veeam

Cloud▸Connect▸Summit

October 2025

Ransomware Trends
and the Future of Data Protection

Rick Vanover

Veeam Product Strategy

RICKATRON

Agenda

Threat actors are adapting

Ransom payments are decreasing, but…

Collaboration reinforces resilience

Serious chat: Actionable insights for the Veeam community

Section 01

Setting the Table: Ransomware Trends for 2025

Top Insights for the Veeam Community

Year after year, we see the same recovery issues

33% of production workloads are disrupted

Showing that attackers remain successful at business disruption despite security improvements

20% of recoverability misses expectations

Less than 1/5 recovered more than 80% of their servers post-attack

66% of backup repositories impacted

With 34% modified or deleted – showing threat actors are aggressive **and successful**

Top Insights for the Veeam Community

Confidence is **not improving** post attack

69% of ransomware victims said they thought they were prepared before being attacked…

That confidence dropped by more than 20% post-attack

In particular, CIO preparedness ratings declined 30% post-attack compared to a 15% decline for CISOs, indicating CISOs have a more accurate understanding of their organization’s security posture.

Download the report
vee.am/RWT25

Post-Incident Advice Top Tips List

Ultra-Resilient copies:

Offline, Air-Gapped, Immutable or Four-Eyes media. 3-2-1-1-0 Rule.

Encryption Passwords:

(Intentional) Encryption, also consider cloud access keys.

Performant Storage:

Backup storage performance on massive recoveries matters.

Section 02

Trend 1:
Threat Actors are Adapting

Lone Wolves are on the Rise

The shutdown of LockBit and the disappearance of BlackCat and Black Basta highlight the impact of ransomware victims collaborating with government agencies.

TTP analysis for 2025

A rise in attacks targeting organizations with lower defenses and faster dwell time

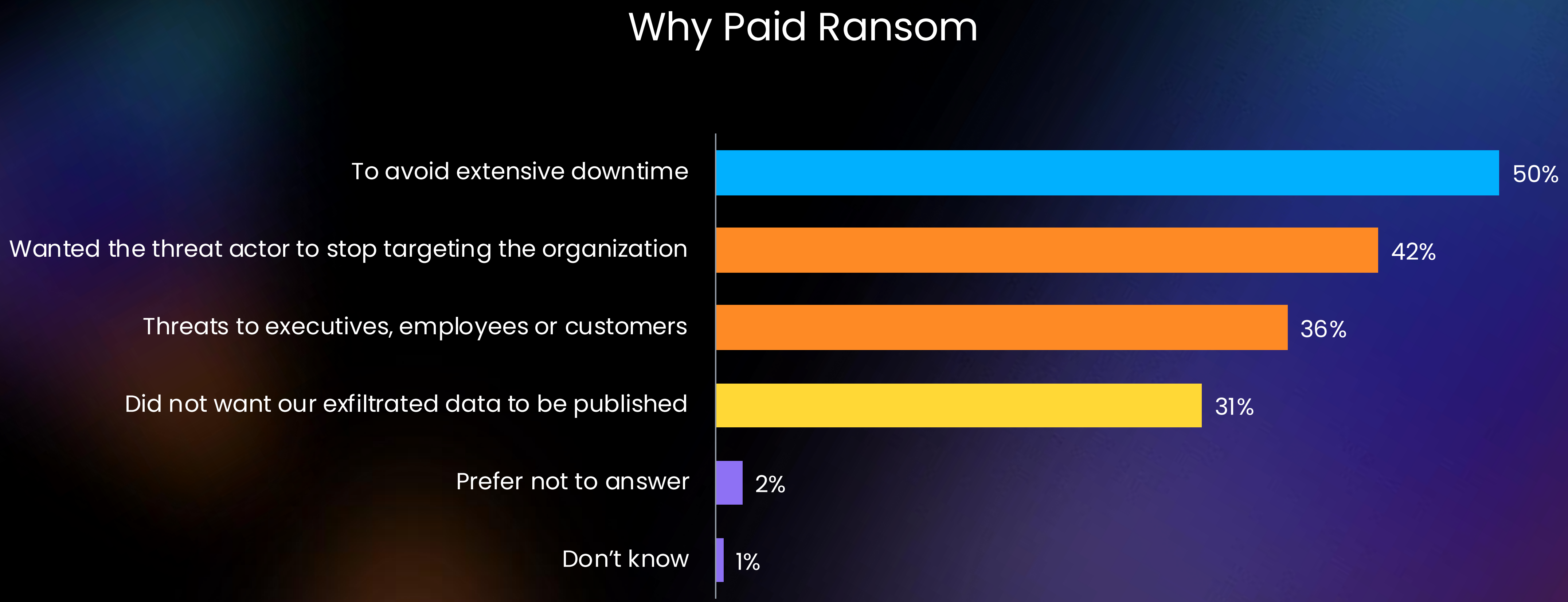
Download the report
vee.am/RWT25

Section 03

Trend 2: Ransomware Payments are Decreasing, but...

