SURELOCK TECHNOLOGY

RANSOMWARE READINESS

What Q1 2026 Threat Activity Means for Schools, Local Government and Mid-Market Organizations

THE OPERATING REALITY

Ransomware actors are moving faster, abusing trusted administrative tools, and returning to encryption as their primary pressure mechanism.

A SureLock Technology white paper | August 2026

Independent analysis informed by CISA, FBI IC3, Verizon, Sophos and Halcyon research

Executive summary

Ransomware is no longer only a criminal encryption event. In Q1 2026, the ecosystem blended financially motivated groups, state-aligned operators, destructive wiping, credential abuse, zero-day exploitation and the misuse of legitimate remote-management tools. For organizations with lean IT teams, the central risk is now the gap between machine-speed intrusion and human-speed response.

Q1 2026 AT A GLANCE

Halcyon recorded 2,108 attack claims involving 75 active groups across 89 countries - a 7.9% quarter-over-quarter increase.

The broader evidence reinforces the urgency. Verizon's 2026 Data Breach Investigations Report found ransomware in 48% of breaches in its dataset. The FBI's 2025 IC3 Annual Report recorded more than 3,600 ransomware complaints and reported losses exceeding $32 million, while cautioning through its complaint-based methodology that reported figures do not capture every incident or cost.

SureLock's conclusion is straightforward: prevention remains essential, but prevention alone is not a resilience strategy. Organizations need layered controls that reduce initial access, detect abnormal behavior, contain lateral movement quickly, protect recoverable data and rehearse business restoration before an incident.

Five findings leaders should act on

- Attack speed is outrunning manual response. Halcyon observed a fastest breakout time of 27 seconds, an average just under 30 minutes, and exfiltration within 72 minutes for the fastest quartile of intrusions.
- Encryption is back at the center of extortion. The leading groups relied on encryption as a primary pressure mechanism, increasing the importance of recovery readiness and anti-encryption controls.
- Trusted tools are part of the attack path. ScreenConnect, AnyDesk, Splashtop, PsExec, WMI, PowerShell and common transfer utilities appeared among abused legitimate tools.
- Edge and management systems remain high-value targets. Vulnerabilities affecting Cisco, Fortinet, Ivanti, BeyondTrust, VMware and Oracle products were prominent in Halcyon's reporting.
- Public-sector and critical-service disruption is operational, not theoretical. Healthcare, utilities and government organizations experienced clinic closures, manual operations and emergency declarations.

What multiple research sources agree on

Research source	2026 finding	Why it matters
Verizon DBIR	Ransomware appeared in 48% of breaches; 69% of ransomware victims did not pay.	Ransomware is widespread, while recovery without payment is increasingly central.
Sophos	79% of surveyed ransomware attacks began with an identity-based approach; 56% encrypted data.	Identity coverage and rapid containment must complement endpoint controls.
FBI IC3	More than 3,600 ransomware complaints and over $32 million in reported losses during 2025.	Critical infrastructure and public-service organizations remain high-value targets.

Research source	2026 finding	Why it matters
CISA StopRansomware	Maintain offline, encrypted backups and test their availability and integrity.	Recoverability must be demonstrated, not assumed.
Halcyon	2,108 Q1 attack claims across 89 countries, up 7.9% quarter over quarter.	Threat-group activity and operational tempo remain elevated.

Sources: Verizon 2026 DBIR; Sophos State of Ransomware 2026; FBI 2025 IC3 Annual Report; CISA StopRansomware Guide; Halcyon Q1 2026 Ransomware Evolution Report.

The Q1 2026 threat picture

Halcyon's dataset reflects publicly claimed ransomware activity, not every intrusion worldwide. It is best used as a directional view of adversary behavior and operational tempo rather than a complete census of incidents.

SureLock compared that threat-actor view with breach data, victim surveys, federal complaint reporting and government mitigation guidance. The sources use different methodologies and should not be combined into a single incident total; together, they provide a more balanced view of frequency, access methods, consequences and defensive priorities.

