KEEPER
Cybersecurity Starts Here®

2021

RANSOMWARE IMPACT REPORT

Contents

Introduction and Methodology

2021 is set to be the Year of Ransomware. As attacks rapidly spike in frequency, increasingly eye-popping ransom demands are grabbing headlines. Consumers, once relatively shielded from any impact, are experiencing product shortages and difficulty accessing services as the organizations they do business with are knocked offline.

But what happens within an organization post-attack? How are internal processes affected? What's the impact on employee efficiency and productivity? To find out, Keeper surveyed 2,000 employees across the U.S. whose employers had suffered a ransomware attack in the previous 12 months.

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.

KEEPER

The Consequences of Poor Cybersecurity Training

Nearly one-third of employees lacked adequate cybersecurity training prior to the attack.

Employee cybersecurity awareness training is crucial to preventing ransomware attacks, particularly since so many involved social engineering:

- Respondents reported that phishing emails caused 42% of ransomware attacks
- Malicious websites accounted for another 23%
- Compromised passwords caused 21%

Yet 29% of respondents told Keeper they didn't know what ransomware was prior to their employers being victimized. This indicates that many, if not most ransomware attacks could be prevented by:

- Adequately and routinely training employees on cybersecurity awareness, especially how to avoid phishing and other social engineering schemes
- Requiring that employees use strong, unique passwords for all accounts and enable multi-factor authentication wherever it's supported

A DAY LATE AND A DOLLAR SHORT?

Respondents told us that post-attack, 87% of organizations enacted stricter security protocols, 90% provided their employees with additional cybersecurity training, and 67% increased their cybersecurity spending.

To Pay or Not to Pay

While everyone agrees that paying ransoms encourages further attacks, whether organizations should give into ransomware demands remains a matter of great debate even within the security community. This is because when an organization is under active attack, its leadership faces tremendous pressure from customers, company stakeholders, and even cyber insurers to solve the problem and get back online as quickly as possible. The pressure is especially intense at healthcare facilities and in the public sector, where system downtime could put human health and lives at risk.

As a result, 49% of respondents told Keeper that their employers paid the ransom. However, this money didn't fall out of the sky: 93% reported that their employers tightened budgets in other areas following the ransom payment.

KEEPER

The High Indirect Costs of Ransomware

Ransomware recovery extracts high indirect costs.

While stratospheric ransom demands trend on social media, organizations incur numerous indirect costs after an attack, particularly involving systems outages. In addition to frustrating customers and partners, these outages prevent employees from doing their jobs.

- 77% respondents were temporarily unable to access systems or networks post-attack
- 28% of outages lasted for a week or longer
- 26% of respondents were unable to fully perform their job duties for at least a week

Even once systems are brought back online, organizations need to make changes to prevent further attacks. The overwhelming majority of respondents (83%) said that their organizations installed new software or made other major updates, such as migrating some assets to the cloud.

In most cases, rolling out these changes further damaged productivity and added to the tally of indirect recovery costs; 71% of respondents said that the process of installing new software and updates was inconvenient or disrupted productivity.

- 64% of respondents lost login credentials or documents
- 38% reported experiencing program or application glitches
- 33% faced a steep learning curve on new protocols
- 40% lost time to frequent computer restarts and updates
- 43% had to keep logging into programs/accounts (vs. staying logged in continuously)
- 21% said their normal online tools and applications weren't available anymore

Unfortunately, just when employees most needed IT support to reset their passwords, attempt to recover lost documents, and get help with new applications and protocols, IT departments often had their hands full. Over one-third (36%) of respondents said they had limited access to IT support for non-security related issues post-attack.

Percent of Attacks that Are Not Disclosed

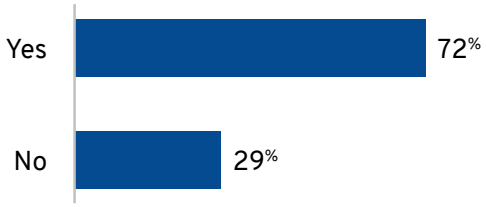
Ransomware attacks are more pervasive because many are not disclosed.

Adding to the pressure that organizational leaders feel to pay the ransom and move on, 64% of respondents felt that suffering a ransomware attack had a negative impact on their organization's reputation. Further, 63% of employees reported that the attack caused them to personally lose trust in their organization.

