

FROM DEFENCE TO RESILIENCE:

A STRATEGIC FRAMEWORK FOR RANSOMWARE PREPAREDNESS



Executive Summary

The ransomware threat landscape has fundamentally transformed from opportunistic attacks into a sophisticated, industrialised ecosystem of criminal enterprise. Traditional cybersecurity paradigms centred on prevention, detection, and response are proving insufficient against adversaries who have professionalised extortion into a repeatable business model.

This whitepaper examines why organisations must evolve beyond conventional defence strategies toward comprehensive resilience frameworks that assume compromise and prioritise operational continuity.

Core to Cloud's strategic collaboration with Halcyon represents a pivotal evolution in how organisations can approach ransomware risk. By integrating purpose-built anti-ransomware capabilities with human-led security operations, vendor-agnostic architecture, and ISO 27001-aligned governance, this partnership delivers what modern enterprises require: the ability not merely to defend against ransomware, but to survive, recover, and maintain business operations in the face of inevitable attacks.

This paper explores the current threat environment, the limitations of traditional approaches, and a comprehensive framework for building genuine ransomware resilience across prevention, detection, response, and recovery domains.



The Ransomware Inflection Point

Across all industries but in particular retail, logistics, finance, healthcare, and the public sector, organisations face an adversary unlike any in cybersecurity history. Ransomware has evolved from isolated incidents perpetrated by individual threat actors into a mature criminal industry characterised by specialisation, innovation, and relentless targeting of organisations regardless of size, sector, or geography.

The statistics paint a sobering picture. Successful ransomware attacks have increased by 104 percent over the past two years, according to recent threat intelligence research. However, the raw numbers only tell part of the story. What has changed more profoundly is the nature of the attacks themselves: sophisticated double and triple extortion tactics, targeting of backup systems, exploitation of legitimate management tools, and increasingly aggressive operational tempo.

Traditional cybersecurity approaches, built on the foundation of "prevent, detect, respond," were designed for a different era. They assume that with sufficient investment in preventative controls and detection capabilities, organisations can keep threats at bay. This assumption no longer holds. Even organisations with mature security programmes, best-in-class endpoint protection, and comprehensive backup strategies find themselves vulnerable to adversaries who have specifically engineered their tactics to bypass these very controls.

The question facing security leaders today is not whether their organisation will face a ransomware attack, but when it will occur and whether the organisation can survive, recover, and continue operating when it does. This fundamental shift requires a corresponding evolution in strategy: from defence-focused to resilience-oriented security architecture.

At Core to Cloud, our mission has always centred on delivering human-led, vendor-agnostic cyber services with genuine incident ownership. Our strategic collaboration with Halcyon extends this mission into a domain where it matters most: ensuring organisations can withstand the most destructive form of cyberattack in existence today.



Understanding the Modern Ransomware Threat

Ransomware as an Industrialised Business Model

Modern ransomware operations bear little resemblance to the opportunistic attacks of the past decade. Today's threat landscape is characterised by:

Professionalisation and Specialisation: Ransomware groups operate with the structure and efficiency of legitimate businesses. They employ specialists in network infiltration, lateral movement, data exfiltration, negotiation, and even customer service. The Ransomware-as-a-Service (RaaS) model has lowered barriers to entry while increasing the sophistication of attacks through specialisation.

Well-Funded Operations: Successful ransomware groups reinvest their proceeds into research and development, acquiring zero-day vulnerabilities, developing custom tooling, and recruiting talented individuals. This creates a positive feedback loop where success breeds further capability.

Sophisticated Targeting and Reconnaissance: Rather than spray-and-pray approaches, modern ransomware operators conduct extensive reconnaissance, identifying high-value targets, mapping their networks, understanding their business operations, and timing attacks for maximum impact. They research organisations' cyber insurance policies, revenue figures, and incident response capabilities to calibrate ransom demands.

Boldness and Aggression: Ransomware groups increasingly target critical infrastructure, healthcare facilities during crises, and public sector organisations, demonstrating a willingness to cause societal harm in pursuit of profit. Their operational tempo is unrelenting, with major groups launching multiple attacks simultaneously.



The Evolution to Multi-Stage Extortion

The attack methodology itself has evolved significantly:

Stage One: Initial Access and Persistence: Attackers gain entry through phishing, credential stuffing, vulnerability exploitation, or trusted vendor compromise. They establish persistent access through multiple backdoors, often maintaining presence for weeks or months before activation.

Stage Two: Privilege Escalation and Lateral Movement: Using a combination of legitimate administrative tools and custom malware, attackers move laterally across networks, elevating privileges and mapping the environment to identify critical systems, backup infrastructure, and valuable data repositories.

Stage Three: Data Exfiltration: Before encryption begins, attackers systematically exfiltrate sensitive data, intellectual property, customer information, financial records, and anything else that could be used for extortion. This establishes a second lever of coercion independent of encryption.

Stage Four: Backup Destruction: Sophisticated attackers specifically target backup systems, shadow copies, disaster recovery infrastructure, and offline backups to maximise leverage and eliminate recovery options.

Stage Five: Encryption and Extortion: Only after establishing complete control and eliminating recovery paths do attackers execute encryption. The ransom demand now carries dual threats: pay to decrypt systems and pay to prevent data publication.

