PEACE OF MIND

Jon Fielding *reveals why we should all be encrypting our data as standard*

The UK Ministry of Justice (MOJ) lost 184 mobile phones, PCs, laptops and tablet devices between September 2020-2021, according to its response to a recent Freedom of Information (FOI) request. NHS Digital recorded 393 lost or stolen devices in the same time period, while Her Majesty's Revenue and Customs (HMRC) reported a total of 346. The FOI requests were submitted by Apricorn to a number of UK government departments, with the aim of establishing the security of devices held by public sector employees.

Research into the Home Office's Annual Report and Accounts 2020-21, meanwhile, highlighted a loss of 1,150 inadequately protected pieces of electronic equipment, devices or paper documents from outside secured government premises, and a further 1,085 from within secured government premises.

The extent to which government-owned devices – and therefore any data held on them – are going missing in action is alarming, given the sensitive nature of the information at risk. However, the response to another question included within the same FOI request was reassuring, and indicates why these losses haven't resulted in one or more disastrous breaches: all the departments that responded confirmed that the devices affected were encrypted, and as a result the data they housed was fully protected.

Mobile and removable devices present a particular point of weakness in the hybrid and remote working environment, for organisations in every sector. The fact is, they're extremely easy to misplace and they are increasingly carried back and forth between different locations as employees move around, making them more vulnerable to loss and theft. HMRC noted that 111 of the devices it reported were lost in tracked transit, on their way to delivery to a final destination, which is likely to reflect staff working from home as a result of COVID-19 restrictions.

Flexible working practices support increased productivity and efficiency, but they also raise cybersecurity risk. It's inevitable that higher volumes of sensitive data will be stored on smartphones and laptops – and this data will be constantly moving beyond the 'safe' network perimeter that security teams carefully built for their companies before COVID-19 blurred the edges.

Cyber criminals have their eye on employees' devices and equipment, looking for gaps in endpoint security that will allow them to access the information on the devices, as well as to use them as a convenient entry point to enterprise networks, systems and apps.

Organisation-wide encryption is being increasingly recognised as a straightforward way of managing risk in this complex new environment, enabling the responsible and secure management of sensitive or valuable information such as personal data and intellectual property.

When data is encrypted, it is rendered unintelligible to anyone without the key. This keeps it secure whether it's on the move or at rest, and from whatever disruption may happen around it – for example a device being dropped on the street, left in an Uber or picked from a pocket.

The UK Information Commissioner's Office backs this up, noting that Article 32 of the General Data Protection Regulation (GDPR) specifically recommends encryption as a method to protect personal data where appropriate. GDPR Article 34 removes the obligation on breached organisations to inform each individual affected if encryption has been applied, while Article 83 suggests that fines will be moderated where a company can show it has been responsible and mitigated damage suffered by data subjects.

WHEN DATA IS ENCRYPTED, IT IS RENDERED UNINTELLIGIBLE TO ANYONE WITHOUT THE KEY

So how are organisations using encryption today? A third of UK organisations now require all corporate data to be encrypted as standard, according to Apricorn's 2021 Global IT Security Survey. This is a step in the right direction, but it appears that the majority of organisations are still not doing so. And this is having an impact: 12 percent of the IT leaders surveyed admitted point-blank that a lack of encryption had been the main cause of a data breach within their company in the last year.

A third (32 percent) of organisations asked revealed that they have increased encryption across all mobile and removable devices in the past year. Use of encryption is particularly advanced when it comes to removable media such as hard drives and USBs – with 77 percent of IT leaders confirming their organisation has a policy that requires encryption of all data held on such devices.

The extent to which government-owned devices – and so data held on them – are going missing in action is alarming, given the sensitive nature of the information at risk

The rise in implementation of encryption looks set to continue: the IT decision makers surveyed said they intended to expand usage on USB sticks (19 percent), laptops (16 percent), desktops (12 percent), mobiles (22 percent) and portable hard drives (18 percent). These findings underline the crucial role encryption has to play in protecting sensitive information.

