KEEPER | PRESS RELEASE

New Survey Reveals Extensive Devastation in the Aftermath of Ransomware Attacks

Keeper Security study finds 93% of companies hit by ransomware attacks reported tightened budgets and ripple impacts on productivity, profitability and security posture

CHICAGO, July 20, 2021 – Nearly one third of employees had never heard the word "ransomware" before their company was attacked, according to Keeper Security's new **2021 Ransomware Impact Report**. The report goes on to confirm that the entry point for about half of ransomware incidents was a phishing email, which is a frightening indication of how lack of awareness remains an achilles heel for too many organizations. After surveying 2,000 U.S. employees, the report provides a truly holistic look at the crippling domino effects felt by companies targeted by ransomware attacks.

The Opportunity Cost of Ransomware

The survey found that 49% of companies targeted by a ransomware attack paid the ransom, and another 22% did not disclose whether or not they paid, indicating the real number could be much higher. In the heat of the moment, corporate leadership feels an incredible pressure to prevent further malicious movement within their network as well as to placate customers. Cybercriminals know and depend on exploiting this frenzied state of mind. Of the nearly half that said their company paid, 78% of employees were informed of how much money was involved. On top of that, 93% noticed budgets tightening in other areas following the ransom payment, emphasizing the need for effective security measures to be put in place before an attack as there might not be funding available for it afterwards.

Haste Makes Waste

The true cost of being targeted by a ransomware attack isn't just financial. In fact, 83% said their organization performed major tech updates following the attack. Of that group, 71% felt that the updates negatively impacted their productivity and ability to carry out daily tasks. An additional 64% even permanently lost login credentials or important documents as a result, further proving that the best time to install significant security updates is before the necessity is demonstrated. Unfortunately, this is still wishful thinking, as 87% of impacted companies enacted strict security protocols following the attack, and a startling 29% of employees were not familiar with ransomware prior to their company being targeted.

The Ransomware Stigma is Real

Most organizations responsibly disclosed the attack to partners and customers, but 15% chose not to, and another 26% didn't disclose it to the public. Ransomware attacks are especially pervasive this way, as cybercriminals know many companies will be embarrassed to admit they were targeted and pay off the ransom as quickly as possible. This isn't surprising, as 64% of employees felt that the ransomware attack had a negative impact on their organization's reputation.

Fortunately, reputations are often repairable, and redemption starts with fundamental improvements. Cybercriminals seek the low-hanging fruit and act in the interest of time. Implementing security measures like MFA (multi-factor authentication) make an organization much less likely to be targeted as they're immediately harder to access. Unfortunately, 62% of respondents said their companies implemented MFA post-attack - indicating it wasn't a standard practice beforehand.

"With each new ransomware incident that makes the news, onlooking companies gain a better understanding of just how financially devastating an attack can be, especially once a ransom is paid" said Mark Cravotta, Chief Revenue Officer at Keeper Security. "Yet, given the overwhelming prevalence of these attacks, it's shocking to see how many employees are left in the dark until it happens to them. Investing in cybersecurity measures like MFA, password management solutions and awareness training might seem like an unnecessary expenditure to companies with tighter budgets, but the costs pale in comparison to the ramifications of being the victim of a ransomware attack."

Other Notable Stats:

- 87% of impacted companies enacted stricter security protocols after the attack.
- 77% reported being unable to access systems or networks as a result. 30% were down for a day or less, 26% were offline for up to seven days and 27% were knocked out for more than a week.
- 42% of ransomware attacks originated from phishing emails, 23% from malicious websites and 21% from compromised passwords.

"The realities of being hit by a ransomware attack, especially for a smaller company, are much more terrifying than most people realize," said Darren Guccione, CEO and Co-Founder of Keeper Security. "Unfortunately, the aftermath of a ransomware incident is often when organizations start to prioritize cybersecurity, which, as this survey proves, isn't a rewarding strategy. Though highly controversial, paying the ransom is extremely common, and many of us can empathize with leadership teams who are doing their best to put out the fire. But the aftereffects of this approach can be detrimental and long lasting. These insights shed some light on what those repercussions look like, and hopefully can assist in the remediation decision-making process."

To download a copy of the 2021 Ransomware Impact Report, infographic and more, visit our dedicated **resources hub**. For more information on Keeper Security, or how to defend your organization from password-related data breaches, go to **keepersecurity.com**.

Methodology

Keeper Security contracted with Pollfish to conduct this survey of 2,000 full time employees in the United States. Only individuals who work full time at companies victimized by ransomware attacks in the last twelve months were included. The survey was completed in June 2021.

About Keeper Security, Inc.

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and data breaches. Keeper is the leading provider of zero-knowledge security and encryption software covering password management, dark web monitoring, digital file storage and messaging. Named PC Magazine's Best Password Manager (2019, 2020) & Editors' Choice (2019, 2020) and awarded the Publisher's Choice Cybersecurity Password Management InfoSec Award (2020), Keeper is trusted by millions of people and thousands of businesses to protect their digital assets and help mitigate the risk of a data breach. Keeper is SOC-2, FIPS 140-2 and ISO 27001 Certified and is also listed for use by the Federal government through the System for Award Management (SAM). Keeper protects businesses of all sizes across every major industry sector.