FORRESTER®

Ransomware Recoverability Must Be A Critical Component Of Your Business Continuity Plans

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY COHESITY OCTOBER 2019

Businesses Are Not Adequately Protecting Themselves Against Ransomware Attacks

Ransomware attacks are increasing in frequency and complexity; businesses must continue to evolve and upgrade their security landscapes to adequately protect themselves and their customers from an attack. According to a recent Forrester report, the number of ransomware attacks on enterprises is up 500% over the past year, and these attacks are projected to cost businesses $11.5 billion, in addition to the cost of loss of customer and partner trust.[1]

As a result, businesses are reevaluating their current backup practices, as well as their recovery processes, with an eye to minimizing the impact an attack could have on their business. Critically, recoverability — or the ability to recover data when and where you need it, without compromise — is at the center of all their efforts.

Key Findings

Businesses have gaps to close in their current approaches. Though 90% of firms said improving their ransomware attack response capabilities is a top priority, less than a quarter have a business continuity contingency for such an attack.

Backups are often fragmented and/or compromised after an attack, causing businesses to lose significant time when recovering data and restoring applications.

Businesses are eager to partner with enterprise backup solution vendors to help with their recoverability and threat intelligence capabilities.

Improving Processes And Threat Intelligence Are Top Priorities

A mere 21% of businesses surveyed have contingency plans for recovering from a ransomware attack; it's no surprise, then, that the top priorities for IT teams in the coming 12 months are improving ransomware attack recovery processes, improving threat intelligence and visibility capabilities, and improving response times to ransomware attacks. Despite the increasing frequency of cyberattacks, the vast majority of businesses are not adequately prepared but recognize that they must begin to not only define processes in response to an attack but also improve their proactive capabilities to identifiy potential threats.

"Which of the following initiatives are likely to be your firm's/organization's IT priorities over the next 12 months?"

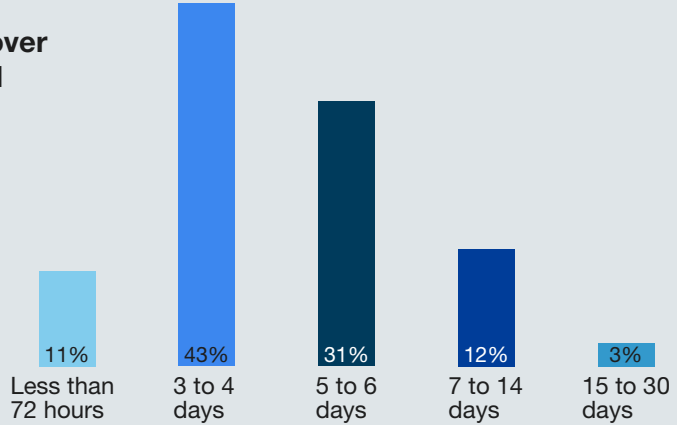
Base: 313 IT infrastructure and operations decision makers in North America, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Cohesity, September 2019

Recovery Is Slow And Incomplete

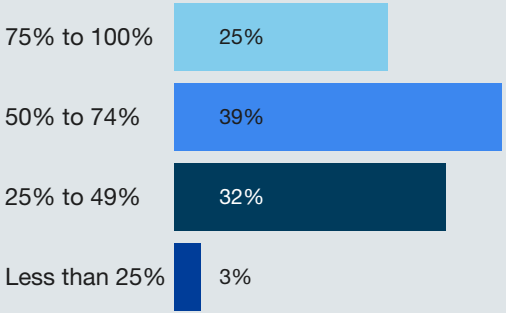
Despite a general confidence in their ability to recover from ransomware attacks — 77% of respondents in a recent Forrester report stated that they are confident or very confident in their ability to recover from a ransomware attack — this confidence is generally unfounded.[2] Currently, only 11% of organizations surveyed reported that they could recover the data and restore the applications within three days after a ransomware attack; on average, these businesses are only recovering 58% of their data after such an attack. A mere 25% are able to recover 75% to 100% of their data.

For 15% of respondents, it can take weeks to recover the data and restore their business applications — and even then, they tend to restore less data than those that can recover more quickly. Two-thirds of respondents who said it takes 15 to 30 days for them to recover data could only restore 25% to 49% of their data.

