KEEPER | PRESS RELEASE

New Report Finds UK Tech Sector Unprepared for Cyberattacks

London, UK, 10 March 2021 – One year on from emergency lockdown measures that forced UK businesses to rapidly provision remote working tools, most IT and technology businesses have done little to bolster their own cyber defences. In fact, more than half of the firms in the sector (59%) say their budgets are still insufficient to cover their cybersecurity needs, according to research conducted by the Ponemon Institute and commissioned by **Keeper Security**.

The risks are real. Over two thirds (69%) of UK technology companies suffered a cyberattack last year, with almost half (47%) claiming the severity of these attacks has increased over the period. Despite the nature of the technology sector, specialist expertise in cybersecurity remains scarce and hard-to-hire, with the majority of UK tech firms (61%) stating that they are without the necessary in-house expertise to prevent cyberattacks or deal with their fallout.

"The technology industry has been targeted by cybercriminals on a mass scale throughout the pandemic, yet with priorities focused on the immediacy of risks that would create tangible damage, it's understandable that priorities have been focused on making sure businesses can simply continue to operate throughout some of the hardest months IT leaders have ever experienced, " says Darren Guccione, CEO and Co-Founder of Keeper Security.

"But keeping data secure is simply a non-negotiable, even more so when disaster strikes. A successful cyberattack and the financial repercussions that come with it are much more likely to prove fatal to a business."

Technology chiefs believe the extraordinary conditions created by lockdowns - remote working and the use of unmanaged devices - heightened this level of risk, with 45% of respondents blaming the conditions caused due to Covid-19 as affecting businesses' online security. The novel working conditions of the last year have also made it harder for IT teams to respond to attacks, with half of UK tech firms (51%) stating the time taken to respond to cyberattacks has increased dramatically during lockdowns.

And the consequences have been damaging: 43% have experienced an incident involving the loss of sensitive information about customers, prospective customers or employees, with 32% of cases having an estimated financial impact at over £175,000 per attack. Yet, while hackers, unmanaged IT equipment and the sudden imposition of remote working has been among the key causes of blame - nobody had a business continuity plan amid a global pandemic.

Budgets have been squeezed more than ever and firms have not been able to afford much-needed investments in large scale security projects. Half of the UK tech sector (49%) do not have sufficient financial resources to successfully prevent cyberattacks. The need to provision equipment and applications for remote working overwhelmingly absorbed company finances, leaving little left for much else.

Perhaps most worryingly, firms have fallen short when it comes to policy and governance around remote working and other related risk factors. A quarter (26%) do not have a cyber incident response plan in place. Over a third (36%) have not formally assessed the risks around remote working, even after months of such measures being in place. Half of the sector (49%) still has no policy on security requirements for remote workers at all. Despite the growing number of high-profile attacks on prominent technology companies, a worrying 64% still don't require the use of a password manager for employees in a remote working environment. It is little wonder therefore that 43% of IT businesses in the UK have experienced an attack involving compromised passwords in the last twelve months.

"We know that identity-based crimes are on the rise. Stepping up security around passwords, through a multi-platform password management and security platform, can be very simple and cost-effective, providing a manifold improvement to organisations' security posture" concludes Guccione.

© 2021 Keeper Security

KEEPER | PRESS RELEASE

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the highly-rated and patented cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. In 2020, Keeper was named PCMag's Best Password Manager of the Year & Editors' Choice for the third time. Keeper has also been named PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM).

© 2021 Keeper Security