Stage Six: Double and Triple Extortion: Beyond encrypting systems and threatening data publication, attackers increasingly contact customers, partners, and regulators directly, threatening to release their data unless additional payments are made. Some groups now target supply chains, demanding payment from both the compromised organisation and its business partners.



Why Conventional Approaches Struggle

Traditional security controls face several fundamental challenges against modern ransomware:

Endpoint Protection Limitations: While endpoint detection and response (EDR) solutions are essential components of security architecture, they face inherent limitations. Ransomware operators specifically test their malware against common EDR platforms, developing techniques to evade detection through legitimate tool abuse, living-off-the-land tactics, and carefully timed execution. EDR solutions designed to address a broad spectrum of threats may not provide the specialised focus required for ransomware's unique kill chain.

Backup Vulnerabilities: Organisations invest heavily in backup infrastructure under the assumption that data availability guarantees recovery. However, modern ransomware specifically targets backups through several vectors. Attackers compromise backup credentials, exploit integration between production and backup environments, encrypt backup repositories themselves, or simply ensure sufficient dwell time to corrupt backup integrity through normal backup cycles. Even air-gapped backups face challenges from the time required to restore operations and validate data integrity.

The Detection-to-Impact Window: The timeline from detection to operational impact has compressed dramatically. Where organisations once had hours or days to respond, modern ransomware can achieve domain-wide encryption in minutes. This compressed timeline often renders traditional incident response processes ineffective, as by the time security teams confirm an alert and initiate response protocols, encryption is already complete.

Human Element Challenges: Security operations centres face alert fatigue, staffing challenges, and the difficulty of distinguishing sophisticated ransomware preparation activities from legitimate administrative actions. The human element, while essential, introduces delays and potential for error at precisely the moments when speed and accuracy matter most.

The Ransomware Gap: Why Traditional Controls Fall Short

Defining the Ransomware Gap

Research into ransomware success rates reveals a troubling reality: despite massive investment in cybersecurity controls, a significant "ransomware gap" persists between theoretical protection and actual resilience.

The ransomware gap represents the disconnect between what organisations believe their security investments protect against and the reality of their ability to prevent, detect, respond to, and recover from ransomware attacks. This gap manifests in several dimensions:

Prevention Gap: The belief that perimeter security, endpoint protection, and access controls will prevent ransomware entry versus the reality that determined adversaries will find a path in through social engineering, zero-day exploitation, or supply chain compromise

Detection Gap: The assumption that security monitoring and EDR will identify ransomware activity in time to prevent damage versus the reality that sophisticated attacks use legitimate tools and credentials that blend with normal administrative activity.

Response Gap: The expectation that incident response procedures will contain and remediate ransomware versus the reality that response timelines exceed attack execution speed.

Recovery Gap: The confidence that backups and disaster recovery plans will restore operations versus the reality that backup compromise, data integrity questions, and restoration timelines create extended downtime.

Assurance Gap: The belief that security investments have adequately addressed ransomware risk versus the inability to provide board-level confidence in the organisation's ability to survive and recover from an attack.



Why General-Purpose Security Tools Struggle with Ransomware

Security solutions claim they protect organisations from ransomware, yet ransomware attacks continue to succeed at an unprecedented pace. The fundamental issue is one of focus and design philosophy. Most security solutions are architected to address a wide range of threats: malware, phishing, data loss, insider threats, advanced persistent threats, and countless other attack vectors. This breadth necessarily creates trade-offs in depth.

Ransomware requires a different approach because it represents a unique threat with a specific, recognisable kill chain. From pre-execution behaviours through data exfiltration to encryption, ransomware attacks follow patterns that, when properly understood and monitored, can be detected and disrupted. However, this requires purpose-built capabilities focused exclusively on the ransomware kill chain rather than generalised threat detection.

The Limitations of "Essential but Not Enough"

Traditional endpoint protection and backup solutions remain essential components of security architecture. They are necessary but not sufficient. EDR provides visibility into endpoint activity, detects many forms of malware, and supports investigation and remediation. Backups provide data durability and recovery options. However, neither was designed with modern ransomware's dual-pronged approach in mind.

The challenge is that acknowledging something is "essential but not enough" requires organisations to think beyond checkbox compliance and layered defence in depth. It requires accepting that even with every recommended control in place, a determined ransomware adversary can still succeed. This acceptance is the first step toward genuine resilience.

Understanding Resilience in the Ransomware Context

The evolution from defence-focused to resilience-oriented cybersecurity represents more than semantic distinction. It reflects a fundamental shift in strategic thinking, investment priorities, and organisational culture around cybersecurity risk.

Resilience, in the context of ransomware, means the ability to:

- **Anticipate:** Understanding that ransomware attacks will occur and proactively identifying vulnerabilities, attack paths, and recovery challenges before they are exploited
- **Withstand:** Maintaining critical business operations even during active attack execution and immediate aftermath
- **Recover:** Restoring full operational capability within acceptable timeframes without succumbing to extortion
- **Adapt:** Learning from incidents and near-misses to continuously improve defensive posture and recovery capabilities

Resilience assumes compromise. Rather than investing solely in preventing breaches, resilient organisations invest equally in their ability to function when prevention inevitably fails. This shift has profound implications for architecture, investment, and governance.