Time to recover the data and restore the applications



Amount of data recovered from the attack



FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY COHESITY OCTOBER 2019

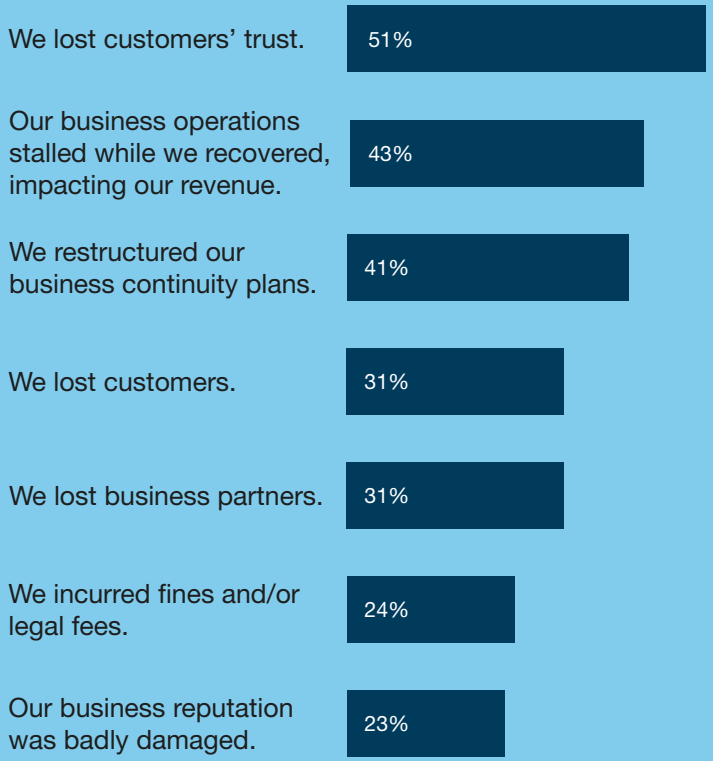
Base: 313 IT infrastructure and operations decision makers in North America, EMEA, and APAC
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Cohesity, September 2019

Ransomware Attacks Carry Serious Business Impacts

Ransomware attacks can have devastating effects on businesses and organizations: Mom-and-pop shops can go out of business just from a single attack; city services can be halted for days or weeks when a small city is attacked, resulting in untold human suffering; and hospitals can be frozen in inaction during an attack, reducing their ability to provide critical care to their population.

Businesses understand that ransomware attacks have serious repercussions: 51% noted that they lost customer trust after an attack while 43% noted that they lost revenue because of a stall in business operations. Interestingly, only 41% indicated that they restructured their business continuity plans, despite their loss in customer trust, revenue, and business partners.

“Which of the following, if any, did your organization experience after your most recent ransomware attack?” (Select all that apply)



Base: 313 IT infrastructure and operations decision makers in North America, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Cohesity, September 2019

Businesses Are Not Confident In Their Ability To Prevent, Detect, And Remediate Attacks

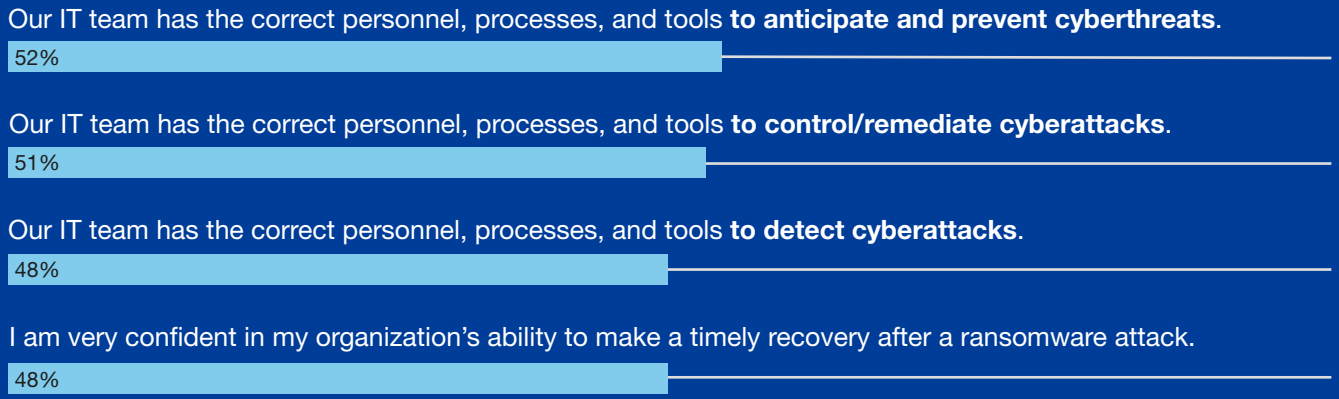
The good news: There is widespread mutual trust across infrastructure and operations (I&O), security and risk (S&R), and the chief information security officer (CISO). Three-quarters of respondents agreed that the CISO trusts I&O professionals; 72% agreed that the CISO trusts S&R professionals; and nearly two-thirds agreed that I&O and S&R teams have clear and open lines of communications.

