JANUS ASSOCIATES

Ransomware Readiness, Response, and Recovery

An Executive Brief for Organizational Resilience

By JANUS Associates

August 2026

JANUS Case Study

This executive brief delivers actionable guidance for cybersecurity leaders and IT professionals confronting ongoing threat of ransomware. It synthesizes the latest research, industry best practices, and real-world lessons to help organizations strengthen readiness, streamline incident response, and accelerate recovery. With authoritative references and practical recommendations, this guide equips experts to minimize risk, ensure resilience, and stay ahead of evolving ransomware tactics.

Table of Contents

Executive Summary

Ransomware remains one of the most pervasive and damaging threats facing organizations globally.

According to the 2026 Verizon Data Breach Investigations Report, 48% of all breaches now involve ransomware, with impacts extending well beyond IT, disrupting core business operations, creating regulatory requirement challenges, and damaging reputations[1].

Attackers have evolved from opportunistic encryption to highly coordinated campaigns involving data theft, double extortion, and extended operational paralysis[2]. In practice, the organizations that navigate ransomware incidents most effectively are not necessarily the ones with the most advanced tools, but the ones prepared for the reality that, sooner or later, an incident will occur.

Readiness, response, and recovery are often discussed as separate capabilities, but in real-world scenarios they are tightly interwoven. Gaps in preparation tend to surface quickly during response, and weaknesses in response often complicate recovery.

Readiness

Response

Recovery

The Evolving Ransomware Threat

Ransomware threat actors have become more sophisticated, often employing **advanced persistent threat (APT) tactics**. Attackers often remain undetected for extended periods, using techniques such as **living-off-the-land (LOTL)**, privilege escalation, and lateral movement to maximize damage and data exfiltration before launching an attack[3][4].

Initial access still frequently comes down to familiar issues: **phishing, exposed remote access services, and unpatched vulnerabilities**. What has changed is what happens next, an ever more dangerous scenario.

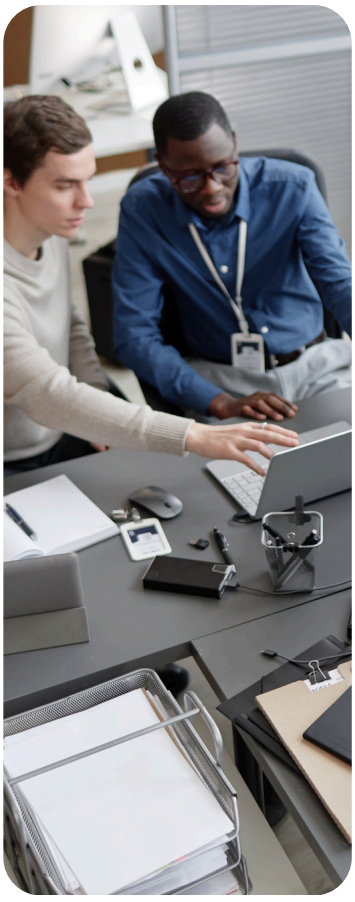
Once inside, attackers tend to move laterally in ways that blend in with normal administrative activity, making early detection harder than many organizations expect.

The impact of these incidents is rarely limited to only IT systems. **Operational downtime, missed service commitments, regulatory exposure,** and **reputational damage** often become the primary concern within hours of an attack.

At that point, the conversation shifts quickly from “what happened” to “how long can we operate like this,” which is where preparation, or the lack of it, becomes very visible.

Readiness: Building a Strong Defensive Foundation

Many organizations already have several of the right controls in place on paper. The challenge is ransomware incidents tend to expose where those controls are incomplete, inconsistently applied, or not tested under realistic conditions.



Robust identity and access management, especially enforcing multi-factor authentication (MFA) for all remote and privileged access, is one of the most effective defenses against initial compromise[5].

Rapid vulnerability management and regular on-time patching are also essential, with special emphasis on internet-facing assets and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) maintains a catalog of known exploited vulnerabilities that should be regularly monitored and prioritized[6].

