Picture credit: Getty

KNOWLEDGE IS POWER

Oliver Paterson *warns about the importance of training security personnel to ensure they are prepared for the worst eventuality*

Research shows that security-related risks are reduced by 70 percent when businesses invest in education

No company is safe from the possibility of cyber attacks, regardless of how big or small they are. This is clear as cyber crime cases are increasing year on year, especially during the peak of the pandemic, with the National Cyber Security Centre (NCSC) of the United Kingdom reporting a 20 percent rise in major threats compared to 2018-2019. Furthermore, cyber attacks are continuously evolving, as we see a rise in new and more sophisticated tactics, such as fileless malware and cryptominers.

It is clear in today's world that organisations of any size must prioritise cybersecurity – and a fundamental part of this is for businesses to consider putting internal security awareness training and awareness programmes in place. This is of utmost importance, as research shows that security-related risks are reduced by as much as 70 percent when businesses make the decision to invest in such education.

The core of any company's cybersecurity strategy must be a trained workforce who are aware of their responsibility in maintaining the protection of business data, combined with digital security solutions to further support them.

When a multi-million pound company is the target of a cyber attack; from companies such as Crypto.com, Microsoft and Cash App, they often make the news headlines. However, small and medium-sized businesses (SMBs) are equally as vulnerable, despite the fact we may not hear about them as frequently. This is specifically highlighted as in the UK, small businesses are the target of 65,000 attempted cyber attacks per day.

Despite it being possible for both a start-up business or an established corporate entity to be attacked, it is the smaller businesses who will suffer the most – as they might not have the same cybersecurity infrastructure in place compared with larger counterparts. Unfortunately, research shows that 60 percent of small organisations normally go out of business within six months following a hack, which is a consequence from lacking the necessary resources to withstand such cyber attacks.

No matter the size of an organisation, the fallout from a cyber attack can be financially impactful, as well as having long-term implications on business reputation and recovery. Businesses, especially those in regulated industries, have reputations to uphold in order to maintain a loyal customer base. Those that fail to protect their customers' confidential or valuable data will have to deal with the negative press and mistrust from existing and potential customers that could seriously impede the organisation as a whole.

VIPRE's whitepaper revealed that research conducted by IBM found ransom requests can reach up to £31-million on average. However, despite businesses paying the ransom, there is no guarantee that the data will be un-encrypted or even returned, and, if the data is stolen it may still be leaked.

A recent study also confirmed that cyber attacks against small businesses are estimated to cost the UK economy £34-billion pounds annually. According to Simon Fell, Chair of the All-Party Parliamentary Group on cybersecurity, the report demonstrated that: "Businesses often lack awareness of the cybersecurity risks they face, the protection they need to mitigate them, and the resources to withstand them," and he referred to it as a problem of national economic resilience.

One example of a small business targeted by a hacker is online food delivery service, DoorDash, which experienced a major data breach where hackers gained the private information of millions of users, costing the company tens of thousands of dollars. Another instance is Volunteer Voyages, a business that connects travellers to humanitarian volunteer opportunities. It lost thousands of dollars after hackers gained access to the owner's bank details. Regrettably, it was never able to recover these losses.

The above highlights just some of the damaging consequences that can affect businesses once they experience a cyber attack – especially SMBs. However, by prioritising and investing in their cybersecurity, as well as by being aware and informed about the threats they face, smaller organisations can safeguard their information and operational security from these types of attacks.

90 percent of businesses experienced a rise in cyber attacks during the COVID-19 pandemic, according to a recent global survey. Cyber attackers who can identify weaknesses within a business are able to use this to their advantage – whether this is moving from office-based working to hybrid working, away from the support of their trusted IT teams or because their employees are being put under more pressure to work harder than ever before.

Even before COVID-19, humans were frequently exploited as a point of entry into an organisation. 90 percent of cyber data breaches are a result of human error, according to data from the United Kingdom Information Commissioner's Office. Employees can be unaware of the vital part they play regularly in keeping personal, confidential and sensitive information secure. Humans will inevitably make mistakes, but employees who are working from the comfort of their own home that are tired, stressed, and possibly distracted, pose even more of a risk to an organisation.

Instead, employees who are educated about the threats they could be vulnerable to, how to identify them and the steps to take in the event of a suspected attack, are a critical asset. To be successful, it is crucial that businesses change the mindset from full reliance on IT, to one where everyone is responsible – and this is where security awareness training plays a pivotal role.

