Ipswitch File Transfer Survey Finds that only 20% of Organisations Have Visibility of Data Being Moved Within and Outside the Organisation

Submitted by: Ipswitch File Transfer Division

Wednesday, 25 April 2012

Only 25% of companies enforce usage of an IT-sanctioned file sharing tool

Wednesday, April 25, 2012 – InfoSecurity, London UK – Ipswitch File Transfer Division, a leading provider of high-performance secure managed file transfer (http://www.ipswitchft.com), electronic data interchange, and business-to-business data gateway solutions, today unveiled results of a study undertaken at the show, examining the flow of sensitive information in the workplace. According to the survey, only 20% of the IT Executives said they have visibility into files and data moving inside and leaving their organisation. The survey also examined the biggest risk for data movement, with 29% perceived moving data back and forth between cloud applications as the biggest risk of data loss.

With the proliferation of the Bring Your Own Device (BYOD) trend, organisations have to monitor devices such as smartphones, tablets, USB drives and sophisticated MP3 players due to file hosting capabilities. The survey found that 72% of respondents use their own portable devices to store confidential work files. This combined with the fact that 55% said they use free cloud based services such as Dropbox® and that 65% use personal webmail to move confidential files. However, the majority of businesses having no visibility into the data that is being moved, leading to concern that the data could be compromised either in transit or through loss of a personal device.

“Cloud computing has presented organisations with a lot of new opportunities when it comes to IT efficiency, but IT managers are still concerned by the security implications associated with moving sensitive business information to and from a cloud-based solution,” says Rich Kennelly, president at Ipswitch File Transfer. “Businesses are moving vast amounts of information and sensitive files per day, whether it is by email, through the cloud or by employees using their own devices to back-up and store data. It is therefore imperative that organisations have a policy in place for approved forms of data transfer and have visibility into files that are being moved, by whom and to what medium. It is always important to note that data loss can incur severe financial penalties for the organisation, as well as damage it reputation.”

The loss of USB devices holding sensitive information has dominated headlines over the past 24 months and the trend sets to continue with, 31% of respondents saying that they have lost either a USB device, a smartphone or other storage device containing sensitive work information. However, 69% failed to report their loss to the IT Department.

“Companies need to secure their data in transit, but the challenge for all organisations is the visibility in to the data that is being shared, by whom, with whom and how,” Kennelly adds. “Data loss is a serious consideration for businesses as there are heavy fines associated with the severe cases of data loss. Whether malicious, or unintentional, data breaches are a serious risk to all organisations; it is therefore imperative that organisations have visibility into the data traffic within the business to protect themselves, partners, employees and customers alike.”

Additional findings of the survey include:

- 78% of respondents said they use email to send classified or confidential information, such as payroll, customer data, financial information and business plans at least once a day, 64% weekly or more often.

- Of those that said they use personal email accounts to send confidential information, 35% stated that personal email is faster and more convenient, while 25% cited that files that are too large to send from work email. Additionally, 15% said they had difficulties connecting with work email while out of the office therefore turned to personal email accounts to send sensitive work files instead of work email accounts.

- Whilst 52% or organisations provide their employees with an IT sanctioned tool for file sharing; only 30% enforce its usage.

Ipswitch offers solutions that empower thousands of healthcare, financial, retail, and government/public sector organizations worldwide to securely send, manage and protect their most critical business data.

Ipswitch's portfolio of high-performance integration and managed file transfer solutions helps IT professionals:

- Manage all file transfer activities, internally and externally

- Create, centrally manage and enforce file transfer and security policies

- Transfer files quickly and securely through Microsoft Outlook or any Web browser

- Archive and retrieve all files and messages for discovery and compliance

- Proactively monitor operations to detect threats to service level agreements

- Translate high-volume, highly complex files easily in a single pass

- Enhance interoperability by scheduling and executing applications on the network

- Migrate EDI systems and consolidate FTP systems

About Ipswitch File Transfer

Ipswitch File Transfer is a global technology provider that builds solutions to securely manage and move your valuable data. We enable companies and people to better manage their data interactions when visibility, management and enforcement matter. Our proven managed file transfer integration technologies deliver the control necessary to enable governance and compliance for 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 integrate 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 Twitter

Contact:

Martin Brindley or Janne Virtanen
Davies Murphy Group
Ipswitch@daviesmurphy.com
+44 1256 807360

Dan Kraus
Ipswitch File Transfer
+1 978-562-4161