The ROI of ransomware recovery

Understanding the return on investment (ROI) for ransomware recovery is essential for businesses.

Total Economic Impact

In 2024, Keepit commissioned a Total Economic Impact (TM) study by Forrester Consulting which revealed significant findings.

Based on interviews with Keepit customers, Forrester created a three-year financial model to determine the financial benefit of using Keepit to protect data in SaaS workloads. The study shows that Keepit's solution offered a 163% ROI over three years, with a net present value of over $800,000.

This demonstrates the substantial economic benefits that can be achieved through strategic investments in ransomware recovery capabilities.

Source: The Total Economic Impact™ Of Keepit SaaS Data Protection, Forrester Study

Key statistics

- **The Forrester TEI** study revealed that Keepit's solution provided a return on investment (ROI) of 163% over three years.
- **Net present value of over $800,000**: The same TEI study indicated that the net present value of Keepit's solution was over $800,000.
- **90% reduction in recovery time**: Customers using Keepit's solution reported a 90% reduction in the time needed for targeted restores after ransomware attacks.
- **Payback within 6 months**: Through its various benefits, the Keepit solution was shown to have a payback period of less than 6 months.

This is especially important as Forrester found a concerning gap when it comes to disaster recovery plans for SaaS platforms, per their research on the state of disaster recovery preparedness in the market.

Speaking on our recent webinar, Forrester senior analyst Brent Ellis said:

"[Out of 2000 enterprise software decision makers], **87%** said they're either currently using a SaaS application, or they plan to in the next 12 months. But [in a separate survey when I asked disaster recovery professionals] if SaaS platforms are within the scope of their organization's disaster recovery planning, only **36%** had a wholehearted yes. And when I asked does your organization currently backup your SaaS hosted data? **14%** said no. And if you're talking about disaster recovery planning and **14%** don't do backup of that data, that leaves a big question mark about whether you're actually able to recover from a particular disaster to that platform."

Sources:
- Keepit Webinar March 2024, 'The ROI of ransomware recovery', featuring Forrester
- Forrester's Software 1 Survey, 2023
- Forrester/Disaster recovery journal, November 2023, Disaster recovery practices and preparedness survey

Risk factors for SaaS data resilience and disaster recovery

1. Shared platform vulnerabilities

- Dependency on shared infrastructure increases risk exposure.
- Potential for simultaneous failure of multiple systems.

2. Exfiltration threats

- Unauthorized data access and transfer by cybercriminals.
- Risk of sensitive data being stolen or leaked.

3. Cyberattacks

- Ransomware targeting SaaS platforms.
- API exploits used to gain unauthorized access.

4. Limited version retention

- Inability to recover older versions of data.
- Increased risk of data loss due to limited backup versions.

5. Malicious data changes

- Intentional alterations to data by internal or external actors.
- Difficulty in detecting and reversing malicious modifications.

6. Accidental data changes

- Unintentional data deletions or modifications by users.
- Potential for significant operational disruption.

7. Role-based access control (RBAC) issues

- Excessive privileges granted to users.
- Increased risk of unauthorized data access and changes.

8. Platform misconfigurations

- Errors in configuring SaaS platforms.
- Increased vulnerability to cyberattacks and data breaches.

9. API exploits

- Attackers leveraging API vulnerabilities to access data.
- Risk of data manipulation and unauthorized actions.

10. Vendor dependency

- Reliance on SaaS vendors for data protection.
- Potential risks if the vendor's security measures are inadequate.

11. Insufficient backup solutions

- Lack of comprehensive backup and recovery plans.
- Risk of extended downtime and data loss in disaster scenarios.

12. Compliance and regulatory risks

- Failure to meet data protection and privacy regulations.
- Potential for legal and financial penalties.

It's vital for organizations to assess and analyze risk profiles for SaaS platforms in use, keeping these risk factors in mind, and understand how this affects their overall resilience. Based on these assessments, businesses can develop prioritized disaster recovery plans.

Strategies for enhancing resilience

To enhance resilience against ransomware and other cyberthreats, organizations should implement several key strategies. First, conducting formal risk assessments is essential to identify critical infrastructure and data assets. Based on these assessments, businesses can develop prioritized disaster recovery plans tailored to their specific needs and vulnerabilities.

Additionally, ensuring that data backups are immutable and tamper proof is crucial. Regular testing and verification of backup integrity can prevent data loss and facilitate quick recovery in case of an attack. Finally, maintaining strong contracts with SaaS vendors is vital to ensure organizational resilience and security requirements are met.

These contracts should clearly define the vendor's responsibilities and the security measures taken to protect data.

What does good recovery look like?

Checklist for disaster recovery and business continuity:

- ☐ You have completed a risk assessment to identify the most critical infrastructure and data assets to protect.
- ☐ You have created a prioritized, granular DR plan supported by your software.
- ☐ You have backed up all your mission-critical data.
- ☐ You regularly test and verify your recovery processes.
- ☐ You are recovering from backups that are immutable and tamper-proof.
- ☐ Your backups remain available on a separate, air-gapped infrastructure.

Here at Keepit we:

Are specialized on SaaS data protection
We support a wide range of commonly used SaaS platforms, such as M365, Entra ID, Salesforce, and more. Our solution is purpose-built and specifically designed for protecting cloud SaaS data.

Deploy leading security measures
We deploy leading security measures, keeping your data safe in a fully air-gapped, separated environment with immutability by default and encryption both in transfer and at rest.

Are a completely independent backup provider
We maintain our own cloud infrastructure and our own data centers across the world. Vendor independence means you'll always have access to your data, even when disaster strikes.

Hold relevant security certifications
As your trusted cloud backup vendor, we're serious about the security of your data. Keepit holds both the ISO/IEC 27001:2013 certification and the ISAE 3402-II certification (audited by Deloitte annually).

Continue the conversation

Watch the on-demand webinar

Watch it now

Keepit provides next-level SaaS data protection purpose-built for the cloud, by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience and future-proof data protection.

For more information visit www.keepit.com or follow Keepit on Linkedin