REDEFINING INFORMATION SECURITY

Brian Wagner, *author of Redefining Information Security: How to Build a Security-Driven Organisation, explains the fundamental principles of building a security-driven organisation*

To meet the challenges of tomorrow's digital landscape, security and technology leaders that represent organisations at the forefront of security innovation must integrate and embed security within their strategic vision. Building a security-driven culture not just safeguards organisation from risk, but actively propels businesses forward to enable innovation and growth in the face of an evolving digital business and threat landscape.

As well as addressing the technical aspects of cyber security, organisational culture, leadership, communication, education and human factors also make up the integral components of a successful security strategy.

Security must be an integral part of an organisation and not simply an afterthought. While the culture of security has made significant progress from being seen as overly restrictive in many cases, it is still often viewed by organisations as a cost rather than an investment. This perception can be a significant barrier to building a strong security posture, as it leads to security initiatives being deprioritised or underfunded.

Seeing security as a cost rather than an investment can be a significant barrier to building a robust posture

This mindset can hinder an organisation's ability to effectively protect itself against evolving threats. For those new to security, it can appear to be relatively mysterious and nebulous; more of an art than a science. But that is true of many unrelated disciplines, such as accounting or musical theory – once you overcome the challenging learning curve, it makes a lot of sense.

The field of cyber security is constantly evolving, with new threats and technologies emerging all the time. This can make it daunting for those who are not immersed in it daily. A multi-faceted approach is crucial, as security is not just about implementing the latest tools and technologies. It requires a deep understanding of risk, human behaviour and the interplay between people, processes and technology. This will empower security leaders to take a more active role in protecting their organisations by exploring these different lenses.

One such lens is risk. Technical teams often overlook risk, but it is really the best conversation starter when it comes to security, because we evaluate risk constantly in our daily lives without even realising it. Risk is a limit forever approaching zero; we can mitigate it, but there is really no such thing as zero risk. For example, there are risks when riding a bicycle. Even with a helmet and safety gear, there is always the chance of an accident or collision. To add to the complexity of that risk, a collision with a pedestrian will likely have a different impact than a collision with a bus. However, most people are willing to accept a certain level of risk in order to enjoy the benefits of cycling, such as exercise, transportation and recreation. Using household appliances also involves risk, such as the risk of being burned or cut if not used properly. Similarly, in the world of cyber security, we must acknowledge that there will always be some level of risk, but the goal is to reduce that risk to an acceptable level through proper planning, implementation and vigilance.

Behind the curtain of security, professionals are evaluating risk, measuring it and comparing it with what the organisation deems to be acceptable – this is where a lot of those denials come from! Even at large organisations, everyone should care about risk and make risk-based decisions in their daily work, because it is impossible to make progress without taking on risk. Understanding and managing risk is a critical component of building a security-driven organisation, as it helps to prioritise and allocate resources effectively.

Another crucial element, alongside understanding risk, is people, or at least the human brain. All people are naturally inclined to seek ease – you, me, every single one of us. We humans instinctively prefer familiarity, ease and comfort, the path of least resistance. Our brains will subconsciously justify this inclination using cognitive biases, such as the authority bias where we place a disproportionate amount of trust in the directives of those perceived to be in a position of power or authority, such as an executive or an IT administrator, which can explain why phishing is so effective. Other biases which contribute to resistance to a security culture are optimism bias ("it won't happen to me"), confirmation bias (interpreting information in a way that confirms existing perceptions), and framing information in such a way that is meant to elicit a specific response from its consumer.

These biases contribute to the challenge of building a security-conscious culture. Thankfully, these biases and other impactful heuristics can be overcome through behavioural changes designed to make risk-based decision-making a more conscious and deliberate act by everyone throughout the organisation using simple user-centric techniques such as gamification and frequent micro-training scenarios.

