Eighty Nine Percent of Organisations have Experienced a Data Breach, with Almost Two Thirds a Direct Result of Human Error

Submitted by: Origin Comms Ltd
Wednesday, 15 May 2019

Almost half of organisation's remote workers have knowingly put corporate data at risk of a breach

MANCHESTER, UK. – 15th June, 2019 – Apricorn (http://www.apricorn.com/), the leading manufacturer of software-free, 256-bit AES XTS hardware-encrypted USB drives, today released new research highlighting the growing threats posed by mobile and remote workers. The research found that eighty nine percent of surveyed organisations have experienced a data breach, and human error is still the prevailing cause.

Almost two thirds (63%) of respondents noted that human error was the main cause of a data breach within their organisation – be it mobile workers, unintentional error, or employees with malicious intent. A lack of encryption and phishing emails also ranked in the top five main causes. This parallels earlier findings from a Twitter poll of 12,500 users carried out by Apricorn in February which found that humans, whether through malicious intent or unintentional error, were almost twice the threat to personal data than technology itself. This demonstrates that businesses need to be investing more time and resources into educating and supporting their employees, especially those working remotely, rather than continually financing new technologies to solve their security challenges.

Almost half of organisations' (47%) remote workers have knowingly put corporate data at risk of a breach, and over a third (34%) of respondents stated that their organisation's mobile/remote workers don't care about security - a staggering sixteen percent increase compared with findings from the previous year.

"It's unfathomable to think that even with GDPR (https://www.apricorn.com/gdpr) now in full swing, employees, and remote workers in particular, have such disregard for the security of corporate data they are responsible for and the risk they pose. To see the numbers increasing year on year, demonstrates the dire state of organisations' data security. Be it ignorance, defiance, or just simply a lack of care, employees are failing to engage even the most basic security measures, with no consideration for the consequences of their actions, or inaction in most circumstances", commented Jon Fielding, Managing Director, EMEA Apricorn.

When questioned on the biggest problems associated with implementing a cyber security plan for remote/mobile working, thirty percent of respondents stated that managing all of the technology employees require for mobile working is too complex. Just under a quarter of respondents (21%) stated that they cannot be certain that their data is adequately secured for remote/mobile working, with fourteen percent highlighting that they have no control over where company data goes and where it is stored. However, this a massive improvement on previous years as this percentage continues to decrease, where in 2018 it was twenty seven percent, and in 2017 thirty eight percent admitted to having no control over where company data goes and is stored.

Additionally, half of the organisations surveyed expect that mobile and remote workers will expose their business to a breach, showing a huge mistrust in their employees' ability to keep data secure. Organisations should identify corporately approved, hardware encrypted devices that are provided to staff

with a justified business case, and whitelisted on the IT infrastructure, blocking access to any non-approved media.

“Organisations need to build a security-first culture to protect data on the move and limit the risks posed by human error. Employees need to be aware of the risks facing them and the serious implications of data loss for their employer”, Fielding added.

Worse still, IT decision makers trust third parties to look after business-critical data more than they trust their own colleagues, with over fifty percent saying they trusted third parties with their critical business data, but they are only provided with access to the data they require or, all the data they share with them is encrypted.

“The fact that organisations have more trust in third parties than their own employees is alarming. If businesses invested more time in educating employees and enforcing the necessary security policies to ensure compliance with data protection regulations, they would find that securing corporate data would be a much less taxing and worrisome process”, Fielding concluded.

###

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 Censuswide, an independent survey company. Censuswide interviewed 100 IT decision makers in the UK, during April 2019. Respondents to this research came from finance, business and professional services, IT, telecoms, manufacturing and utilities organisations with more than 1,000 employees.

Media Contact
Paula Averley
Origin Comms (https://origincomms.com/)
t. 020 3814 2941
e. apricorn@origincomms.com