95% of UK businesses struggle with secure mobile working; one third have experienced data loss or breach (Apricorn study)

Submitted by: Origin Comms Ltd
Wednesday, 6 June 2018

Ninety-Five Percent of UK Businesses Still Struggling with Mobile Working and Security of Data Continues to Cause Concern

A third of organisations have experienced a data loss or breach as a direct result of mobile working

MANCHESTER, UK. – 6th June, 2018 – Apricorn, the leading manufacturer of software-free, 256-bit AES XTS hardware-encrypted USB drives, today announced new research highlighting that 95 percent of surveyed organisations in the UK recognise problems with mobile and remote working, and, worryingly, nearly one in five (18%) suggest their mobile workers don't care about security.

All (100%) surveyed IT decision makers noted that they had employees who work remotely at least some of the time, with an average of over a third (37%) of staff members who do so. With an increase in the numbers working remotely, this means more data moving beyond the confines of the corporate network, and organisations need to ensure that any data, be it at rest, or on the move, remains secure.

While many are taking steps, such as implementing security policies for mobile working and bring-your-own-device (BYOD), to ensure their data is protected, just under half of respondents (44%) still agree that their organisation expects their mobile workers to expose them to the risk of a breach. Roughly a third (32%) say that their organisation has already experienced a data loss or breach as a direct result of mobile working and, to add to this, 30 percent of respondents from organisations where the General Data Protection Regulation (GDPR) applies are concerned that mobile working is an area that will most likely cause them to be non-compliant.

Fifty-three percent cited that one of their top three biggest problems with remote working is due to the complexity and management of the technology that employees need and use. Over half (54%) say that while their organisation's mobile workers are willing to comply with requests relating to security measures, employees lack the necessary skills or technologies required to keep data safe. Nearly a third (29%) take the radical approach of physically blocking all removable media, and a further 22% ask employees not to use removable media although they have no technology to enforce this.

"The number of organisations blocking removable media has increased compared with responses to the same question in 2017, when 18% said they were physically blocking all removable devices. A unilateral ban is not the solution and ignores the problem altogether whilst presenting a barrier to effective working. Instead, businesses should identify corporately approved, hardware encrypted devices that are only provided to staff with a justified business case. The approved devices should then be whitelisted on the IT infrastructure, blocking access to all non-approved media," said Jon Fielding, Managing Director, EMEA, Apricorn.

Despite strict security policies, mobile working can still leave organisations wide open to the risk of a data breach. Half (50%) of respondents admitted one of the three biggest problems with mobile working is that they cannot be certain their data is adequately secured. Only around half enforce encryption and are

completely confident in their encrypted data in transit (52%), in the cloud (52%) and at rest (51%).

“Whilst the new GDPR legislation requires the pseudonymisation and encryption of personal data, encryption is not a new concept, and keeping data secure has always been imperative to any organisation handling sensitive information,” adds Fielding.

“Organisations are simply not following security best practices. They need to implement and enforce policies and provide employee training to ensure compliance with data protection regulations. Failing to put processes in place is putting confidential data at risk and with the GDPR legislation in place, organisations face the prospect of being fined even before a breach has occurred,” advised Fielding.

About Apricorn
Headquartered in Poway, California, Apricorn provides secure storage innovations to the most prominent companies in the categories of finance, healthcare, education, and government throughout North America, Canada and EMEA. Apricorn products have become the trusted standard for a myriad of data security strategies worldwide. Founded in 1983, numerous award-winning products have been developed under the Apricorn brand as well as for a number of leading computer manufacturers on an OEM basis.

About the survey

The research was conducted by Vanson Bourne, an independent specialist in market research for the technology sector. Vanson Bourne interviewed 100 IT decision makers in the UK, during April 2018. Respondents to this research came from private sector organisations with more than 1,000 employees.

Vanson Bourne’s reputation for robust and credible research-based analysis is founded upon rigorous research principles and their 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 https://www.vansonbourne.com.

Media Contact

Paula Averley
Origin Comms
t. 020 3814 2941
e. apricorn@origincomms.com