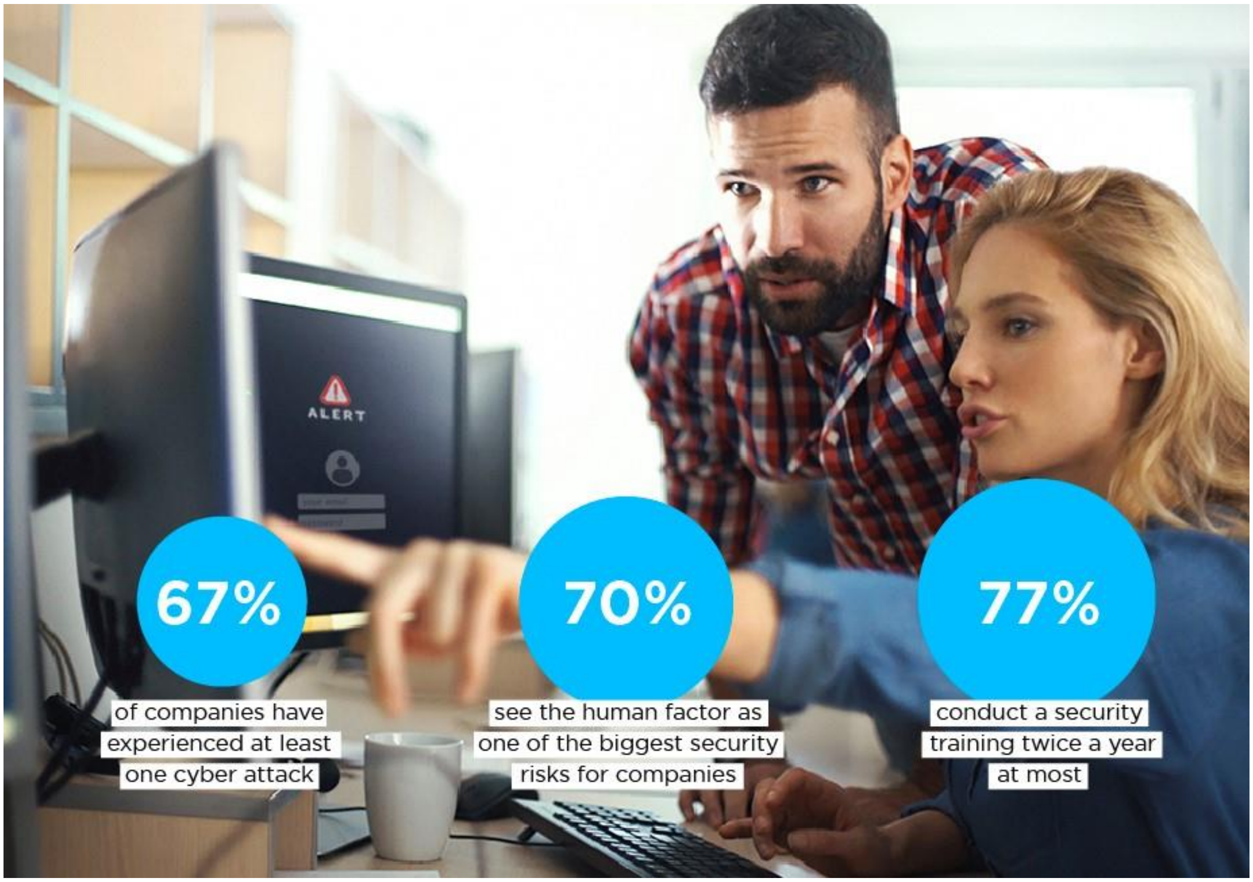
Cybersecurity Awareness Experts: Heralds of Security’s Hidden Benefits

Written by Joshua Bucheli, AI Ethics Researcher and Fellow at the ForHumanity Center, in Collaboration with Sascha Maier, Head of IT and Cyber Resilience at IWC Schaffhausen, and Peter Kosel, Founder of cyberunity


ALERT
67%
of companies have experienced at least one cyber attack
70%
see the human factor as one of the biggest security risks for companies
77%
conduct a security training twice a year at most

In the corporate world, digitisation is pretty much ubiquitously recognised, not only as a worthy investment, but as a deeply exciting field presenting virtually endless future business opportunities. Cybersecurity, on the other hand, has a less enviable reputation amongst businesses, many of whom see it as nothing more than the distasteful ‘flip-side of the coin’ that is digital innovation.

As the popular twist on the well-known saying goes, when life gives you lemons, make lemonade and sell it for a profit! Indeed, whenever a new paradigm shift gives rise to new costs, those who find ways to leverage these costs into opportunities end up thriving – the issue of cybersecurity is no different.

For corporations, this means a shift in mindset away from perceiving cybersecurity as a drain on resources and towards recognising it as an investment – a long term opportunity which, if given the proper attention, can be leveraged for considerable returns.

Where does Cybersecurity Awareness Stand Today?

“Since the onset of the pandemic, the idea of paying attention to cybersecurity has gained traction. And yet, most companies still struggle to fully recognize the cultural benefits that cybersecurity awareness can bring”, says Sascha Maier, Head of IT and Cyber Resilience at IWC Schaffhausen.

