Human Cyber Risk – The first line of defence

Essays and articles about cyber risk often refer to human error as a major driver of cyber incidents and the financial losses arising from them – up to 95% of all breaches[1]. But what is human error and how are human traits and behaviours exploited by malevolent actors? By better understanding these vulnerabilities, more can be done to address them and build greater cyber resilience.

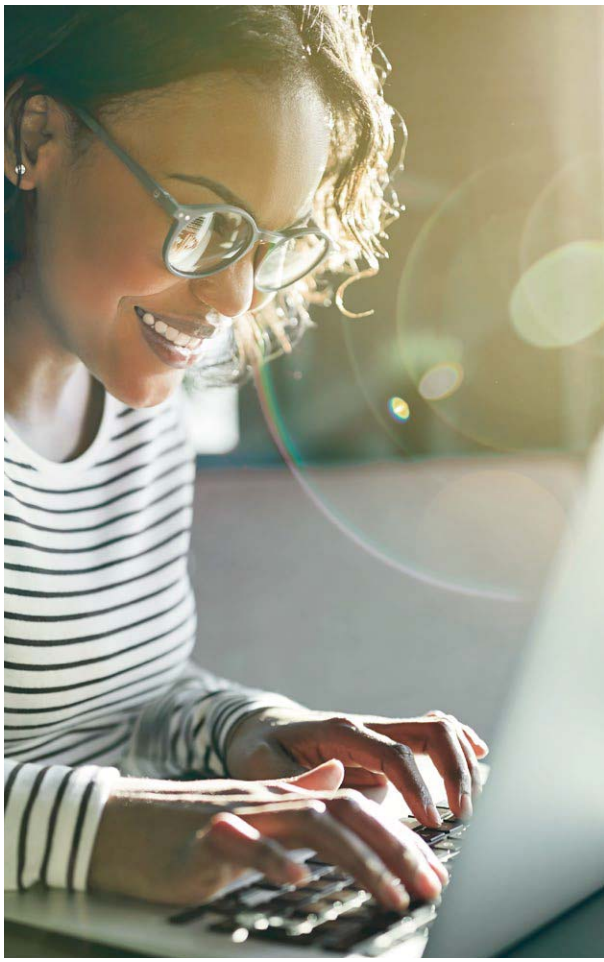
This paper explores the human factor in relation to cyber vulnerabilities, considering a range of scenarios in which end users and infrastructure are exploited by hackers and fraudsters. It considers the different types of human vulnerability and how it might be reduced through better awareness and training and a more robust IT infrastructure.

Against a backdrop of global pandemic, we also consider the additional exposures businesses face when their staff are working remotely. In times of crisis, employees may be forced to fall back on dated, unpatched devices and software and are potentially more vulnerable to scams that prey on their natural fears.

Rather than blaming employees for making mistakes, the report argues it is time to take a new approach to addressing the human side of cyber risk, by identifying and addressing the underlying root cause: human behaviour. It is an approach which recognises all the nuances of what is primarily a sentient threat with recommendations and solutions, but without stigmatising the user as the culprit.

We replace the term 'human error' with 'human factor' in an attempt to move away from negative connotations while also offering more scope for organisations to identify opportunities in addition to threats.

Organisations are investing heavily in protecting their IT systems with security controls and other infrastructure with spending set to surpass $42 billion in 2020[2]. But is the corporate world investing as much as it needs to in ensuring that its people are the first line of defence when it comes to protecting their data and systems?



What is the cyber human factor?

The human factor has less to do with actual error and more to do with inadequate security cultures and the exploitation of human behaviour and goodwill. By better understanding the way in which people operate in the workplace, as well as how malicious actors set out to exploit classic human traits, it is possible to identify and address areas of human fallibility.

Senior and middle management are more likely to be exploited by cyber criminals in a targeted attack than lower ranking employees[3]. This is because they tend to hold valuable information and/or have a high degree of access to such data. C-level executives are nine times more likely to be the target of social engineering than they were in years gone by[4].

