CLOUDIAN®

2021

Ransomware Victims Report

Three key lessons highlight need for greater focus on recovery

The Cold Reality of Ransomware Attacks

Ransomware is one of the most widely discussed threats in cybersecurity. However, not enough research exists about the experiences of organizations that have actually suffered from ransomware attacks.

For this report, Sapio Research Ltd—an independent research firm—surveyed 200 IT decision makers whose organizations experienced a ransomware attack between 2019 and 2021.

The findings reveal the cold, hard truth about such attacks:

1. **They are hard to prevent even when you're prepared.**
2. **Ransomware can penetrate quickly, significantly impacting an organization's financials, operations, customers, employees and reputation.**
3. **Even if you pay the ransom, there are other related costs that can be significant.**

All this highlights the need for organizations to put more focus on ensuring they can recover quickly and easily from an attack without having to pay ransom. At the end of this report, we offer suggestions for how IT leaders can do so.

But first, let's look at three key lessons from the survey.

Lesson #1: Despite defensive measures, ransomware gets in

All survey respondents had one or more security measures in place, but ransomware was still able to penetrate the defenses.

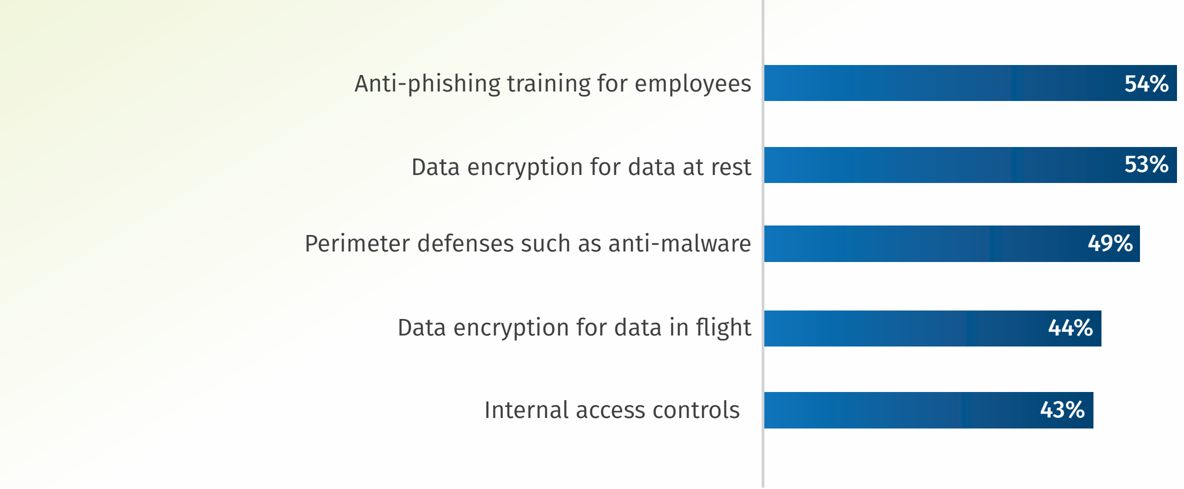
Phishing continues to be one of the easiest paths for ransomware

Phishing was one of the most common points of entry, with 24% of ransomware attacks starting this way. That number rises to 41% when looking at organizations with fewer than 500 employees.

Phishing succeeded despite the fact that 65% of those that reported it as the entry point had conducted anti-phishing training for their employees. This reflects the increasing sophistication of phishing schemes, with attackers now mimicking emails from trusted associates such as high-level executives (known as "whaling" attacks). These emails will sometimes include personal details, usually gleaned from social media, making it more likely that even a wary individual will fall prey.

Phishing wasn't the only defensive measure that fell short. 49% of survey respondents reported having perimeter defenses in place prior to the successful ransomware attack.

DEFENSES IN PLACE PRIOR TO THE ATTACK



The public cloud isn't necessarily safer

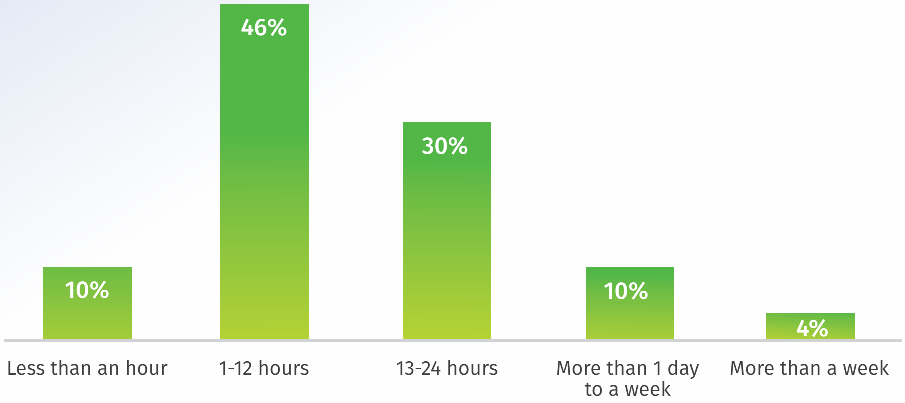
Almost half of the IT decision makers that stored data on-premises or with an external service provider believed that the public cloud would have been a safer place to store their data. However, the public cloud was actually the most common point of entry for ransomware attacks, with 31% of respondents being attacked this way.

