

Human-Centered Cybersecurity is the Key to Combatting Cyber Fatigue

As our workplaces become progressively digital and mobile, and as cybersecurity threats become increasingly sophisticated, it is easy for employees to feel overwhelmed by a myriad of security measures, leading to fatigue and reduced alertness. At Risk Pilot, we combine our technical expertise and our knowledge of human behaviours, abilities and limitations to identify practical solutions to support customers in developing an effective, sustainable human-centered cybersecurity culture. Click on this article to find out more:



Despite businesses' best efforts to protect their data and their systems, the cybersecurity threat landscape continues to evolve. Recently, technological advancements such as AI have quickly and radically changed the environment for cyber threats. At the same time, the global Covid-19 pandemic significantly altered how we work, with more people now working remotely and almost entirely digitally. Such combinations of factors create the perfect conditions for new security vulnerabilities to emerge. In this article, we explore some ways in which the cybersecurity threat landscape is evolving, what this means for employees and employers, and what can be done to mitigate the effects of these changes.

AI and cybersecurity

For many, 2023 will be remembered as the year that [AI went mainstream](#), with powerful tools like ChatGPT3 being released for free to the public, quickly followed by the even more powerful ChatGPT4 (available to paid subscribers only). At first glance, ChatGPT seems like a standard chatbot whereby you provide a question or prompt, and it returns an answer. But users quickly noticed the tool's advanced capabilities to generate text that made it seem like they were communicating with a real person. Within 5 days of its release, ChatGPT had gained [1 million users worldwide](#). Suddenly it seemed that we were bombarded with all kinds of generative AI tools that could create incredibly realistic text and images. It wasn't long before people started to question the ways in which such tools could be (mis)used and whether the results constitute plagiarism, whether the tools could be a potential threat to creative jobs, and whether they could be used to influence people and create harm to society as well as to businesses.

There is no doubt that AI offers tremendous advantages to the modern business, not least in terms of cybersecurity. For example, AI algorithms can analyse huge amounts of data much quicker than a human can, detecting subtle patterns and enabling quicker and more accurate attack identification. Unfortunately, advanced AI tools are also accessible to cyber criminals and can be used, for example,

to repeatedly launch more complex attacks at a faster pace, to feed existing algorithms with false, inaccurate or misleading data, or to create fake documents, audio or videos to lure people into providing sensitive information or to spread misinformation.

Generative AI tools can be used to create more convincing phishing campaigns, to more accurately mimic the content, design, tone and language of legitimate communications, even in multiple languages. In the past, clumsy language and spelling mistakes were a giveaway in detecting fake emails, but tools like ChatGPT can eliminate these vital clues, making attack campaigns more convincing. A recent report by [Deep Instinct](#) revealed [that](#) “75% of security professionals witnessed an increase in attacks over the past 12 months, with 85% attributing this rise to bad actors using generative AI”.

The rise of “cyber fatigue”

While cyber criminals gain access to more sophisticated tools enabling more complex and dangerous attacks, the global workplace has also significantly evolved in recent years, largely as a result of the global Covid-19 pandemic. In the time between 2020 and 2023, large numbers of employees have started to [work remotely](#), and as a result the workplace has become increasingly de-centralised and digital. Many people nowadays use multiple devices to do their work, including laptops, tablets and mobile phones, and these devices run multiple work software programs, applications and communication tools. Employees are often required to remember many login passwords, to communicate across several channels, and to interface with remote individuals whom they may not know and may have never even seen in person. The potential for security vulnerabilities is significant.

Cybersecurity professionals have, for many years, acknowledged that IT infrastructure alone cannot protect a business against cyber attacks or data breaches. Although security-compromising mistakes at work are happening less frequently, a [2022 study](#) by Professor Jeff Hancock at Stanford University and security firm Tessian revealed that, for example, more than one in four employees (26%) have fallen for a phishing attack at work in the past 12 months. In fact, the study concluded that [88% of data breaches](#) occur as a result of human error.

Experts have started to note a rise in a phenomenon called “[cyber fatigue](#)” (also referred to as [security fatigue](#) or [alert fatigue](#)). This is often reported on in relation to cybersecurity professionals, but in the months and years since the Covid-19 pandemic, it is increasingly applied to non-security professionals who work in digital and/or remote environments. The Hancock/Tessian study attributes much of the human security errors to people feeling distracted, stressed or tired at work, under pressure to respond quickly, and burned out, often as a result of remote or hybrid working. Others acknowledge the sheer overwhelm that employees face when [inundated with too many security measures](#) in the digital workplace. Multiple unique passwords that are required to be changed frequently, 2 (or more)-factor authentication, repeated security warnings and IT alerts, repetitive security training videos, etc. It can be difficult for employees to maintain cybersecurity alertness in the face of all these security measures on a daily basis.

The need for a human-centered approach

In the face of more advanced cybersecurity attacks, an increasingly digital and remote work environment, and the overwhelm associated with security measures, what can businesses do to keep their data and systems secure? A good first step is to understand that cybersecurity depends on more than just sophisticated IT infrastructures and tools; people are the key to a successful cybersecurity defence. But inundating people with continuous security warnings, alerts and requirements can quickly lead to disengagement, frustration and cyber fatigue. This is not because

people don't care about security but rather because cybersecurity measures can be overwhelming, repetitive and can often be viewed as over the top, or pointless.

Successful implementation of cybersecurity measures, that are sustainable over time, requires both a **human-centered approach**, and adoption of a [cybersecurity culture mindset](#) within the business. It is important to think about how the employees work, and what they need to achieve success in their jobs, in order to create security protocols and initiatives that make sense to the employees and don't compromise their goals. Equally, to embed a cybersecurity culture mindset, employees need to be engaged and involved in the development of security measures, and the business needs to adopt a culture of learning from mistakes and continuous improvement to ensure that good practices do not drift as time goes by. Understanding the human factors of cybersecurity is the key to combatting cyber fatigue.



At [Risk Pilot](#), we have over 20 years' experience of human-centered design and safety culture evaluation and implementation years' experience of human-centered design and safety culture evaluation and implementation. Our Human Factors team is passionate about identifying practical solutions for the real problems faced by businesses. Combining our technical expertise with our knowledge and experience of human behaviours, abilities and limitations, we work closely with our customers to deliver tailored solutions to meet their needs.

If you are interested to learn more about how Risk Pilot can help you to implement a human-centered cybersecurity culture at your organisation, please contact:

Claire Blackett

claire.blackett@riskpilot.se