Key points

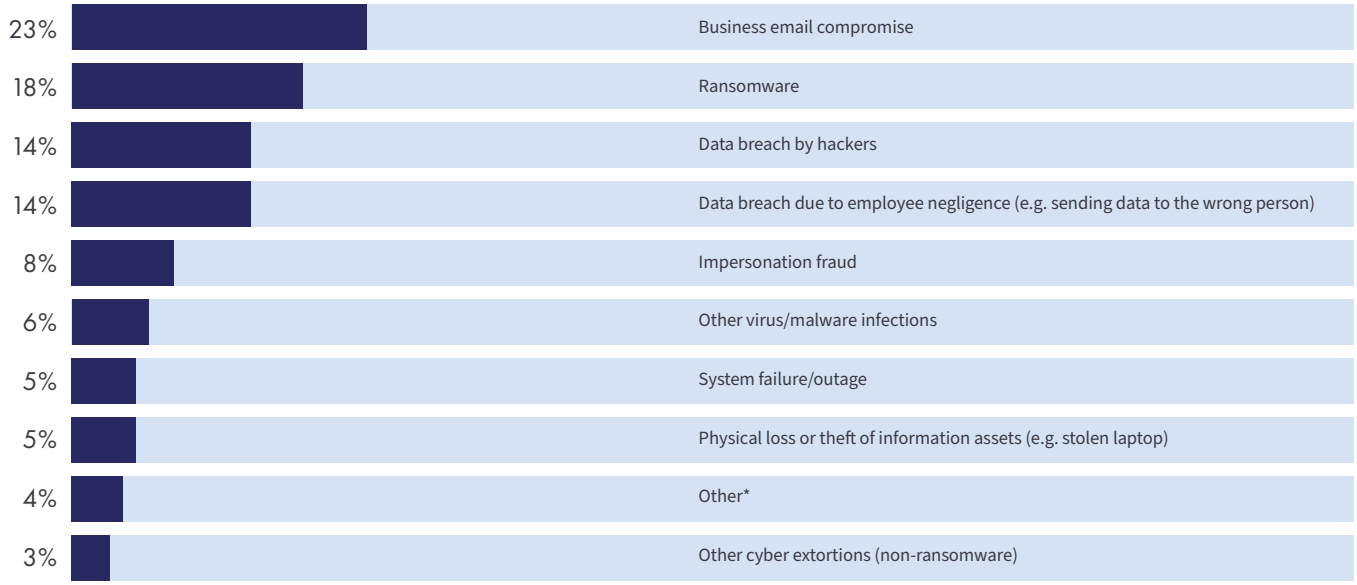
- 'Human error' implies that people are to blame for cyber breaches. In reality, inadequate security cultures facilitate people-centred attacks
- The focus of social engineering attacks is becoming more targeted – seeking to compromise those with sufficient access and privilege
- At a time of increased home working, individuals are more vulnerable than ever to exploitation by malicious actors

Remember:

- Be aware: Regularly assess your cyber risks and prioritise actions based on impact and budget
- Be proactive: Remember security basics and proactively test for vulnerabilities
- Be prepared: Have your incident response plan in place, your workforce prepped, and alternatives decided ahead of time

1 https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches
2 https://www.weforum.org/agenda/2019/07/can-cybersecurity-offer-value-for-money/
3 https://www.cio.com/article/3247428/safeguarding-your-biggest-cybersecurity-target-executives.html
4 https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

Fig 1 Cyber Claims received by AIG EMEA (2018) – By reported incident



*Denial of Service Attacks, Legal/Regulatory Proceedings based on violations of data privacy regulations

Social engineering and business email compromise

Social engineering is the art of tricking, seducing or scaring/blackmailing an individual into giving away personal or corporate information or taking action, such as authorising a payment. Email remains the main attack vector for social engineering, ranging from malicious spam through to business email compromise (BEC), or imposter attacks, that can cost organisations millions of dollars. Such methods are popular because they require minimal hacking expertise and attacks have a high success rate.

Perpetrators of BEC often target individuals responsible for sending payments, including company CFOs. Through social engineering, they use psychological manipulation to encourage users into providing information or making a financial transaction. There are different approaches to social engineering, ranging from simple lures that are designed to spark curiosity, such as sending a fake invoice to an accounts payable team, through to more elaborate schemes.

Attackers may use stolen branding to create landing pages or domains that appear – at first glance – to be legitimate. These techniques are used in BEC attacks, where threat actors attempt to convince their victims that they are communicating with a trusted entity and pretending to be a CEO, colleague, business partner or even support staff.

According to the 2019 AIG EMEA Cyber Claims Intelligence Report, BEC has overtaken ransomware and data breach by hackers as the dominant driver of cyber insurance claims. Nearly a quarter of incidents reported to AIG in 2018 were due to losses arising from BEC, with anecdotal evidence that even very senior members of organisations had fallen victim to these scams. Globally, businesses have lost an estimated $26 billion to BEC over the last three years[5].

As Sebastian Hess, Cyber Risk Advisor for AIG Europe, explains, one reason for this is the use of social engineering, which creates emails that appear legitimate, even to the well-trained eye.

“Social engineering continues to be one of the top threats, resulting in security incidents caused by targeting employees and senior management,” he says. “New trends involve email scams utilising social engineering techniques to harvest key data or money. These attacks are becoming more sophisticated and targeted with attackers stepping up their game and finding ways to counter protections.”