Lesson #2: Attackers move fast, and the impact is widespread

Once cybercriminals are able to insert ransomware, they can quickly take over. 56% of survey respondents reported that attackers were able to take control of their data and demand ransom within just 12 hours, and another 30% said it happened within 24 hours.

In the case of phishing-led attacks, 76% of victims stated that the attackers took control within 12 hours.

HOW QUICKLY CYBERCRIMINALS TOOK CONTROL OF DATA AND DEMANDED RANSOM



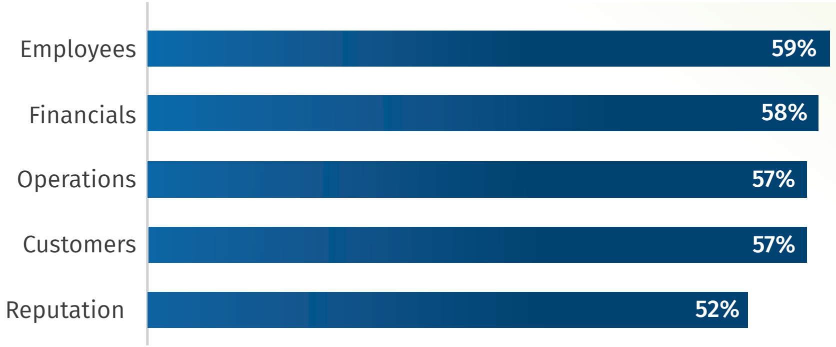
Attacks affect every aspect of an organization

On average, 44% of respondents' total data was held hostage, with financial, operational, customer and employee data all being targeted.

The average downtime across respondents was just over 3 days, with 1 in 10 reporting downtime of a week or more. Although the average downtime was lower than that reported in other surveys, this was still enough to do notable damage.

More than half of IT decision makers reported a significant impact across all aspects of their business – including reputation – with 30% describing the impacts as "severe."

PERCENTAGE THAT REPORTED AT LEAST A "SIGNIFICANT IMPACT" ON THESE ASPECTS OF THEIR BUSINESS

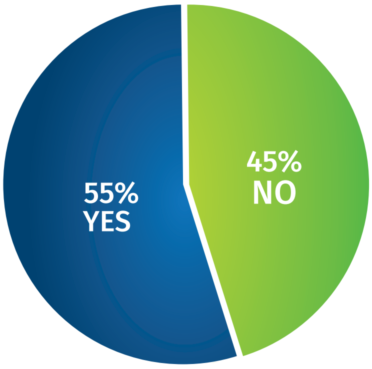


Lesson #3: The financial costs go beyond just ransom payments

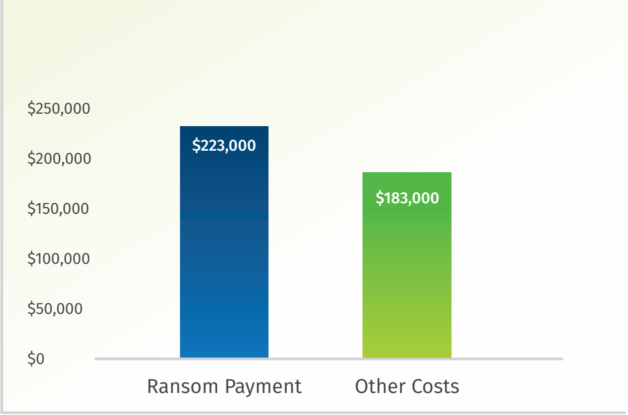
When it came to a decision about whether to pay ransom, 55% chose to do so. The average ransom payment was $223,000, with 14% paying $500,000 or more.

In addition, those organizations that paid ransom still spent an average of $183,000 more for other costs resulting from the attack, with 37% of respondents paying at least $100,000 more.