The Three Pillars of Ransomware Resilience

A comprehensive ransomware resilience framework rests on three interconnected pillars:

Pillar One: Prevent

Risk reduction through security hardening, architecture design, continuous vulnerability management, and regular testing remains foundational. This includes:

- Identity and access management with least privilege principles
- Network segmentation to limit lateral movement
- Application allowlisting blocking unauthorised executables
- Restrict and monitor system tools to prevent misuse of legitimate utilities
- Vulnerability management and patching cadence
- Security awareness and phishing-resistant authentication
- Autonomous penetration testing and red team exercises
- Attack surface reduction

However, prevention alone is insufficient. The goal shifts from "preventing all attacks" to "making attacks more difficult, costly, and time-consuming" while buying time for detection and response.

Pillar Two: Detect and Respond

Human-led threat hunting, 24/7 security operations, rapid incident response, and vendor-agnostic monitoring provide the detection and response capabilities necessary to identify ransomware activity and initiate containment. Key elements include:

- 24/7 security operations centre with human threat hunters
- Vendor-agnostic SIEM and security orchestration
- Behavioural analytics focused on ransomware kill chain indicators
- Exfiltration detection that flags massive data transfers and suspicious C2 activity
- Rapid incident response protocols with clear ownership
- Key material capture of asymmetric encryption keys
- Identification of EDR tampering, blinding or bypassing
- Integration across cloud and on-premises environments
- Continuous threat intelligence integration

Detection and response buy time and limit damage, but they cannot guarantee prevention of all encryption or data exfiltration.

Pillar Three: Recover and Resilient Operation

This pillar represents where many organisations fall short. Recovery and resilient operation requires:

- Ransomware-specific recovery capabilities that function even when backups are compromised
- Warranty-backed assurance that provides financial and operational guarantees
- Recovery time objectives measured in hours, not days or weeks
- Validation of data integrity and completeness post-recovery
- Continuity of critical business functions during recovery
- Documentation and evidence preservation for legal and insurance purposes

The integration of these three pillars creates genuine resilience: layered prevention to increase attacker cost, detection and response to limit damage and preserve evidence, and recovery capabilities that ensure business continuity regardless of attack success.

Why Resilience Matters Now: The Convergence of Pressures

Several forces have converged to make ransomware resilience a strategic imperative:

Regulatory Pressure: Regulators across sectors increasingly expect organisations to demonstrate not just compliance with security standards, but genuine cyber resilience. Incident disclosure requirements, mandatory breach notifications, and regulatory scrutiny following incidents create compliance risk that extends beyond the immediate attack impact.

Cyber Insurance Evolution: The cyber insurance market has matured rapidly in response to ransomware losses. Insurers now conduct detailed assessments of ransomware preparedness, require specific controls as prerequisites for coverage, and increasingly refuse coverage or dramatically increase premiums for organisations unable to demonstrate resilience. Insurance is shifting from a safety net to a validation mechanism for security investment.

Board and Executive Accountability: Boards of directors face increasing scrutiny over cyber risk governance. Directors are asking harder questions: How long can we operate if systems are encrypted? What is our recovery time objective? What assurance do we have that our investments will protect us? Security leaders must provide board-ready answers, not technical explanations.

Reputational and Competitive Impact: Ransomware incidents that result in extended downtime, data breaches, or publicised ransom payments create lasting brand damage. In competitive markets, the inability to serve customers or protect their data can result in permanent market share loss. For public sector organisations, ransomware can undermine public trust and confidence in service delivery.

Financial Materiality: The direct costs of ransomware extend far beyond potential ransom payments. Business interruption, incident response, forensic investigation, legal fees, regulatory penalties, customer notification, credit monitoring, system restoration, and long-term security improvements can exceed tens of millions of pounds. For smaller organisations or those operating on thin margins, a major ransomware incident can threaten organisational viability.

For regulated sectors especially, finance, healthcare, and the public sector, the cost of downtime, data loss, or extortion is no longer simply financial. It is reputational, regulatory, and potentially existential. Board members now demand to know: How long can we stay down? How fast can we recover? What happens if extortion occurs even after we've detected and contained encryption?

The Core to Cloud and Halcyon Strategic Framework

The collaboration between Core to Cloud and Halcyon represents a synthesis of complementary capabilities designed to address the full spectrum of ransomware resilience.

Core to Cloud's Foundation: Human-Led, Vendor-Agnostic Security Operations

Core to Cloud has built its reputation on several foundational principles:

Human-Led Detection and Response: While automation and machine learning provide essential capabilities, human expertise remains irreplaceable for threat hunting, context-aware decision-making, and incident ownership. Our security operations centre combines advanced tooling with experienced analysts who understand the business context behind security alerts.

Vendor-Agnostic Architecture: Technology ecosystems are heterogeneous by necessity. Organisations use Azure and AWS, Microsoft Sentinel, various EDR platforms, and diverse infrastructure. Rather than forcing technology choices, we integrate with existing investments, ensuring our security operations span the entire environment regardless of underlying vendor choices.

ISO 27001 Alignment: Information security management system standards provide governance frameworks that ensure consistent, auditable, and continuously improving security operations. Our services align to ISO 27001 principles, providing the governance and documentation that regulated organisations require.

Genuine Incident Ownership: When incidents occur, accountability must be clear. We take ownership of incident response, coordinating across teams, communicating with stakeholders, and driving resolution. This ownership extends from initial detection through full recovery and post-incident review.



