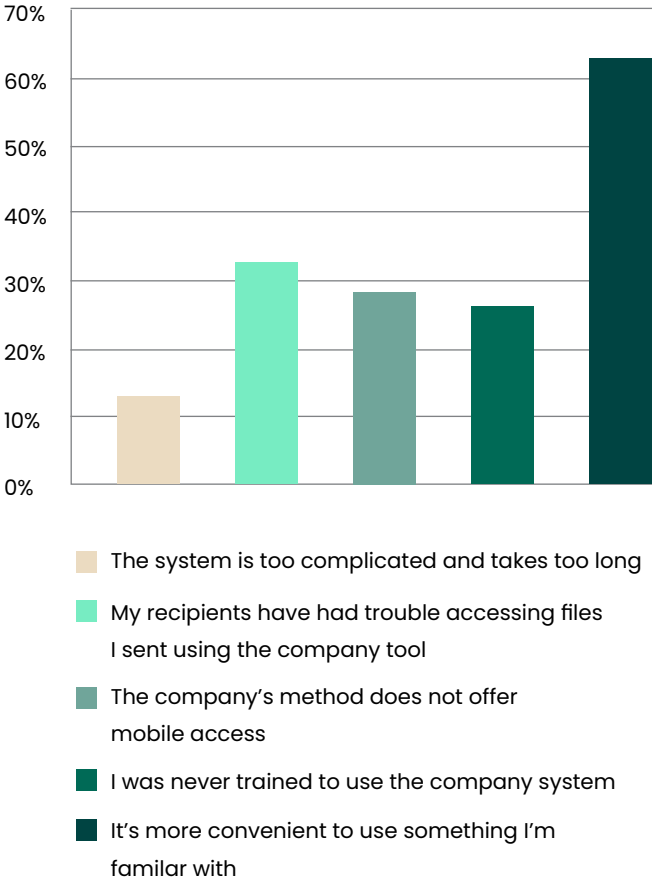
The reality is that security regularly takes a backseat to productivity and efficiency. If enterprises have any hope of managing and securing the sensitive data leaving their organizations, they need to provide solutions that easily integrate into the daily routines of their employees.

## Where Do Companies Go From Here?

Consumer-grade file sharing poses significant compliance, security and governance threats to organizations. Here's how to gradually work them out of your environment, and re-train employees to be more secure:

**If enterprises have any hope of managing and securing the sensitive data leaving their organizations, they need to provide solutions that easily integrate into the daily routines of their employees.**

## Why do you use an alternative to your company approved tool?
(check all that apply)



1. Educate all employees on the security risks of non-sanctioned information- sharing tools. It's safe to assume that most employees don't understand what is and isn't considered compliant, or that sharing confidential files through Gmail or Yahoo is risky business.

2. Audit technology and policies to uncover the tools or mandates that limit productivity. Employees will do everything necessary to remain productive. If the technology provided slows employees down, or the policies limit productivity, employees will find a workaround.

3. Provide easy-to-use, secure, file-sharing solutions that integrate with the daily routines of employees. The solutions should meet compliance standards, offer military-grade security, provide IT with visibility, and most importantly, make it easy for employees to do their jobs.

4. Regularly revaluate technologies and policies as new tools are introduced to the workforce. The information-sharing needs of today's workforce are rapidly evolving. Failing to transform with technology will set you up for negative ramifications down the road.

Learn more about Dangerous File Sharing at **www.globalscape.com.**

FORTRA

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.