Ransomware and Cyber Extortion

A DJND field guide to response, recovery, and prevention

SOURCE	Condensed from *Ransomware and Cyber Extortion: Response and Prevention* by Sherri Davidoff, Matt Durrin, and Karen Sprenger (Pearson, 2023).
SCOPE	Impact, attack lifecycle, crisis management, containment, investigation, negotiation, payment, recovery, and prevention.
USE	Operational reference for defenders, responders, technical leaders, and crisis stakeholders. It is not legal advice or a replacement for an incident-specific response plan.

The point

Ransomware is usually the loudest part of a longer intrusion. By the time the note appears, the attacker may already have credentials, persistence, internal knowledge, and copied data. Treating the encrypted files as the whole incident is how reinfection gets invited back in.

- Stop the damage without destroying the evidence.
- Run technical response, business recovery, legal analysis, and communications as one coordinated incident.
- Restore into a controlled environment. A backup is useful only if it is clean, reachable, and tested.
- Payment and negotiation are risk decisions, not technical shortcuts.

Contents

Currency warning

The source was published in 2023. Threat actors, sanctions, reporting rules, insurance requirements, cryptocurrency controls, and government guidance change. Verify current legal and regulatory requirements with qualified counsel and current official sources during an incident.

PART I

Understand the Threat

Extortion weaponizes business impact. Encryption is only one way to create leverage.

What cyber extortion targets

The attacker pressures confidentiality, integrity, or availability to force action or payment.

- **Denial:** block access to systems or data through encryption, deletion, or service disruption.
- **Modification:** threaten or perform unauthorized changes that undermine trust in data or systems.
- **Exposure:** steal information and threaten publication, sale, or disclosure.
- **Faux extortion:** claim access or theft without proving it. A threat is evidence of a claim, not evidence of compromise.

Why the impact spreads

- Operational outages interrupt services, safety processes, revenue, and customer access.
- Costs include response, restoration, legal work, notifications, downtime, new infrastructure, and long-term monitoring.
- Exposure can trigger contractual duties, regulatory scrutiny, litigation, and reputational damage.
- A compromised MSP, cloud provider, software vendor, or technology supplier can scale one intrusion across many victims.

The Criminal Operating Model

Ransomware became an industry

Asymmetric cryptography, cryptocurrency, anonymizing networks, standardized tooling, and ransomware-as-a-service lowered the barrier to entry. Specialized operators can sell access, deploy payloads, negotiate, process payments, publish stolen data, or support affiliates.

- Opportunity and targeting can coexist. Broad scanning finds access; research determines what that access may be worth.
- Double and multicomponent extortion combine encryption, theft, publication threats, denial of service, and contact with customers or partners.
- Attackers use portals, countdowns, media pressure, and scripted communication because the pressure campaign is part of the product.

> The malware family matters. The business process matters more.

Victim selection

- **Opportunistic:** the victim exposes a weakness that the attacker can exploit at scale.
- **Targeted:** the attacker selects an organization and develops access deliberately.
- **Hybrid:** the initial access is opportunistic, then the attacker appraises the victim and decides how much effort and pressure to apply.

Anatomy of an Extortion Attack

1. Entry	Phishing, exposed remote access, stolen credentials, unpatched software, or a compromised supplier.
2. Expansion	Persistence, reconnaissance, credential access, privilege escalation, and lateral movement broaden control.
3. Appraisal	The attacker identifies valuable systems, data, backups, insurance clues, revenue pressure, and operational dependencies.
4. Priming	Security tools, processes, logging, accounts, and recovery mechanisms may be weakened or disabled.
5. Leverage	Data is copied, systems are encrypted or deleted, or services are disrupted.
6. Extortion	The attacker delivers demands, contacts third parties, sets deadlines, or publishes data.

The ransom note is not patient zero. It is the attacker announcing that earlier controls already failed.

Detection opportunities

- Unexpected remote logons, new accounts, privilege changes, suspicious scheduled tasks, and unusual administrative tooling.
- Security software disabled, logs cleared, backup systems accessed, or monitoring interrupted.
- Large outbound transfers, unusual cloud storage use, archive creation, or traffic to unfamiliar infrastructure.
- Rapid file changes, extensions changing, inaccessible shares, ransom notes, or simultaneous failures across systems.

PART II

Take Control of the Crisis

The first hours need ownership, priorities, and controlled communication. Panic is not an incident-management framework.

Activate the response

- Appoint an incident manager with authority to coordinate work, maintain status, and resolve conflicts.
- Bring in security, IT, legal or breach counsel, leadership, finance, communications, insurance, business owners, and external responders as required.
- Establish an out-of-band communication method if email, identity, or collaboration systems may be compromised.
- Start a protected incident record: decisions, evidence, actions, owners, timestamps, costs, and unresolved questions.