Home working/quarantine stresses

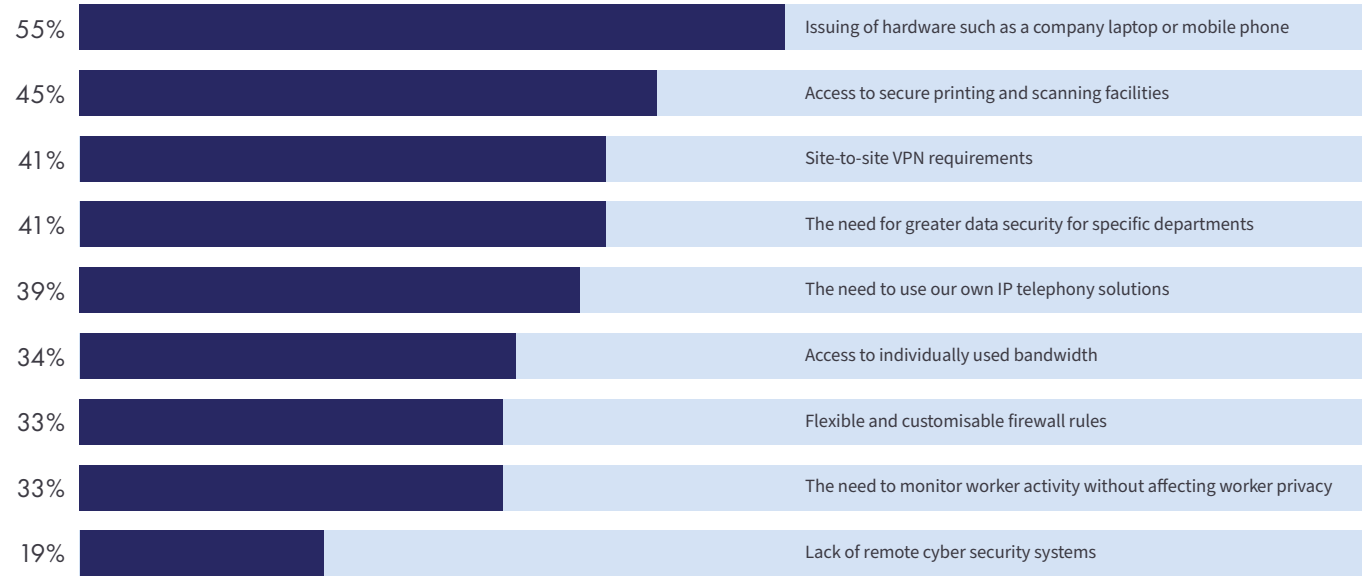
Around the world, businesses are faced with the growing reality of home working amid quarantine and social distancing restrictions. As they enact emergency business continuity plans, they and their staff are highly exposed to cyber threats. Employees doing their best in a difficult situation are often forced to fall back on personal devices that are less secure at a time when increased stress levels potentially make them easier to exploit.

Increased home working inevitably heightens employees’ risk to exploitation by malicious actors. While presently these risks have come to the fore as governments impose quarantine restrictions, such exposures are also a part of a wider shift as businesses embrace digitisation and new ways of working.

Among the business challenges associated with home working are concerns over data security and ensuring workers have access to all the technology they need in order to work productively. In normal times, businesses can carefully consider their technology requirements when introducing or expanding flexible working practices and setting ‘bring your own device’ (BYOD) policies. This is not as easily done during an emergency.

5 https://www.securityweek.com/loss-bec-fraud-now-claimed-be-26-billion

Fig 2 Technology requirements businesses typically take into account when introducing/expanding flexible working practices



Source: International Workplace Group

When staff are suddenly forced to work remotely, they may need to rely on home computers and other personal devices. As demand for PCs grows amid disruption in the supply chain, there may be a shortfall in availability of laptops and other devices for organisations to provide for their staff.

Personal devices are unlikely to have the same protections as those in the workplace, or the same capacity to monitor activity. Firms therefore need to ensure they maintain high standards of IT security and help their employees ensure personal devices are secure.

Additionally, businesses are introducing new capabilities to allow remote connectivity, e.g. Remote Desktop Protocol (RDP), to enable their staff to work from home. But were security considerations part of this service introduction? Is the access appropriately secured?

Employers and their staff should be alert to these scams as well as all the usual pitfalls of day-to-day cyber security, ensuring staff continue to use two-factor authentication and strong passwords, for instance. Staff should be sent regular reminders of what to be alert to from a cyber security perspective, and what to do if they inadvertently click on a link in a phishing email or suspect they have been targeted by a cyber attack.

