

U.S. and UK businesses call for improvement as employee education singled out as the biggest weakness during lockdown

Submitted by: Origin Comms Ltd

Wednesday, 28 October 2020

Thirty per cent of respondents admit to using unencrypted devices according to latest Apricorn poll
MANCHESTER, UK. – 28 Oct, 2020 – Apricorn (<https://apricorn.com>) the leading manufacturer of software-free, 256-bit AES XTS hardware-encrypted USB drives, today announced new findings from a Twitter poll exploring the data security and business preparedness for remote working during the pandemic. More than 30 per cent of respondents singled out employee education as being the biggest area where companies needed to make changes to improve cybersecurity.

The poll was issued over 6 days and targeted employees in both the U.S. and UK. In addition to concerns about employee education, respondents also flagged updates to hardware (29%), endpoint control (21%) and enforcing encryption (19%) as areas of weakness, where organisations need to make changes to improve cybersecurity. Given that almost 30 per cent of respondents admitted to using unencrypted devices during the pandemic, this raises many concerns particularly at a time when we are seeing a dramatic increase in the volume of data being downloaded, and a potential for more data on the move.

Kurt Markley, Director of Sales at Apricorn commented - "Employees have a critical role to play in their organisation's cyber security processes, from recognising the tools required, through to the policies in place to protect sensitive data. Whether it be through the delivery of awareness programs or ongoing training, establishing a culture of security within the workforce is essential.

Endpoint security is critical, and deploying removable storage devices with built-in hardware encryption, for example, will ensure all data can be stored or moved around safely offline. Even if the device is lost or stolen, the information will be unintelligible to anyone not authorised to access it."

In addition, more than 40 per cent of respondents admitted that, as an individual, they were not fully prepared to work at home securely and productively. Almost a fifth (18 per cent) said they lacked the right technology to do so, 16 per cent were not sure how to, and just over 20 per cent said they were still not able to work remotely.

"Many businesses will now have witnessed the positive productivity and financial impact of a remote workforce, but without the right tools, processes and security in place, this can very easily backfire" Markley continued.

With the poll results showing that more than 60 per cent of respondents are planning to work remotely, all, or some of the time following the pandemic, the threat to corporate data is only going to mount. Almost 20 per cent admitted that the experience of working from home highlighted major gaps in their employer's cybersecurity strategy/policies.

When questioned as to whether their company had experienced a data breach as a result of remote working during the pandemic, over 20 per cent said yes, but a further 22 per cent said they didn't know if they had suffered a breach.

According to Jon Fielding, Managing Director, EMEA at Apricorn, "IT and security teams had to scramble to respond to this crisis and in doing so, left a lot of companies wide open to breach. Nine months into employees working remotely, some know already that they have been attacked. Others think they may have been but can't be sure. In the same way that we had to learn how to protect ourselves from illness and modify our behaviour, we had to also learn how to protect our data outside of the firewall and more important, to remain vigilant about it."

Methodology

Comprising of six question and answer options and drawing 23,537 responses, the Apricorn Twitter poll was

conducted during the week of 15-22nd October

About Apricorn

Apricorn provides secure storage innovations to the most prominent companies in the categories of finance, healthcare, education, and government throughout EMEA, North America and Canada. Apricorn products have become the trusted standard for a myriad of data security strategies worldwide. Founded in 1983, numerous award-winning products and patents 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 102956

e. apricorn@origincomms.com