Almost half of organisations have been reported to the ICO for a potential data breach

Submitted by: Origin Comms Ltd
Thursday, 14 May 2020

94 percent of organisations now have a policy that requires encryption of all data held on removable media

MANCHESTER, UK – 14 May, 2020 – Apricorn (http://www.apricorn.com/), the leading manufacturer of software-free, 256-bit AES XTS hardware-encrypted USB drives today announced findings of its annual survey into the attitudes towards data breaches and the implementation of encryption technology within organisations. Almost half (43 per cent) of surveyed IT decision makers said that their organisation has been reported to the ICO since the General Data Protection Regulation (GDPR) came into effect. The survey also highlighted an increase in the implementation of encryption and endpoint control since GDPR was enforced.

A quarter of respondents (25%) said they had notified the ICO of a breach or potential breach within their organisation, whilst 21 per cent have had a breach or potential breach reported by someone else. Over 160,000 breach notifications have been made to data supervisory authorities in the European Economic Area (EEA) since GDPR came into play, according to a data breach survey carried out by law firm DLA Piper (https://www.dlapiper.com/en/global/insights/publications/2020/01/gdpr-data-breach-survey-2020/), up to the end of January 2020.

“The fact that so many businesses are now choosing to notify of a potential breach is positive, but likely precautionary to avoid falling foul of the requirements and any significant financial or reputational ramifications,” commented Jon Fielding, Managing Director EMEA, Apricorn.

However, these concerns are being mitigated by an increase in encryption and endpoint control. Nearly all respondents (94%) say their organisation has a policy that requires encryption of all data held on removable media. Of those that encrypt all data held on removable media, more than half (57%) hardware encrypt all information as standard on all removable media.

Of those with an information security strategy that covers employees’ use of their own IT equipment for mobile/remote working, Forty two per cent said they permitted only corporate IT provisioned/approved devices, and have strict security measures in place to enforce this with endpoint control, which shows a huge rise compared with 12 per cent in 2019, highlighting a positive shift in focus towards endpoint control.

When questioned on whether they had seen an increase in the implementation of encryption in their organisation since GDPR was enforced, nearly four in ten (39%) have noticed an increase, and their organisation now requires all data to be encrypted as standard, whether it's at rest or in transit. This is a positive step given the number of employees now working remotely as a result of the current pandemic.

Whilst many businesses are currently encrypting devices, they also highlighted that they have no further plans to expand encryption on USB sticks (38%), laptops (32%), desktops (37%), mobiles (31%) and portable

hard drives (40%). This is worrying given the risks posed to corporate data being held on unencrypted devices. Businesses should allow only corporately approved, hardware encrypted devices that are whitelisted on the IT infrastructure, and block access to all non-approved media through end point control.

“The wide variety of options for encryption deployment can be intimidating, and companies haven’t been using it effectively. Organisations are now beginning to recognise the importance of endpoint hardware encryption and the need to implement and enforce policies to protect corporate data, ensure compliance with data protection regulations, and reduce the potential for a data breach,” points out Fielding.

When asked about the impact of a data breach on their organisation, more than a third (35%) of respondents cited that damage to the brand and reputation of the business is their main concern. This was followed by concerns over financial costs for incident response and clean-up (28%), loss of customer trust (18%) and financial costs resulting from a fine (12%).

“Focusing on how best to manage and respond to a potential breach in cooperation with data protection authorities is essential. Being able to establish a cause and remediate quickly will put businesses in good stead for breach recovery,” added Fielding.

Employees unintentionally putting data at risk remains the leading cause (33%) of a data breach, with lost or misplaced devices now the second biggest cause (24%), and third parties mishandling corporate information not far behind (23%). This correlates with the fact that despite more than a third (35%) of the survey respondents having complete visibility of which devices employees are using to access the corporate network, they are not certain that all are secure.

Fielding said ‘it’s clear that GDPR is finally having some impact, but businesses need to recognise that compliance is ongoing and they should continue to enforce and update all policies. Equally, more needs to be done in terms of employee awareness and education if they want to reduce the risk of a data breach, particularly given the increase in data moving beyond the corporate network.”

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