September 2022

Poll of IT security pros suggests gaps in UK cyber defence

iStorage calls for mass adoption of encryption to help stem the rise of cyber crime and limit the impact of ransomware following snapshot survey at Infosec 2022

A recent poll to take a snapshot of opinion and behaviour of over 100 IT security professionals reveals a stark contrast in attitudes versus action when it comes to limiting the impact of cybercrime. As cyber-related criminality continues to make headlines around the world, the poll, conducted by iStorage, a trusted global leader of hardware encrypted portable data storage & cloud encryption devices, looked at three key areas around remote working, use of cloud and ransomware.

Nearly 9 in 10 work remotely but too few encrypt the data
86% of polled IT security professionals said they took their device away from the office to work remotely. However, best practice when it comes to data backup and security is in short supply with approximately one third reporting they do not back-up data to a data storage device (29%), and of the 71% who said they do back-up data to a data storage device, 48% said that data was not encrypted.

- The UK's National Cyber Security Centre advocates a 3-2-1 back-up strategy to protect against cyber attack - over half (56%) of IT security professionals don't follow it.

CEO of iStorage, John Michael, explains: "To minimise risk and maximise protection it's essential to consider encrypting files both in transit and at rest, so that if a device does fall into the wrong hands, the data it contains cannot be accessed. We hear stories of business executives losing data storage devices containing personal and confidential data every day[1], and in most cases, that data is not encrypted. We need our IT community to be setting a model example by encrypting data."

Another recent study by Verizon[2] found that with the increase in hours, locations and devices that employees are using, there has been a corresponding increase in vulnerability for companies with security teams facing an uphill battle as the number of remote workers increases. By encrypting data, businesses can enhance the security of their files as well as any communications that take place between client apps and servers.

More than 9 in 10 now view ransomware as a major concern
91% of IT security professionals who were polled agreed that the threat of ransomware was a cause for concern in their organisation. The latest threat landscape report by ENISA[3], the European Union Agency for Cybersecurity, also warns of a surge in cyber

[1] https://www.information-age.com/two-laptops-left-tube-every-day-reveals-transport-london-123461389/
[2] https://www.verizon.com/business/resources/reports/mobile-security-index/
[3] https://www.enisa.europa.eu/news/enisa-news/hackers-for-hire-drive-the-evolution-of-the-new-enisa-threat-landscape

criminality, and details how ransomware has become the prime cybersecurity threat facing organisations today, much of it driven by the monetisation of attacks.

Cyber criminals trigger a ransomware attack by secretly compromising networks, often via phishing attacks, infiltrating cloud services or exploiting vulnerabilities[4]. The iStorage poll revealed that nearly half (47%) of IT security professionals assumed cloud providers are responsible for data in the cloud. In addition, 34% do not encrypt data before sharing with colleagues – such as over a cloud file-transfer service - when working remotely.

However, cloud providers include a 'Limitations of Liability' clause which places data-security responsibility with the cloud user. Since the cloud user is liable, organisations must establish their own security measures to ensure data protection and privacy. One vital step is encryption.

In order to ensure the data is kept confidential even if the cloud account is hacked via, for example, a phishing email, the user should retain full control of the encryption key. Removing the encryption key from the cloud and physically storing it within a PIN-authenticated external USB module will allow users to access data stored in the cloud in the most secure way possible, while also being able to securely encrypt information from a local computer, a network drive, or sent via email or file-sharing service.

John Michael concludes, "Ransomware is the most significant cybersecurity threat facing organisations today as increasingly professional and sophisticated cyber criminals skilfully follow the money in order to maximise the profit from illicit campaigns. We cannot afford to be complacent. Encryption isn't just for the likes of the secret services, it should be used now as part of business modus operandi and is a relatively simple measure to reduce the impact of cyber crime which continues to cost global economies billions."

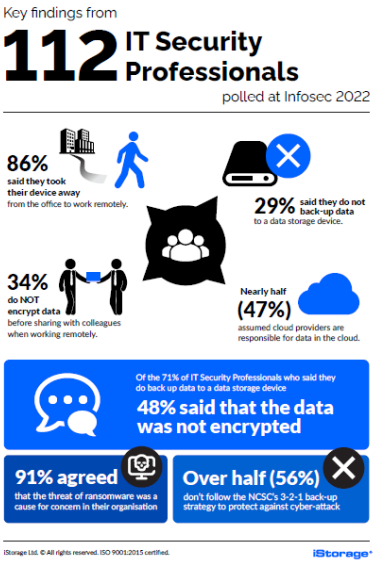
Notes to Editor:

Key findings from 112 IT Security Professionals polled at Infosec 2022:

- 86% said they took their device away from the office to work remotely.
- 29% said they do not back-up data to a data storage device.
- 34% do not encrypt data before sharing with colleagues when working remotely.
- Nearly half (47%) assumed cloud providers are responsible for data in the cloud.
- Of the 71% of IT security professionals who said they do back up data to a data storage device, 48% said that data was not encrypted.
- 91% agreed that the threat of ransomware was a cause for concern in their organisation.
- Over half (56%) don't follow the NCSC's 3-2-1 back-up strategy to protect against cyber attack

Learn more about iStorage's range of award-winning data-storage solutions: www.istorage-uk.com

[4] https://www.zdnet.com/article/ransomware-these-are-the-two-most-common-ways-hackers-get-inside-your-network/



[Image:** iStorage calls for mass adoption of encryption as poll of IT security pros suggests gaps in UK cyber defence**]

For further information about iStorage, please contact:

Grant Powell | Matt King, Media Safari

***T**: +44 (0)1285 700715 | **E**: grant.powell@mediasafari.co.uk*

Tina Symeon, Marketing Manager, iStorage

***T**: + 44 (0) 20 8991 6260 | **E:** tina.symeon@istorage-uk.com*

About iStorage

iStorage is the trusted global leader of award-winning, PIN authenticated, hardware encrypted portable data storage & cloud encryption devices. iStorage offers the most innovative range of products to securely encrypt, store and protect data to military standards; safeguarding valuable and sensitive data to ensure compliance with stringent regulations and directives such as GDPR, HIPAA, SOX, NRC, GLB and DHS Initiatives. Today, iStorage products are used by government, military, multinational corporations as well as consumers in over 50 countries, with the mantra that encryption is an essential commodity required by all. Learn more at https://istorage-uk.com