A New Paradigm: From Defence to Resilience

Halcyon's Specialisation: Purpose-Built Ransomware Resilience

Halcyon brings focused capabilities specifically engineered for ransomware:

Purpose-Built Platform: Unlike general-purpose security tools that must address numerous threat types, Halcyon focuses exclusively on detecting and disrupting ransomware before damage occurs. This specialisation enables deeper visibility into ransomware-specific behaviours, from pre-execution reconnaissance through data exfiltration to encryption and telemetry.

Comprehensive Kill Chain Coverage: Halcyon's platform protects across the entire ransomware kill chain: from pre-execution activities through data exfiltration to encryption. This comprehensive coverage addresses both prongs of modern ransomware attacks—encryption and data theft—simultaneously.

Integrated Ransomware SOC: Beyond technology, Halcyon provides a dedicated 24/7 ransomware-focused security operations centre. This isn't a bolt-on service; it's a committed team whose charter is exclusively ransomware detection, analysis, and response. This specialisation ensures that alerts are triaged by experts who understand ransomware tactics, techniques, and procedures at the deepest level.

Warranty and Recovery Services: Halcyon provides ransomware warranty and recovery services as part of their offering. This financial and operational assurance demonstrates confidence in their capabilities while providing organisations with concrete risk transfer. The warranty covers both the costs associated with ransomware incidents and the recovery services necessary to restore operations.

Flexible Integration: Rather than requiring organisations to replace existing security investments, Halcyon integrates with current infrastructure. This approach respects the reality that organisations have made significant investments in endpoint protection, SIEM, and other security tools that remain valuable for addressing non-ransomware threats.

A New Paradigm: From Defence to Resilience

The Synergy: Combining Depth and Breadth

The strategic collaboration creates capabilities greater than the sum of individual components:

Holistic Threat Coverage: Core to Cloud's vendor-agnostic SOC provides comprehensive threat detection and response across all attack vectors, while Halcyon adds specialised depth specifically for ransomware. This ensures organisations are protected against the full spectrum of threats without ransomware falling into a gap between general security and specialised requirements.

Unified Incident Response: When ransomware is detected, whether by Halcyon's purpose-built sensors or Core to Cloud's broader monitoring, incident response is coordinated seamlessly. Clear ownership, established communication protocols, and integrated playbooks ensure rapid, effective response without confusion over roles and responsibilities.

Enhanced Recovery Assurance: Core to Cloud's incident response and business continuity expertise combines with Halcyon's ransomware-specific recovery capabilities and warranty to provide board-level assurance. Organisations can quantify their recovery time objectives, understand their financial protection, and demonstrate resilience to insurers and regulators.

Continuous Improvement: The feedback loop between operational detection, incident response, recovery activities, and strategic planning enables continuous improvement. Lessons learned from incidents and near-misses inform architecture improvements, control enhancements, and playbook refinements.

Implementing comprehensive ransomware resilience requires structured methodology that addresses technical, operational, and governance dimensions.

Phase One: Readiness Assessment

The foundation of any resilience programme is understanding current state. Our readiness assessment evaluates:

- **Architecture Review:** We examine network topology, segmentation, identity management, privileged access controls, and attack surface to identify potential ransomware attack paths. This includes understanding cloud architectures (Azure, AWS, hybrid), on-premises infrastructure, and integration points.
- **Backup Posture Analysis:** Critical evaluation of backup infrastructure including backup frequencies, retention policies, offline/air-gapped backups, backup credential management, and restore testing procedures. We identify vulnerabilities in backup architecture that ransomware could exploit.
- **Response Playbook Evaluation:** Review of existing incident response plans specifically for ransomware scenarios. This includes evaluating decision trees for containment versus preservation of evidence, communication protocols, stakeholder notification procedures, and regulatory reporting requirements.
- **Resilience Gap Identification:** Systematic mapping of gaps between current capabilities and resilience requirements. This includes technical gaps (missing controls, visibility limitations), process gaps (untested procedures, unclear ownership), and governance gaps (inadequate metrics, missing board reporting).
- **Recovery Time Objective Validation:** Testing whether claimed recovery time objectives are achievable under realistic ransomware scenarios. This often reveals significant gaps between theoretical recovery capabilities and practical limitations.

Phase Two: Design and Roadmap Development

Based on assessment findings, we develop a comprehensive roadmap:

- **Architecture Design:** Detailed design for how Halcyon's platform integrates within the existing technology stack. This includes sensor placement, data flows, alert routing, and integration with existing security tools. The design respects vendor-agnostic principles, ensuring the solution works regardless of platform.
- **SOC Integration Planning:** Mapping of alert flows, escalation procedures, playbook development, and coordination protocols between Core to Cloud's SOC and Halcyon's ransomware SOC. This ensures clear ownership, eliminates gaps, and prevents duplication of effort.
- **Recovery Architecture:** Design of ransomware-specific recovery capabilities, including, key material capture and decryption, rapid restoration procedures, data integrity validation, and business continuity arrangements. This layer goes beyond traditional backup restoration to address ransomware-specific challenges.
- **Governance Framework:** Development of metrics, reporting structures, board-level dashboards, and continuous improvement processes. This includes defining key risk indicators for ransomware exposure, recovery time objectives, warranty status, and cyber insurance alignment.
- **Phased Roadmap:** Recognition that transformation cannot occur overnight. We develop a phased approach that prioritises critical systems, achieves quick wins, and builds capability progressively while maintaining security during transition.

