White Paper

halcyon

Ransomware Resilience in Financial Services:

Beyond Prevention to Recovery and Response

Executive Summary

Ransomware is no longer solely an IT challenge in financial services; it threatens business continuity, customer trust, and economic stability. The financial sector faces unique vulnerabilities: zero tolerance for downtime, highly interconnected systems, and the custody of sensitive financial data that makes them high-value targets.

This white paper examines the critical shift required in ransomware defense strategy, moving from prevention-focused approaches to comprehensive resilience frameworks. Key findings include:

- **The Prevention Paradox:** Organizations can no longer rely exclusively on preventive controls. Sophisticated threat actors will find a way through even the most robust defenses, making recovery capabilities equally critical.
- **The Real Cost of Ransomware:** Average recovery costs reached $2.5 million in 2024, but the true impact extends far beyond ransom payments to include business interruption, customer attrition, regulatory penalties, litigation, and permanent reputational damage.
- **Supply Chain Cascade Effects:** A single attack on a critical vendor can paralyze operations across hundreds of dependent organizations, as evidenced by recent incidents affecting dealership networks and payment processors.
- **The Containment Gap:** Most organizations significantly underestimate their actual recovery time by focusing solely on backup restoration while neglecting the time required to contain, eradicate, and verify system integrity before restoration can begin.
- **AI-Powered Adversaries:** Threat actors now leverage artificial intelligence to accelerate vulnerability exploitation, create highly credible phishing campaigns, and deploy autonomous ransomware that operates without human intervention.
- **Identity-Based Attacks:** 98% of successful attacks use valid credentials, rendering traditional perimeter defenses ineffective. Attackers increasingly "log in, not hack in" by exploiting help desk procedures and multi-factor authentication fatigue.
- **Regulatory Evolution:** Bipartisan legislation and updated frameworks signal growing government recognition that cybersecurity is essential to financial system stability, with increased accountability requirements on the horizon.

Financial institutions must adopt a whole-of-society approach to ransomware defense, uniting boards, executive leadership, operational teams, legal counsel, communications, third-party vendors, and government partners in coordinated preparation and response. Without this comprehensive strategy, ransomware will continue to threaten customer trust, market stability, and the integrity of the financial system.

Financial institutions must adopt a whole-of-society approach to ransomware defense in coordinated preparation and response.

The Evolution of Ransomware in Financial Services

From IT Problem to Business Crisis

The ransomware threat has undergone a dramatic transformation over the past decade. What began as opportunistic attacks using relatively unsophisticated malware has evolved into a criminal enterprise targeting high-value organizations.

Financial institutions now face adversaries whose operational sophistication rivals that of nation-state actors. These criminal organizations invest heavily in research and development, constantly evolving their tactics to bypass the latest security controls. They study their targets meticulously, understanding not just technical vulnerabilities but also business operations, regulatory requirements, and the specific pressures that make financial services firms more likely to pay ransoms quickly.

Industry regulators worldwide have responded to the ransomware crisis by dramatically increasing their expectations for cyber resilience. In the United States, the Securities and Exchange Commission's 2023 cybersecurity disclosure rules require public companies to report material cyber incidents within four business days. The Cybersecurity and Infrastructure Security Agency has designated financial services as critical infrastructure, subjecting firms to heightened scrutiny and potential penalties for inadequate cybersecurity.

Through the Digital Operational Resilience Act (DORA), European regulators have established comprehensive requirements for financial institutions to manage ICT risk, including specific provisions for operational resilience testing, third-party risk management, and incident reporting.

This regulatory evolution reflects a fundamental shift in how authorities view cyber risk. Ransomware attacks are no longer seen as unfortunate but unpreventable incidents. Instead, they are viewed as failures of governance and risk management.

Ransomware attacks are no longer seen as unfortunate but unpreventable incidents. Instead, they are viewed as failures of governance and risk management.

Why Financial Services is a Prime Target

Financial institutions present an irresistible target profile for ransomware operators:

- **Zero Tolerance for Downtime:** Every minute of system unavailability translates to immediate revenue loss and customer dissatisfaction. In banking, trading, and payment processing, even brief outages can cascade across the entire financial system.
- **High-Value Data:** Financial institutions hold not only personal and financial data but also proprietary trading information, deal structures, and market-sensitive intelligence that attackers can monetize through multiple extortion tactics.
- **Interconnected Ecosystems:** Modern financial services operate through complex webs of third-party relationships. An attack on a single vendor can paralyze dozens of dependent institutions.
- **Regulatory Pressure:** Financial institutions face strict requirements for customer notification, regulatory reporting, and potential penalties for inadequate cybersecurity controls, amplifying the pressure to pay ransoms quickly.
- **Thin Operating Margins:** Many financial institutions operate on razor-thin margins, making the financial impact of prolonged downtime potentially existential, particularly for smaller regional banks and credit unions.

