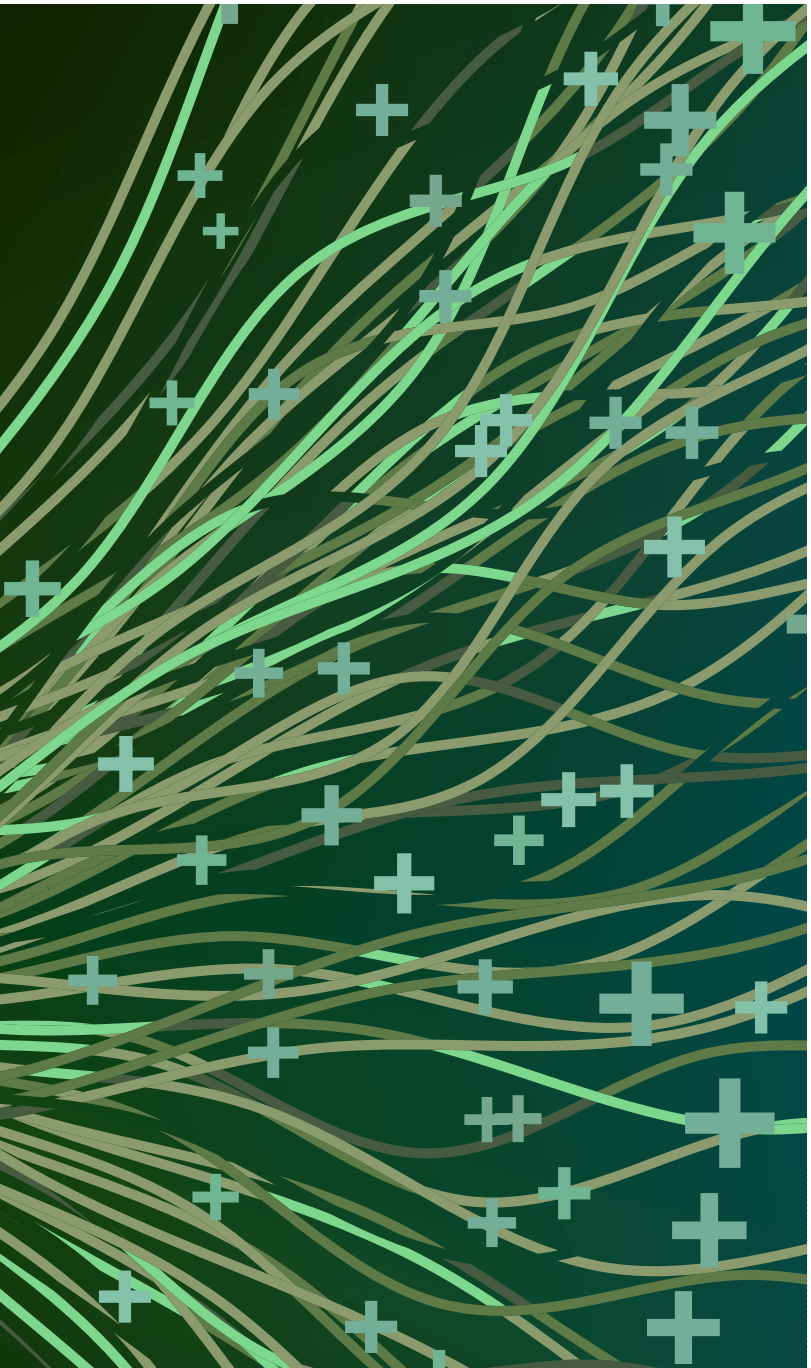
SearchContentManagement



E-Guide

WHAT IT MANAGERS NEED TO KNOW ABOUT RISKY FILE-SHARING

TechTarget

SearchContentManagement

EMPLOYEES ARE CIRCUMVENTING IT protocols and turning to unsanctioned tools such as file-sharing, messaging, collaboration and social media tools in record numbers. This high level of unchecked file transfer methods poses a major risk for companies and their security measures. IT managers today face diverse challenges with this. In this E-Guide, learn what IT managers need to know about risky file-sharing, as well as best practices.

SPONSORED BY OPENTEXT

WHAT IT MANAGERS NEED TO KNOW ABOUT RISKY FILE-SHARING

There is a danger in employees being tech-savvy – they can use devices and means to transport and exchange files that are beyond the control of IT management. Employees may simply see webmail, file-sharing services, cloud storage, USB sticks and smart devices as easier to use than traditional corporate tools to transfer files.

