In conversation

Human-centred security starts with understanding humans and their interaction with technologies, controls and data. By discovering how and when humans 'touch' data throughout the working day, organisations can uncover the circumstances where psychological-related errors may lead to security incidents. For years, attackers have been using methods of psychological manipulation to coerce humans into making errors. Attack techniques have evolved in the digital age, increasing in sophistication, speed and scale. Understanding what triggers human error will help organisations make a step change in their approach to information security.

So, what can be done? I recommend that organisations identify key risks and threats to the business and/or industry area. Targeted scenario planning and training, such as table-top exercises or phishing campaigns, can then be tailored to improve responses to specific threats and enable employees to better react to stressful situations that may trigger cognitive biases.

CEO: The world is becoming increasingly digitised, and organisations can no longer rely solely on reactive measures when it comes to cybercrime. With heightened global mistrust and rising geopolitical tensions, how can organisations and individuals be better prepared? Additionally, what does the security workforce of the future look like in the face of this evolving technology and AI?

SD: Driven by demands for increased speed, automation and efficiency, organisations are facing a period of significant technological upheaval as they transition into a hyperconnected digital world. Supporting this world will be new, innovative technologies and business models that will create an illusion of stability, reliability and security. However, new and reenergised threats will compromise success and shatter that illusion. The impact on security is significant as threats become more tailored, specific and potentially damaging. The increase of nation state sponsored attacks in particular will force a more collaborative approach to threat intelligence and threat response between public and private sector. In addition, the advent of AI and machine learning and the very real ways that such systems can create a more challenging environment for attackers of all descriptions may allow security professionals to re-address the balance in favour of the defender.

When looking at AI, we must understand that true AI, as opposed to machine learning, is still in its infancy and we have seen a number of instances where AI has not produced the output or decisions that had been expected. If defensive AI systems are left entirely autonomous and have the power to force-cut connections to suspect devices or shut down critical applications, for example, then the impact of a mistake by the AI could well be greater than from a malicious external attack. Organisations can and should not rely entirely on AI – humans are still the most important piece of the InfoSec puzzle.

> **"Digital transformation is now top of the challenge list for many businesses and operating in the digital world is increasingly a matter for effective management of risk."**

Organisations need to establish a series of strategic objectives that provide a foundation for building tomorrow's security workforce. With clear direction and leveraging fundamental HR concepts, organisations can develop an approach that formalises the structure of the security workforce, harnessing the appropriate talent and skills to achieve the organisation's security objectives.

As the security workforce matures, embracing the vast amounts of untapped talent with the right aptitude, attitude and experience, the exaggerated myth of a future global security workforce shortage will be debunked. A robust security workforce will also enable organisations to effectively manage future workforce challenges, such as automation, role and functional amalgamation and outsourcing. Our members are already demonstrating success, building tomorrow's security workforce with the necessary skills and expertise, developing and retaining employees in a progressive and engaging environment.

A sustainable security workforce is essential if the information security function is to become a partner to the business and effectively manage the increasing security burden.

CEO: The ISF hosted its Annual World Congress in Dublin, Ireland on October 26-29. Over 1,000 cyber security experts attended, discussing the key security challenges and opportunities that organisations are facing. Can you let CEO Insight readers in on the key discussions and findings?

SD: Our 30th Annual World Congress featured a series of keynote presentations, workshops and networking sessions from the world's leading international security experts. These experts discussed the key challenges and opportunities that ISF member companies and

businesses will face in the years to come. Topics included: cyber security in the boardroom, Threat Horizon 2022 (due out in March 2020), managing risk and providing assurance, and human-centered security. ISF Member-led sessions provided guidance on the latest ISF Tools Suite, including Information Risk Assessment Methodology 2 (IRAM2), Quantitative Information Risk Analysis (QIRA) and the latest ISF research.

Once again, the topic of cyber security in the boardroom was of great interest to attendees. As we continue to note, an organisation's board would be very foolish today to say that it had no interest in understanding the company's security posture and what steps were being taken to protect its critical assets. We live in a world of increasing regulation and legislation with punitive financial penalties for negligent loss of data in an environment where barely a day goes by without another breach being reported. The board has a duty of care to ensure that it both understands the risks the company is operating under and has clearly articulated a risk posture that is understood across the company. Measuring performance and conformance should be key agenda items on the board meeting and indeed are for responsible boards today.

CEO: The ISF is the world's leading authority on cyber, information security and risk management. What can we expect from the organisation in the new decade?

SD: The ISF serves both our global member organisations and the broader information security community. Working with organisations from the Fortune and Forbes to mid-size, from government to academia, the ISF delivers valuable, independent and actionable insight resulting in a growing membership and sought-after perspective and services from members and non-members alike.

Over the coming years, the ISF's position as a global leader in the field of information security and risk management will be ever more important as business leaders turn to independent organisations such as the ISF for advice and guidance on cyber issues across the enterprise. Positioning the organisation for sustainable long-term growth with agility and flexibility, building on the sustained investment in our members and staff are also key initiatives for myself and my team. This will allow the organisation to continue to be seen as a thought leader in the information security industry worldwide. Last, but most certainly not least, the ISF people will determine the success of our business. In a competitive market, our people are our key differentiator. Over the coming years, we plan to substantially grow our workforce and this will mean having to put in place attraction and retention programs that continue to be world class to ensure that our people remain one of the primary reasons members join the ISF and continue to work with us to address their evolving information security and risk needs. ●