As Oliver Newbury, former Barclays CISO and now Halcyon Chief Strategy Officer, notes: “In financial services, because a lot of the offerings are quite commoditized, if you don’t handle it in the right way, the biggest cost can be business that goes away in the crisis to one of your competitors that never comes back.”

The False Choice: Prevention vs. Recovery

The Misconception of "Enough" Prevention

One of the most dangerous myths in financial services cybersecurity is that sufficient investment in preventive controls eliminates the need for robust recovery capabilities. The assumption being that if you build the walls high enough, you'll never need to test whether you can rebuild.

Industry research demonstrates that determined threat actors with sufficient resources will eventually penetrate even robust defensive controls. This reality challenges the long-held belief that prevention alone provides adequate protection.

Gary Hayslip, former SoftBank CISO and current Halcyon Field CISO, encountered this mindset repeatedly: "One of the biggest things I was running into a lot was, 'Well, we have backups.' And I'm like, 'Well, that's great, but do you understand how long it's going to take to backup 5,000 endpoints, or backup critical servers that you've got your sales portals on which are in production and actively making like $300,000 an hour. If these portals and their servers are down, are we going to have to rebuild them all? So, you start asking those questions they had never really thought of, through a resiliency lens."

Expert Insight

The Prevention Paradox

Many financial institutions fall into the trap of believing that sufficient investment in preventive controls eliminates the need for robust recovery planning. This represents the dangerous assumption that building high enough walls means you'll never need to test whether you can rebuild. Industry experts emphasize that this thinking is no longer viable, determined threat actors with adequate resources will eventually find a way through even the most sophisticated defenses.

The reality is that backups alone do not constitute a recovery strategy. Organizations must understand how long restoration will take in a real-world scenario, whether backup systems themselves are protected from ransomware, if backups are tested regularly under crisis conditions, whether the organization can operate during the restoration period, and what the cumulative cost of downtime will be.

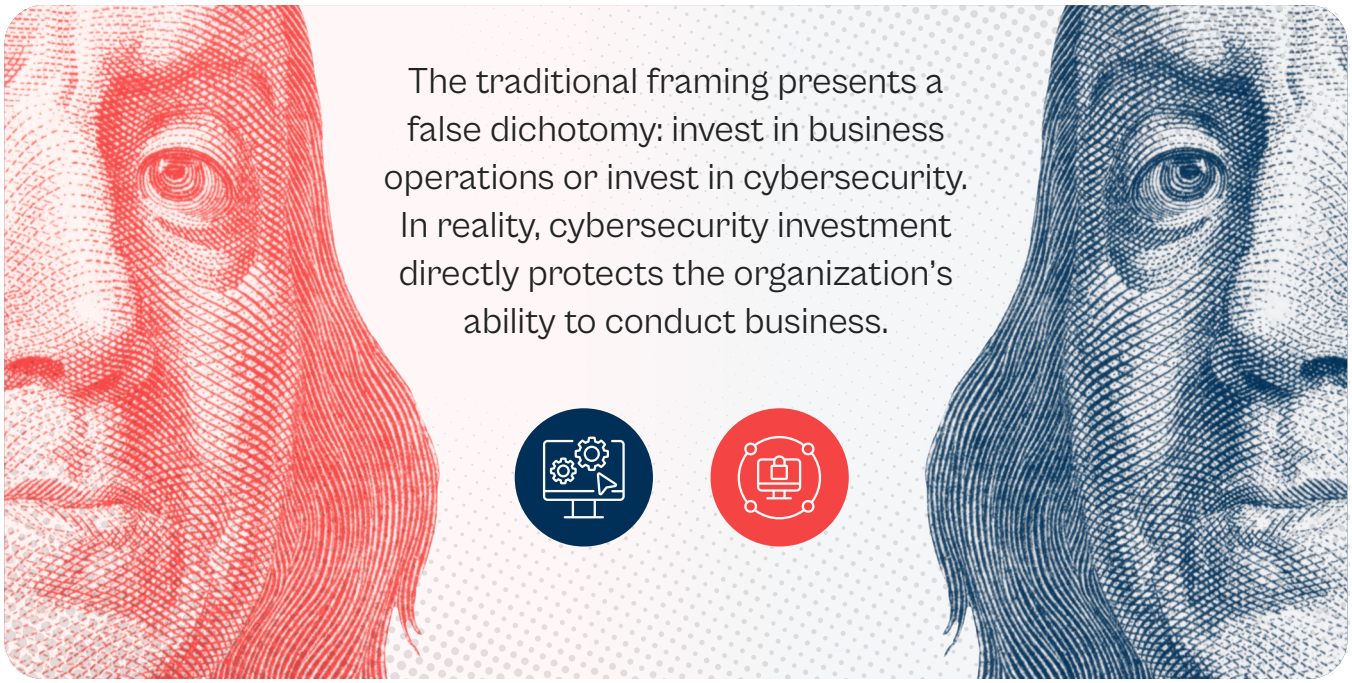
Investing in Cyber Defense is Investing in Business Continuity

The traditional framing presents a false dichotomy: invest in business operations or invest in cybersecurity. In reality, cybersecurity investment directly protects the organization's ability to conduct business.

