

Cybersecurity can't be ignored post-pandemic

Victims of phishing and ransomware attacks can experience huge financial losses, with studies showing that on average ransomware attacks cost businesses \$133,000



While the world has paid great attention to physical health and wellbeing over the past 18 months amid the events of the Covid-19 pandemic, digital wellness has also shot up the agenda of governments, corporations, and individuals.

Remote working, designed to help prevent the spread of the virus, accelerated the amount of corporate activity and business conducted in the digital space. However, despite the range of benefits, the rush to take business online has made companies and individuals more susceptible to a different illness, in the form of a cyberattack.

Seizing on opportunities presented by companies lacking the right levels of cybersecurity or awareness of the importance of having the right systems in place, cybercriminals launched 726 million attacks around the world in 2020 against online resources, while a report from cybersecurity specialists Deep Instinct states that malware increased by 358 per cent last year.

Lacking budget, cybersecurity knowledge or willingness to invest in



GEORGES
CHIDIAC

EVP

DAMANA

online protection, small to medium enterprises (SMEs) became an obvious target, particularly in this region where SMEs amount for approximately 90 per cent of the business base. Indeed, data from Trend Macro shows that in the first half of 2020 alone there were more than 50 million cyberattacks in the GCC.

To better understand the cybersecurity needs in the region, we surveyed Damana's client portfolio, canvassing the views of CEOs and senior management at SMEs across the region on the impact of online attacks. The findings show that more needs to be done to raise awareness of the importance of cybersecurity protection within organisations and making staff aware of their role in protecting critical information both online and offline.

Some 60 per cent of those surveyed said they had experienced an email phishing attack within the

past 12 months, while 42 per cent said they had experienced ransomware attack.

Victims of phishing and ransomware attacks can experience huge financial losses, with studies showing that on average ransomware attacks cost businesses \$133,000. More damaging for companies is the impact of data breaches.

With SMEs such a crucial cog in the region's economic wheel, it is clear that cybersecurity can no longer be low on the priority list. There are positive signs, with 64 per cent of respondents to the Damana survey recognising the importance of cybersecurity and cyber awareness training for their staff. Equipping teams with the right tools and knowledge to understand cyber risks, how to detect them and how to handle a situation are key to ensuring better protection. Training will ensure a strong layer of defence.

Although awareness training is vital in protecting companies, it is also critical that SMEs take further steps to ensure protection. Insurance against cyberattacks may well seem an unnecessary cost, however it significantly mitigates financial and reputational damage.

With the digital world continuously evolving, now is the time for business leaders to take appropriate action to protect their company and teams. We believe that all businesses, no matter the size, should take the time to research and identify the right approach to ensure protection. Don't wait until it happens, stay ahead of the issue so that you aren't part of the statistics.

EQUIPPING TEAMS WITH THE RIGHT TOOLS AND KNOWLEDGE TO UNDERSTAND CYBER RISKS, HOW TO DETECT THEM AND HOW TO HANDLE A SITUATION ARE KEY TO ENSURE BETTER PROTECTION