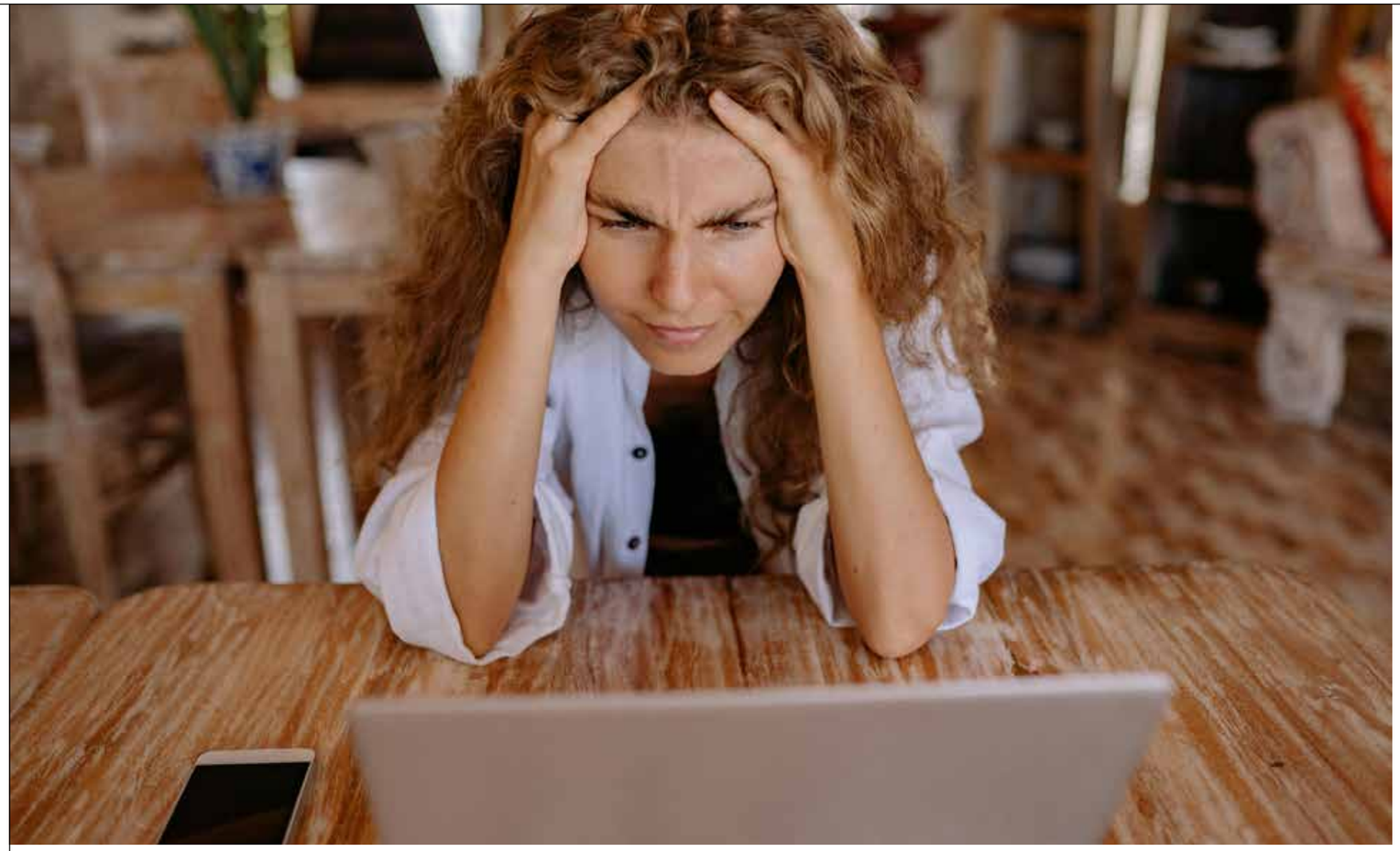

FIGHTING BACK

Phil Robinson *provides some top tips to beat hackers*

The attacker is winning in the perpetual battle over assets. There's been a 30 percent year-on-year increase in cyber attacks as of Q2 2024, according to Check Point Research, which suggests that technological advancements are not seeing defenders gain the upper hand. So, what should organisations be doing to beat the hackers?