The bad news: Businesses are far less confident in their abilities to prevent, detect, and remediate attacks. In fact, only 48% are very confident in their organizations' ability to make a timely recovery after a ransomware attack.

About half of all respondents are not confident in their ability to prevent, control, and detect cyberattacks.

"Please state your level of agreement to the following statements."

- Strongly agree/agree



Base: 313 IT infrastructure and operations decision makers in North America, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Cohesity, September 2019

Rigid Processes And Poorly Defined Responsibility Slow Down Response Rates

The top-noted challenge organizations face when responding to a ransomware attack is rigid processes: Half of all respondents noted that their backup recoverability processes are too rigid and don't allow for time-sensitive adjustments. When minutes and hours matter, this rigidity slows down recovery and muddies responsibilities.

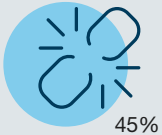
On top of challenging processes, over 40% of respondents noted that poorly defined recoverability responsibilities and poor communications slow down their ransomware attack response times. Despite mutual trust, I&O and S&R teams still struggle to react to ransomware attacks in a coordinated manner; without cross-team collaboration, business continuity efforts will always suffer.

"Which of the following process-focused challenges does your organization face when responding to ransomware attacks?"

(Select all that apply)

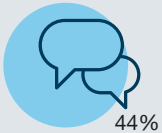
50%

Our backup recoverability process is rigid, not allowing for time-sensitive adjustments.



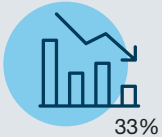
45%

Recoverability responsibility is poorly defined across infrastructure and operations (I&O) and security and risk (S&R) teams.



44%

Our security teams are unable to communicate with the infrastructure operations teams.



33%

We don't have a well-defined flowchart for our infrastructure and operations (I&O) and security and risk (S&R) teams to follow.

21%

We do not/cannot verify backup copies for vulnerabilities before performing recovery.

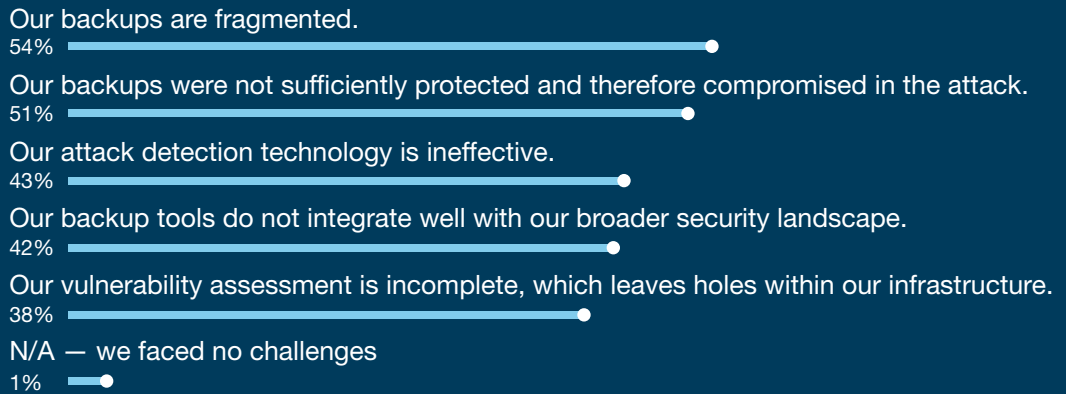
Base: 313 IT infrastructure and operations decision makers in North America, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Cohesity, September 2019

Fragmented And Poorly Secured Backups Create Recovery Challenges

At the same time, business continuity efforts are stymied by underperforming backups. The top technology-centric challenge businesses face when recovering from a ransomware attack is a fragmented backup. Additionally, 51% noted that their backups were not sufficiently protected and therefore were compromised in the attack, fundamentally undermining their purpose.

Beyond backups, businesses struggle with attack detection, leaving them unable to proactively disable potential threats and instead having to react to attacks

"Which of the following technology-focused challenges does your organization face when responding to ransomware attacks?"
(Select all that apply)



Base: 313 IT infrastructure and operations decision makers in North America, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Cohesity, September 2019