But recovery still fails without a plan

Why Organizations Paid the Ransom



You Don’t Have to Pay – If You’re Ready

Call to action: Focus on what’s in your sphere of control

69%

Paid but were attacked **again**

IT operations must focus on what they can control

NIST Cybersecurity Framework

Govern **Identify** **Protect** Detect **Respond** **Recover**

Download the report
vee.am/RWT25

Non-Technical (ish) Post-Incident Advice

Cyber Insurance Policy

Hide this with the ultimate secrecy, if possible.

Credential Rotation

Is a must-do post-incident, now would be a good time to make this familiar.

Root Cause

Be prepared to find root cause but also be prepared to not be able to find it.

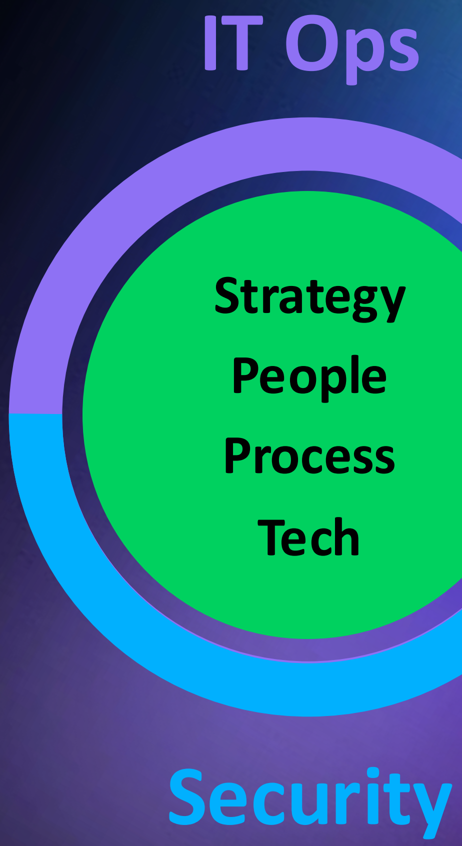
Section 03

Trend 3:
Collaboration Reinforces Resilience

Collaboration is the **Key to Success**

20-20 hindsight shows that significant improvement in collaboration is needed

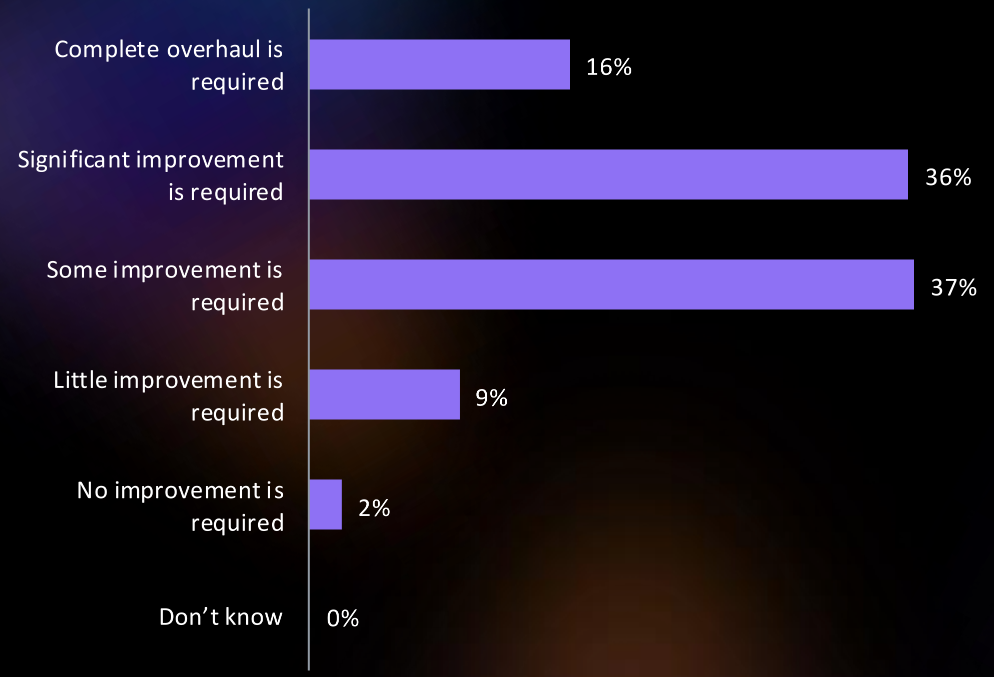
Download the report



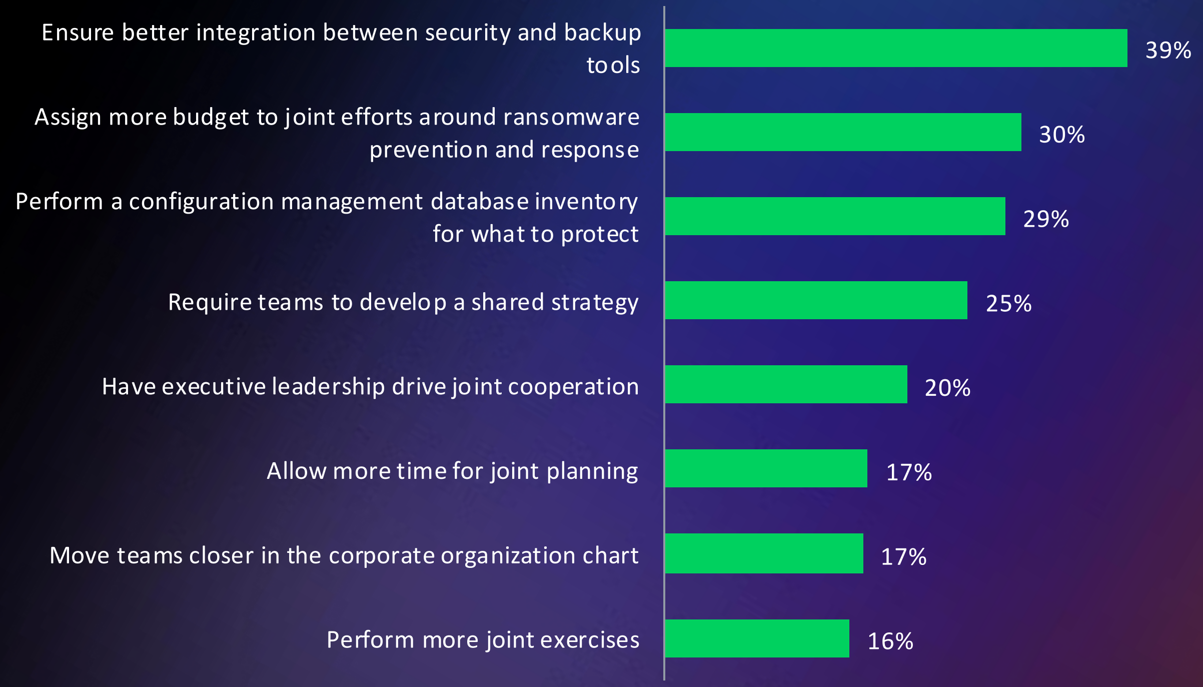
Collaboration is the Key to Success

20-20 hindsight shows that significant improvement in collaboration is needed