Distraction and mobile devices

Mobile device users are more susceptible to phishing, social media attacks and spoofing – which attempts to mimic legitimate web pages – than desktop users, according to Verizon. It attributes this to the design of mobile devices and how users interact with them.

Relatively limited screen sizes restrict what can be accessed and viewed clearly and apps often restrict the availability of information, making it more difficult to check the veracity of emails and requests. Mobile devices are also often used when individuals are walking, talking and doing other activities that may distract them from being more vigilant. The risks associated with mobile devices, including tablets and smart phones, is clearly more of an issue for organisations at times when large numbers of staff are working remotely.

Automatic and unconscious behaviours

Numerous softer factors, such as the natural desire to be helpful, come into play when it comes to end user risks. In many ways, cyber crime is an evolution of more traditional crimes, such as extortion, blackmail and fraud. Although the scale of the activity has grown, the same sort of techniques are used to defraud and manipulate.

From a psychological perspective, engaging in compassionate actions activates the parts of the brain associated with the reward system, with positive feelings then reinforcing altruistic behaviours. It is not just about people making mistakes, as is implied by the label 'human error'. While large and sophisticated companies spend significant resources on developing technological barriers to cyber threats, are they doing enough from a human behavioural perspective?

Training and awareness is growing. Employees are less likely to fall for phishing attacks today than they did seven years ago, down to three percent from 24% according to Verizon research[6]. However, people are still clicking on links they should not, particularly as phishing emails become more convincing.

To a certain extent, human behaviours – such as clicking on links – becomes automated. If users are 'rewarded' by getting what they expect when they carry out such actions, such as gaining access to a webpage, these repeat behaviours become even more of a challenge to break because they are done almost unconsciously. There are many behavioural reasons why users may not comply with cyber security best practice (see information box).

In psychology, procedural memory describes a type of implicit memory which stores information on how to perform certain functions, such as walking, talking and the acquisition of motor skills and habits. Through procedural memory, users can become habituated to the 'I accept' button and, for instance, GDPR cookie warnings on websites, where it becomes second nature to click on a button.

Reasons for non-compliance with cyber security best practice
(source: UK Government Office for Science)

- The need to be connected often outweighs the risk of insecure connection.
- People are habituated to the 'I accept' button and warning messages.
- Convenience always wins over security.
- No perceived benefit – belief that behaviours will not make a difference to security.
- Lack of knowledge and skills – knowledge about what to do and how to do it, and skills to detect fraudulent activity.
- Simply forget to behave securely when distracted by other things when online.

How password hygiene has evolved

Poor password hygiene is an issue that has not gone away, although best practice approaches have evolved. Simple passwords are typically the weakest link in otherwise secure networks. Attackers often use password-cracking tools to circumvent an encrypted password and gain access to a user's account. This is easier to do if the password is simple, such as 'password', 'qwerty' or '1234567'. These brute force methods were behind the 2014 iCloud breach where attackers gained access to a number of celebrities' personal pictures.

Whereas the advice was once to change passwords regularly, today it is deemed more useful to have a strong password and to stick with it. The National Institute of Standards and Frameworks' (NIST) recommends a minimum password length of eight characters while also encouraging very lengthy passwords of easy-to-remember words or a passphrase. It advises against using too much password complexity.

In 2017 when its guidelines were last modified, NIST also recommended removing resets requiring users to change their passwords every few months or so. Password strength should be about quality, not quantity, it argued.

6 https://enterprise.verizon.com/resources/reports/dbir/

Social engineering – so much data, so little time

The idea behind social engineering is to exploit the potential victim's natural tendencies and emotional reactions, such as an employee's desire to help a colleague. A criminal might pose as a co-worker in order to gain trust while manufacturing pressurised situations – such as critical deadlines – so that individuals 'act first and think later'.

Types of social engineering attack include baiting, phishing, email hacking and spamming and vishing (the same scam as phishing but carried out over the phone). Sextortion scams, where victims are told compromising footage or images will be released to friends and family unless they pay (or give access to information), are also rooted in social engineering.

Social engineering occurs both online and offline, with fraudsters making use of all manner of information – including data harvested through social media accounts – to make themselves appear genuine.

Antivirus software provider Norton[7] recommends the following tips to avoid falling victim to social engineering:

- Consider the source. A found USB stick isn't necessarily a good find and could be loaded with malware. In this day and age consider all email sources suspicious.
- Slow down. Social engineers count on their targets to act quickly, without considering whether a request is genuine. Stop to think and ask questions, however intense your workload.
- Is it too good to be true? How likely is it that a Nigerian prince would reach out to you for help? Investigate any requests for money or personal information before handing it over.
- Update and patch your operating systems to ensure they are prepared for the most recent security threats.
- Use email software to filter out junk mail, including scams.

