Over half of organisations expect their remote workers to expose them to the risk of a data breach

Submitted by: Origin Comms Ltd
Wednesday, 22 April 2020

More than a third of IT leaders state their remote workers don't care about security, according to annual survey by Apricorn

MANCHESTER, UK – 22 April, 2020 – More than half (57 percent) of UK IT decision makers still believe that remote workers will expose their organisation to the risk of a data breach, according to an annual survey – conducted between 25 and 27 March 2020 – commissioned by Apricorn (http://www.apricorn.com/), the leading manufacturer of software-free, 256-bit AES XTS hardware-encrypted USB drives. This figure has inclined steadily from 44 percent in 2018 and 50 percent in 2019. The rise could reflect a corresponding increase in the number of people working remotely, or an enhanced awareness of the risks of doing so as the UK's workforce began to follow government guidelines to work from home.

In 2019 almost half of respondents (47 percent) admitted that their remote workers had already knowingly put corporate data at risk of a breach in the last year; this has now dropped slightly to 44 percent. Apathy continues to be a major problem, with just over a third (34 percent) of IT leaders saying their remote workers simply don't care about security – exactly the same percentage as last year – which suggests organisations are struggling to get employees to buy into the security strategy.

Jon Fielding, Managing Director EMEA, Apricorn, says: "This year, the need for organisations to facilitate effective and secure remote working has been cast into the spotlight to an extent no-one could have anticipated. Our survey shows that while progress has been made in some key areas since 2019, some of the same risks – such as employee apathy or error – remain a problem. In these currently challenging times, when UK workers are being urged to work from home, it's all the more important that security is a priority for everyone."

Organisations have increasingly recognised the importance of endpoint control as remote working has become more prevalent. Nearly all (96 percent) mitigate the risks of BYOD (bring your own device) with a security strategy that covers employees' use of their own IT equipment out of the office. Of those, 42 percent only allow the use of devices that have been provisioned or approved by IT, and enforce this with strict security measures. This is a significant rise on 2019, when just over 1 in 10 (11 percent) did so.

"Strengthening endpoint controls allows organisations to trust in the integrity of their data and systems wherever the employee is accessing them, and whatever device they're using. The fact that businesses are recognising and enforcing this is a positive step," comments Fielding.

This change is crucial given that lost or misplaced devices is now the second biggest cause of a data breach – cited by almost a quarter of respondents (24 percent), up from 17 percent a year ago. Employees unintentionally putting data at risk remains the leading cause (33 percent), with third parties mishandling corporate information cited as one of the main causes by 23 percent.

Despite this, the majority (87 percent) of UK IT decision makers agree that their organisations' remote

workers are aware of cybersecurity risks and practices, and follow required policies at all times.

“Remote working is not a new concept, but with so many employees now having had a taste for home working, it might be hard for businesses to put that particular lid back on – so they need to figure out where their vulnerabilities lie now, and address them,” adds Fielding.

When it comes to the challenges of implementing a cybersecurity plan for remote working, almost a fifth of IT decision makers (19 per cent) say managing all the technology employees need is the biggest problem, a drop from 30 percent in 2019, which suggests that organisations are getting a handle on the complexity involved in the technology aspect. In addition, fewer IT leaders believe that difficulties with GDPR compliance is the biggest problem with mobile working: 16 percent agreed, compared with 20 percent in 2019, suggesting that this aspect may have been less of a challenge than they originally anticipated.

About the survey
The research was conducted between 25.03.2020 - 27.03.2020, by Censuswide. Respondents were 100 UK IT decision makers (CIOs, Heads of IT, IT directors, Senior IT managers etc.) from enterprise organisations (1000+ employees) within the financial services, IT, manufacturing, business and professional services sectors. Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles.

About Apricorn
Headquartered in Poway, California, Apricorn (http://www.apricorn.com/) 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.

Media contact
Alicia Broadest
Origin Comms
t. 07729 102 956
e. apricorn@origincomms.com