KEEPER | PRESS RELEASE

Surge in Remote Work Weakens Security Posture of Many U.S. Companies

Challenges brought about by remote work, including lack of training and emerging tech trends, have significantly increased risk, according to new survey from Keeper Security and The Ponemon Institute

CHICAGO, Oct. 13, 2020 – Businesses around the U.S. have experienced a significant and correlating spike in cyberattacks since remote work began in early 2020. **Cybersecurity in the Remote Work Era: A Global Risk Report**, sponsored by **Keeper Security** and conducted by The Ponemon Institute, surfaced and examined the most pertinent new challenges organizations today face in preventing, detecting and containing cybersecurity attacks in the colloquial "new normal."

A striking 63% of U.S. companies have seen an increase in phishing/social engineering during the pandemic, 52% noted a jump in credential theft and 50% reported a rise in incidences of account takeover. The study also revealed the three major contributing forces that have led to this stark rise in attacks:

- A glaring lack of training and guidance for employees working remotely
- An ill-equipped and overwhelmed IT security workforce
- And a massive surge in new technology being used to facilitate remote collaboration

"The abrupt and chaotic shift to remote work earlier this year rattled the status quo for companies in the U.S and around the world," said Darren Guccione, CEO and Co-Founder of Keeper Security. "Unfortunately, it was fairly easy to predict this global disruption becoming a colossal risk to cybersecurity. Our hope is that by shedding some light on the complexities of what's gone wrong, organizations will have some guidance and direction into how to strengthen approaches to security in the remote world."

Remote employees are major liabilities, but it's not entirely through a fault of their own

Following this monumental shift to remote work, 24% of respondents feel their organization has not provided any or adequate education regarding the security risks brought about by remote work. The study revealed more than half (53%) of organizations do not have a policy on the security requirements for remote employees.

The vast majority of the U.S. IT security pros (67%) believe remote employees' use of their own mobile devices to access business-critical applications and IT infrastructure has had a negative impact on their organization's security posture. Further illustrating the concern, 58% think smartphones represent their organization's most vulnerable endpoint. These risks are not exclusive to the U.S. More than 65% of organizations overseas believe the Bring Your Own Device trend has decreased their security posture.

Organizations fear a lack of control, but they feel helpless

Employers are at a loss. The inability to protect employees' devices and activity while they work from home is a major concern, and nearly half (45%) of IT admins expressed worry over the lack of physical security in remote workspaces. An additional 25% are anxious about their inability to secure communications on external networks, and 24% are concerned about the prospect of criminals taking advantage of this by gaining control of personal devices and stealing sensitive information.

Cybercriminals are clearly more than happy to add fuel to the pandemic fire, as half of organizations surveyed in the U.S, as well as 46% overseas, say they've experienced an attack that specifically leveraged COVID-19 as a threat vector.

"Cybercriminals are quick to exploit any vulnerability, and this year has exemplified that in a major way," said Dr. Larry Ponemon, chairman and founder, The Ponemon Institute. "Cybersecurity in the Remote Work Era: A Global Risk Report presents the perspective of just how universal threats, and the heightened sense of anxiety they induce, have become yet another discouraging side effect of the pandemic. The results truly conclude that prioritizing security should be at the top of the list as organizations continue to structure their remote work environments."

Uncover the research findings live with Dr. Larry Ponemon and Darren Guccione

Join renowned cybersecurity expert Dr. Eric Cole on Tuesday, Oct 13 at 1:00 PM CT, as he moderates a dynamic discussion with The Ponemon Institute's Dr. Larry Ponemon and Keeper Security CEO and Co-Founder Darren Guccione, as they unveil the U.S. results of "Cybersecurity in the Remote Work Era: A Global Risk Report", including:

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

To download a copy of the Cybersecurity in the Remote Work Era: A Global Risk Report, please visit **keepersecurity.com/ponemon2020.html**. For more information on Keeper Security, please go to **keepersecurity.com**.

Methodology

The survey collected responses from 2,215 IT and IT security personnel in the United States, United Kingdom, DACH (Germany, Austria and Switzerland), Benelux (Belgium, the Netherlands, and Luxembourg), Scandinavia and ANZ (Australia and New Zealand). All respondents work for organizations that have furloughed or directed their employees to work remotely as a result of COVID-19. These organizations had an average of 22% of employees working remotely pre-pandemic, and that has since jumped to 58%. A collective average of 33% employees were furloughed.

About Ponemon Institute

Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries.

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 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). Learn more at **keepersecurity.com**.