Phase Three: Onboarding and Integration

Implementation follows structured methodology to minimise disruption:

- **Halcyon Platform Deployment:** Systematic deployment of Halcyon's anti-ransomware and recovery capabilities across the environment. This includes agent installation, configuration, baseline establishment, and validation of detection capabilities.
- **SOC Workflow Integration:** Integration of Halcyon alerts and telemetry into Core to Cloud's SOC workflows. This includes alert correlation, enrichment with context from other security tools, integration with ticketing and case management systems, and establishment of escalation procedures.
- **Playbook Activation:** Implementation of ransomware-specific incident response playbooks that leverage both Core to Cloud's incident response capabilities and Halcyon's specialised recovery services. Playbooks cover detection, initial response, containment, eradication, recovery, and post-incident activities.
- **Team Training:** Ensuring that Core to Cloud SOC analysts, client IT teams, and relevant stakeholders understand the new capabilities, know how to interpret alerts, and can execute response procedures effectively.
- **Validation Testing:** Conducting controlled tests to validate detection capabilities, response procedures, and recovery processes before going fully operational.

Phase Four: Operate and Continuously Test

Resilience is not a point-in-time achievement but an ongoing state:

- **Continuous Monitoring:** 24/7 monitoring for ransomware indicators across the full kill chain. This includes pre-execution reconnaissance, lateral movement, data exfiltration attempts, and encryption activity.
- **Proactive Threat Hunting:** Regular threat hunting exercises specifically focused on ransomware tactics, techniques, and procedures. Hunters look for indicators of compromise that automated detection may have missed, including subtle signs of reconnaissance or credential harvesting.
- **Simulated Ransomware Exercises:** Regular simulation of ransomware incidents to test detection, response, and recovery capabilities. These exercises reveal gaps in procedures, identify areas for improvement, and build muscle memory for incident response teams.
- **Efficacy Testing:** Validation that prevention controls remain effective, detection capabilities maintain sensitivity without excessive false positives, and recovery procedures meet recovery time objectives.
- **Continuous Improvement:** Regular review of lessons learned from exercises, near-misses, and actual incidents to refine architecture, enhance controls, update playbooks, and improve response effectiveness.

Phase Five: Govern and Report

Executive and board-level governance ensures ongoing attention and investment:

- **Board-Ready Dashboards:** Development of executive reporting that communicates ransomware resilience posture in business terms. This includes recovery time objectives, warranty coverage, recent threat activity, testing results, and risk trends.
- **Ransomware Exposure Metrics:** Ongoing measurement of organisation-specific ransomware risk based on threat intelligence, attack surface, control effectiveness, and environmental changes.
- **Recovery Time Objective Tracking:** Regular validation that recovery time objectives remain achievable and aligned with business requirements.
- **Warranty Status Reporting:** Clear communication of warranty coverage, conditions, and any actions required to maintain coverage.
- **Cyber Insurance Alignment:** Documentation and evidence that supports cyber insurance requirements, potentially reducing premiums or improving coverage terms.
- **Regulatory Reporting:** Maintenance of documentation and evidence required for regulatory compliance and incident disclosure should ransomware attacks occur.

Different sectors face unique ransomware challenges based on their operating models, regulatory environments, and business criticality.

Financial Services

Financial institutions face particularly acute ransomware risk due to several factors:

- **Regulatory Scrutiny:** Financial regulators expect robust operational resilience, with specific attention to cyber risk. Incidents can trigger regulatory investigations, enforcement actions, and mandatory remediation programmes.
- **Transaction Criticality:** Even brief interruptions to transaction processing can have cascading effects across the financial system. Recovery time objectives must be measured in hours, not days.
- **Data Sensitivity:** Financial data represents high-value extortion material. The combination of regulatory breach notification requirements and reputational sensitivity creates acute pressure to prevent data exfiltration.
- **Interconnection:** Financial institutions' deep integration with counterparties, payment networks, and market infrastructure means ransomware at one institution can propagate effects across the ecosystem.

Ransomware Resilience Priorities:

- Ultra-low recovery time objectives for critical transaction systems
- Segregation of critical trading and settlement systems
- Enhanced monitoring of privileged access to core banking systems
- Regular testing of recovery procedures with regulatory observers
- Clear communication protocols with regulators, customers, and counterparties



Photo by Sean Pollock on Unsplash

Healthcare

Healthcare organisations represent particularly attractive ransomware targets:

- **Life-Critical Operations:** Healthcare delivery cannot be deferred or delayed without patient harm. Ransomware that disrupts electronic health records, diagnostic systems, or treatment delivery creates immediate patient safety risk.
- **Data Value:** Health records command premium prices in criminal markets due to the richness of personal, financial, and medical information. This increases extortion leverage.
- **Operational Constraints:** Healthcare organisations often operate on thin margins with limited IT investment. Legacy systems, medical devices, and operational technology create unique challenges for security controls.
- **Regulatory Requirements:** Healthcare data protection regulations create significant penalties for breaches, adding financial risk beyond operational disruption.