It may not be headline grabbing, but one of the most effective steps is to address the bare basics by adopting good cyber hygiene – several practices that together can significantly improve the resilience of the business. Most cyber attacks are relatively unsophisticated and even opportunistic, so can be mitigated by adopting some simple measures. Even the NCSC has stated that: "Most ransomware incidents typically result from cyber criminals exploiting poor cyber hygiene, rather than sophisticated attack techniques".

Good cyber hygiene can be considered as taking a series of steps to implement and maintain security through best practice such as updating malware protection, password policies, cloud back-ups, network firewalls and restricting administrative access. Yet despite its simplicity, few organisations have taken the necessary steps to address these. In fact, the Cyber Security Breaches Survey 2024 carried out annually by the UK government, found that none of the 2,000 businesses questioned had implemented all 15 of the controls advocated.

Despite its simplicity, few organisations have taken the necessary steps to implement good cyber hygiene

While the majority had up-to-date malware (83 percent), firewalls (75 percent) and user-based access controls (73 percent), under half had in place rules for storing and moving personal data securely (48 percent), two-factor authentication (39 percent), separate wi-fi for staff and visitors (35 percent), policies to apply software security updates within 14 days (34 percent), VPNs for remote staff (32 percent), or monitoring in place to govern user activity (30 percent). What's more, in terms of technical controls among large businesses there has been no increase in comparison with 2023.

Those looking to address their cyber security hygiene would also be advised to look at the NCSC 10 steps to Cyber Security which seeks to provide medium and large businesses with a guide on the areas that should be addressed to prevent the majority of cyber attacks. Surprisingly, the breaches survey reveals that only 13 percent of businesses are aware of the guidance and of those questioned only 39 percent were observing at least five or more of the steps and only 3 percent all ten steps.

RISK-BASED APPROACH

It advocates the use of a risk-based approach to secure data and systems through the implementation of best practices processes and technology. For instance, the guidance recommends security awareness training, asset management, system design and management including configuration, incident response and supply chain security, which are largely process driven while the likes of vulnerability management, identity and access management (IAM), logging and monitoring, and data security measures are likely to feature some element of automation.

The 10 steps are still fairly high-level, however, so those looking for more practical guidance and to document their security posture may want to look at complying with Cyber Essentials or Cyber Essentials Plus, both government-backed schemes. In most cases organisational compliance is driven by client demand (it's often a requirement when bidding for public sector contracts) or pressure from the board and it's this mindset that needs to change.

Cyber Essentials aims to help businesses implement fundamental technical controls that increase resilience, manage third-party security risks and enable the business to cite the certificate to give assurance to the market and its stakeholders. It takes a practical approach, focusing on five controls: configuration, firewalls, user access, the management of updates and malware protection. To achieve certification, the business must perform a self-certified assessment in the form of a questionnaire, which a board member then attests is true with the assessment then reviewed by a qualified assessor. Once approved, the certificate lasts for a year. Cyber Essentials Plus is its big brother and has more rigorous criteria. It requires the business to be Cyber Essentials certified first and is based upon an independent assessment carried out in person by a qualified third party.

It's important to state that Cyber Essentials is not a silver bullet, but rather a base level of security that aims to mitigate the risk of the organisation falling victim to the most common forms of cyber attack. The most common forms of attack continue to be phishing (90 percent) of which nearly half (43 percent) were successful and hacking – unauthorised access or online takeover – (10 percent) of which just over a third (35 percent) resulted in fraud. However, the processes and controls advocated do lend themselves to improving defence against emerging attacks.

One example is the recent spate of deep fake attacks using Generativ AI (GenAI). The State of Information Security 2024 report from ISMS. Online found that 32 percent of UK businesses had experienced deep fake scams with Business Email Compromise (BEC) the most common form. Prime examples of this in action include the video group meeting that compromised an employee at UK engineering firm Arup, resulting in the transfer of $25-million, the impersonation of the LastPass CEO in a vishing attack against an employee, and another attack where advertising firm WPP saw their CEO cloned.