BUILDING A SECURITY-DRIVEN ORGANISATION IDEALLY REQUIRES A MULTIFACETED APPROACH

This type of security education is far different from the traditional, comprehensive training that we've seen over the years, but addressing the human factor in security is a cornerstone of good cyber security posture. Have you ever just clicked through your annual security training and repeated the quiz at the end of the section until you clicked the right things and passed? Did you feel empowered to support the organisation and do your part for security? Probably not, and that is the nature of a compliance-led approach to security: it doesn't connect with the individual.

Organisations can foster a more security-conscious culture where employees actively participate in risk mitigation efforts by understanding and addressing these cognitive biases.

It may be surprising that 'technology' is not first on the list of perspectives that shape cyber security, but the reality is the nature of cyber threats hasn't changed much; insider threats, ransomware, phishing, unauthorised access, for example, but how these threats manifest themselves and how we defend against them has – and will continue to – change rapidly.

At the forefront of the defence against these threats is technology: email systems protecting against phishing, firewalls inspecting network traffic, in-house software which doesn't allow data exfiltration – everything is in scope.

Technology is where the practical application occurs, so to speak, and attackers know this. In fact, it is in the reconnaissance phase of a cyber attack where an attacker might send bots to scan a number of network-exposed devices such as servers, security cameras and firewalls, running an old version of its software known to be exploitable (there are even entire databases cataloguing these devices).

Attackers can sometimes use these devices to access other more sensitive devices with more access to valuable information, which makes it important for administrators and software engineers to keep up the latest security best practices on resources – which otherwise would not undertake new changes.

This is tricky, especially in large organisations, but by democratising and demystifying security, the

Picture credit: AdobeStock

burden of security can be spread throughout the culture where everybody contributes just a little bit, creating a snowball effect.

Embedding security into technology is absolutely a team effort and it requires not only technical expertise, but also empathy and teamwork. Even with a core dedicated team of security engineers, they are often significantly smaller in size when compared with the rest of the engineering team at a large organisation, and are not able to be involved in every single project. This is why embedding security in the culture is so important, and the only way to really scale good security efforts.

ALTHOUGH WE CAN MITIGATE RISK, THERE IS REALLY NO SUCH THING AS ZERO RISK

Somewhere between a tenured security professional and an everyday individual who is unconsciously assessing risks by leaving the house, driving a car or using cutlery, everybody has the capacity to contribute to the overall security uplift of any organisation they are part of, big or small. For those who don't immerse themselves in it every day, you might be surprised to see their contributions if they are educated, supported and recognised for all of their work in support of the security cause.

Phishing rates will go down, responsible use of end-user technology will increase, and conversations are less combative. This all stems from a healthy security culture at an organisation, and somebody has to take the lead. Simple, practical education on risks and dangers of rogue cloud storage accounts and accepting cool IoT devices from vendors or salespeople will shift the risk-based decision making from the subconscious to the conscious part of the brain, and employees will start to notice things that maybe they didn't notice before. This culture of security is really what underpins and enables all aspects of cyber security.

The security community has previously been misunderstood, which has caused it to appear insular and closed off. It takes a collective effort to defend against the latest tools and technologies that attackers are using. It is also becoming increasingly difficult to determine what is real and what is not thanks to the advances made in artificial intelligence. For example, we need people to be vigilant and aware of these dangers so that they can challenge what they see. As it is often said in the security industry: "trust, but verify".

Building a security-driven organisation requires a multifaceted approach that goes beyond just implementing the latest security technologies. It involves understanding and managing risk, addressing the human factors that can undermine security efforts and embedding security into the very fabric of the organisation's culture and technology.

Taking a holistic view and empowering everyone to contribute to the security cause creates a resilient and proactive defence against current and future threats ●

Brian Wagner is CTO of Revenir and a seasoned expert in cloud technology and security, with over 20 years of experience in the industry, particularly in the global financial services sector.

Organisations can foster a more security-conscious culture where employees actively participate in risk mitigation

Picture credit: AdobeStock