White Paper

halcyon

What Boards Of Directors Must Know About Ransomware

BY GARY HAYSLIP | CISO, AUTHOR & CYBERSECURITY EXECUTIVE

Ransomware is no longer a disruptive IT incident contained within the walls of the security operations center. It has become a defining enterprise risk, one capable of halting operations, destroying customer trust, triggering regulatory scrutiny, and erasing significant shareholder value, sometimes simultaneously. Boards of Directors who still treat ransomware as a technology problem to be managed by the CISO are dangerously exposed.

The threat landscape has shifted irrevocably. What began as opportunistic attacks against poorly secured systems has evolved into a multi-billion-dollar criminal industry characterized by AI-enhanced reconnaissance, coordinated extortion, and supply-chain compromise at scale. As stewards of corporate value, boards must govern ransomware risk with the same rigor applied to financial, operational, and regulatory threats. That starts with understanding how this threat has evolved and what it costs the business when it lands.

How Ransomware Has Evolved in the Age of AI

The ransomware ecosystem has begun to be transformed by the addition of artificial intelligence. Several aspects of this ongoing change were documented in the recently published report by Halcyon's Threat Research Center titled, "*How AI is (and is Not) Changing Ransomware*." Criminal enterprises now operate with the efficiency, specialization, and scalability of sophisticated technology companies. Boards must understand what this means in practical terms.

AI-Driven Reconnaissance and Targeting

Threat actors are no longer guessing. They use large-scale data scraping, credential harvesting, and behavioral analytics to identify the highest-value targets within an organization; including which systems to encrypt, which executives to impersonate, and which data to steal for maximum leverage. Time-to-compromise has been dramatically reduced, and the precision of attacks has increased proportionally.

Automated Phishing and Executive Impersonation

Generative AI has made phishing attacks nearly indistinguishable from legitimate communications. Criminals deploy perfectly localized phishing campaigns, real-time voice cloning, and deepfake video of senior executives to try and social engineer authorized fraudulent wire transfers, credential disclosures, or system access. These attacks consistently bypass traditional awareness training because they are not generic but tailored, contextually aware, and devastatingly convincing.

Autonomous Malware and Rapid Lateral Movement

Once inside a network, AI-enhanced malware identifies domain controllers, backup repositories, ERP systems, and operational technology with minimal human intervention. What previously took attackers days or weeks to achieve manually now happens in minutes to hours. By the time detection occurs, the damage may already be done, and the attackers have left the building with your data.

Double and Triple-Extortion Business Models

Encryption alone is no longer the primary weapon. Modern ransomware operations are designed to extract maximum leverage by simultaneously encrypting systems, stealing sensitive data, and threatening to expose that data publicly or directly contacting customers, investors, and regulators. In many incidents, operational disruption becomes secondary to the reputational blackmail. Organizations that believe their backups will protect them are only solving one-third of the problem.

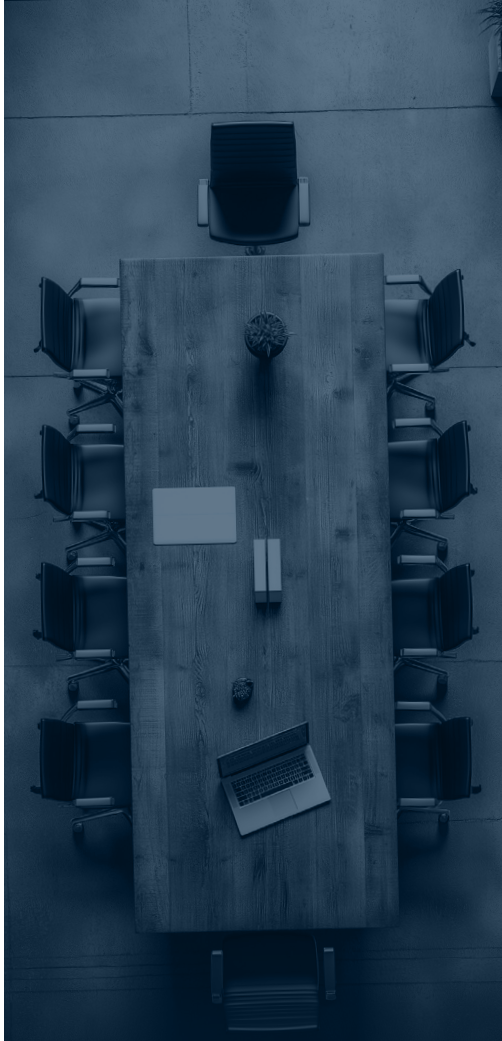
Criminal enterprises now operate with the efficiency, specialization, and scalability of sophisticated technology companies. Boards must understand what this means in practical terms.