PAID RANSOM



AVERAGE TOTAL COST OF ATTACK FOR THOSE THAT PAID RANSOM: $406,000



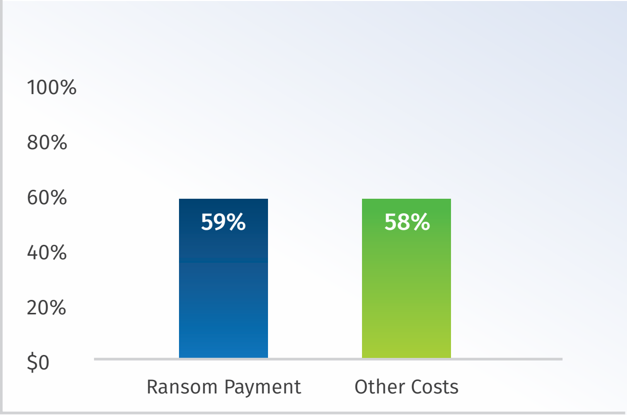
Most noteworthy, even after incurring an average total cost of $406,000—reflecting both the ransom payment and other costs—only 57% of respondents that paid ransom got all their data back.

Cyber insurance doesn't solve everything

79% of respondents had cyber insurance, which—on average—covered only about 60% of the ransomware payment and other costs incurred by those that paid ransom, presumably reflecting deductibles and coverage caps.

Of those that had cyber insurance, 88% have had their rates increased post-attack, with an average increase of 25%.

COSTS COVERED BY CYBER INSURANCE FOR THOSE THAT PAID RANSOM



What this means for organizations’ cybersecurity strategy: focus more attention on recovery

The survey results show that even when organizations take preventative measures, ransomware attackers can still move fast and cause notable damage in a number of ways.

In addition, the financial costs of recovering from ransomware are significant, even with cyber insurance, and there’s no guarantee of getting all your data back. Moreover, the negative impact on an organization’s reputation and customers can be hard to reverse.

The harsh reality is that organizations need to assume ransomware attacks will get through and, therefore, have a cyber strategy that focuses greater attention on how to recover their data quickly and easily without having to pay ransom.

The best way to ensure quick and easy recovery is to have an immutable backup copy of your data, and a recent Gartner report stated that “having an immutable copy of the backup is the most important item to start protecting backup data” from ransomware.* Data immutability prevents hackers from encrypting or deleting data for a specified period of time, meaning organizations can recover an unencrypted copy of their data in the event of a ransomware attack without having to pay ransom.

By enabling victims to recover their data without paying ransom, immutability also helps to break the cycle of ransom payments funding cybercriminals’ ability to conduct further attacks.

In addition, data immutability can help with cyber insurance—in obtaining ransomware coverage, ensuring that an insurance claim will be covered (e.g., some insurers may refuse to pay claims if organizations have not adequately protected their data) and/or securing a discount for the insurance (currently as much as 20% in some cases).

* Gartner Report: “Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults” – May 27, 2021

Cloudian S3 Object Lock enables fast, easy data recovery without paying ransom

Cloudian provides data immutability—validated in U.S. government certification testing — through a solution called S3 Object Lock, which provides a virtual air gap and easily integrates into an end-to-end, on-premises backup architecture. This solution is part of the company's HyperStore object storage platform, which includes additional features to secure data such as system-level hardening and root disable that go beyond protections available from any other on-premises object storage provider.

HyperStore is one of only two object storage offerings with Common Criteria certification, signifying that the storage is tamper-proof so immutability cannot be compromised. In addition, it is the only independent object storage platform in the industry that has obtained both Common Criteria and Federal Information Processing Standard certification (FIPS). HyperStore also provides AES-256 server-side encryption for data at rest and SSL for data in transit, which protects against cybercriminals publicly exposing sensitive data. Other security features include secure shell, integrated firewall, RBAC/IAM access controls and certifications with SEC Rule 17a-4(f), CFTC Rule 1.31(c)-(d) and FINRA Rule 4511.

Cloudian's Object Lock solution has received several industry honors, including Best Business Continuity/Disaster Recovery Solution in the 2021 SC Awards. These awards are recognized throughout the security industry as the gold standard of excellence in cybersecurity, with winners chosen by a distinguished group of leading IT security professionals.

To learn more about Cloudian's ransomware-proof data protection, go to Lock Ransomware Out - Keep Data Safe | Cloudian.

Survey Methodology

The survey was conducted among 200 it decision makers in the us whose organization had experienced a ransomware attack in the last 2 years. The interviews were conducted online by sapio research in april 2021 using an email invitation and an online survey.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. In this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 6.9 Percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

Sapio research is a global, full-service market research consultancy providing high quality insights which deliver against key business objectives and inform messaging.

Cloudian, Inc.
177 Bovet Road, Suite 450, San Mateo, CA 94402
Tel: 1.650.227.2380 | Web: Cloudian.com | Contact Cloudian