Measure	Q1 2026 observation	Leadership implication
Claimed attacks	2,108	Volume remains elevated; assume continued exposure.
Active groups	75	Defenders face a diverse and replaceable adversary ecosystem.
Countries targeted	89	Geography offers little insulation.
Quarterly change	+7.9%	The threat environment expanded from Q4.
Fastest breakout	27 seconds	Containment cannot depend only on a person seeing an alert.
Fastest-quartile exfiltration	Within 72 minutes	Identity, network and data controls must work together.

Who is under pressure

Manufacturing led the reported industry distribution at 23.3%, followed by business services (12.4%), construction (8.7%), legal services (6.4%) and retail (6.0%). Although education was not listed among the top five, school systems share several of the same risk factors: distributed locations, broad identity populations, aging infrastructure, third-party access and limited 24/7 staffing.

Government accounted for 67 attack claims (3.2%), while energy, utilities and waste recorded 71 (3.4%) and healthcare services 149 (7.1%). These percentages can appear modest until the operational impact is considered: interrupted clinics, manual utility operations, exposed regulated data and unavailable public services.

How ransomware operations are changing

1. Criminal and state-aligned activity is converging

Halcyon reported ransomware-linked activity associated with North Korea, China and Iran. This convergence matters because an incident may pursue payment, intelligence collection, disruption, destruction or several objectives at once. A response plan designed only around ransom negotiation can miss the actual mission of the operator.

2. Encryption has regained leverage

Data-theft-only extortion has not disappeared, but Halcyon observed weakening economics for exfiltration-only campaigns and renewed reliance on encryption among leading groups. Organizations must therefore plan for both confidentiality loss and operational paralysis.

3. Affiliates and brands change faster than defenses

Qilin led the quarter, while TheGentlemen accelerated after splitting from Qilin and DragonForce advanced through a cartel-style affiliate model. Group names may change, merge or disappear; durable defenses should be mapped to behaviors - credential theft, remote access, lateral movement, exfiltration and encryption - rather than to one threat brand.

4. Legitimate administration tools create a dual-use problem

Remote support, scripting and file-transfer tools are indispensable to IT operations. They are also attractive to adversaries because they can blend into normal activity. The objective is not to ban every tool. It is to know which tools are authorized, restrict who may run them, require strong authentication, log their use and alert on unusual execution paths or destinations.

The SureLock ransomware resilience model

A practical program should reduce the probability of compromise while limiting blast radius and shortening recovery. SureLock recommends six mutually reinforcing layers.

Layer	Core objective	Priority actions
1. Govern	Create accountability	Name owners; maintain an asset inventory; rank critical services; define incident authority.
2. Reduce exposure	Close likely entry paths	Patch internet-facing systems; harden VPN/RMM; remove stale accounts; apply MFA and conditional access.
3. Detect	Identify abnormal behavior early	Centralize logs; monitor identity and endpoint behavior; maintain 24/7 escalation for high-severity events.
4. Contain	Limit lateral movement	Segment networks; restrict admin paths; isolate affected endpoints; protect privileged credentials.
5. Recover	Restore trusted operations	Use immutable/offline-capable backups; verify coverage; test restores; document dependencies and recovery order.

Layer	Core objective	Priority actions
6. Improve	Turn exercises into action	Run tabletop exercises; measure response time; track findings to closure; update playbooks after change.

DESIGN PRINCIPLE

No single product provides ransomware resilience. The control system must still work when one identity, endpoint, remote tool or security layer is compromised.

A 90-day action plan

Days 0-30 | Establish visibility and close obvious gaps

- Confirm ownership, support status and patch level for every internet-facing firewall, VPN, email gateway, RMM, hypervisor and management appliance.
- Inventory remote-access and file-transfer tools; remove unauthorized instances and document approved business use.
- Review privileged and service accounts, enforce MFA where supported, rotate exposed or shared credentials and disable dormant access.
- Verify that every critical server and SaaS data set is included in backup scope, with protected copies that cannot be altered using ordinary administrator credentials.
- Document who can declare an incident, isolate systems, contact legal counsel, notify cyber insurance and communicate with executives.