Level of Improvement Needed



Key Actions Needed



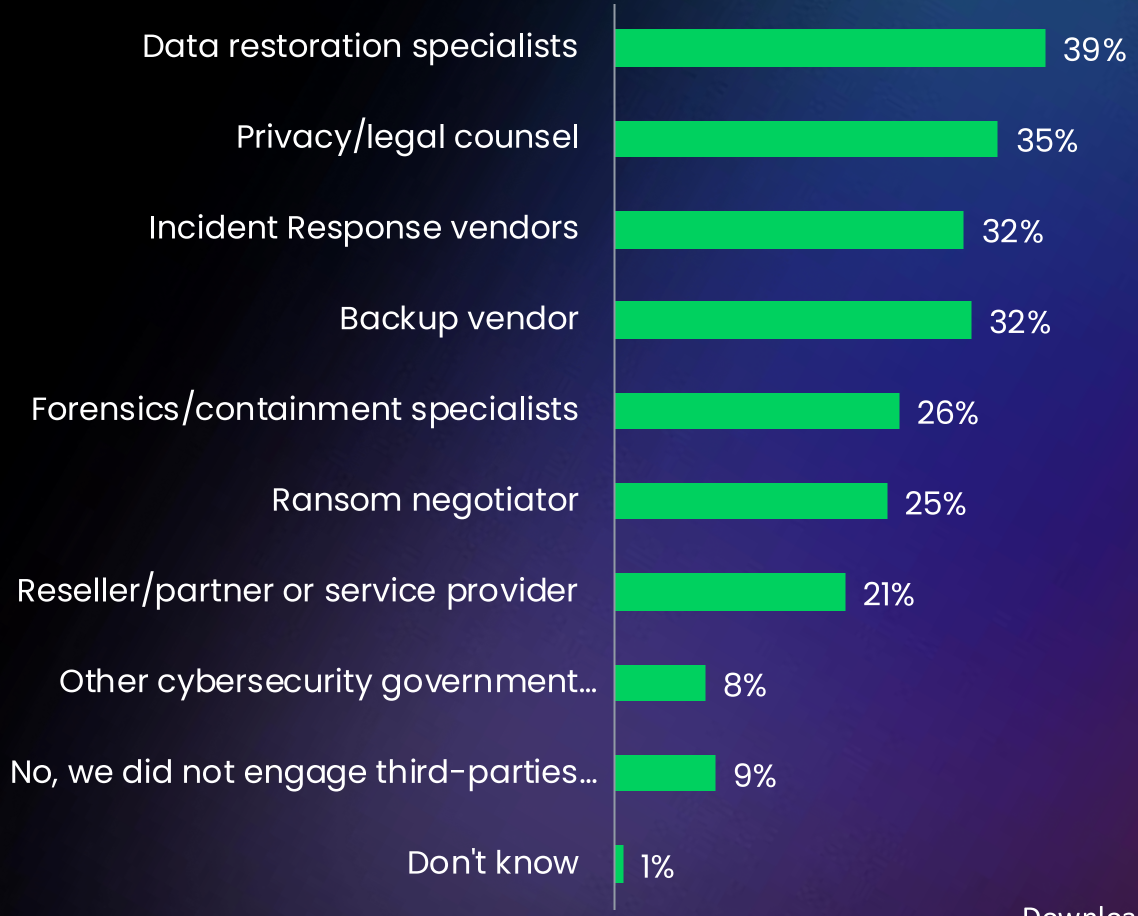
Download the report
vee.am/RWT25

Outside Expertise Plays

Most organizations are seeking some level of expertise across their goals

Most organizations rely on external experts for **ransomware remediation**.

Data restoration (**39%**), legal (**35%**), backup (**33%**), and incident response (**31%**) specialists are the most sought after.



Download the report
vee.am/RWT25

Section 03

Serious Chat: Actionable Insights for the Veeam Community

Playbook of Approaches: Pre-and Post-Attack

The elements most-often used by those who recover successfully (vs. their internal benchmarks)

Accountability

Successful organizations are less likely to hold individuals responsible – the industry is shifting to balance carrots and sticks.

Training/Awareness

Successful organizations were also more likely to bolster employee training and awareness, which can help mitigate social engineering attacks like phishing.

Pre-Defined Strategy

Only 26% of organizations have a determined plan for whether they'll pay ransom, notify law enforcement, etc.

Chain of Command

An in-place plan helps ensure proper authorization ladders and approvals for critical decisions during incident response.

Playbook of Approaches: Pre-and Post-Attack

The elements most-often used by those who recover successfully (vs. their internal benchmarks)

Software Updates

Organizations with documented and enforced software update policies reduced their risk.

Pen Testing

Organizations who execute penetration testing more frequently were better prepared.

Increased Budget

Organizations who have increased their spend on resilience (ops and security) have better outcomes – no surprise there!

Playbook for Successful Recoveries Post-Attack

The elements most-often used by those who recover successfully
(vs. their internal benchmarks)

67%
Verified backups and checked frequency regularly

59%
Ensure backup copies are clean prior to restore

46%
Alternate infrastructure arrangements

41%
Had containment or isolation plans in place

FROM RISK TO RESILIENCE

veeam Insights

Ransomware Trends and Proactive Strategies 2025

Download the full report – and share with
your cross-functional team!

Download the report

vee.am/RWT25