Ransomware Resilience Priorities:

- Segmentation between clinical systems and administrative networks
- Offline backups of critical patient data with rapid restoration capabilities
- Manual procedure fallbacks for critical clinical processes
- Clear protocols for patient safety during cyber incidents
- Integration with emergency management and business continuity planning



Public Sector

Public sector organisations face distinct challenges:

- **Service Criticality:** Government services often lack alternative providers. When ransomware disrupts council services, benefits administration, or emergency services, citizens have no alternative.
- **Budget Constraints:** Public sector budgets face constant pressure, making it difficult to fund cybersecurity at levels commensurate with risk.
- **Diverse, Legacy Technology:** Public sector IT estates often span decades of technology, with mission-critical systems running on platforms that lack modern security capabilities.
- **Political and Media Attention:** Ransomware incidents at public sector organisations generate intense media coverage and political pressure, amplifying reputational damage.

Ransomware Resilience Priorities:

- Prioritisation of critical citizen services for resilience investment
- Cross-agency coordination and information sharing
- Clear communication strategies for public notification
- Regulatory compliance with government cyber security standards
- Evidence preservation for law enforcement cooperation



Photo by Kostiantyn Vierkieiev on Unsplash

Retail and Logistics

Retail and logistics sectors face ransomware risk shaped by their operating models:

- **Seasonal Criticality:** Peak trading periods (holidays, promotional events) represent periods of maximum vulnerability when disruption carries greatest business impact.
- **Supply Chain Complexity:** Modern retail and logistics depend on intricate supplier networks, creating multiple potential entry points for ransomware and cascading disruption risk.
- **Point-of-Sale and Operational Technology:** Ransomware that impacts point-of-sale systems or warehouse automation creates immediate revenue disruption.
- **Customer Data:** Retailers hold valuable customer payment information and personal data, creating extortion leverage.

Ransomware Resilience Priorities:

- Enhanced monitoring during peak trading periods
- Supply chain security requirements for vendors and partners
- Segregation between corporate IT and operational technology
- Rapid recovery capabilities for point-of-sale and e-commerce systems
- Clear customer communication protocols following data exfiltration



Photo by The Nix Company on Unsplash

Effective governance requires meaningful metrics that translate technical security into business outcomes.

Key Resilience Metrics

Recovery Time Objective (RTO) Achievement: The elapsed time from ransomware detection to full operational recovery. This metric must be tested regularly under realistic conditions, not simply asserted based on theoretical backup restoration times.

Recovery Point Objective (RPO) Verification: The maximum acceptable data loss measured in time. Regular testing should validate that RPO targets remain achievable even when ransomware compromises primary backup systems.

Ransomware Detection Time: The elapsed time from initial ransomware execution to security operations centre detection. Reduction in detection time correlates directly with reduction in damage potential.

Containment Time: The elapsed time from detection to full containment of ransomware propagation. Faster containment limits the scope of encryption and data exfiltration.

Ransomware Exposure Score: A composite metric reflecting the organisation's vulnerability to ransomware based on attack surface, control effectiveness, threat intelligence, and architectural risk factors. This provides a single number that boards can track over time.

Warranty Coverage Percentage: The percentage of potential ransomware costs covered by Halcyon's warranty, indicating financial risk transfer achieved.

Exercise Success Rate: The percentage of ransomware simulation exercises where recovery time objectives were met and recovery was successful. Declining success rates signal degradation in resilience that requires attention.



Board-Level Reporting Framework

Security leaders must translate technical metrics into board-ready communication:

- **Resilience Posture Summary:** High-level assessment of current ransomware resilience using standardised scales (e.g., inadequate, developing, defined, managed, optimising).
- **Trend Analysis:** Direction of travel for key metrics, highlighting improvements or areas of concern.
- **Recent Threat Activity:** Summary of ransomware threats targeting the organisation or sector, contextualising the threat environment.
- **Testing Results:** Outcomes from recent simulations, penetration tests, or red team exercises, with clear explanation of findings and remediation plans.
- **Investment Requirements:** Clear articulation of budget required to maintain or improve resilience, with business case justification.
- **Regulatory and Insurance Alignment:** Status of compliance with regulatory expectations and cyber insurance requirements related to ransomware.
- **Incident Summary:** If incidents have occurred, clear explanation of what happened, response effectiveness, and lessons learned.

Continuous Governance

Ransomware resilience governance should be integrated into existing risk management frameworks:

- **Regular Risk Committee Review:** Quarterly review of ransomware resilience metrics, testing results, and threat landscape evolution.
- **Annual Strategy Refresh:** Annual evaluation of ransomware strategy considering changes in threat landscape, business operations, regulatory requirements, and technology capabilities.
- **Post-Incident Review:** Structured review following any ransomware incident or significant near-miss, with clear accountability for implementing improvements.
- **Integration with Enterprise Risk Management:** Ransomware should be explicitly addressed within enterprise risk registers, with clear ownership, risk ratings, and mitigation plans.
- **Stakeholder Communication:** Regular communication with cyber insurers, regulators, and other stakeholders to maintain alignment and demonstrate ongoing commitment to resilience.

Justifying investment in ransomware resilience requires articulating costs, benefits, and alternatives in business terms.