Days 31-60 | Build machine-speed detection and containment

- Tune endpoint, identity, firewall and cloud alerts around credential theft, abnormal remote execution, lateral movement and bulk data transfer.
- Establish 24/7 monitoring and a tested high-severity escalation path; define when automated isolation is appropriate.
- Segment management networks and restrict administrative access through hardened jump paths.
- Test restoration of one representative identity service, application server and data workload; record actual recovery time and dependencies.

Days 61-90 | Prove operational resilience

- Run an executive tabletop covering encryption, data theft, destructive wiping and third-party compromise.
- Conduct a technical recovery exercise using clean-room assumptions and known-good credentials.
- Resolve the highest-risk findings, assign dates for the remainder and report exceptions to leadership.
- Create a quarterly cadence for exposure review, restore testing, incident exercises and executive metrics.

Questions executives should ask

- Can we identify every externally accessible management system and its accountable owner today?
- Which alerts receive a response at 2:00 a.m., and how quickly can an endpoint or account be contained?
- Could a compromised domain administrator delete or encrypt our backups?
- What are the first five services we must restore, and have we tested that sequence?
- Where are remote administration tools permitted, and how do we detect unauthorized use?
- How would we operate for 24, 48 and 72 hours without core systems?
- When did leadership last practice the legal, insurance, communications and operational decisions required during ransomware?

Metrics worth reporting

Metric	What good looks like
External attack surface	Known assets, accountable owners and remediation dates for material findings.
Critical patch latency	Risk-based SLA with tracked exceptions and executive visibility.
MFA coverage	All privileged and remote access covered; gaps explicitly accepted.
Detection-to-containment	Measured in minutes for high-confidence events, including after hours.
Backup recoverability	Documented coverage, protected copies and successful restore evidence.
Exercise closure	Findings assigned, dated and verified closed.

How SureLock can help

SureLock Technology helps organizations turn cybersecurity tools into an operating resilience program. Engagements can be scoped to the customer's current environment and risk profile, including:

- Ransomware readiness and security posture assessments
- Firewall, network segmentation and secure remote-access design
- Identity, endpoint, email and vulnerability-management improvements
- 24/7 security monitoring and incident escalation
- Backup, disaster recovery and recovery validation
- Incident-response planning, tabletop exercises and executive reporting

RECOMMENDED NEXT STEP

Begin with a focused ransomware readiness review that validates external exposure, privileged access, monitoring coverage, containment authority and recoverability of critical systems.

The goal is not to promise that an incident can never occur. It is to make intrusion harder, detection faster, impact smaller and recovery more predictable.

Methodology, attribution and use

This white paper is an original SureLock Technology analysis drawing on public research from the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation's Internet Crime Complaint Center (FBI IC3), Verizon, Sophos and Halcyon Tech, Inc. The sources use different datasets and methodologies, including breach investigations, victim surveys, public attack claims, complaint reporting and government guidance. Their statistics should be interpreted within those individual methodologies and should not be added together as a single incident count.

Selected statistics and factual observations are attributed to their respective publishers; the interpretation, recommendations and resilience model are SureLock's own. The publishers' reports, brands, wording, graphics and underlying presentations remain the property of their respective owners and licensors. SureLock does not claim sponsorship, endorsement or affiliation, and no third-party graphic or substantial passage has been reproduced in this paper.

Legal and professional notice: This publication is for general informational purposes and is not legal advice, a guarantee of security, or a substitute for an organization-specific technical, legal, insurance or regulatory assessment.

Research sources

CISA. StopRansomware Guide. View source

Federal Bureau of Investigation, Internet Crime Complaint Center. 2025 IC3 Annual Report. View source

Verizon. 2026 Data Breach Investigations Report. View source

Sophos. The State of Ransomware 2026. View source

Halcyon Tech, Inc. Ransomware Evolution Report, Q1 2026. View source

Sources accessed August 17, 2026.

About SureLock Technology

SureLock Technology is a Georgia-based technology solutions provider serving K-12 education, local government, higher education and commercial organizations. SureLock delivers cybersecurity, networking, data center, backup and disaster recovery, managed services and professional services designed to improve security and operational resilience.

SureLock Technology | Buford, Georgia