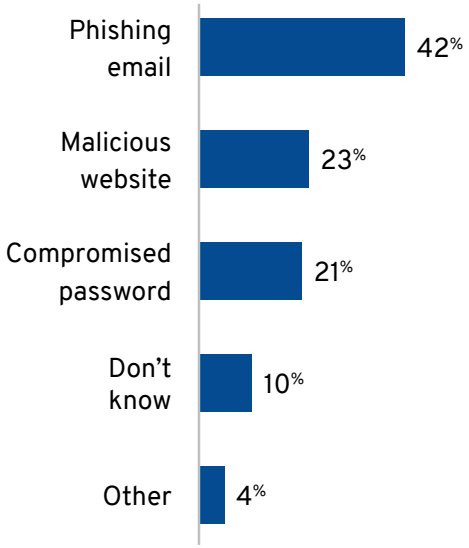
With this in mind, it's not surprising that 26% of respondents reported that their employers disclosed the attack only to partners and customers (not the general public), while 15% didn't tell anyone. This indicates that ransomware attacks are likely far more pervasive than anyone realizes.

Full Data

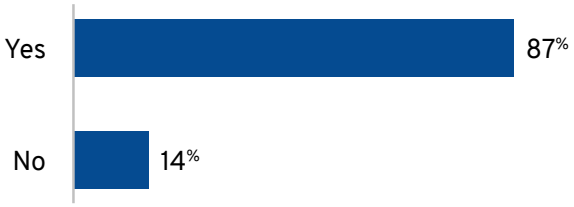
Q1. Before the attack, did you know what ransomware was?



Q2. What was the root cause of the ransomware attack on your company?

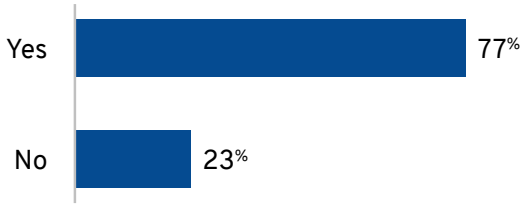


Q3. Has your company enacted stricter security protocols as a result of the ransomware attack?

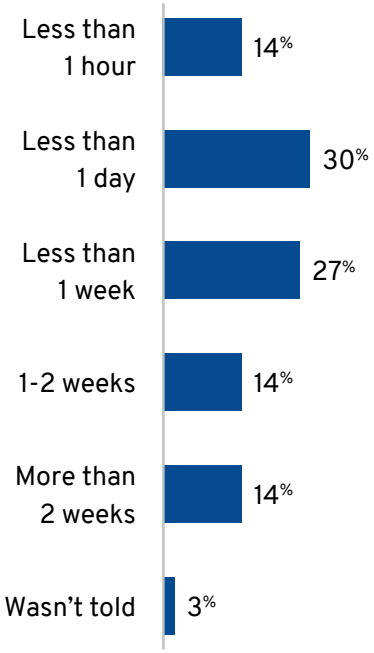


Response Findings (Some responses may >100% due to rounding)

Q4. Was your company taken offline (e.g. unable to access systems or networks) for any period of time because of the ransomware attack?

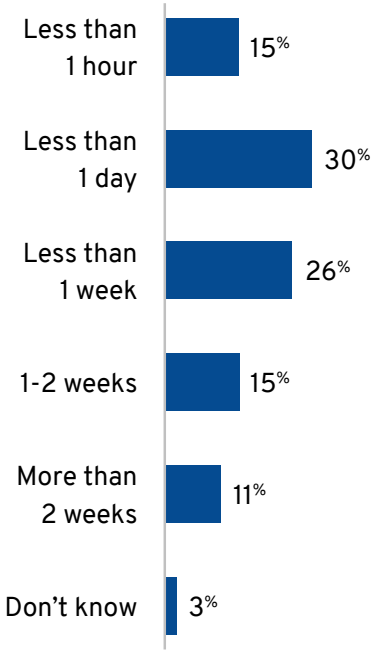


Q5. If yes, how long was your company down for?