When ransomware encrypts core banking systems, trading platforms, or payment processing infrastructure, the immediate business impact is indistinguishable from any other operational failure, except recovery may take weeks rather than hours.

Even when endpoint protection and endpoint detection and response (EDR) tools are deployed, sophisticated attackers routinely bypass them using trusted system processes (also known as "Living Off the Land"), Bring Your Own Vulnerable Driver (BYOVD) attacks, valid credential abuse, and EDR tampering.

Without sufficient funding and executive-level prioritization, organizations cannot maintain the around-the-clock monitoring, behavioral analytics, and dedicated anti-ransomware capabilities required to defend against modern threats.



The True Cost of Ransomware

Beyond the Ransom: Quantifying Total Impact

Average recovery costs in 2024 reached $2.5 million, with most ransom demands exceeding $1 million. However, this headline figure dramatically understates the total financial impact of a ransomware incident.

The comprehensive cost structure includes business interruption losses (trading platform unavailability, payment processing disruptions, online banking outages, branch system failures, customer service disruptions), forensic and restoration costs, regulatory and legal expenses, customer impact and credit monitoring, and brand damage with customer attrition.

Financial services experts observe that brand strength can significantly influence recovery outcomes following a ransomware incident. Organizations with established, beloved brands often experience less secondary damage and customer attrition compared to institutions with weaker brand recognition.

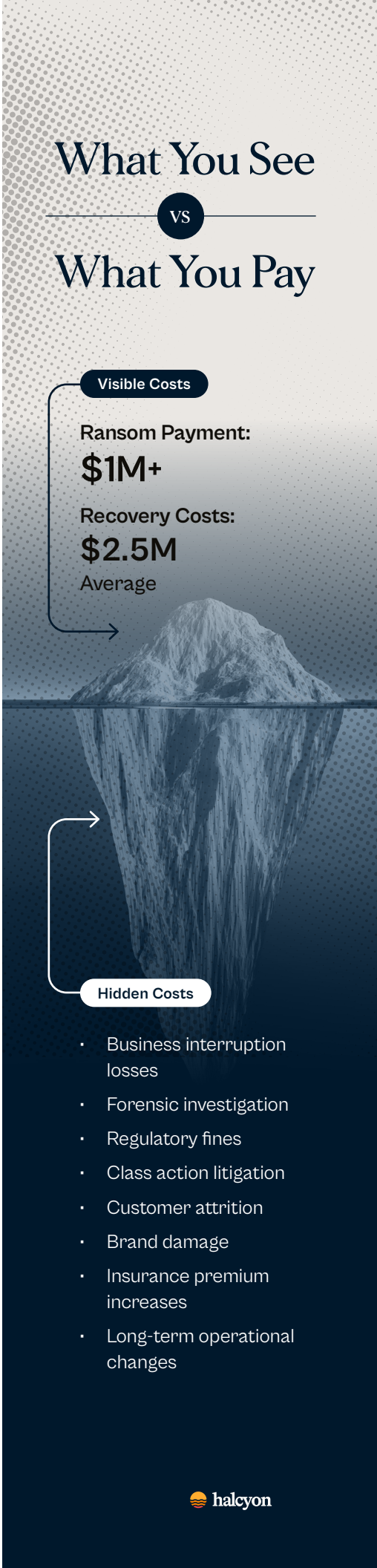
However, the inverse is also true. Institutions without strong brand loyalty can suffer permanent customer losses. In markets with frictionless switching mechanisms, such as the UK's open banking regulations, customers can transfer their accounts between financial institutions with a single click. When trust erodes following a cybersecurity incident, customer departure can be immediate and permanent.

Oliver Newbury notes the M&A impact: "For financial services firms that are involved in M&A transactions, where companies are in a process around M&A, like in the private equity space, there can be impact for those companies that are about to be acquired."

The 22-Day Reality

According to Gartner research, it takes an average of 22 days to recover from a ransomware attack. Many organizations hearing this statistic for the first time find it difficult to believe and assume their backup and recovery processes will enable much faster restoration.

This disconnect stems from a fundamental misunderstanding of what "recovery" actually entails.



* "Source: Halcyon Ransomware Research Center 2025

The Containment Gap: Understanding True Recovery Time

The Hidden Timeline Most Organizations Miss

Oliver Newbury identifies what may be the most critical oversight in ransomware planning: “People sort of gloss over this. They test their recovery time from backup and say, ‘This is how long it takes me to recover.’ But if that takes a week or two weeks, and you don’t have the right strategy to contain and eradicate quickly, your overall recovery time is actually far longer than you think.”