The encryption of information needs to be firmly embedded into an organisation's ways of working and governance framework if it is to be effective. The encryption of all data – whether it's in transit or at rest – should be mandated in policy and enforced at an operational level. Policies should clearly set out exactly how and when encryption must be implemented, and include specific policies drawn up for remote and hybrid working situations. These should cover when and how employees are permitted to use their own devices or equipment for work purposes.

Educating the entire workforce in the use and importance of encryption is also vital. Every individual must understand how to correctly apply the tools and technologies they're equipped with for encrypting information or handling encrypted information. They should also have complete clarity on the 'why': the risks associated with a lack of encryption, the specific data privacy legislation the organisation is subject to, and the consequences if data is breached, lost or exfiltrated. All policies and training programmes must be regularly revised in line with regulations, emerging threats and evolving company working practices to ensure continued relevance and compliance.

Ideally, the use of removable media should be restricted to hardware-encrypted devices that have been approved for use by the organisation. This policy can be enforced by whitelisting on the IT infrastructure, locking down ports on employees' machines so they can only accept an approved device. Even if the device itself is lost or stolen and inserted into another host computer, the information stored on it will remain unreadable without authorised and authenticated access. This means that all data can be stored or moved around safely, offline.

Properly implemented and certified, built-in hardware encryption with onboard authentication affords a higher level of protection than software-based encryption, which can present portability challenges and introduce device vulnerabilities such as counter resets, software hacking, screen capture and keylogging. When held safely in a hardware crypto module, encryption keys are protected from brute force attacks and unauthorised access.

Hardware-encrypted devices with onboard authentication use internal features to protect the information on them. All cryptographic operations take place within the device, meaning no additional software is required that could itself be vulnerable to attack, while critical security parameters, such as passwords and key data, are never shared with the host computer.

Enterprise data encryption and cryptographic techniques continue to develop at pace, ensuring that organisations can keep a step ahead of the hackers. Global encryption standards such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197) – part of FIPS Federal Information Processing Standards (FIPS), developed by NIST (the National Institute of Standards and Technology) in the US – also continue to advance.

> **ORGANISATION-WIDE ENCRYPTION IS A STRAIGHTFORWARD WAY OF MANAGING RISK**

Having data backups in place, in addition to a policy of encryption, further increases resilience – allowing mission-critical applications to remain functional in the case of a data breach or loss and ensuring information can be recovered and restored quickly.

A regular and reliable back-up process will protect organisations from unexpected data loss from all potential angles. The back-up mantra has always been the '3-2-1 rule': have three copies of data, on two different media, one of which is offsite – and this still holds true. However, in the era of cloud computing, disparate workforces and evolving cyber threats, this may no longer be enough. If an enterprise only backs up data online, or relies on just one single type of offsite backup solution, it could still leave itself vulnerable to costly downtime and possible financial and reputational damage.

Best practice back-up strategies should be multi-layered and hybrid, incorporating more than one type of offsite location – ideally one online and one offline. And all information, wherever it's being stored and held, must be encrypted. Backing up copies of important files on hard drives or other storage devices connected to corporate systems or networks ensures the organisation can always restore from a clean, protected data set. This is especially pertinent in light of the growing ransomware threat. When not being backed up to, the devices should be disconnected from the network to create an air gap between data and any threat.

Protecting critical data assets wherever they are, and regardless of the endpoints used, is entirely achievable via end-to-end encryption coupled with rigorous back-up strategies. Encryption enables organisations to reap the benefits of hybrid home/office working practices, allowing employees to use their own hardware safely.

The growing use of encryption across organisations is hugely positive, but implementation must be ramped up further and faster to avoid a surge in data breaches in the hybrid working environment. Employees will be accessing networks, systems and databases from a multitude of locations, using a mix of personal and corporate devices. With such a disparate and mobile workforce, any gaps in security posture will create unacceptable risk.

Encryption – especially when it's automated and enforced – is the surest, most straightforward way of keeping ahead of evolving cyber threats, remaining compliant with regulations and mitigating human error. It really should be high on every organisation's priority list ●

Jon Fielding is managing director EMEA at Apricorn

Flexible working practices support increased productivity and efficiency, but also raise cybersecurity risk