The Cost of Ransomware Incidents

Understanding potential incident costs provides context for resilience investment:

Direct Financial Costs:

- **Ransom payment (if paid):** £100,000s to £10,000,000s depending on organisation size
- **Incident response and forensics:** £250,000 to £2,000,000+
- **Legal fees:** £100,000 to £1,000,000+
- **Regulatory fines:** Up to 4% of global revenue under GDPR and other frameworks
- **Crisis communication and public relations:** £50,000 to £500,000
- **System restoration and recovery:** £500,000 to £5,000,000+

Business Interruption:

- **Revenue loss during downtime:** Varies by sector; can exceed £100,000s per hour for large organisations
- **Lost productivity:** Organisation-wide impact during incident and recovery
- **Customer churn:** Permanent loss of customers due to service disruption or data breach
- **Contract penalties:** Service level agreement violations and penalties

Long-Term Impact:

- **Brand and reputation damage:** Difficult to quantify but potentially exceeding direct incident costs
- **Increased insurance premiums:** 50-300% increases common following incidents
- **Loss of competitive position:** Market share erosion during extended recovery
- **Employee morale and retention:** Impact on workforce confidence and retention
- **Strategic opportunity cost:** Diversion of leadership attention and resources from growth initiatives

Existential Risk:

For smaller organisations or those operating on thin margins, a major ransomware incident can threaten viability. Studies indicate that a significant percentage of small to medium enterprises never fully recover from major cyber incidents.

The Value of Resilience Investment

Resilience investment delivers multiple forms of value:

- **Risk Reduction:** Quantifiable reduction in probability and impact of successful ransomware attacks through enhanced prevention, detection, and recovery capabilities.
- **Reduced Recovery Costs:** Purpose-built recovery capabilities reduce the time and cost of restoration compared to traditional disaster recovery approaches. Hours of downtime avoided translate directly to revenue preserved.
- **Insurance Premium Reduction:** Demonstrable resilience can reduce cyber insurance premiums by 20-40% or more, with payback periods of 2-3 years in some cases.
- **Regulatory Confidence:** Proactive resilience investment positions organisations favourably with regulators, potentially reducing scrutiny and enforcement risk.
- **Competitive Differentiation:** In sectors where customers have choice, demonstrated cyber resilience can become a competitive advantage, particularly in B2B contexts where supply chain security matters.
- **Strategic Optionality:** Organisations confident in their resilience can pursue digital transformation, cloud migration, and other strategic initiatives without cyber risk becoming a blocking factor.
- **Peace of Mind:** While difficult to quantify, the confidence that comes from knowing the organisation can survive and recover from ransomware has value for executive teams and boards.

Alternative Approaches and Their Limitations

Organisations considering resilience investment should understand alternatives:

- **"Do Nothing":** Maintaining current security posture without ransomware-specific enhancement. This approach accepts ransomware risk at current levels, appropriate only if current risk is genuinely acceptable and threat landscape stable (rarely the case).
- **Point Solution Addition:** Adding individual security tools without integrated strategy or recovery capabilities. This may improve detection but typically fails to address the resilience gap, leaving organisations unable to recover quickly or with confidence.
- **Insurance Only:** Relying on cyber insurance without underlying resilience investment. Insurance provides financial risk transfer but does not prevent operational disruption, reputational damage, or customer impact. Moreover, insurers increasingly require demonstrable resilience as a prerequisite for coverage.
- **Backup Enhancement Only:** Investing in backup infrastructure without ransomware-specific recovery capabilities. While necessary, this approach fails to address the targeted destruction of backups that sophisticated ransomware employs.

Building the Business Case

Effective business cases for resilience investment should include:

- **Risk Quantification:** Use frameworks like Factor Analysis of Information Risk (FAIR) to quantify probable ransomware losses given current controls versus proposed resilient state.
- **Return on Investment Calculation:** Compare total investment (Halcyon platform, Core to Cloud services, internal resources) against expected risk reduction, insurance savings, and avoided incident costs.
- **Strategic Alignment:** Connect resilience investment to broader strategic objectives such as digital transformation, regulatory compliance, or competitive positioning.
- **Comparative Analysis:** Benchmark against peer organisations and industry standards to demonstrate alignment with sector norms and leading practices.
- **Scenario Analysis:** Present board-level scenarios illustrating business impact of ransomware with and without resilience investment, making abstract risk concrete.
- **Phased Approach:** Propose phased investment that allows for validation of value delivery before full commitment, reducing perceived risk of the investment itself.

The Strategic Imperative

Ransomware has evolved from a technology problem to a strategic business risk that demands board-level attention and investment. The question facing organisations is not whether ransomware will be attempted against them, but whether they will survive, recover, and continue operating when attacks occur.

Traditional security paradigms built on prevention, detection, and response remain necessary but are no longer sufficient. The ransomware gap - the disconnect between what security investments promise and what they actually deliver in ransomware scenarios - leaves organisations vulnerable despite substantial security expenditure.

The strategic collaboration between Core to Cloud and Halcyon addresses this gap by combining human-led, vendor-agnostic security operations with purpose-built ransomware resilience capabilities. This integration provides what modern organisations require: comprehensive protection across the ransomware kill chain, rapid response when incidents occur, and guaranteed recovery capabilities that ensure business continuity.