7 https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

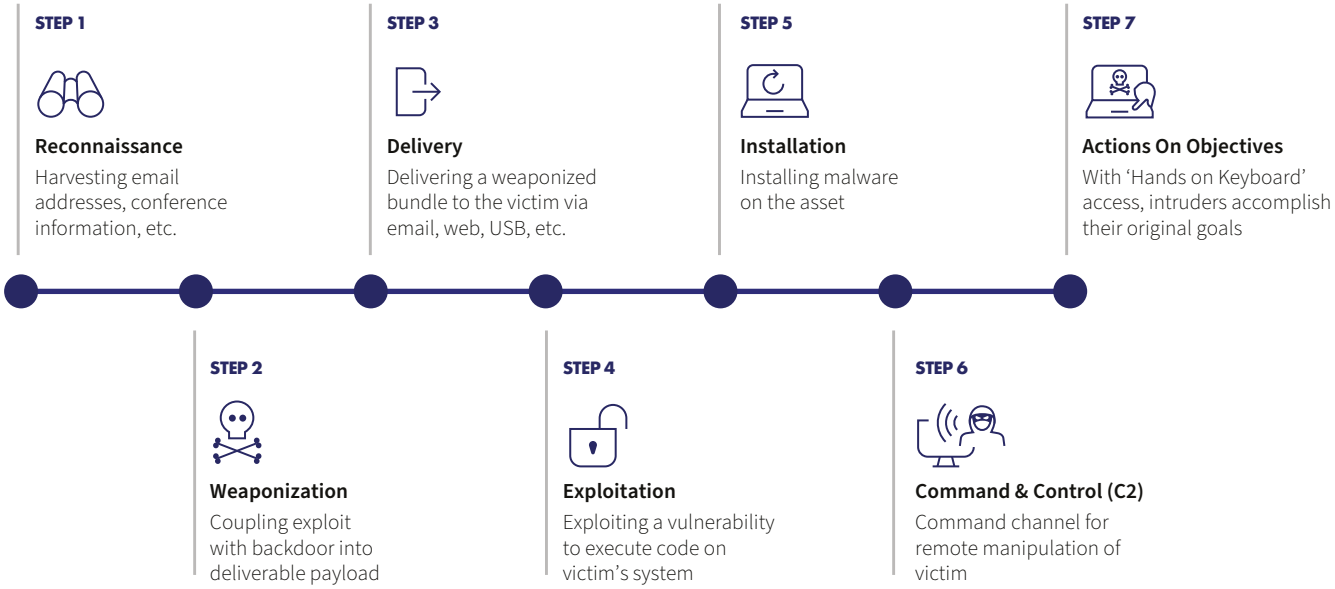
Cybercriminals and their mind games

Understanding the different types of cyber attackers and their characteristics can help organisations prepare their workforce to better identify potential threats. From nation-state actors to socio-political 'hacktivists', different attackers are motivated in different ways. However, the fallout can be much broader than their actual target, as was the case in the NotPetya attack.

Cybercriminals are generally motivated by monetary gain and seek the easiest methods of extracting what they want. They tend to be part of structured organisations, are highly motivated, highly skilled and have unlimited time and resources. They love playing mind games[8]. It is easier for them to pick up the phone and impersonate an official or technical support to get the information they need to breach corporate networks, than it is to spend months trying to hack in using brute force.

The cyber kill chain is a series of steps typically taken by cybercriminals as they move from the early reconnaissance stages to the exfiltration of data. The human factor is a critical element in disrupting the kill chain as organisations seek to combat ransomware, security breaches and other attacks.

Fig 3 The Lockheed Martin cyber kill chain methodology – how humans are the first line of defence



8 https://home.kpmg/uk/en/home/insights/2018/07/mind-games-how-to-protect-your-business-against-cyber-crime.html

Protecting people from themselves

Addressing the cyber human factor is an essential part of an organisation's overall approach to putting in place a robust cybersecurity framework. Success comes by taking small everyday actions, including:

- Incident Response Capability
- Security Awareness Training
- Patch Management Program
- Network Security Principles
- Proactive Security Testing
- Secure Data Backup