Organizations routinely test backup restoration in isolation, measuring how long it takes to restore systems from tape or cloud backup storage. They use this number as their expected downtime in a ransomware scenario. This is fundamentally flawed.

Before restoration can begin, the organization must detect and verify the breach, contain lateral movement, eradicate all attacker presence including malware, backdoors, and compromised credentials, verify environment integrity, and only then begin restoration.

Each of these stages can take days or weeks, particularly when security teams are overwhelmed, third-party forensics firms must be engaged, attackers have disabled logging systems, the full scope is unclear, and regulatory obligations must be addressed simultaneously.

The Recovery Timeline Gap

What Organizations Believe:

Hours
to Days to Recover

VS

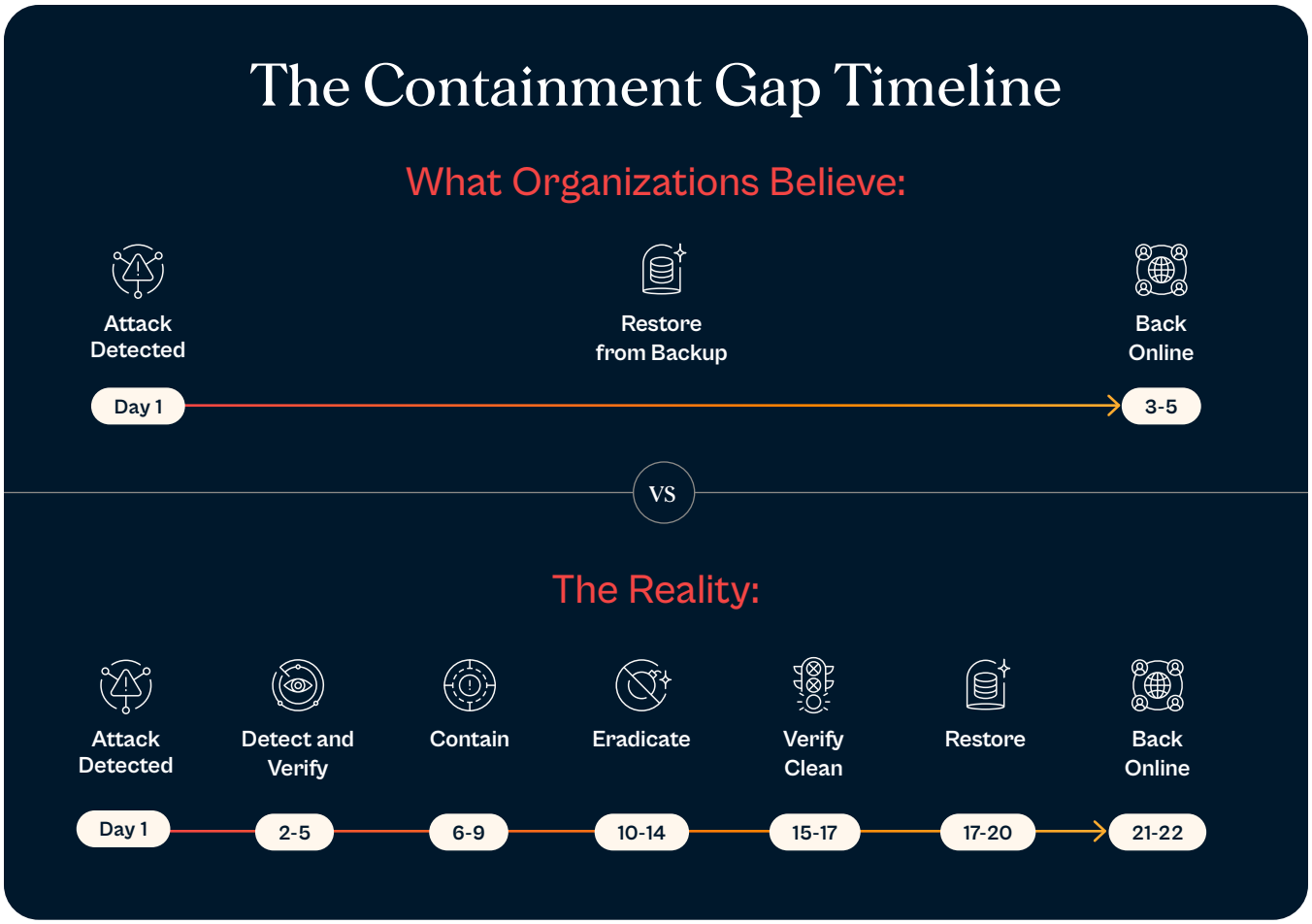
The Reality:

22 Days
to Recover

The Hidden Stages

- Detect and Verify (days)
- Contain Movement (days)
- Eradicate Threats (days)
- Verify Integrity (days)
- Restore Systems (days-weeks)

Source: Gartner Research



As Newbury emphasizes: "Having the right tools and also the right people, third-party expertise, and support to contain and eradicate really quickly, to get a clean environment that you can rebuild into as fast as possible, saves you a lot of time."