For IT managers, however, users with unchecked file transfer methods represent unacceptable security risks with regulatory implications. The internet is an empowering thing, but the proliferation of uncontrolled user tools is high and you cannot put that genie back in the bottle.

IT managers must accept a degree of cultural change, then provide attractive alternatives that allow them to monitor, quantify and model file transfers. A responsible reaction to this unconstrained business risk is driving businesses around the world to look for a simple, user-friendly route to protecting their most valuable data assets.

IT managers today face diverse challenges and have to balance many

simultaneous projects. They must always be open to new ways to become more efficient and security conscious, such as increasing the security and management of business file transfer.

INSECURE METHODS ARE STILL BEING USED TO SEND CONFIDENTIAL FILES

Employees are circumventing IT protocols and turning to unsanctioned tools such as file-sharing, messaging, collaboration and social media tools in record numbers.

This has resulted in a lack of visibility and control for IT departments, exposing organisations to security and compliance risks. Both the means by which users can share information, and the sheer volume of data changing hands between individuals and between businesses, has skyrocketed.

MANY EMPLOYEES CHOOSE TO ATTACH PRIVATE COMPANY DOCUMENTS AND DATA TO PERSONAL EMAIL

Recent surveys have shown that a vast majority (84%) of business users send classified or confidential information via corporate email attachments. Of those, 72% do so weekly and 52% daily.

IT managers have limited control because users are sending a clear message

with their file-sharing habits. They cannot afford delays or slowdowns associated with jumping through perceived hoops to send out information and files that keep business humming.

And if IT managers do not provide the tools they need to send large and confidential attachments – or if the processes are too difficult to use – then users will take matters into their own hands.

EMPLOYEES NEED ALTERNATIVES TO CONSUMER-GRADE FILE TRANSFER SERVICES FOR BUSINESS USE

If corporate email systems limit the size of file attachments, or if IT vetoes service requests, then resourceful employees do not just throw up their hands in resignation, they look for workarounds.

The growing popularity of file transfer sites and cloud services aimed at consumers is making it easier for business users to sidestep IT. Moreover, it is not just individual employees who are going rogue – entire departments discretely bypass sanctions. This behaviour makes it harder for IT managers to stay in control of sensitive files and data leaving the corporate walls.

Basic file transfer protocol (FTP) tools, for example, have been around for a long time, and are frequently used to send sensitive information containing

usernames and passwords. Often these tools increased in popularity without developing more sophisticated security precautions.

IT managers must demand greater security controls, such as 256-bit data encryption, validated cryptography, OpenPGP file encryption, file integrity checking and file verification.

RISK OF DATA LOSS AND THEFT REMAINS HIGH WITHOUT GREATER CONTROL AND MANAGEMENT

When business users are not turning to personal email accounts or free file-sharing services, they are often sticking files on USB thumb drives, smartphones or other external devices. Unfortunately, recent surveys show that almost one-third have lost a USB device, smartphone or other external device containing business or personal information in the past – a tremendous risk for any organisation.

This can result in unhappy customers, brand harm and reputation loss. High leakage levels make it a pretty tough world for an IT manager.

The sheer number of devices and removable media tools people are carrying in their pockets mean it is no longer about controlling desktops. Users have smartphones and tablets and want to use them at home and in the office.

LOW VISIBILITY INTO DATA MANAGEMENT ONLY RAISES RISK AND HINDERS COMPLIANCE

Most companies create and maintain policies that mandate the use of approved tools for moving and sharing information. However, research suggests that fewer than 32% strictly enforce the policies, making these mandates largely meaningless.

One reason these policies may not be strictly and consistently enforced is that IT managers cannot track the files entering and leaving the company. No visibility means no compliance with internal policies or, potentially, with external regulations and laws.

IT MANAGERS MUST TAKE STOCK, REGAIN CONTROL AND WORK TO TRUST USERS AGAIN

The file-sharing habits of today's employees may be risky, but ultimately are driven by a desire to get work done efficiently. This need must be balanced with the necessity for IT managers to control file-sharing intelligently.

IT managers need to better understand who their users are exchanging information with, why they are doing it, and what type of tools they prefer to use. In this way they can better understand where they stand and how best to

help the situation.

Fortunately, companies do not have to choose between risky behaviour and productivity. Using the right technologies can give employees the convenience, ease of use and speed they need while IT managers retain the control, visibility, security and compliance. It is a win-win situation.

SearchContentManagement

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

SearchContentManagement

RELATED TECHTARGET WEBSITES

ComputerWeekly

SearchBusinessAnalytics