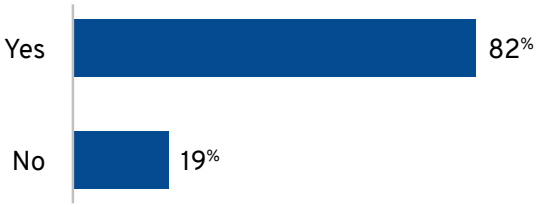


Response Findings (Some responses may >100% due to rounding)

Q6. If yes, how long were you not able to fully work?



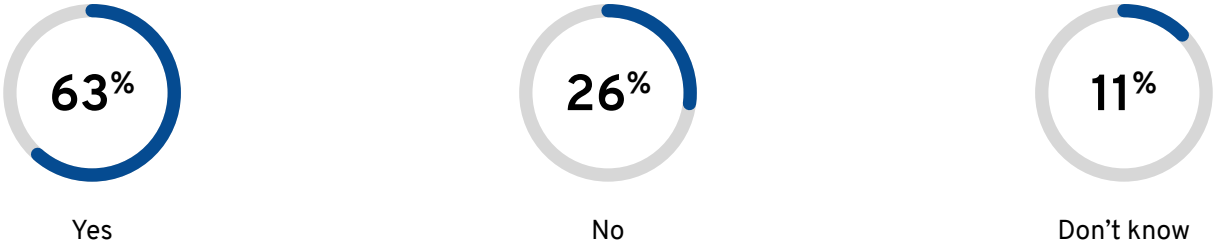
Q7. Do you feel that your organization's leadership communicated effectively with employees following the ransomware attack?



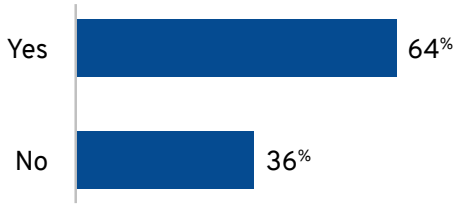
Q8. Did your company alert customers and partners of the attack?

Response Findings (Some responses may >100% due to rounding)

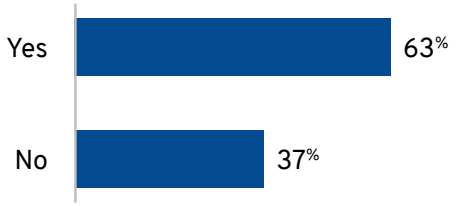
Q9. Did your company release a public reactionary statement about the attack?



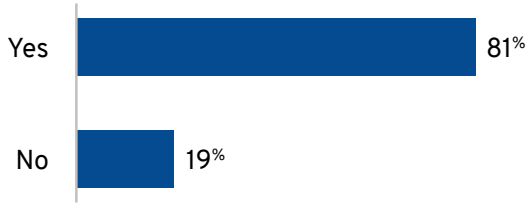
Q10. Do you feel that the ransomware attack negatively impacted your company's reputation?



Q11. Did the ransomware attack impact your trust in your organization?

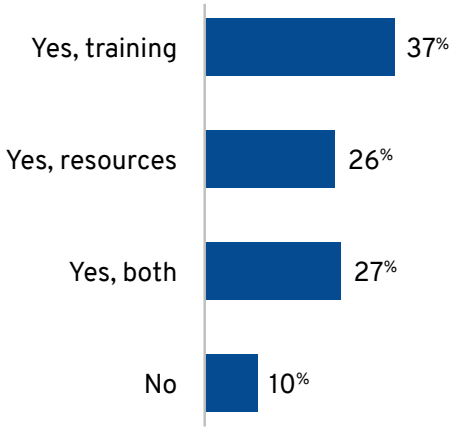


Q12. Prior to the ransomware attack, did you regularly install software updates when prompted?

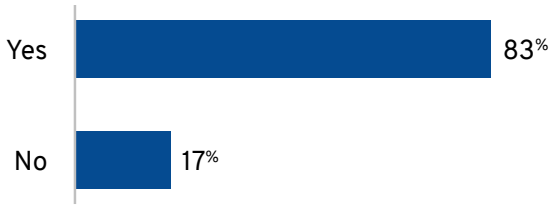


Response Findings (Some responses may >100% due to rounding)

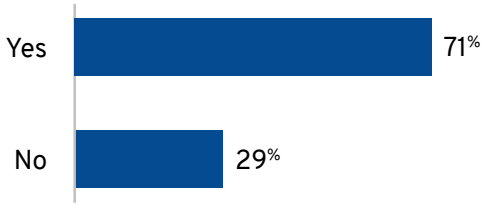
Q13. Following the attack, did your company provide cybersecurity training or resources?