Endpoint detection and response (EDR) solutions provide critical visibility for early detection, but they must be properly configured, continuously monitored, and regularly tested. Automated alerting, threat intelligence integration, and incident response playbooks greatly enhance EDR effectiveness[7].

Backups are essential, but their value depends on isolating them from the production environment (for example, using immutable storage or offline backups[8]) and conducting regular, comprehensive restoration tests. The National Cyber Security Center (NCSC) recommends periodic verification and air-gapped solutions to ensure recoverability[9].

User awareness also plays a larger role than many organizations expect. While training alone will not stop a determined attacker, timely reporting of suspicious activity has made the difference in more than one incident by allowing containment before widespread impact.

Response: Acting Decisively During an Incident

When ransomware is detected, the first challenge is often not technical; it is organizational. Teams need to shift quickly from normal operations to incident response mode, and that transition is rarely seamless without prior preparation.

1. One priority is establishing a clear picture of what is actually happening. This sounds straightforward, but in practice it is often complicated by incomplete visibility, conflicting alerts, or assumptions made too early. Taking the time to confirm the scope of affected systems and determine whether data exfiltration has occurred is critical, even under pressure.

2. Containment actions need to be taken quickly, but they also need to be coordinated. Isolating systems, disabling accounts, and restricting network access can limit the spread of the attack, but uncoordinated actions can also disrupt business operations in unintended ways. Striking that balance is one of the more difficult aspects of response and is where experienced leadership makes a noticeable difference.

3

As the situation stabilizes, attention shifts toward removing the attacker's access and understanding how the environment was compromised. This is where many organizations realize that the initial point of entry was only part of the issue. Persistence mechanisms, credential exposure, and lateral movement often need to be addressed before the environment can be considered stable.

Communication must be structured and role-based throughout the response. Leadership requires timely updates to guide operational and legal decisions, while public relations and regulatory communications should follow pre-established procedures to minimize risk and misinformation.

Engagement with law enforcement (such as the FBI or national cybersecurity agencies) is strongly recommended, particularly for incidents involving data breaches or critical infrastructure, as outlined in CISA and NCSC guidance[10][11].

Organizations should address ransom payment in advance through policy, legal counsel, and insurance carrier requirements. Authorities such as the U.S. Department of the Treasury discourage payment due to legal and ethical risks, and research shows that paying a ransom does not guarantee data recovery or prevent further extortion[12][13].

Recovery: Restoring Operations and Strengthening Resilience

Recovery is often assumed to be the straightforward part: restore systems, bring operations back online, and move forward. It is, however, frequently more complex than the response phase.

The first challenge is ensuring the environment is fully prepared for restoration. Bringing systems back online too quickly, without confirming that the threat has been completely removed, can result in reinfection or continued attacker access. This is why recovery needs to be closely coordinated with the teams responsible for eradication and investigation.

Restoration itself often reveals gaps that were not obvious beforehand. Dependencies between systems, undocumented configurations, and incomplete backup coverage can all slow down recovery efforts. In many cases, organizations discover that restoring a single system is relatively straightforward, but restoring an entire business process requires significantly more coordination.

Prioritization is critical. Focus on restoring essential business functions first, guided by a **business impact analysis (BIA)** and **predefined recovery time objectives (RTOs)** as recommended by NIST SP 800-34[14]. Restoring all systems simultaneously can cause unnecessary delays and complications.

Post-restoration, organizations should enforce heightened monitoring and threat hunting to detect lingering threats or reinfection attempts. **Leveraging endpoint telemetry, network analytics, and forensic reviews** is considered best practice for validating eradication efforts and ensuring a secure return to operation [15].

The post-incident review is where many of the long-term benefits of an incident are realized, assuming it is done thoroughly. This is where organizations move beyond identifying what failed and begin to understand why. In practice, this often includes gaps in visibility, delays in escalation, unclear roles during response, or overreliance on controls assumed to be effective but not.