Ensuring that workforces are able to comprehend possible hazards, recognise them and stop them from happening is crucial. Unfortunately, research shows that 81 percent of small and micro-businesses do not have cybersecurity training in place, and as a result lack the tools and information necessary to defend themselves against an attack. Businesses need to prioritise their security investment by making education and awareness a top priority. Organisations cannot expect their employees to remain ahead of the evolving cybersecurity risks without this training. Instead, initiatives such as security awareness training and phishing simulation tools can help reduce this cyber risk and drive secure user behaviour.

IT IS IMPORTANT THAT ORGANISATIONS OF ANY SIZE TAKE MEASURES TO PRIORITISE CYBERSECURITY

However, implementing a yearly security awareness training programme may satisfy urgent needs, but it does not build a strong, solid strategy for keeping secure against cyber threats. To get the most value and retention out of this learning, businesses must ensure that training is continuous and fits the demands of the organisation.

When selecting a security awareness training programme there are a number of factors to be taken into consideration, because it should not be a one-size-fits-all strategy. This includes the length of the course, the level of engagement, making sure it is applicable to a global audience, as well as the variety of multimedia content offered. Training should be conducted on a regular basis, targeted to each user's particular vulnerabilities, while including a diverse range of authentic situations. This involves the implementation of phishing simulations, which will aid in the replication of realistic scenarios that frequently occur, particularly via email, so that staff members can recognise potential warning signs and know how to act on this. These training programmes give businesses insight into their staff's level of security knowledge, exposing any flaws within the organisation and enabling IT to provide extra training where it is needed.

As a result, these programmes will support the business to stay one step ahead of attackers and strengthen the workforce's security culture. If a business's first line of defence isn't strong, they face leaving the door open for a potential attack to occur. Users need to feel confident and empowered as part of the businesses' overall cybersecurity strategy to support the prevention of such attacks.

It's not unexpected that sending and receiving emails frequently can result in cyber attacks, especially since

human mistake is the primary cause behind a majority of them. Email is the primary method of internal and external communication across businesses, yet email malware attacks were up by 600 percent compared with 2019. Additionally, mistakes can always happen; including sending a private document to the incorrect person or clicking on a phishing email. However, these accidents can have negative repercussions.

60 PERCENT OF SMALL ORGANISATIONS GO OUT OF BUSINESS WITHIN SIX MONTHS OF A HACK

Digital security solutions can be used in conjunction with the adoption of anti-malware tools and technology, to remind employees about double-checking their email recipients and attachments before sending an email. This means that the individual can be shielded against potentially harmful emails, such as those that include phishing links or infected attachments, before they even reach them by adding advanced threat prevention tools to your email security. By having technology solutions in place that alert individuals when they may be about to make a mistake over email – it not only reduces errors, but it also improves and strengthens the businesses email security culture, while enhancing compliance credentials.

When organisations' communication relies so heavily on email, accidental data leakage is a significant, yet seemingly unavoidable risk. AI (Artificial Intelligence) and ML (Machine Learning) technologies are also crucial additions in endpoint and email security services. Implementing systems such as URL sandboxing solutions and email security attachments allow the email attachment or link to be opened and analysed using Artificial Intelligence in an isolated environment away from the user's network.

The role of IT teams in making sure the right security measures are in place is widely acknowledged, as it is their sole responsibility to defend the organisation against cyber attacks. However, for smaller organisations, this is not the case as they may not have a specific IT team to depend on. Instead, it is essential that all employees are educated and trained on the possible security threats – allowing the wider team to understand their responsibility when it comes to the security of the organisation's IT infrastructure. This is more crucial than ever, especially in light of the fact that many teams are still operating remotely as a result of the pandemic, and are therefore not in the instant remit of IT professionals.

The obligation to protect data and defend against impending threats must be emphasised throughout the entire organisation. After all, the final decision of whether to download an external file or share personal information over email lies with each individual.

Working with an effective vendor who offers the required security solutions can help chief information security officers (CISOs) in integrating security into the overall business's vision and core values. The most recent report by Forrester claims: "Organisations with strong security cultures have employees who are educated, enabled and enthusiastic about their personal cyber safety and that of their employer" – reiterating the importance of having a strong security culture throughout.

It is crucial that organisations adopt a layered security strategy, which combines cutting-edge digital tools, frequent security training and an engaged workforce. It shouldn't be the case of one or the other. Businesses cannot rely solely on technologically driven-based solutions to safeguard their workforces, data and operations. They also need to embed security awareness training throughout their organisation to ensure that their staff are vigilant and security conscious. This combination enables businesses to reinforce important cybersecurity preventative messaging, while keeping safe against the modern threat landscape ●

Oliver Paterson is Product Expert – VIPRE Security Awareness Training and Safesend.

Small businesses in the UK are the target of 65,000 attempted cyber attacks per day