SOLVING FOR RANSOMWARE THREATS: INSIGHTS INTO CURRENT LEADERSHIP ACTIONS

Data collection: February 20, 2022 - March 15, 2022
Respondents: 100 IT decision-makers
SOLVING FOR RANSOMWARE THREATS: INSIGHTS INTO CURRENT LEADERSHIP ACTIONS

Solving ransomware threats is a top concern among many company leadership teams, not just those in IT departments. To properly prepare for such a threat, businesses must begin taking a much more comprehensive approach, emphasizing the recovery aspects that too often get less attention.

To delve into the perspectives surrounding ransomware threats and what organizations are currently doing to shore up weaknesses and prepare for potential attacks, Pulse and InterVision surveyed 100 IT leaders.

Decision-makers consider ransomware to be the top threat to their business and struggle to stop threats early

Ransomware was the top threat for 45% of respondents, while data breaches were the top threat for just over one-quarter (27%).

<table>
<thead>
<tr>
<th>Threat</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware</td>
<td>45%</td>
</tr>
<tr>
<td>Data breaches</td>
<td>27%</td>
</tr>
<tr>
<td>Human-induced outages and network issues</td>
<td>14%</td>
</tr>
<tr>
<td>Climate change</td>
<td>7%</td>
</tr>
<tr>
<td>Market influence</td>
<td>2%</td>
</tr>
<tr>
<td>Supply chain issues</td>
<td>2%</td>
</tr>
<tr>
<td>COVID-19</td>
<td>1%</td>
</tr>
<tr>
<td>Human resources (training and access to recover)</td>
<td>1%</td>
</tr>
<tr>
<td>Natural disasters (regular weather-related)</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
</tr>
</tbody>
</table>

What do you consider to be the biggest threat to technology-related business continuity?
When responding to a cybersecurity breach, 34% of respondents say their biggest gap is their ability to stop threats before they get in. For 30%, it is the ability to detect bad actors in their environment.

Technology and process were the top-cited areas for improvement when it comes to ransomware threats. People — the most expensive resource — was the least common choice.
Businesses focus primarily on ransomware attack recovery, not prevention

More than double the number of respondents say their business’ priority is around the ability to recover from a ransomware attack (46%) versus setting preventative measures (21%).

Which of the following best describes your business’ priority around ransomware attacks?

- **46%** The ability to recover from a possible ransomware attack
- **33%** Prevention and recovery receive equal attention
- **21%** Preventative measures against ransomware attacks
- **0%** None of these

Nearly 90% of respondents say their organization has a recovery plan in place.

Does your organization have a recovery plan in the event of a ransomware attack?

- **88%** Yes
- **4%** No
- **8%** Unsure
Over three-quarters of respondents say their business conducts tests on their ability to recover from a ransomware attack.

Does your organization test its ability to recover from a ransomware attack?

- Yes: 76%
- No: 14%
- Unsure: 10%

Most respondents feel their organization is least prepared with either staffing to monitor (27%) or tools to protect (25%) against ransomware.

When it comes to ransomware, in what area is your organization LEAST prepared?

- Staffing for 24x7x365 monitoring: 27%
- Tools for protection: 25%
- Tools for monitoring: 14%
- Tools for recovery: 13%
- Disaster recovery planning: 6%
- Incident management: 4%
- Security posture review: 3%
- None of these: 6%
- Unsure: 2%
- Other: 0%
Decision-makers want the best technology for ransomware protection and most start by consulting peers or research analysts. 78% of respondents believe that a reliable and comprehensive ransomware solution is possible.

But for most (42%), having the best technology is more important than having a single comprehensive solution.
When deciding how to protect against ransomware, 43% of leaders first seek the guidance of a peer, while 36% turn to analyst firms to start.

When beginning your research to protect the organization from ransomware, what source do you typically start with?

- **43%** Peer conversations
- **36%** Analyst firms
- **9%** Third-party provider websites
- **8%** Media articles
- **4%** Google search
- **0%** Other

Effective ransomware protection demands a comprehensive and holistic approach from organizations

93% of leaders agree that organizations need a comprehensive approach to ransomware.

To what extent do you agree or disagree with the following statement: “Organizations need a comprehensive approach to ransomware that will protect, detect, and restore both critical information and business operations.”

- **30%** Strongly agree
- **63%** Agree
- **6%** Neutral
- **1%** Disagree
Not a single respondent disagreed that cybersecurity and disaster recovery teams must work together to solve ransomware challenges.

To what extent do you agree or disagree with the following statement: “Organizations need to pair cybersecurity and disaster recovery teams together to solve ransomware challenges from a holistic perspective.”

- **Agree**: 64%
- **Strongly agree**: 27%
- **Neutral**: 9%
- **Disagree**: 0%
- **Strongly disagree**: 0%

There is an appetite for a solution as almost all (90%) respondents have heard of or are interested in learning more about RPaaS.

- **Yes**: 46%
- **No, but tell me more**: 44%
- **Unsure**: 3%
- **No, not interested**: 7%
Respondent Breakdown

Region

100% North America

Title

- C-Suite: 17%
- VP: 27%
- Director: 41%
- Manager: 15%

Company Size

- 1,001 - 5,000 employees: 37%
- 5,001 - 10,000 employees: 26%
- 10,001+ employees: 37%

Insights powered by PULSE