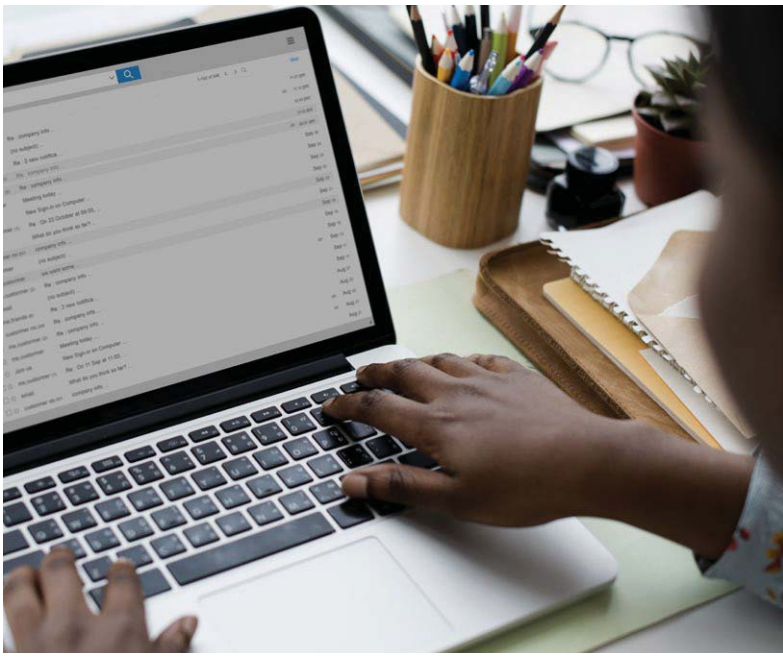
Employers need to consider the psychological levers that cybercriminals pull when they use human behaviours to trick employees into clicking on links and giving away passwords. Examples include goodwill, slips and lapses, being 'in a rush', being too trustful and the principle of reciprocity[9]. By understanding how these traits are exploited, it is possible to forewarn staff and implement security protocols – such as two-factor or multi-factor authentication – to override these tendencies.

In an ongoing battle against cyber threats, organisations need to let go of the term 'human error' and instead look at how they can empower their workforce to be more secure. As Usecure blogger Micke Ahola explains, 'a lack of knowledge is almost never the fault of the user – but should be addressed by the organisation'[10]. The onus is therefore on employers to ensure end-users have the knowledge and skills they need to keep themselves and their businesses secure.

Employees will make better security choices if they receive regular training in the form of workshops, meetings, guest speakers, cross-functional teams, tests, internal resources and weekly updates. Gamification is one strategy employers are using to better engage staff in cyber security training. This is where executives participate in 'wargaming' simulations as a way of improving awareness and developing good habits in a fun way that promotes learning.

Another tactic is to put staff through their paces by subjecting them to regular ethical hacking attacks. Just as fire drills ensure everyone remembers the correct evacuation procedure in the case of a fire, simulated phishing attacks can test staff's ability to spot suspicious emails and keep them safe in the virtual environment. Allowing employees to experience a (simulated) phishing scam has been shown to increase risk perception, encouraging them to apply a higher degree of suspicion to future emails.

Behavioural science is increasingly being used to better understand the human factor in relation to cyber risk. The MINDSPACE framework has been successfully used in a number of settings including financial, healthy eating and sustainability, to help design successful behaviour change interventions using public policy. By using such an approach, there are ways in which users can be subconsciously influenced to make the right choices, actively interrupting the user to ensure that insecure sites are more noticeable for instance.



Least privilege

Good security hygiene is also an essential part of the toolkit. Training users to play their role in securing critical information assets is one aspect of the approach organisations need to take. Another is protecting more vulnerable users. This can be achieved through a strong security program which emphasises firewalls, anti-virus software, patching, strong passwords and other basic security solutions.

