THE WEAKEST LINK?

Arun Chauhan *discusses the 'human element' of cybersecurity and explores how you can avoid falling victim to cyber fraud.*

Fraud can occur in many forms within a business – from cyberattacks by third parties to misappropriation of funds by those within your business. Whatever the type of fraud, often during an investigation, it is lapses in human judgement or human error that are identified as being a major cause. This is no different when considering instances of cybercrime against a business.

Cybersecurity refers to the measures taken to protect a person or business from unauthorised access to information systems. This is particularly important for the vast majority of businesses especially with the COVID-19 era of many employees working from home. The use of computerised technology is now commonplace for the day-to-day operations of many. If a system is breached, the unauthorised user has the capability to cause damage for a business, its customers, any other stakeholders and potentially even the wider public. With a cyberattack occurring every 39 seconds globally, ensuring the security of your systems and that your procedures are fit for purpose is crucial, but each business needs to recognise that policies and procedures alone do not protect you.

95% of cybersecurity breaches occur as a result of human error

Cybercrime, through hacking or intelligence leaks, is extremely common and can cause substantial losses for business and the public sector – including both financial and data losses. However, the success of cybercrime often relies upon or targets a momentary lapse in human judgement.

Whether we're stressed, tired or even simply distracted, we are prone to occasional lapses in judgement. In a business, this can manifest itself in a number of ways, such as a team member clicking on a suspicious link which may be harmful or entering credentials into an unknown platform without consulting other team members or management first. These lapses in judgement can result in falling victim to cybercrime as businesses can allow fraudsters to gain access to sensitive data or private, otherwise secure systems.

Often, end users of software are seen as the 'weak link' in a business' defence against cybersecurity, with 95 percent of cybersecurity breaches occurring as a direct result of human error. These end users operate the systems on a daily basis to complete their job, but all have varying levels of competency. Some are tech-savvy, others simply know the very basics of the system and how to use it and many lie somewhere between the two.

There are numerous ways in which end users can fall victim to common cybercrime scenarios. For example, they enter their user credentials into phishing sites, click on malicious links, visit malware-laden websites or simply leave devices unattended. These instances of cybercrime often arise as a result of a lack of education surrounding cybersecurity or by employees not engaging with the training they receive because they are simply not engaged to see it as anything more than a tick-box exercise.

By educating your teams about the risks associated with cybersecurity, how to avoid them and most importantly, why this is so important by reference to the role each employee plays in your cybercrime defence procedures and the loss they can save for you, you can effectively address the 'human element' in your business' defence against cybercrime. Investing in your systems is not enough on its own to combat your business' security risks, leadership, culture, education and training all play an equally vital role.

Taking a specific case study to highlight the point, Red Kite Community Housing was defrauded of

ENGAGED TEAM MEMBERS WILL BE BOTH OPEN TO LEARNING AND MORE VIGILANT TO ATTACKS

almost £1-million in 2019. The investigation into the £932,691.48 loss is currently underway. Red Kite Community Housing suffered these losses after cybercriminals mimicked the domain and email details of known suppliers and requested changes to payment details.

Cybercriminals were able to recreate an email thread which misled those who were copied in into believing that the email they received was a follow up to an existing conversation. This lead to members of the team updating payment details to what they believed to be the new payment details for existing suppliers.

Mike Gahagan, chair of Red Kite Community Housing, said: "I would encourage all organisations urgently to review their processes for a single point of failure. We regularly detect and dismiss fraudulent attempts and our processes worked for seven years. However, our lesson is that human error can occur even with clear processes and training, so providing secondary checks are a necessary protection."

This highlights the importance of ensuring that an organisation's approach to training and education of procedures is as important as the procedures themselves. Ensuring training resonates and is bought into by employees is vitally important to ensure there is effective application defence processes to fraud risk.

Instances of cybercrime and fraud can be difficult to identify within a business. All too often, they can go unidentified until irreparable damage has already occurred. However, there are a number of things you can do to help you to prevent and identify any cyber fraud within your business – before any loss occurs.

Education for teams surrounding cyber security is one of the most effective measures for combatting cyber fraud. Teach teams about how they can

recognise suspicious pop-ups, flag suspicious emails and be vigilant when browsing and encourage communication among the team if in doubt. This will help to significantly reduce your risk of falling victim to cybercrime.

Some businesses are known to send dummy phishing emails to their teams – monitoring which team members fall victim and click on the harmful links. These emails are used to identify those who may need additional training and to highlight any shortfalls in a business' current training programme.

KEEPING WATCH

Keeping security logs and analysing for suspicious activity is an important preventative tool in your journey to secure systems. Regular and consistent logs will make it easier for you to identify any suspicious activity and subsequently investigate. For example, you could monitor new log-ins or application uses. If any instances of these occur outside of business hours, these will then be highlighted, enabling you to flag and investigate them appropriately.

Regularly updating system software ensures the latest security measures are in place and can help to keep most cyber criminals from gaining easy access to your systems.

Many businesses use automation to assist in preventing cybercrime. However, this automation can lend itself to predictability, as security scans are often run at the same time each day, week or month. This kind of predictability can leave businesses vulnerable to cybercrime so to reduce the risk, systems should be regularly assessed but on a random time basis.

By instilling a culture of trust, openness and information sharing, team members will feel comfortable in flagging any possible security breaches to their leadership teams. This can allow any issues to be resolved efficiently, mitigating any potential damage to the business.

A fundamental, influencing factor of fraud in any business lies with its leadership team. Leadership style plays a pivotal role in the culture of any organisation, as leaders are able to either make or break the culture of their team and drive behaviours. Leaders who instil a positive, supportive culture will often benefit from a highly engaged and motivated team, who will share information with their employer comfortably.

Poor leaders have the potential to create a toxic working environment by setting unattainable performance targets, focusing heavily on KPIs or demonstrating a maximum tolerance for small wrongdoings. This saps the heartbeat of successful teams and leaves individuals focusing on protecting themselves more than your organisation.

STAYING ENGAGED

A poor workplace culture can result in unmotivated, disengaged employees and can even encourage dishonest behaviour, as employees grapple to reach – or appear to reach – high performance targets. When employees are no longer engaged, their focus may then turn to self-preservation – resulting in usually out of character behaviours, to preserve their jobs and appear to be achieving unattainable targets.

If your leaders instil a positive workplace culture, they will benefit from engagement in your policies, procedures and reasons behind why they exist. Engaged team members will be open to learning about cybersecurity protocols and will be more vigilant in their implementation of these. They will also be more likely to report any concerns, offering the opportunity for early remedy for any security breaches.

When it comes to ensuring the cybersecurity of a business, the importance of human behaviour should not be ignored. This is where education, training and a culture of information sharing are all key ●

Arun Chauhan is the founder of Tenet Compliance & Litigation – a law firm which specialises in helping businesses to reduce their risk exposure to fraud. Arun is also the deputy chair of the Fraud Advisory Panel.

It is vital to educate staff about the risks associated with cybersecurity and how to avoid them