Q14. Following the attack, did your company install software or make other major tech updates (e.g. moving things to the cloud)?

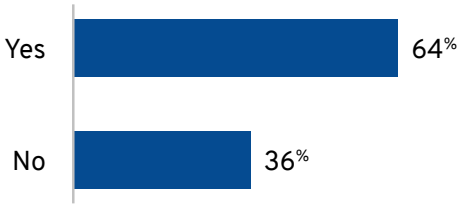


Q15. If yes, do you feel the process of installing new software/updates caused any inconvenience or disrupted productivity?

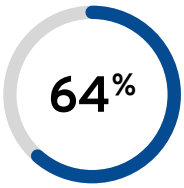


Response Findings (Some responses may >100% due to rounding)

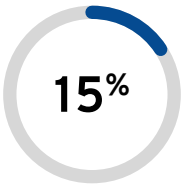
Q16. If yes, did you lose any information, such as login credentials or documents, in the process of updating your devices?



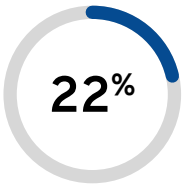
Q17. If yes, how do you feel the updates have impacted your daily work routines?



Positively

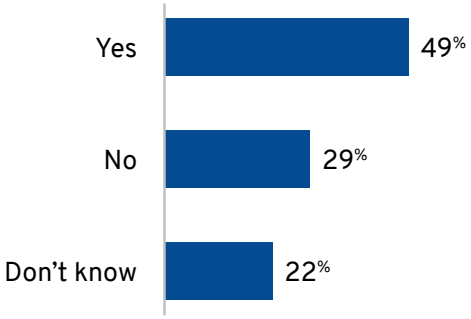


Negatively



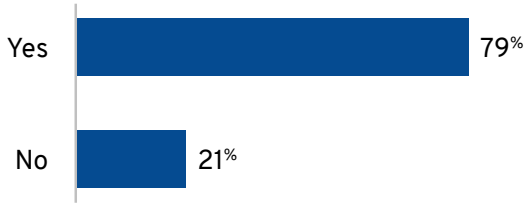
Not at all

Q18. Did your company pay the ransom?



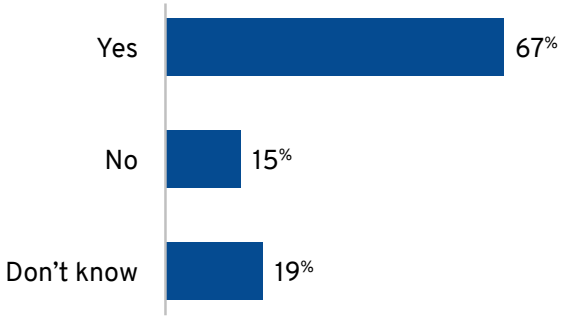
Response Findings (Some responses may >100% due to rounding)

Q19. If yes, was the amount disclosed to employees?



Q20. If yes, have you noticed your organization tightening budgets in other areas following the payment?

Q21. Did cybersecurity spending at your company increase after the attack?



Response Findings (Some responses may >100% due to rounding)

About Keeper

Keeper protects organizations against ransomware attacks with robust administration, controls and visibility over strong password security and real-time dark web monitoring.

Keeper's zero-knowledge, enterprise-grade password security and encryption platform helps thousands of companies all over the world prevent password-related cyberattacks, improve productivity, and enforce compliance.

Keeper gives IT administrators complete visibility into employee password practices, enabling them to monitor adoption of password requirements and enforce password security policies organization-wide, including strong, unique passwords and multi-factor authentication (2FA). Fine-grained access controls allow administrators to set employee permissions based on their roles and responsibilities, as well as set up shared folders for individual groups, such as job classifications or project teams.

For enhanced protection, organizations can deploy valuable add-ons such as Keeper Secure File Storage, which enables employees to securely store and share documents, images, videos, and even digital certificates and SSH keys, and BreachWatch™, which scans Dark Web forums and notifies IT administrators if any employee passwords have been compromised in a public 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.

To learn more visit **keeper.io/ransomware-impact**.