Why Backup Alone Is Insufficient

Gary Hayslip encountered this misconception repeatedly: "One of the biggest things I was running into a lot was, 'Well, we have backups, so we don't need to really invest in a lot of other things, we just have backups.' That's great, but do you understand how long it's going to take?"

Moreover, attackers specifically target backup systems. Nearly two-thirds of healthcare ransomware cases involved attacks on backups, and this pattern holds across industries. Sophisticated threat actors identify and encrypt backup repositories, delete backup catalogs and recovery points, corrupt backup integrity verification, compromise backup administration credentials, and encrypt backup servers.

Organizations discovering that their backups are also compromised face catastrophic recovery timelines or impossible choices about ransom payment.

Across industries, nearly two-thirds of ransomware cases involved attacks on backups.

The Evolving Threat Landscape

AI-Powered Adversaries

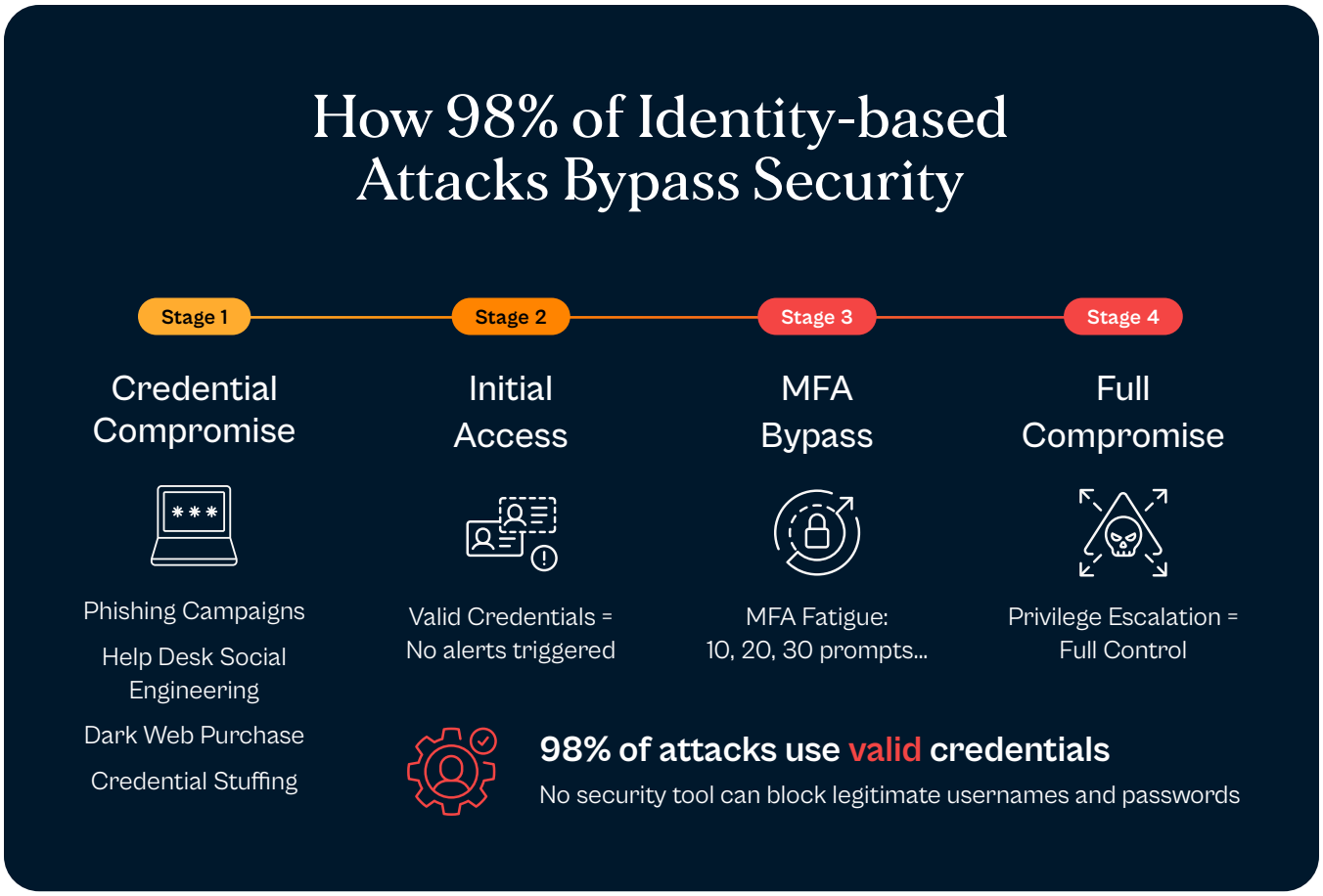
Gary Hayslip, who spent significant time evaluating AI security companies at SoftBank, observed the emerging threat firsthand: "The criminal syndicates that are ransomware operators, are using agentic AI to test various types of ransomware attacks, to test their responses to shut off EDR, to slowly exfiltrate data, and then drop the ransomware package afterwards."