Key Recommendations for Security Leaders

Based on the analysis presented in this whitepaper, we recommend security leaders take the following actions:

- **Conduct a Ransomware-Specific Readiness Assessment:** Evaluate current architecture, backup posture, response capabilities, and recovery processes specifically through a ransomware lens. Identify the ransomware gap in your organisation.
- **Establish Board-Level Ransomware Governance:** Ensure ransomware resilience is explicitly addressed in board risk discussions with meaningful metrics, regular testing, and clear accountability.
- **Adopt a Resilience Framework:** Move beyond prevention-focused thinking to embrace comprehensive resilience across prevention, detection, response, and recovery domains.
- **Invest in Purpose-Built Capabilities:** Recognise that general-purpose security tools, while necessary, require augmentation with ransomware-specific capabilities that address the unique characteristics of ransomware attacks.
- **Implement Continuous Testing:** Regular simulation of ransomware scenarios, penetration testing, and red team exercises to validate that theoretical capabilities translate to operational effectiveness.
- **Develop Recovery Assurance:** Move beyond backup strategies to comprehensive recovery capabilities that address ransomware-specific challenges including backup compromise, data integrity validation, and rapid restoration timelines.
- **Align Insurance and Warranty:** Ensure cyber insurance coverage is adequate and complemented by warranty-backed guarantees from technology providers who share accountability for resilience.
- **Foster Cross-Functional Collaboration:** Ransomware resilience requires coordination across IT, security, business continuity, legal, communications, and executive leadership. Break down silos and establish clear incident command structures.



The Path Forward

For organisations ready to move from "Will we be hit?" to "When we are hit, we will survive, recover, and continue operating," the path forward requires:

- **Strategic Partnership:** Working with partners who take genuine ownership of incident response and recovery, not simply providing technology and walking away.
- **Human-Led Approach:** Recognising that while automation and AI enhance capabilities, human expertise remains essential for threat hunting, contextual decision-making, and incident management.
- **Vendor-Agnostic Architecture:** Ensuring resilience capabilities integrate with existing technology investments rather than requiring wholesale replacement.
- **Purpose-Built Focus:** Augmenting general security capabilities with ransomware-specific detection, response, and recovery that addresses the unique characteristics of ransomware attacks.
- **Continuous Improvement:** Treating resilience as an ongoing journey rather than a point-in-time project, with regular testing, refinement, and evolution.

Why Core to Cloud and Halcyon

The strategic collaboration between Core to Cloud and Halcyon brings together complementary capabilities that address the full spectrum of ransomware resilience:

Core to Cloud provides the human-led security operations, vendor-agnostic architecture, ISO 27001 governance, and genuine incident ownership that form the foundation of comprehensive security programmes.

Halcyon delivers purpose-built ransomware resilience with comprehensive kill chain coverage, dedicated ransomware SOC, warranty-backed recovery assurance, and specialised expertise.

Together, we provide organisations with genuine resilience: the ability to prevent what can be prevented, detect what prevention misses, respond rapidly when detection occurs, and recover with confidence when attacks succeed.

This integration ensures that organisations can meet board expectations, satisfy regulatory requirements, maintain cyber insurance coverage, and most importantly, survive and recover from ransomware attacks that would otherwise threaten operational continuity.

Call to Action

If your organisation is ready to evolve from reactive defence to proactive resilience, we invite you to engage with Core to Cloud to explore how our strategic collaboration with Halcyon can address your specific ransomware challenges.

We begin with a comprehensive readiness assessment that evaluates your current posture, identifies gaps, and develops a tailored roadmap for achieving genuine ransomware resilience. From there, we work collaboratively to implement capabilities, integrate with your existing environment, and continuously test and refine your resilience posture.

The ransomware threat is not diminishing. The sophistication, frequency, and impact of attacks continue to escalate. The question is whether your organisation will be prepared when the inevitable attack occurs.

The time to build resilience is now, before the incident, not during the chaos of an active attack or the aftermath of a successful encryption. The investments made today in comprehensive ransomware resilience will determine whether tomorrow's attack is a manageable incident or an existential crisis.



About CORE TØ CLOUD™

We help organisations understand, optimise, and strengthen their cybersecurity.

At Core to Cloud, we specialise in cutting through the noise to deliver real, actionable insight and solutions that protect your business - without overcomplicating it. From critical visibility gaps to fast-moving threats, we work with you to design, implement, and manage cybersecurity strategies that are both robust and realistic.

We support public sector bodies, enterprises, and growing organisations with services and solutions that solve real-world security challenges:

- Managed Detection & Response (MDR) – 24/7 monitoring and expert-led threat response
- Security Testing – Autonomous, scalable testing tailored to your risk landscape
- Dark Web Monitoring – Stay ahead of exposed credentials and compromised data
- Third-Party Risk Management – Understand and reduce supplier-related risks
- Crisis Simulation – Test your readiness for the worst-case scenario

We don't push products. We build roadmaps. Every engagement is designed to meet your needs, not industry trends. Whether we're offering a fully managed service or tailored support, we're here to empower your team, not replace it.

No jargon. No inflated promises. Just clarity, expertise, and solutions that work.

About halcyon

Halcyon is the leading anti-ransomware company, purpose-built to defeat ransomware through comprehensive protection across the ransomware kill chain. With integrated ransomware SOC capabilities, warranty-backed recovery assurance, and a singular focus on ransomware resilience, Halcyon provides organisations with the specialised capabilities required to address the most pressing cyber threat of our time.

For more information about building ransomware resilience for your organisation, please contact Core to Cloud.

This whitepaper reflects the ransomware threat landscape and mitigation strategies as of October 2025. Given the rapidly evolving nature of ransomware tactics and defensive capabilities, organisations should regularly reassess their resilience posture and update strategies accordingly.