


White Paper
Digital wellness
The newest pillar of
employee wellbeing



Digital wellness - the newest pillar of employee wellbeing

We live online. Data from the US shows that people spend an average of seven hours a day connected, on top of their working time online.

However, they often face the potential dangers that lurk on the internet on their own and inadequately.

Many employers have embraced the importance of physical, mental and financial wellbeing for their staff, but they are still largely oblivious to the online threats that can affect employees. Is it time for digital wellness to be considered the newest pillar of employee wellbeing?

Swiss Life Network CEO Michael Hansen believes that time has come, arguing that taking care of employees' online health is a benefit that will soon become as ubiquitous as attention to their physical wellbeing.

"About 10 years ago, at a workshop in Silicon Valley, I was put in the same activity group as people from a couple of cybersecurity companies," Hansen recalls. "At first I thought: what am I doing with these people?"

"But one of them said: 'Actually, we are both protecting something people care about. It's just that what I am protecting is more important than what you are protecting...'. Thinking about it, I realized this is what a lot of people feel. The immediate sense of what we have, our life, is there in front of us on our screens. It was the wake-up call I needed."

This was the seed of an idea that has led Swiss Life and cybersecurity group McAfee to establish a partnership that the insurer believes is going to change the nature of its conversations with multinational clients. While many people might find this link-up incongruous, the partners are convinced it makes perfect sense.

Ever-present dangers

What threats do our online lives entail?

According to the FBI's first Internet Crime Report, over the period from 2017 to 2022 financial losses from cybercrime increased by almost 400%, and the reports of attacks received by the law enforcement agency rose by 191%.

Worldwide, three billion phishing emails are sent out every day, 24,000 mobile apps are blocked and nearly seven million accounts hacked. In 2021, 40 million people

reported they were victims of ID theft and suffered \$52 billion in losses.

Behind these figures are people, both employees and employers, who have to deal with the disruption, financial damage and mental stress arising from cybercrime. According to research from the first quarter of 2023, co-authored by HR.com and McAfee through the HR Research Institute, nearly half of HR professionals say mental health issues may follow identity theft. Then there is the wasted time: an ID theft can take 200 hours across six months to resolve fully.

Given that 95% of online security breaches are caused by human error, failing to help protect and educate employees on security, especially those using personal devices for work purposes, could exacerbate the risk of financial and reputational damage for the company in terms of fines, compensation, regulatory penalties and higher cyber-risk insurance premiums.

It seems evident that there is great untapped potential for insurers and their clients to come together to examine how these risks can be reduced, avoiding disruption and loss of efficiency in the workplace while boosting employees' wellbeing.

Says Hansen: "If an employer takes care of me and, in this case, my digital wellbeing, that's an employee benefit. If there is a way to structure that, it will give clients peace of mind regarding cybersecurity in their operations, and in the long-term claims will be reduced."

The cybersecurity threat has become ever-present, according to McAfee senior vice-president and chief people officer Jeff Ryan.

"When people's digital security is at risk, this can extend to employers, especially since so many employees are using personal devices and working remotely."

McAfee's accumulated experience from more than 35 years in the cybersecurity industry is that most people intrinsically know they need to protect themselves and their families from digital threats.

However, working out what they need to do to ensure their personal safety and security and how to achieve it can be daunting – and can even lead to inaction for fear of failing to make the right choices. For example, people might take steps to protect their devices from viruses and malware, but still expose their identities and risk losing control of their personal data and privacy.

Digital wellness and the broader wellbeing landscape

Says Ryan: “Digital wellness means protecting the whole person, shoring up weak spots in their security, protecting their privacy and regaining control over their personal data – who can access it and how it’s used.

“I’m convinced digital wellness is the next massive trend.”

He argues that digital wellness is where financial wellness was a decade or so ago, when companies remained unsure whether or how it played a part under the overall umbrella of wellbeing.

However, this changed as people joined the dots to discover how their financial position and planning can have a big impact on the quality of life of an individual or family. In the same way, digital wellness is a pillar supporting people’s overall wellbeing – taking care of it can reduce stress from financial losses or unknown risks and enable more secure and happier lives.

“Digital wellness has a direct impact on other elements of the welfare landscape,” Ryan says.

“If someone is hacked, it can affect their mental and physical health because of the extra stress. There can also be an impact on their time and finances while they work to become whole again. These factors can boost absenteeism and reduce focus on work, which in turn impacts their employer’s productivity.”

According to the HR.com/McAfee study, awareness of the importance of digital wellness is now trickling through. Of 221 human resources professionals from companies with more than 1,000 employees in a broad range of sectors, 94% say digital wellness as an employee benefit would enhance an organization’s cybersecurity, and 86% believe it would improve employees’ safety and wellbeing. Perhaps more interestingly, 81% say it could help recruitment of employees and an even larger proportion (87%) see it helping to retain existing ones.

With the demand for digital wellness benefits so evident, Swiss Life and McAfee plan to start exploring how this new pillar of employee wellbeing can be addressed through the insurer-client relationship.

Hansen believes there is no doubt that “this is the next big thing”. The job in hand now, he says, is to create awareness of its potential and start working out how to “put digital wellness into a package”.

The job in hand now is to create awareness of its potential and start working out how to “put digital wellness into a package”.

Adds McAfee’s Ryan: “By offering our holistic solution spanning all devices and operating systems through an employee benefit format, we can help meet the challenge of keeping employees safe.”

It’s time to start that conversation.

Authors

Michael Hansen
 CEO Swiss Life Network

Jeff Ryan
 Senior vice-president and chief people officer, McAfee

About

Swiss Life Network

The Swiss Life Network was founded in 1962 as a multinational risk pooling mechanism. Today, we support our clients with more than 90 leading insurance and business partners in creating employee benefits that can be tailored to individual needs. We are a leading provider in comprehensive global employee benefits solutions for multinational companies.

McAfee

McAfee is a leading online protection company that strives to make life online safe and enjoyable for everyone. We deliver comprehensive protection to safeguard people's privacy and identity in addition to our award-winning antivirus that helps keep them safe – across activities, devices, and locations. Our protection frees and empowers our customers to confidently live life online.