Most organizations make meaningful improvements after a ransomware incident, but the ones that gain the most value treat recovery as an opportunity to make targeted, lasting changes. This may include **tightening access controls, improving backup isolation, refining detection capabilities**, or **clarifying decision-making processes during incidents**.

Conclusion

Ransomware is not a theoretical risk, and it is not a problem that technology alone can solve. It is a business risk that requires coordination across technical teams, leadership, and operational stakeholders.

Organizations best positioned to respond are those that regularly test their incident response plans, conduct tabletop exercises, and perform red team assessments to validate security assumptions. Continuous improvement, driven by post-incident reviews and lessons learned, is essential for long-term resilience[16]. That level of preparation does not eliminate the risk of ransomware, but it does significantly reduce the likelihood that an incident will escalate into prolonged disruption. In an environment where attacks are increasingly common, that distinction matters.

Why Partner with JANUS

About Us

Our expert team helps organizations reduce cyber risk through independent cybersecurity, compliance, and privacy consulting.

Since 1988, clients have trusted JANUS for executive-ready cyber insights, vulnerability assessments, actionable gap analyses, and practical plans their teams can execute. JANUS's role is to provide clear, independent guidance that strengthens resilience before an incident and supports sound decision-making when pressure is highest.

For ransomware readiness engagements, JANUS does more than identify gaps. The firm helps clients translate assessment findings into a structured cyber risk strategy, including:

- Risk registers and remediation roadmaps
- NIST CSF and CIS Controls alignment
- IT risk assessments and compliance audit readiness
- Vulnerability management and advanced penetration testing
- Cloud security and identity-control reviews
- Incident response planning, tabletop exercises, and digital forensics support
- Business continuity and recovery planning
- Ongoing managed security services and program maturity support

Ransomware readiness should be tested before an incident occurs. JANUS can help your organization build a prioritized, framework-aligned plan for stronger cyber resilience, compliance confidence, and operational continuity.

Remove Risk By Adding JANUS

Contact Us Today

PHONE

+1(203)251-0200

EMAIL

INFO@JANUSASSOCIATES.COM

WEBSITE

JANUSASSOCIATES.COM

References

1. Verizon Data Breach Investigations Report 2026 {https://www.verizon.com/business/resources/reports/dbir/}
2. Coveware Ransomware Quarterly Reports {https://coveware.com/category/quarterly-report/}
3. MITRE ATT&CK Framework {https://attack.mitre.org/}
4. CrowdStrike Global Threat Report 2026 {https://go.crowdstrike.com/2026-global-threat-report.html}
5. NIST SP 800-53: Security and Privacy Controls {https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final}
6. CISA Known Exploited Vulnerabilities Catalog {https://www.cisa.gov/known-exploited-vulnerabilities-catalog}
7. Gartner Insights Abstract Effective Strategies to Mitigate Attacks on Endpoint Detection and Response (EDR) {https://www.gartner.com/en/documents/7064698}
8. JANUS Case Study: Immutable Backups {https://info.janusassociates.com/hubfs/Case%20Studies/JANUS%20Case%20Study%20-%20Immutable%20Backups%20for%20Healthcare%20Provider%20Cyber%20Resilience.pdf}
9. NCSC: Ransomware Guidance for Organizations {https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks}
10. CISA Ransomware Response Checklist {https://www.cisa.gov/ransomware-response-checklist}
11. NCSC Incident Management Guidance {https://www.ncsc.gov.uk/collection/incident-management}
12. U.S. Department of Treasury: Ransomware Advisory {https://ofac.treasury.gov/recent-actions/20201001}
13. Sophos State of Ransomware 2026 {https://www.sophos.com/en-us/blog/sophos-state-of-ransomware-2026}
14. NIST SP 800-34: Contingency Planning Guide {https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final}
15. SANS Institute: Incident Handler's Handbook {https://www.sans.org/white-papers/33901}
16. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile {https://csrc.nist.gov/pubs/sp/800/61/r3/final}