ORGANISATIONS NEED TO BE CONTINUALLY TAKING STEPS TO IMPROVE THEIR SECURITY POSTURE

These modern incarnations of CFO fraud/whale phishing aren't particularly easy for technology to detect, which means that the best means of currently countering these attacks is through a combination of security awareness training and additional verification processes.

Employee training programs therefore need to be updated to include ways to spot deep fakes, such as by looking for tell-tale signs. In video, AI can find it challenging to accurately render digits and lip syncing, but it can relatively easily fake audio and photos in comparison, so these should be regarded with the highest levels of scepticism.

Verification can be enhanced when it comes to sanctioning payments. In its report, The battle against digital manipulation, Deloitte recommends a multi-layered approach to approving transactions such as code words, token-based systems or live detection verification such as taking a selfie or video recording, which is already in use today in the banking sector.

IAM, one of the 10 steps and controls advocated in Cyber Essentials, can also help here. Businesses should seek to restrict access through the implementation of least privilege and more secure access methods, particularly for remote workers. The adoption of new approaches such as Zero Trust can also reduce exposure and limit the potential for abuse of existing access technologies such as VPNs.

In the event that the attack does proceed, there needs to be a series of processes in place to handle incident reporting and response. Again, this requires updating existing processes such as phishing attack exercises so that employees are subjected to visual and audio attacks and providing them with suitable channels to report any suspicious incidents. The security team, too, needs to know precisely how to respond, making it vital that the business puts in place AI governance in the form

of a risk-based framework such as the NIST AI Risk Management Framework.

Ransomware, too, is evolving with extortion now commonplace. This means that backup is no longer a sufficient defence, making it critical that the organisation seeks to bolster network defences. Basic practices such as log monitoring and network segmentation are therefore essential to spotting and arresting such attacks. Segmentation can prevent the attacker from moving laterally across the network, reducing the risk of data exfiltration. The State of Exposure Management Report 2024 , for example,

GOOD CYBER HYGIENE CAN SIGNIFICANTLY IMPROVE THE RESILIENCE OF YOUR BUSINESS TO ATTACKS

illustrates that the chance of attackers compromising critical assets increases in relation to the number of hops made across the network, from 62 percent in one hop to 80 percent with four. That ability to move around the network also increases the risk to cloud assets as those able to hop from on-premise to cloud were able to compromise in-cloud assets 93 percent of the time.

Essentially, in order to successfully defend the network, the organisation needs to be aware of and continually taking steps in order to improve its security posture. Cyber hygiene provides a foundation or starting point, but the ideal is to then build upon that, working towards the nirvana of a cyber mature business.

Cyber maturity is all about the readiness of the business to react to threats and vulnerabilities and so differs from organisation to organisation, and in order to achieve it it's necessary to measure the security posture in relation to the threat spectrum. However, only 65 percent of organisations measure their maturity today, according to ISACA's The State of Cybersecurity 2023 report, revealing that there simply isn't sufficient awareness of how effective defences are nor where the gaps currently lie. Until organisations attend to their cyber hygiene and measure their maturity they will continue to suffer from holes in their defences and fall victim to common forms of attack.

There are plenty of horror stories concerning organisations that have fallen victim to attacks because they haven't attended to the basics. Misconfigured servers, failing to patch systems in a timely manner, to implement multi-factor authentication (MFA) and password management, or to lock down the risk associated with third parties – all of these can provide the attacker with the toehold they need to gain access to the network and escalate an attack. In fact, the 2024 Global Cyber Confidence Index found more than half (51 percent) of those organisations surveyed had experienced cyber events that could be directly attributed to poor cyber hygiene, illustrating that many have still a long way to go in achieving a base level of security to thwart the attacker before they can then seek to address their cyber maturity ●

Phil Robinson – Principal Security Consultant at Prism Infosec – has over 25 years' experience in the infosecurity industry and is an (ISC)2 CISSP, ISACA CISA, Cyber Scheme Team Leader (CSTL), and a PCI Qualified Security Assessor (QSA).

The NCSC provides medium and large businesses with a guide on the areas that should be addressed to prevent the majority of cyber attacks

Picture credit: NCSC