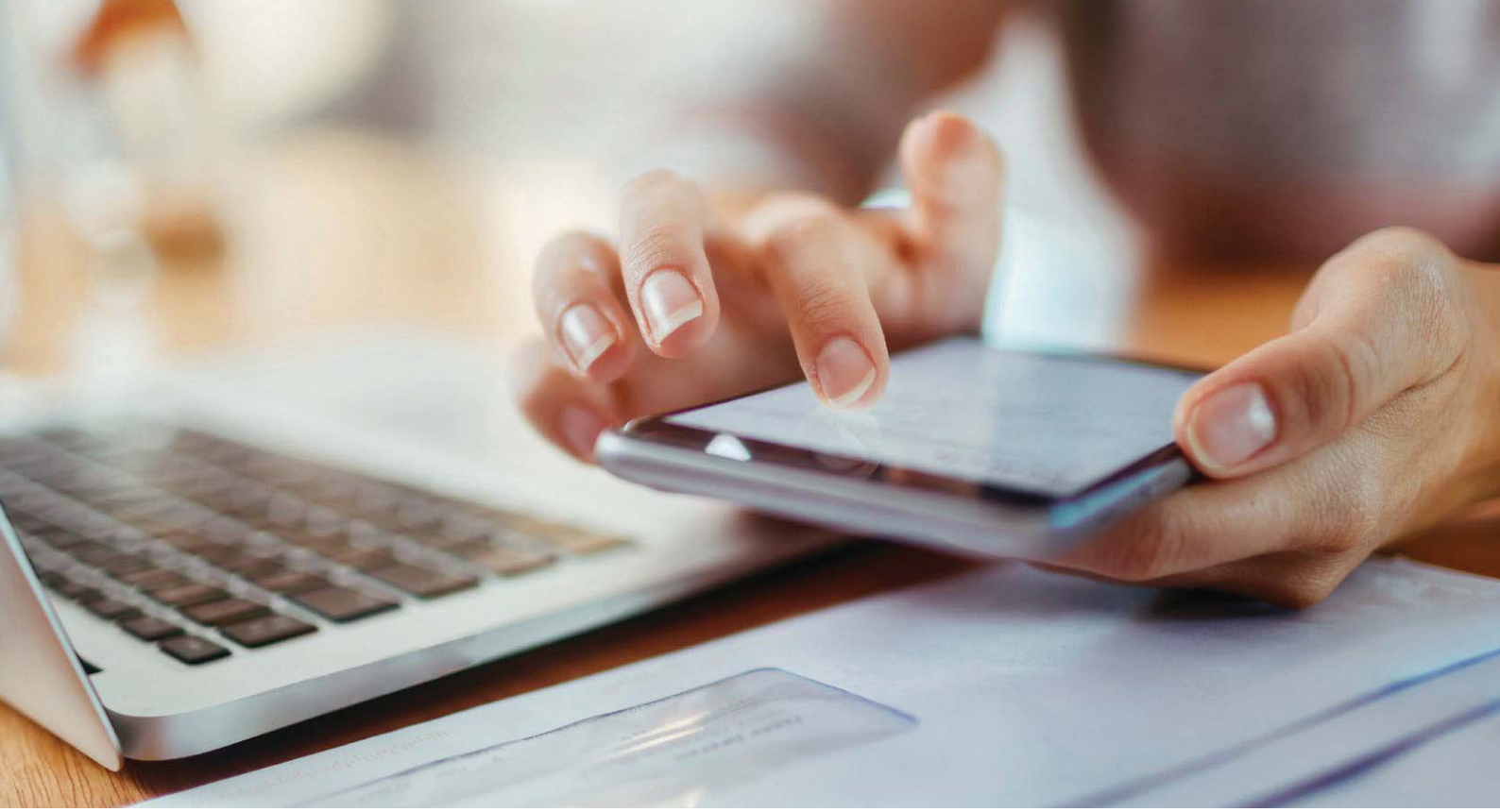
Security policies and procedures are a big part of a resilient defence. Multi-factor authentication, 'buddy systems' and managing user privileges make it less likely that mistakes will be made, can minimise insider threats and limit overall fallout if and when accounts are compromised.

Multi-factor authentication best practice typically includes the following:

- A **knowledge factor** is something the user knows, such as a password, a PIN or some other type of shared secret.
- A **possession factor** is something the user has, such as an ID card, a security token, a smart phone or other mobile device.
- An **inherence factor**, more commonly called a **biometric factor**, is something inherent in the user's physical self, such as fingerprints authenticated through a fingerprint reader or facial and voice recognition.
- A **location factor**, usually denoted by the location from which an authentication attempt is being made, can be enforced by limiting authentication attempts to specific devices, IP addresses and/or GPS data.
- A **time factor** restricts user authentication to a specific time window in which logging on is permitted, and restricting access to the system outside of that window.

9 https://theconversation.com/five-psychological-reasons-why-people-fall-for-scams-and-how-to-avoid-them-102421

10 https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches



The UK's National Cyber Security Centre warns against giving users unnecessary data access rights and recommends that granting of highly elevated system privileges should be carefully controlled and managed[11].

"Highly privileged administrative accounts should not be used for high risk or day to day user activities, for example web browsing and email," it says. "Monitor user activity, particularly access to sensitive information... respond where activities are outside of normal, expected bounds."

There are roles for AI and machine learning, with nearly a quarter of organisations already using security technologies that "augment or replace human intervention in the identification and containment of cyber exploits or breaches", according to research by Ponemon Institute. It found that high automation organisations are better able to prevent security incidents and disruption to IT and business processes.

In order to deliver a robust cyber security program, it is important for different departments to collaborate in order to protect staff from cyber threats. Cyber security may traditionally have been seen as a job for IT departments and CISOs, but as threats change it has become a strategic, company-wide challenge involving senior management, HR and risk and insurance professionals among others.