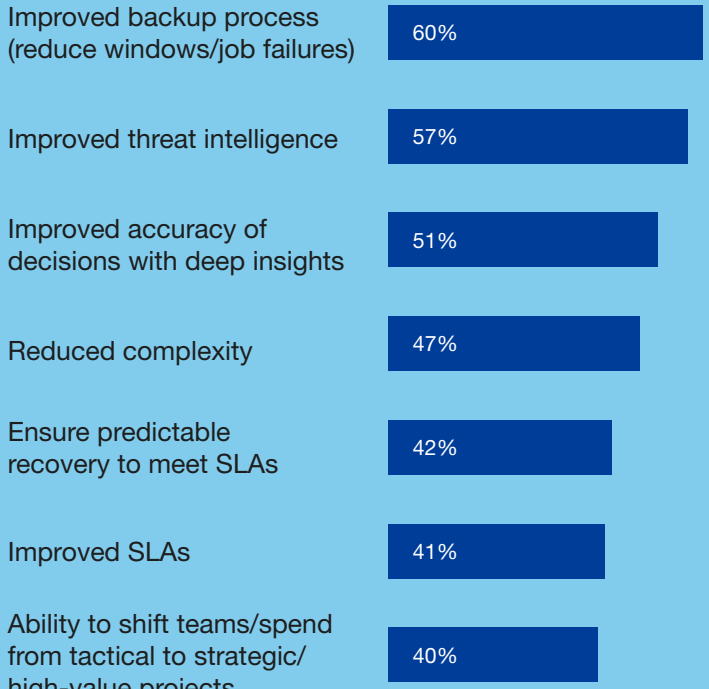
Vendors Are Seen As The Solution To Achieve Predictable Recovery

Businesses are eager to partner with a vendor to evolve their enterprise backup solutions; many look to vendors to reduce backup job failures and improve threat intelligence — which had been noted as their top priorities for the next 12 months. Specifically, nearly two-thirds of respondents are looking to a partnership with a vendor to reduce their backup windows/job failures, and 57% anticipate improved threat intelligence from a vendor. Notably, nearly half of respondents anticipate a reduction in complexity of their security landscapes after partnering with a data management vendor.

Forty percent of respondents also indicated that a partnership will enable them to empower teams to spend more time on strategic/ high-value projects, rather than day-to-day backup management.

“What benefits have you achieved/do you anticipate achieving by partnering with a vendor to run or augment your enterprise backup solution?”

(Select all that apply)



Base: 313 IT infrastructure and operations decision makers in North America, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Cohesity, September 2019

Predictable Recovery, Easy Cloud Integration, And Instant Recovery Are The Most Valuable Capabilities

Businesses want a technology that can simplify their backup management, all while ensuring recoverability — i.e., a predictable recovery — and easily integrating into the cloud.

Additionally, with increasing business and client expectations, recovery time is under significant pressure, requiring instant recovery at scale. And with the possibility of recovering from infected backups, I&O professionals are looking to a solution to assist them with visibility into potential vulnerabilities.

With the ever-increasing threat of ransomware attacks, businesses are eager to be proactive with their defense to minimize the potential impact of an attack and develop a comprehensive defense against ransomware attacks.

“How valuable do you find the following backup and recovery features/capabilities?”

Base: 313 IT infrastructure and operations decision makers in North America, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Cohesity, September 2019

Conclusion

Ransomware attacks will happen; IT teams must be proactive in their threat intelligence capabilities and their backup recoverability to minimize an attack's impact on their business.

- Ransomware attacks have serious business repercussions; the top-noted impact of an attack was a loss of customer trust, which has significant impacts on a business's growth.
- Despite mutual trust across I&O and S&R teams, businesses struggle with rigid, siloed processes and unclear lines of communication when responding to ransomware attacks. Additionally, backups are often compromised in an attack, resulting in significant challenges in extracting critical data and restoring applications.
- As a result, businesses are looking to partner with backup solution vendors to help with predictable recovery in the near term and threat intelligence looking forward.

Project Director:
Ana Brzezinska, Market Impact Consultant
Contributing Research:
Forrester's Infrastructure & Operations research group

Methodology

This Opportunity Snapshot was commissioned by Cohesity. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 313 IT infrastructure and operations decision makers (manager+). The custom survey began and was completed in September 2019.

ENDNOTES

[1] Source: "Forrester's Guide To Paying Ransomware," Forrester Research, Inc., June 5, 2019.

[2] Source: "Ransomware Is A Business Continuity Issue," Forrester Research, Inc., May 22, 2018.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Demographics

GEOGRAPHY

- 33% US, Canada
- 34% UK, France, Germany
- 34% Australia, Japan

COMPANY SIZE

- 57% 1,000 to 4,999 employees
- 28% 5,000 to 19,999 employees
- 14% 20,000 or more employees

TOP 3 INDUSTRIES

- 14% Retail
- 12% Financial services
- 8% Technology

TOP IT GROUPS

- 50% Security
- 24% Data center infrastructure operations
- 15% Backup and recovery
- 11% Storage architect


FORRESTER®