The implications are sobering. Autonomous ransomware powered by AI can analyze target environments independently, identify valuable data for exfiltration, determine optimal encryption strategies, evade detection through adaptive behavior, and operate across multiple targets simultaneously.

Security experts note that the rapid evolution of zero-day exploitation presents an escalating challenge. The time from vulnerability disclosure to active exploitation has collapsed dramatically, creating what many describe as a fundamental shift from human-speed to machine-speed cyber risk. This acceleration represents one of the defining challenges organizations must address in their security strategies.

Recent research found that AI systems can now generate working exploits for published CVEs for only $2.74, potentially increasing the exploitable percentage of the CVE database from 1% to 50% or more.

AI also enables highly credible social engineering, generating convincing phishing emails with perfect grammar and context, creating deepfake voice and video for CEO fraud, personalizing attacks based on social media intelligence, and conducting large-scale campaigns with minimal human involvement.



Financial institutions report experiencing increasingly sophisticated phishing campaigns, with AI-generated emails displaying perfect grammar, appropriate context, and convincing personalization. In one documented case, a compromised business banking customer account generated 35 malicious emails that were sent to relationship managers, all from trusted email addresses. Only advanced AI-powered detection that had learned normal communication patterns was able to identify and quarantine these threats before they could compromise additional accounts.

Identity as the New Perimeter

Oliver Newbury highlights a fundamental shift in attack methodology: "Attackers are now logging in, not hacking in. There are an increasing number of attacks where they don't need to start with a vulnerability. If a criminal is able to socially engineer your help desk to give them a valid credential and log in as a legitimate employee, no patching in the world is going to save you."

The statistics are stark: 98% of successful attacks use valid credentials. This means attackers are using legitimate usernames and passwords obtained through phishing, credential stuffing, help desk manipulation, or purchase on dark web markets to access systems.

Common identity-based attack techniques include help desk social engineering (attackers call internal help desks pretending to be employees who have forgotten passwords), MFA fatigue (repeatedly triggering MFA prompts until the frustrated user approves one), credential harvesting (large-scale phishing campaigns), and privilege escalation (exploiting misconfigurations to gain administrative access).

The sobering reality is that no cybersecurity tool exists to block valid credentials. If the username and password are correct, and the user approves the MFA prompt, the system has no technical basis to deny access.

The Supply Chain Cascade Effect

COMPROMISED VENDOR

- Examples: CDK Global and Change Healthcare
- See overview breakdowns of both attacks below

DIRECT IMPACT

- 10-15 connected institutions
- Hundreds of dependent organizations

CASCADE IMPACT

- 20-30 organizations
- Thousands of dealers/providers affected

COMMUNITY IMPACT

- Entire communities lose services

CDK Global Attack:

- Thousands of dealerships paralyzed
- Billions in lost vehicle sales
- Weeks of downtime
- Permanent business closures

Change Healthcare:

- 6TB of data exfiltrated
- $22M ransom (no decryption keys)
- Nationwide payment disruption
- Estimated billions in industry impact

Main Impacts

- Billions in lost sales
- Furloughed employees
- Class action lawsuits
- Permanent closures
- Months-long recovery

Supply Chain as Attack Vector

Recent incidents have demonstrated the devastating potential of supply chain attacks against financial services:

- **CDK Global (2024):** A ransomware attack against automotive dealership software provider CDK Global paralyzed car sales across thousands of dealerships for weeks, resulting in billions in lost vehicle sales, furloughed dealership employees, class action lawsuits from dealers, and permanent business closures for some dealers.
- **Change Healthcare (2024):** The BlackCat/ALPHV ransomware group attacked Optum's Change Healthcare subsidiary, a critical payment processing and claims clearinghouse. The impact included over 6TB of sensitive health and billing data exfiltrated, $22 million ransom paid (though decryption keys were not provided), healthcare providers nationwide unable to process payments, months-long recovery process, and estimated billions in industry impact.

Oliver Newbury says: "Third parties are increasingly becoming part of the technique for adversaries to cause maximum impact. Building resilience to ransomware attacks across your supply chain is critical."

