More than 60% of security decision makers expect employees to put corporate data at risk according to Apricorn research

Decision makers say corporate data knowingly put at risk by 55% of mobile workers

POWAY, CALIF., USA, June 19, 2024 /EINPresswire.com/ -- Apricorn, the leading manufacturer of software-free, 256-bit AES XTS hardware-encrypted USB drives, has today announced findings from global research into the security and storage of data. The research uncovered that 63% of surveyed* UK and U.S. IT Security Decision Makers expect their mobile/remote workers to expose their organization to the risk of a data breach.

This lack of trust in employees seems justified when 55% surveyed* noted that their mobile/remote workers have knowingly put corporate data at risk of a breach over the last year. In fact, 40% in the UK and U.S. said their mobile/remote workers don't care about security.

Ninety-five per cent of those surveyed* in the UK and U.S. agreed that their organization's mobile/remote workers were aware of IT security risks and practices and followed required policies to protect the data they work with at all times. Unfortunately, 73% of remote employees, lack the skills and technology needed to keep data safe, despite being willing to comply with these security measures.

"Organizations must bridge the gap between trust and capability to establish a robust and secure data environment. Investing in comprehensive training programs and the necessary tech to equip employees to safeguard data is crucial. Providing employees with removable USBs and hard drives that automatically encrypt all data written to them, ensures companies can give everyone the capability to securely store data whether at rest or on the move," said Kurt Markley,

Managing Director, Americas Apricorn.

> Organizations must bridge the gap between trust and capability to establish a robust and secure data environment."
>
> *Kurt Markley, Apricorn Managing Director, Americas*

Unsurprisingly, phishing (31%) and employees unintentionally putting data at risk (30%) took the top spots as the main causes of a data breach within organizations in the UK and U.S., closely followed by ransomware (29%).

The good news is that while employee risk and distrust have increased, organizations are making a definite move to protect their data. When asked if their organization has an information security strategy/policy that covers employees' use of their own IT equipment for mobile/remote working, 54% IT security decision makers surveyed in the UK and U.S. said they allow employees to use their own IT equipment remotely. Furthermore, they control this access to systems and data through software they install. This shows businesses are clearly doing their part to lock down the use of employee devices and regain control of corporate data.

Positively, when asked if their organization notified the appropriate authorities of a breach/potential breach or if they were aware they had been reported by someone else, organizations are being accountable and self-reporting. Just 11% of respondents said they had been reported to the authorities by others, with 63% saying they themselves notified the authorities.

"Data breaches are an unfortunate reality, but it's encouraging to see that businesses are taking proactive measures to mitigate these risks. Companies are now implementing more robust controls and investing in advanced technologies to safeguard sensitive information. Businesses have made significant strides in improving their response and reporting processes and the need for transparency and accountability when it comes to notifying regulatory authorities.

"The fact that businesses are actively working towards better data security and response mechanisms is a positive sign. It shows a commitment to evolving and adapting to the threat landscape and containing the impact of breaches to allow for a more efficient and effective recovery process," added Markley.

Methodology
The research was conducted by Censuswide with 604 UK and U.S. IT security decision makers (manager level +) of large companies in the UK and U.S. between May 7, 2024 May 10, 2024. Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles and are members of The British Polling Council.

*"Strongly agree" and "agree" answers combined

###

About Apricorn
Apricorn provides secure storage innovations to the most prominent companies in the categories of finance, healthcare, education, and government throughout North America and EMEA. 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.

Sarah Hawley
Origin Communications
480-292-4640
email us here
