MINIMISING RISK

Jon Fielding *reveals what needs to be done to control the risk amid the growing trend for hybrid working*

Picture credit: Shutterstock

It's often the human element in the business that proves to be the weakest link in the cybersecurity chain, with the World Economic Forum reporting that 95 percent of cybersecurity issues can be traced to human error. And it's an issue that has only been exacerbated by hybrid working, with a survey conducted by the UK Office for National Statistics last year revealing 84 percent of workers intended to continue working remotely to some extent in the future – and for good reason.

However, hybrid working has brought a host of new security risks. Those on the move are more likely to tap into unsecure public wi-fi networks and without the presence of security personnel to offer advice and guidance, staff members may also fail to update company devices in a timely fashion, creating issues of patch lag. Shadow IT, too, continues to be an increasing problem, with many opting to use unmanaged devices to access corporate networks.

In the eyes of security decision makers, problematic employee behaviours such as these often stem from poor knowledge of common security mistakes. In a recent Apricorn survey of 201 security leaders across large companies in the UK, well over a third (37 percent) thought their staff are continually (albeit unintentionally) putting data at risk. Further, one in five (21 percent) stated that lost or misplaced devices containing sensitive corporate information were also a common issue.

Human error will always be unavoidable. Even the most cyber-savvy network users may slip up from time to time, with cyber criminals laying increasingly sophisticated social engineering traps. However, it is concerning that organisations clearly feel that large swathes of their employees lack the basic cyber awareness and skills needed to address simple errors.

And remote and hybrid working isn't helping. When asked about the key problems they face with implementing a cyber security plan for remote and mobile working, survey respondents revealed that the biggest issue (as cited by 28 percent) was a lack of awareness among employees of the risks to data when working away from the office.

For security leaders, it's clearly not just an issue of poor employee awareness, however. Negligence was a big one with almost half (48 percent) of those questioned in the survey admitting that their company's mobile or remote workers have knowingly exposed data to a breach over the last year, a rise from 29 percent in 2022, while 46 percent stated that their remote workers "don't care" about security – up from 17 percent the previous year. On the question of key problems faced when implementing a cyber security plan, almost a quarter (23 percent) also revealed that staff who are aware of security risks will still take action that results in data being exposed or lost.

It is concerning that organisations feel that some employees lack basic cyber awareness and skills

Clearly, there appears to be a lack of buy-in, and in some cases a blatant disregard for the need to follow cyber security policies. The survey also found that the most common reasons remote security policies weren't followed were staff members not prioritising security practices despite being informed about them (51 percent) and using personal devices for working purposes (40 percent).

Alongside negligence, 20 percent said employees with malicious intent had been behind a breach at their company, a rise from 10 percent last year. The cost-of-living crisis hasn't helped matters. There's already evidence that employees are exfiltrating sensitive information when they are made redundant or even accepting payments from hacker groups in return for planting malware.

The latter is an avenue that threat actors are capitalising upon in the current economic environment, tapping into the financial hardships of individuals by attempting to convince them to hand over credentials or valuable information in exchange for financial reward.

Outside of the employee base, organisations are also having to concern themselves with their digital partners' security. Critically, 21 percent of respondents to the survey experienced a breach as a result of third parties mishandling corporate information – up from 12 percent last year. As organisations increase their reliance upon public cloud and other critical services from third party providers, this is an attack avenue that will only continue to be more actively exploited.

The survey clearly indicates businesses don't trust employees to live up to their responsibilities around protecting data – particularly among staff working remotely. If employees are left to their own devices, even the best technical measures may fail. So, how can firms narrow the knowledge gap and support employees more effectively?

Proactively creating stronger security cultures with transparently defined and easy to follow policies is a good starting point. But identifying vulnerabilities and strategising relevant protective protocols is only one aspect to this – ensuring rules are adhered to is just as important.

EVEN THE MOST CYBER-SAVVY NETWORK USERS MAY MAKE MISTAKES FROM TIME TO TIME

From opening suspicious emails to delaying security software updates on devices, poor security hygiene can lead to serious consequences. But, if staff members don't understand the potential risks associated with certain behaviours, they will continue to perform them. So firms must establish training and education programmes built to maximise understanding, creating a culture in which everyone embraces a security-first mindset. However, this will only be successful if security works for the individual. Security can't impede productivity or create frustration. If it does, staff members will ignore controls, or even find ways to circumvent them.

