KEEPER | PRESS RELEASE

Remote Working Reality Leaves UK Businesses More Vulnerable than Ever to Cyberattacks

Sixty per cent of organisations represented in this research experienced a cyberattack over the last 12 months, yet UK businesses remain ill-equipped to deal with them.

LONDON, UK, 14 October, 2020 – While 60% of respondents say their organisation had a cyberattack, 37% of respondents say their organisations do not have a cyber incident response plan in place, according to new research published by the Ponemon Institute and commissioned by Keeper Security. This research, now in its fourth consecutive year, specifically focuses on the cybersecurity risks created by remote working environments. According to the research, 44% of respondents say their organisations experienced a data breach over the past 12 months.

The report paints a bleak picture of businesses' porous cybersecurity defences. Of the 60% of respondents who say their organisations had a cyberattack, 50% say it was a general malware attack (above the global average of 42%) while 47% of say they had a phishing/social engineering attack over the past year (about the same as the average of 48%).

COVID-19 has caused mass disruption to the way we work, and with this comes a whole wave of new cyber challenges companies cannot afford to ignore. On average, 63% of employees in organisations represented in this research are working remotely. Almost one-third (32%) of attacks were caused by compromised or stolen devices. Despite the new concerns that come with working away from the office, more than half (57%) of respondents admit their IT security budget is inadequate for managing and mitigating these cybersecurity risks. Perhaps even more worrying, 60% claim the time to respond to a cyberattack has become longer, with one in five (19%) claiming this had increased 'significantly'.

Other key findings from the report include:

- 44% of respondents say their organisations had a data breach in the past 12 months
- Of the 60% who report their organisation had a cyberattack, 51% say they experienced credential theft, and 50% say it was a general malware attack
- Of those companies who have experienced a data breach during the past 12 months, the blame is placed heavily on cyberattacks like phishing (63%), followed by third-party mistakes (36%), and negligence from employees or contractors (36%)
- With an average of 63% of employees working remotely having access to critical, sensitive, and proprietary information, businesses are most concerned about a lack of physical security in the worker's new place of work (48%) and devices becoming infected with malware (34%).

European comparisons:

- In the UK, 79% of respondents say there has been an increase in phishing/social engineering attacks since COVID-19 which is much higher when compared against DACH (49%), Benelux (65%), and Scandinavia (53%)
- The UK ranks much lower than European regions for organisations having experienced an attack that specifically leveraged COVID-19 as a threat vector (39%), DACH (52%), Benelux (46%), and Scandinavia (39%)
- The UK (43%) lags in organisations having a policy on the security requirements for teleworkers against DACH (59%), Benelux (51%), and Scandinavia (50%)
- The UK (43%) has faced more attacks involving the compromise of employees' passwords in the past year against DACH (36%) Benelux (37%), and Scandinavia (42%)

KEEPER | PRESS RELEASE

Darren Guccione, CEO & Co-founder of Keeper Security says, "The findings revealed today present a worrisome picture of the state of online safety for businesses across the UK and Europe. As we enter a prolonged period of remote working, it is critical that businesses feel sufficiently protected from possible cyberattacks. IT security systems are not keeping up with the demands of the new way we work. We commission this annual research with the Ponemon Institute because it is imperative that organisations turn this cybersecurity epidemic around.

"The good news is there is a solution to ensuring businesses' data is safe, regardless of where staff are based. Keeper prevents password-related data breaches by creating random, high-strength passwords and providing all employees with a private, encrypted vault for storing all credentials and private data. We need to ensure all businesses wake up to the realities of working during this pandemic and prioritise investing in a strong, reliable cybersecurity infrastructure."

Larry Ponemon, Chairman and Founder at the Ponemon Institute says, "COVID-19 and widespread remote working has provided cybercriminals with a new means to attack businesses with greater levels of intensity and frequency. Cybersecurity in the Remote Work: A Global Risk Report highlights how cyberattacks on businesses across the UK and Europe are at risk in the era of remote working and should be making this a top priority and installing the most protective software out there."

Uncover the research findings live with Larry Ponemon and Darren Guccione

Keeper will be hosting an **exclusive webinar** on Wednesday, 21 October at 4 PM BST to discuss the results of the UK & European research findings: Cybersecurity in the Remote Work Era: A Global Risk Report - UK & Europe.

Join best-selling author and technology journalist Neil Hughes as he moderates a dynamic discussion with the Ponemon Institute's Larry Ponemon and Keeper Security CEO and Co-Founder, Darren Guccione, as they unveil the UK and Europe results of Cybersecurity in the Remote Work Era: A Global Risk Report, including:

- The effect of COVID-19 on cybersecurity posture in UK organisations
- The most common types of attacks faced in 2020
- The measures organisations need to plan to successfully mitigate a data breach

You can **download the full report** and **register here** to attend the webinar.

About the Ponemon 2020 Cybersecurity in the Remote Work Era: A Global Risk Report

Ponemon Institute surveyed 2,215 IT and IT security personnel in the United States, United Kingdom, DACH, Benelux, Scandinavia and ANZ (Australia and New Zealand). All respondents in this research are in organizations that have furloughed or directed their employees to telework because of COVID-19. According to the findings, before COVID-19, an average of 22% of these organizations' employees worked remotely, and due to COVID-19, an average of 58% of employees now work remotely. An average of 33% of employees was furloughed.

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. Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards including the G2 High Performance Fall Europe Report and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified. Learn more at **keepersecurity.com**.

Cybersecurity in the Remote Work Era: A Global Risk Report underscores the cybersecurity concerns, challenges, and attitudes of business execs over the past year, including the change in attack tempo and threat types since the advent of mass remote working in the wake of the pandemic changing working life.

Press contact: **keeper@marlinpr.com**