



PRESS RELEASE

Contact

Silja Ingham
Origin Communications
E-Mail: imation@origincomms.com
+44 208 398 6588

REMOTE WORKING PUTS BUSINESS DATA AT RISK, WITH OVER A THIRD OF OFFICE WORKERS HAVING LOST DEVICES IN A PUBLIC PLACE

One in four employees interviewed admit breaking security policies to work remotely and the vast majority aren't concerned about losing confidential business data

Derby, UK, **5. November 2014** – Poor security and impugned responsibility are putting business data at risk for those working remotely, according to new research from global data storage and information security company [Imation Corp.](#) (NYSE: IMN). Workers are taking confidential information away from the office, often without the knowledge of their employer, and losing unsecured and unencrypted business data in places such as pubs, trains and hotels.

According to the survey of 1,000 office workers from the UK and Germany, nearly two in five of respondents, or someone they know personally, have lost or had a device stolen in a public place. Three quarters of these devices - such as laptops, mobile phones, and USB sticks - contained work-related data. This included confidential emails (37%), confidential files (34%) and customer data (21%). Around one in ten lost financial data or access details such as login and password information, potentially exposing even more confidential information to the risk of a data breach.

What makes these findings even more concerning is that a large proportion of data taken outside the workplace is not adequately secured. As many as three quarters of respondents said they had taken digital files with them outside work, yet many do not use standard security measures such as encryption, password protection or remote wiping to protect the data from unauthorised access.

Nearly half (44%) of respondents said that data is never encrypted when taken out of the office. Three out of ten respondents admitted they do not protect their data with passwords, and nearly one in ten workers who take digital files outside of the office do not secure them at all. Office workers it seems aren't losing any sleep over losing confidential business data when they take work home, with only one in sixteen worrying about this.

“Companies may not be aware of the amount of data that's leaving offices unsecured. In addition, half of respondents said that nobody would notice, at least some of the time, if they were to take data away from the office and lose it. It's obvious that poor security and lack of understanding of what happens to corporate data are putting organisations at risk of a data breach,” said Nick Banks, VP EMEA and APAC, Imation's IronKey™ Solutions.

Even though eight in ten of the employees interviewed read or write work emails on the move, and around seven in ten work on electronic documents outside their office,

businesses are failing to provide their employees with secure tools for remote working, and not putting the right security policies in place.

Fewer than six out of ten respondents said their organisation had a remote working policy. Of those that do have a policy, over a quarter admitted they had broken the policy in order to work remotely. Eight percent had knowingly broken the policy, and a further 18% say they had unknowingly broken it.

Equally, of those who do secure data that they take outside of the office, just over half said that their employer or a third party supplier provides the remote working security measures. One in five respondents reported that just they themselves provide the security measures.

“These figures emphasise the urgent need for businesses to ensure that their employees have the necessary tools to work flexibly and securely, without further hindering productivity,” commented Nick Banks. “The reality is that people are working in cafes, on aeroplanes, in their GP's waiting rooms and even while they take their children to the park. Organisations are tasked with a monumental challenge of providing secure access to corporate networks and data. Data protection is a huge concern for employers who are battling to manage security and privacy for employees on the move,” added Banks.

Other research highlights include:

- As many as 41% suggested that they either do not have the right tools to work remotely, or that their tools could be improved.
- Three in five respondents would tell their boss if they lost a storage device with company data on it. However, nearly one in ten would do nothing. Less than a third said they have policies that dictate who should be notified depending upon the data lost.
- Almost a quarter have looked over the shoulder of someone working on a laptop/tablet in a public place or noticed someone looking over their shoulder. And 6% would let someone else use their work laptop, tablet or smartphone outside the office.
- Around half (48%) of respondents that take digital files with them outside of the office do not fully separate their work and personal data – putting their personal data at risk of being wiped when business data is compromised.
- Just 70% of respondents report that they protect their data with passwords, and only 36% encrypt their data. Only a small proportion of respondents are using biometric technology (14%) or remote wiping (7%) to secure their data.
- Public areas such as pubs, cafes and restaurants (22%), and public transport (29%) are some of the most common locations for respondents to read or write work emails when outside of their home.

About Imation Corp.

Imation is a global data storage and information security company. Our products and solutions help organisations and individuals store, manage and protect their digital content. Imation's storage and security portfolio includes Nexsan™ high-density, archive and solid-state optimised unified hybrid storage solutions; IronKey mobile security solutions that address the needs of professionals for secure data transport and mobile workspaces; and consumer storage solutions, audio products and accessories sold under the Imation™, Memorex™ and TDK Life on Record™ brands. Imation reaches customers in more than 100 countries through a powerful global distribution network. For more information, visit www.imation.com.

Imation, the Imation logo, IronKey, the IronKey logo, Nexsan and Memorex are trademarks of Imation Corp. and its subsidiaries. TDK Life on Record is used under a trademark license from TDK Corporation. All other trademarks are property of their respective owners.

#

Notes to Editors

The research was conducted by Vanson Bourne.

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis, is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com. To download full report click [here](#).

The research consisted of 1000 online interviews.

One thousand interviews were carried out during summer 2014 with office workers in businesses of at least 250 employees. Five hundred respondents work in the UK, and 500 respondents work in Germany. Eighty percent of respondents were required to work remotely for at least part of their working week.

Respondents to this research came from a range of industry sectors. Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated, results discussed in the main narrative are based on the entire sample.

- ends -