Of course, improving awareness and ease of compliance among employees is key. But there are other levers which can simultaneously be pulled. While the survey shows that security leaders believe their organisation's employees are continually putting sensitive data at risk of a breach, many firms aren't taking the necessary steps to limit the risks.

Despite awareness of the 'insider threat', companies are not applying the policy and technology measures necessary to prevent data being compromised. Of those that do allow employees to use their own IT equipment remotely, only 14 percent manage the risks this creates by controlling access to systems and data using software – a drop from 41 percent in 2022.

Nearly a quarter (24 percent) require employees to receive approval to use their own devices, but do not apply any controls, while 17 percent don't require approval or apply any controls, a rise from 8 percent last year. Further, 15 percent only allow corporate IT provisioned devices to be used but have no way of enforcing this.

Decentralisation of IT may be behind the slip in control that security teams have over the endpoint. The employee technology platform is moving further and further away from the organisation, especially where people are using their own devices. But security teams must get a grip on the situation by implementing controls. Fortunately, there are several ways in which enterprises can restore responsibility and ensure security is upheld. These include:

ZERO TRUST

Zero trust ensures that no device, user, interaction or endpoint is trusted until its identity has been verified. The idea is to eliminate implicit trust which can undermine effective security setups should a threat actor gain access to a target network. Instead of assuming everything behind a corporate firewall is safe, it demands that every user request is reviewed and approved to mitigate risky actions or malicious behaviours.

Zero trust also advocates the principle of least privilege – a fundamental aspect of NCSC-advocated strategies that ensures that the access of every individual within a network is limited to only those software solutions and systems that are truly needed to carry out a job, to both reduce digital footprints and in turn exposure.

UNMANAGED DEVICES

Enterprises should work to limit the opportunity for individuals to either intentionally or accidentally cause a breach by ensuring all staff members only use managed devices when accessing a corporate network.

From reducing visibility to undermining security protocols and expanding an organisations attack surface, unmanaged devices pose several security threats, while adversaries are increasingly focusing their efforts on targeting individuals. They provide threat actors with unimpeded avenues to gain a foothold on a network, and therefore must be eliminated as standard practice.

EMBRACING ENCRYPTION

If devices holding sensitive information such as USBs, laptops or mobile phones are lost or left in public places, encryption ensures that the next person to pick them up isn't able to access key data and potentially leak it into the public domain.

Alarmingly, only 12 percent of organisations currently encrypt data on all laptops according to the survey, compared with 68 percent in 2022, while 17 percent encrypt data on all desktop computers, down from 65 percent last year. It's a similar story for mobile phones, with 13 percent encrypting on all versus 55 percent in 2022; USB sticks, with percent encrypting today, down from 54 percent; and portable hard drives – a drop to just 4 percent from 57 percent.

This significant drop needs to be reversed. Indeed, lack of encryption was cited by 17 percent of the security leaders surveyed as having been a main cause of a data breach within their organisation – a steady rise from 12 percent in 2021.

BACKUPS

Backups are essential should preventative security measures fail, but companies shouldn't rely on just one form of backup. A multi-layered recovery strategy must be established, incorporating both physical backups located off-site and cloud recovery solutions.

Adopting the 3-2-1 rule is a sound principle in developing a resilient back-up strategy. This should see at least three copies of data held on at least two different media with at least one held off site. That held off-site should ideally be held offline and be encrypted to ensure it cannot be compromised. With this approach, information can always be recovered at speed if networks are compromised, serving to help organisations get back up and running quickly and effectively.

Ultimately, it is important to understand that there is no silver bullet solution that can protect companies from an increasingly volatile, voluminous and potentially harmful threat landscape. As attack methods evolve and escalate, organisations need to ensure that they have all their security bases covered, working to eliminate poor practices and mitigate the opportunities for threat actors to exploit a growing range of vulnerabilities.

By using a combination of methods to enhance employee awareness and reign in staff responsibilities, human-led risks can be more effectively managed in an increasingly remote and hybrid world. To reiterate, human error will always be somewhat unavoidable, and the likelihood that staff will be tricked will only heighten as social engineering attacks become more intelligent, tailored and convincing. But as of now the survey shows that negligence and malintent are threats that must be addressed.

By both improving awareness and reigning in responsibility, employees will be less likely and able to put highly sensitive data at risk. And even if they do, attackers will find it much more difficult to manipulate previously advantageous positions ●

Jon Fielding is Managing Director, EMEA for Apricorn.

Shadow IT is an increasing problem, with many opting to use unmanaged devices to access corporate networks