Companies are largely still lagging behind the frightening pace at which new cyber-threats are evolving and many business executives still approach the matter of security too frugally, implementing piecemeal security solutions targeted at individual problems as they arise:

“Too many still approach the issue with an ‘accomplish rather than achieve’ mindset – they mandate the occasional e-learnings and carry out intermittent phishing-tests because they *have* to, and not out of any sincere commitment to security.”

According to Sascha, the solution to this is ‘Awareness’ with a capital ‘A’:

“Companies need to realise that, if they take cybersecurity seriously and frame it properly – if they internalise a genuine concern for it into their corporate culture and marketing strategies – they will not only better protect themselves and their stakeholders, but will also stand to profit from doing so. Instead, corporate security awareness remains in its infancy.”

Where is Cybersecurity Awareness Headed?

As evidenced by publications like SANS OUCH!, the concept of cybersecurity awareness has entered the stage. What needs to happen now is for it to be brought to life – it needs to become recognised as a main character rather than an anonymous extra.

Good awareness is ubiquitous and involves proactive security training, diligent follow-ups after breaches, and a recognition of the fact that such dedication to cybersecurity can be leveraged for a valuable corporate image. To this end, a good awareness campaign also takes into account the culture of its target group, whether it be a specific department or a company as a whole.

“Those who want to take ‘Awareness’ seriously need to *live* it, otherwise, the benefits of cybersecurity expenditures fizzle out pretty quickly”, warns Sascha.

As the home of the world renowned Crypto Valley, and thanks to the international recognition of its forward thinking, innovation-friendly regulations, Switzerland exemplifies how a strong reputation for cybersecurity can bring investments, innovation, and other opportunities. Consequently, it also represents one of the most promising places to be when it comes to careers at the forefront of cybersecurity.

“Most large corporations are already well on their way towards leveraging the true potential of cybersecurity’s role in their corporate success. SMEs, on the other hand, still have a ton of catching up to do”, observes Sascha.

All departments within a company will need to get stuck in and embrace an engaged and innovative approach that frames cybersecurity in an exciting, positive light. Individuals who can catalyse this change by incorporating interactive tools into awareness and branding campaigns are therefore essential. Good examples of such tools include Lego Serious Play, Spiral Dynamics Integral’s framework, or SANS’ Security Awareness Planning Kit.

Cybersecurity Awareness Specialists – Hard Skills and Qualifications

Whether you want to help forward-looking businesses build their corporate culture as an external consultant, or whether you are more interested in becoming part of the proverbial ‘tip of the spear’ by joining corporations who are already at the forefront of this paradigm shift, there is no shortage of opportunities.

Regardless of your chosen route, certain skills and competencies will be key:

When it comes to qualifications, the usual certificates like CISSP, CISA, and CISM, while worth mentioning, are not as vital as in other cybersecurity sectors.

Much more important is evidence of a firm grasp of the human risks to information security and how to address them, professional degrees like ICT Security Expert ED and Cyber Security Specialist EFA, proven knowledge of industry compliance standards, and advanced training in ICS.

Digicomp also offers a good starting point which Sascha highly recommends for those hoping to gain insight into the basic tools and strategies of cybersecurity awareness raising and an overview of how to set up their first campaign – key for anyone aspiring to head up a cybersecurity-aware business.

Beyond Technical Know-How

Besides technical know-how, well-developed social and communication skills are a must for cybersecurity awareness experts – “improving cybersecurity awareness is more a question of emotional intelligence than technical expertise – it takes people who pick up on psychological nuances more so than technical intricacies. For this reason, pure technophiles will not be the solution”, says Sascha.

Instead, companies are increasingly going to rely on individuals who can persuade business stakeholders that an honest commitment to cybersecurity is important – people who can identify the needs of everyone from the CEO to investors and production workers, and who can frame the issue of cybersecurity in their terms.

Closely related to this, and as in other cybersecurity careers, an empathetic streak is also worth emphasising in applications. The ability to put yourself in other people's shoes and to see things from their perspective is key to understanding how to present information to them in the most effective way.

What the industry needs above all are specialists with the ability to change mindsets, reframe problems, and define the future of cybersecurity's public image, both across industries and within individual corporate cultures.

This means individuals who are able to design, execute, and reflect on the efficacy of awareness campaigns – people who can put together focus groups of relevant stakeholders from throughout corporate hierarchies in order to identify and address cybersecurity concerns as comprehensively and proactively as possible. It means people with backgrounds in marketing, business communications and journalism, creatives coming from R&D departments, and even individuals with experience in HR.

In the end, it's marketing skills, evidence of creative, out-of-the-box problem solving, a passion for cybersecurity, and a knack for getting people excited and involved that will round off a strong cybersecurity awareness expert's profile.

As Peter Kosel, Founder, Talent Community Manager, and pioneer of the KNOW YOUR TALENTS recruitment approach at cyberunity concludes:

"Cybersecurity awareness is a matter where interdisciplinary cooperation is centre-stage. Anyone who views corporate cybersecurity as an annoyance or a purely compliance-driven issue to be swept aside will reap neither its security nor its cultural benefits. In the end it all comes down to attitude because Mindset Matters! Cybersecurity awareness and associated resources like Digicomp's leadership seminar are valuable opportunities for employers to better acquaint themselves with their employees and to work together with them to build pervasive corporate cultures of security to everyone's benefit – after all, *Cybersecurity means KNOW YOUR PEOPLE.*"