The True Business Impact: Beyond the Ransom Demand

Boards must internalize that ransomware is a multi-dimensional business crisis, not a technical failure. The ransom itself is often the smallest line item in the total cost of an incident. Consider what a serious ransomware event looks like:

Impact Area	Business Consequences
Operations	Shutdown of critical services, supply-chain delays, and complete halt in revenue generation.
Financial	Ransom payments, regulatory fines, legal fees, soaring insurance premiums, and class-action litigation.
Brand & Market Confidence	Loss of customer trust, equity devaluation, and sustained negative media coverage.
Regulatory & Legal Exposure	Data breach notification obligations, shareholder litigation, and regulator required material incident reporting.
Customers & Partners	Data theft, service disruptions, and unsafe product outcomes; especially critical in healthcare, IoT, and autonomous systems.

These are not hypothetical outcomes. They are the documented aftermath of incidents at Colonial Pipeline, MGM Resorts, Change Healthcare, CDK Global, and dozens of other organizations that experienced ransomware in the last several years. The common thread: in every case, the board was left responding to a crisis that better governance could have anticipated and mitigated.



Boards must internalize that ransomware is a multi-dimensional business crisis, not a technical failure.

What Boards Should Be Asking

Effective cybersecurity governance is not about micromanaging security operations. It is about asking the right questions and demanding answers that are business-focused, quantifiable, and honest. If your executive team cannot answer these questions clearly, that is itself a material risk.

Strategic Alignment and Risk Posture

- How does our ransomware resilience plan align with our overall business strategy and stated risk appetite?
- Which critical business processes would face immediate shutdown if we were compromised today?
- Do we have quantified risk metrics that translate potential ransomware scenarios into financial impact estimates?
- When did our board last receive a ransomware-specific risk briefing, and was it tied to actual business outcomes rather than technical controls?

Operational Readiness and Recovery

- How quickly can we detect, isolate, and recover from a ransomware campaign under current capabilities?
- Have we tested our incident response and recovery plans within the last twelve months; including a full tabletop exercise at the executive level?
- Are our backups immutable, segmented from production environments, and verifiably recoverable at scale?
- Do we understand the level of effort required to conduct backup recovery for our networks at scale if required and how it would impact current business operations?
- Can we restore critical systems without paying a ransom, and how long would a complete operational recovery realistically take?

AI Risk and Threat Evolution

- How are adversaries likely to leverage AI specifically against our environment, our industry, and our supply chain?
- Are we deploying AI defensively to improve detection, containment, and recovery as part of our business resilience plan? If not, do we have a roadmap for doing so?
- What governance exists to prevent misuse of AI within our own organization that could introduce new attack surfaces?

Effective cybersecurity governance is not about micromanaging security operations. It is about asking the right questions and demanding answers that are business-focused, quantifiable, and honest.

Third-Party and Supply-Chain Exposure

- How are we evaluating the ransomware risk inherited through our vendors, suppliers, and technology partners?
- Do our contracts include explicit notification timelines, liability clauses, and data-handling requirements in the event a vendor is compromised?
- Have we validated the recovery capabilities of our most critical suppliers?

Questions Boards Must Ask Directly of the CISO

The board's relationship with the CISO is one of the most consequential governance dynamics in modern enterprise security. Boards should not simply receive reports from the CISO, they should demand a candid, metrics-driven dialogue. The following questions are examples of ones that should be asked directly, and the answers should be clear, specific, and actionable.

On Detection and Response:

- What tools, telemetry, and AI capabilities are in place for real-time threat detection and behavioral anomaly identification?
- How do we monitor for data exfiltration in progress, and what is our current mean-time-to-detect?
- What decisions during a ransomware incident require board involvement, and has that protocol been documented and rehearsed?

On Vulnerabilities and Attack Surface:

- What are the top ransomware attack vectors currently threatening our organization, and how are we actively reducing exposure?
- Do we maintain a complete, current inventory of legacy and unpatched systems and is there a prioritized remediation plan with executive accountability?
- How are we addressing the risks of credential theft, phishing success rates, and lateral movement within our environment?

On Recovery Confidence:

- If we were hit tomorrow, could we restore critical systems without paying the ransom and how long would it take?
- Are our backup systems isolated from potential domain compromise?
- Have our recovery plans been independently validated, not just internally reviewed?