Data Exfiltration and Double Extortion

Nearly two-thirds of ransomware incidents now involve data theft alongside encryption. Attackers exfiltrate sensitive data before deploying ransomware, then leverage multiple extortion tactics including primary extortion (payment demanded for decryption keys), secondary extortion (additional payment to prevent public release of stolen data), and triple extortion (demands extended to affected third parties).

For financial institutions, exfiltrated data can include customer account information, transaction histories, proprietary trading strategies, deal structures and M&A information, employee personal information, internal communications, and regulatory reporting data.

The exposure of such data triggers mandatory regulatory breach notifications, individual customer notifications, credit monitoring obligations, potential SEC disclosure requirements, class action litigation, and criminal investigations. Even after successfully decrypting systems and restoring operations, organizations face months or years of legal, regulatory, and reputational consequences from the data breach component alone.

Building Resilience: A Comprehensive Framework

Leadership and Governance

Board-Level Accountability: Cybersecurity must be a standing board agenda item, integrated across risk committee oversight, audit committee review, compensation committee considerations (CISO retention and incentives), and full board strategic planning.

Security leaders emphasize that automation within Security Operations Centers and Security Orchestration, Automation, and Response (SOAR) platforms has evolved from a luxury to a necessity. The ability to respond to attacks in an automated fashion has become table stakes rather than a competitive differentiator, driven by the need to match machine-speed threats with machine-speed defenses.

Executive Participation in Incident Response: CISOs should not be solely responsible for incident response planning. Oliver Newbury recommends: "Board and executives would benefit from incident response training tailored to the special roles they will be expected to play during a crisis. This training is good preparation, and it can inspire constructive feedback and accountability from an organization's top level before an attack occurs."

Pre-Established External Relationships: Organizations should establish relationships before crisis with third-party incident response firms, forensics specialists, legal counsel with cyber expertise, crisis communications firms, cyber insurance carriers, regulatory liaisons (FBI, CISA, financial regulators), and industry information sharing groups (FS-ISAC).

As Gary Hayslip notes: "You're not going to know these things unless you've run through these kind of scenarios, and people know who they're supposed to talk to, what the response should be, and who's going to be overall responsible."

Technical Controls and Architecture

Architectural Resilience: Leading financial institutions are implementing multi-environment architectures that enable rapid failover when components are compromised. This includes running critical infrastructure across both public and private cloud environments, allowing organizations to quickly isolate and remove compromised segments while maintaining operations. This approach recognizes that resilience is not solely a security posture issue but fundamentally an architectural challenge requiring comprehensive strategic planning.

Third-Party Risk Management

Third-Party Risk Checklist

Based on Gary Hayslip's Framework:

- ☐ **Identify your 20-25 critical vendors**
  (Necessary for business to run)
- ☐ **Obtain and review SOC 2 reports**
  (Verify security maturity)
- ☐ **Conduct security assessments**
  (Beyond contractual requirements)
- ☐ **Include in tabletop exercises**
  (Test communication and response)
- ☐ **Plan vendor loss scenarios**
  (Know your alternatives)
- ☐ **Establish 24-hour notification clauses**
  (Contractual requirement)
- ☐ **Monitor vendor security posture**
  (Continuous assessment)

Traditional Thinking: Only two options when ransomware strikes

New Reality: Encryption key capture provides a third option

When Ransomware Strikes, Choose Your Recovery Options Wisely

CRITERIA	OPTION 1: Pay The Ransom	OPTION 2: Restore From Backup	OPTION 3: Halcyon Key Capture
Recovery Time	Hours-Days (If They Cooperate)	2-3 Weeks Average	Hours-Days
Cost	$1M+ Ransom Payment	$2.5M+ Recovery Cost	Included in Platform
Repeat Attack Risk	80% Attacked Again	Moderate	Eliminated
Data Protection	No Guarantee	If Backups Uncompromised	Guaranteed
Operational Impact	Funds Criminals	Weeks of Downtime	Minimal Disruption
Regulatory	Potential Violations	Maintains Compliance	Maintains Compliance

Identity and Access Governance: Given that 98% of attacks use valid credentials, organizations must implement phishing-resistant MFA everywhere, monitor and restrict administrative access, enforce least-privilege principles, conduct regular access reviews, revoke access immediately upon role changes, and deploy behavioral analytics to detect anomalous credential use.

Endpoint Protection: Traditional EDR is necessary but insufficient. Attackers routinely disable endpoint protection before deploying ransomware. Organizations need anti-tamper protections for security tools, behavioral monitoring that survives EDR disablement, dedicated anti-ransomware solutions, and automated response capabilities.

Backup Strategy: Follow the "3-2-1 principle" (3 copies of data, 2 different media types, 1 copy offline or immutable). Critical additions include testing recovery regularly under crisis conditions, ensuring backups are segmented from production networks, verifying backup integrity continuously, protecting backup administration credentials rigorously, and maintaining detailed recovery runbooks.