"We are seeing cybercriminals moving towards softer targets and carrying out attacks that take advantage of human behaviour and how the brain works," says Mark Camillo, Head of Cyber, EMEA at AIG. "Organised criminal gangs are using tactics that allow them to make the most money easily and right now that is business email compromise. Clearly, a more holistic approach is needed to understand how fraudsters are stealing and diverting company funds in this way."

Managing internal threats, such as training staff to identify phishing emails, to improve password hygiene and protect the network against unsecured devices takes up time and resource. By putting users at the heart of their cyber security strategy and gaining buy-in and participation from the various lines of business, cyber security departments can free up time to focus on managing external threats and take a more strategic approach to their organisation's overall cyber security.

Top tips for good security hygiene

- Do not reuse the same passwords
- Use complex passwords (employers should require a predetermined password strength)
- Utilise a password vault
- Enable multi-factor authentication
- Do not access personal accounts when connected to an employer's network
- Connect via a VPN prior to engaging in work-related tasks
- Never expose services like RDP directly to the internet without securing them properly
- Apply filtering measures to online activity
- Complete cyber security training

11 www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/the-10-steps/managing-user-privileges

Conclusion

There is a recognition that the IT systems of even the most sophisticated organisations can be breached. Too often, it is not their technology that fails them, but the frameworks and systems (or lack thereof) that have been put in place to protect their people.

Humans naturally want to work at speed – to please their line manager and co-workers and to get things done. This leads to a tendency to overlook security processes, particularly those measures that appear to go against productivity, workplace satisfaction and convenience. However, a balance needs to be maintained if companies are to succeed in protecting their staff.

It is time to move beyond the simple catch-all phrase of 'human error' and for organisations to understand and address the critical vulnerabilities faced by end users. This means reducing the opportunity, improving company culture and empowering employees with better knowledge and training.

As the cyber threat landscape grows and evolves, the most resilient organisations will be those that tackle the threat on both a technological and behavioural level, working collaboratively across organisations, with buy-in at every level. The tone of any organisation's cyber security culture should be set at the top with Boards taking an active role in how they are addressing the cyber human factor.

Key questions Boards should ask themselves

- How robust and up-to-date is your basic cyber security, e.g. firewalls, anti-virus software, patching, password hygiene?
- What security protocols do you have in place to protect your staff against being targeted by cyber attackers, e.g. email software filters, multi-factor authentication, reporting procedures and controlling access to sensitive information?
- What cyber security training and information do you provide for your employees? Is it at all levels of the organisation and could engagement be improved?
- Who is responsible for cyber security at your organisation? Do you take a holistic, enterprise-wide approach?
- Is all email from outside the company domain marked 'External'? Are hotlinks turned off? Are macros banned?
- Do you have an effective BYOD policy? This is particularly important with more staff working remotely.
- Do you ensure all electronic wire transfers need a second manual authorisation/check in order to prevent BEC?

For more information on how Boards need to manage their cyber risk please see **Cyber Risk Oversight 2020: Key Priorities and Practical Guidance for Corporate Boards** from the ISA (Internet Security Alliance) and Ecoda (organisation representing the main national institutes of directors in Europe).

Mark Camillo
Head of Cyber, EMEA
T: +44 (0)20 7651 6304
M: +44 (0)7860 261 692
mark.camillo@aig.com

Sebastian Hess
Cyber Risk Advisor, EMEA
T: +49 69 97113-572
M: +49 159 04611288
sebastian.hess@aig.com

www.aig.com

American International Group, Inc. (AIG) is a leading global insurance organisation. Building on 100 years of experience, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange. Additional information about AIG can be found at www.aig.com and www.aig.com/strategyupdate | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: www.linkedin.com/company/aig. AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties.

American International Group UK Limited is registered in England: company number 10737370. Registered address: The AIG Building, 58 Fenchurch Street, London EC3M 4AB. American International Group UK Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (FRN number 781109). This information can be checked by visiting the FS Register (www.fca.org.uk/register). AIG Europe S.A. is an insurance undertaking with R.C.S. Luxembourg number B 218806. AIG Europe S.A. has its head office at 35D Avenue John F. Kennedy, L-1855, Luxembourg. AIG Europe S.A. is authorised by the Luxembourg Ministère des Finances and supervised by the Commissariat aux Assurances **11 rue Robert Stumper, L-2557** Luxembourg, GD de Luxembourg, Tel.: (+352) 22 69 11 - 1, caa@caa.lu, www.caa.lu/.

GBL00003685 0620