Boards should not simply receive reports from the CISO, they should demand a candid, metrics-driven dialogue.

If the answers to these questions are vague, exclusively technical, or absent of measurable outcomes then that should be treated as a governance gap. Boards should treat unclear answers the same way an audit committee treats unclear financial disclosures: with urgency and a request for an immediate improvement plan.

What Boards Must Do Now

It is essential to understand a threat, but that's not enough. Boards must also take deliberate steps to ensure their organizations can withstand and recover from ransomware attacks.

1. Treat Ransomware as an Enterprise Risk, Not just an IT Problem

Integrate cybersecurity into financial, operational, and strategic governance frameworks. Ransomware risk should appear on the enterprise risk register alongside financial risk, supply-chain risk, and regulatory exposure with the same ownership and reporting cadence.

2. Fund Capabilities That Reduce Impact

Boards must ensure the organization is investing in the right defensive capabilities. Prioritize funding for:

- Zero-trust identity and access management architectures
- Anti-ransomware resilience platforms with autonomous detection and containment
- Network segmentation and micro-perimeters to limit lateral movement
- Managed Detection and Response (MDR) with 24/7 coverage
- Immutable, air-gapped cloud backup with validated recovery capabilities

3. Demand Rehearsed Playbooks and Participate in Them

Tabletop exercises and crisis simulations should include board members, not just the security team. Boards need to understand their role in a ransomware crisis: when to communicate with investors, when to engage legal and law enforcement, and how to make time-sensitive decisions under adversarial pressure. Governance that only activates during a crisis has already failed.

4. Establish Shared Accountability Across the Leadership Team

Security is not the CISO's problem alone. The CFO owns the financial risk and recovery budget. The COO owns operational continuity. Legal owns regulatory response and disclosure. HR owns a part of insider threat and workforce resilience. Product and Engineering own secure architecture. Boards should confirm that ransomware accountability is distributed across the executive team and that no single leader is isolated with the full weight of a crisis.

It is essential to understand a threat, but that's not enough. Boards must also take deliberate steps to ensure their organizations can withstand and recover from ransomware attacks.

Final Thoughts

Ransomware is evolving faster than traditional defenses can keep pace. With AI-enhanced attacks, multi-extortion business models, and supply-chain compromise as standard playbook entries, organizations that are not investing in resilience are not simply lagging, they are accepting an asymmetric level of risk that their stakeholders have not been told about.

Boards that embrace their governance role in cybersecurity will do more than protect operations. They will build the stakeholder trust, brand resilience, and long-term continuity that define enduring enterprise value. The question is not whether a ransomware campaign will be attempted against your organization. The question is whether your organization is prepared to absorb the impact, respond decisively, and continue to operate.

In the infinite game of cybersecurity, the goal is not to eliminate adversaries but to ensure you are still standing and still playing when they come.

In the infinite game of cybersecurity, the goal is not to eliminate adversaries but to ensure you are still standing and still playing when they come.

About the Author

Gary Hayslip is a CISO, cybersecurity executive, and co-author of the CISO Desk Reference Guide Series. He has led security programs for federal agencies, global enterprises, and high-growth technology companies. He currently serves as a CISO in Residence at Halcyon.ai and is a frequent speaker on cybersecurity strategy, board governance, and executive leadership.

What Governance Requires. What Halcyon Delivers.

Halcyon is the first dedicated anti-ransomware platform, purpose-built to detect, disrupt, and defeat ransomware at every stage of the attack lifecycle–from pre-execution through data exfiltration to encryption key material capture and rapid recovery. Unlike general-purpose security tools adapted for ransomware, Halcyon was architected from the ground up to address the specific threat boards are now being asked to govern.

Every Halcyon deployment includes the Ransomware Operations Center (ROC), a 24/7 team of ransomware specialists who monitor, investigate, and respond to threats on behalf of customers–at no additional cost. The ROC handles what security teams cannot build internally: around-the-clock expert coverage, active threat eviction, and recovery support the moment an attack is detected.

The Halcyon Ransomware Warranty formalizes the outcome boards need to be able to report: if an attack succeeds despite Halcyon's protection, expert responders engage within 120 minutes–guaranteed–with full incident response and recovery support until operations are restored.

For boards that have asked their CISO the questions in this white paper and want to know what purpose-built ransomware defense actually looks like, Halcyon is the answer.

Ready to see what purpose-built ransomware defense looks like?
Schedule a briefing with a Halcyon ransomware expert.

halcyon.ai/get-a-demo