Recovery and Resilience Technologies

Traditional approaches present organizations with two options: pay the ransom or restore from backups, which can take weeks.

Oliver Newbury describes a third way: "(Halcyon) technology allows you to actually capture the encryption keys that the adversaries are using, then use those same keys to begin reversing decryption in situ on the boxes that were actually affected. You can bring the infrastructure back to life at roughly the same speed it took the adversary to encrypt it."

This approach provides dramatic reduction in downtime (hours vs. weeks), elimination of ransom payment necessity, preservation of system configurations and recent data, faster return to operations, and lower total cost of recovery.

Combined with robust prevention and detection, such recovery capabilities create comprehensive ransomware resilience.

Key Recommendations

For Boards and Executive Leadership

Elevate cybersecurity to strategic priority with regular board discussion and appropriate budget allocation. Establish clear governance around cyber risk with defined roles, responsibilities, and escalation procedures. Participate in incident response planning through tailored exercises that prepare executives for crisis decision-making. Build relationships before crisis with incident response firms, legal counsel, regulators, and industry partners. Understand the true cost of ransomware beyond ransom payments. Test recovery capabilities under realistic crisis conditions, not just backup restoration in isolation. Recognize the false choice between investing in operations vs. cybersecurity–robust security protects business continuity.

For CISOs and Security Teams

Implement defense in depth across prevention, detection, response, and recovery capabilities. Deploy dedicated anti-ransomware solutions that protect even when EDR is disabled or bypassed. Focus on identity security given that 98% of attacks use valid credentials. Architect for resilience with segmentation, redundancy, and ability to isolate compromised systems. Maintain immutable backups following 3-2-1 principles and test recovery regularly. Monitor for data exfiltration to detect and prevent double extortion scenarios. Automate response to achieve machine-speed defense against machine-speed attacks. Prioritize critical third parties for enhanced due diligence and scenario planning. Practice through tabletop exercises, red team assessments, and recovery drills. Build a culture of security where every employee understands their role in defense and response.

For the Financial Services Industry

Share threat intelligence rapidly through FS-ISAC and peer networks. Develop common standards for vendor security requirements and assessment. Support smaller institutions through shared services, resources, and expertise. Engage constructively with regulators to shape appropriate requirements. Invest in industry-wide resilience recognizing that every compromise weakens collective defense. Advocate for law enforcement action against ransomware operators and safe haven countries.

Conclusion: From Prevention to Resilience

The days of prevention-focused cybersecurity strategies are over. Modern ransomware threats–leveraging AI, exploiting identities, targeting supply chains, and deploying at machine speed–will eventually penetrate even the most robust defenses.

Financial institutions must shift from asking "Are we secure enough to prevent attacks?" to "Are we resilient enough to maintain operations when attacks succeed?"

This shift requires leadership commitment to cybersecurity as business continuity, comprehensive planning across technical, operational, legal, and communications dimensions, regular testing under realistic crisis scenarios, investment in recovery capabilities, third-party coordination to extend resilience across the ecosystem, and whole-of-society collaboration uniting industry, government, and communities.

The stakes are clear. Ransomware threatens customer trust built over decades, market stability and systemic resilience, economic vitality of communities, competitive position of individual institutions, and the integrity of the financial system itself.

Organizations that embrace comprehensive resilience will not only survive ransomware attacks–they will emerge stronger, more trusted, and better positioned for long-term success.

The choice is not whether to invest in ransomware resilience, but whether to do so proactively or to bear the far greater costs of reactive response after catastrophic failure.

The stakes are clear. Ransomware threatens customer trust built over decades, market stability and systemic resilience, economic vitality of communities,

Detect. Disrupt. Defeat Ransomware.

Halcyon is the leading anti-ransomware solution provider, purpose-built to defeat ransomware attacks. Our technology takes an end-to-end approach to proactively disrupt threats at every stage of the attack lifecycle, from pre-execution to data exfiltration and encryption.

For Financial Services Institutions, Halcyon Provides:

Prevention: AI and behavioral models trained exclusively on ransomware stop threats before execution while preventing attackers from disabling endpoint defenses.

Data Exfiltration Protection: Detection of bulk data movement stops data theft and double extortion while shielding security operations from tampering.

Recovery: Unique key capture and decryption technology reduces downtime from weeks to hours, without relying on backups.

24/7 Ransomware Operations Center (ROC): Our team of experts handles the fight against ransomware for you, at no additional cost.

The Halcyon Guarantee: Reduce risk with our comprehensive ransomware warranty and recovery services.

With Halcyon, financial institutions can:

- Eliminate ransom payments
- Ensure operational continuity
- Prevent data extortion
- Protect customer trust
- Maintain competitive position
- Meet regulatory requirements

Learn more at halcyon.ai or schedule a demo today.