Triage before improvising

- Identify what is happening now: encryption, theft, denial of service, persistence, or an unverified claim.
- Map affected identities, systems, locations, business services, data, third parties, and cloud environments.
- Define recovery objectives and the minimum services required to operate safely.
- Assess available people, evidence, credentials, tooling, documentation, insurance, and budget.
- Build a living response strategy with goals, tasks, owners, timing, dependencies, and costs.

Communication Is a Control

Internal coordination

Use a fixed reporting rhythm. Separate confirmed facts, working hypotheses, decisions, and requests. If all four are mixed together, the status meeting becomes another incident.

- Limit sensitive details to people who need them. Assume compromised systems may be monitored.
- Use one authoritative timeline and task register.
- Give leadership operational impact, options, costs, risks, and decision deadlines—not a stream of raw indicators.
- Prepare shift handoffs. Long incidents punish undocumented memory.

Affected parties and the public

- Coordinate statements with counsel, communications, leadership, and applicable regulators or insurers.
- Do not speculate, minimize, exaggerate, or promise outcomes the investigation has not established.
- Prepare for the attacker to contact employees, customers, media, partners, or executives directly.
- Track notification obligations and approval paths. A technically accurate statement can still create legal or operational damage if released badly.

PART III

Contain and Investigate

Containment stops the current damage. Investigation tells you what else must be stopped.

Contain active harm

- Gain trusted administrative access. Do not rely on credentials or tooling the attacker may control.
- Stop encryption or deletion by restricting access, isolating hosts, killing malicious processes, or removing power when the evidence and operational tradeoff justify it.
- Block exfiltration paths, suspicious cloud services, unauthorized forwarding rules, and malicious outbound traffic.
- Mitigate denial-of-service activity using network, provider, and application controls.
- Preserve encrypted data and affected systems when they may be needed for recovery, decryption, legal analysis, or evidence.

Containment is a sequence of risk decisions. Pulling every plug may stop one process while deleting volatile evidence and taking critical services with it.

Lock out the attacker

- Disable malicious remote access and unauthorized persistence.
- Reset compromised local, domain, cloud, service, and privileged credentials in a controlled order.
- Audit new accounts, tokens, keys, sessions, forwarding rules, applications, and trust relationships.
- Enforce multifactor authentication where feasible and close unnecessary perimeter exposure.
- Restrict third-party access and assess whether trusted software or supplier channels were compromised.

Threat Hunting and Investigation

Hunt beyond the obvious systems

- Use EDR, SIEM, NDR, identity logs, vulnerability data, cloud logs, email records, network telemetry, and system artifacts.
- Search for the same identities, infrastructure, tools, persistence, access methods, and behaviors across the environment.
- Isolate suspicious hosts, deactivate malicious accounts, remove unauthorized software, and update detections with confirmed indicators.
- Record negative findings and coverage limits. “Nothing found” means very little when the telemetry never existed.

Questions the investigation must answer

- How did the attacker enter, and when?
- Which identities, systems, data, tenants, and third parties were affected?
- What persistence and privileges remain?
- Was data accessed, modified, destroyed, or exfiltrated?
- Which evidence supports each conclusion, and where are the gaps?
- What legal, regulatory, contractual, insurance, and notification duties may apply?

Preserve evidence

Prioritize volatile sources while keeping chain of custody, integrity, access control, retention, and legal requirements in view.

- Memory, active connections, processes, sessions, and transient cloud data can disappear quickly.
- Preserve logs, ransom notes, communications, malware, disk and system artifacts, authentication history, network records, and third-party evidence.
- Coordinate collection decisions with responders and counsel. Rebuilding first and asking questions later usually leaves expensive questions unanswered.

PART IV

Negotiate and Evaluate Payment

Communication with an extortionist may buy information or time. It does not create trust.

Before contact

- Define the goal: time, information, proof of access, proof that decryption works, reduced demand, or an agreement.
- Set authority, budget limits, deadlines, information-sharing boundaries, and escalation paths.
- Use an experienced negotiator and a controlled communication channel.
- Prepare stakeholders for pressure tactics, deadlines, threats, direct outreach, and publication claims.

During negotiation

- Keep the tone neutral, professional, brief, and factual.
- Do not disclose insurance limits, revenue pressure, internal conflict, recovery status, or facts that increase leverage.
- Do not bluff, threaten, insult, or make promises you cannot keep.
- Require proof of life appropriate to the claim: sample decryption, evidence of possession, or other verifiable capability.
- Treat proof as limited. Decrypting a sample does not prove every system can be restored or that copied data will be deleted.

The Payment Decision

Payment can fund crime, may be prohibited, may fail, and does not erase the breach. Refusing payment can also carry severe operational consequences. The decision belongs to authorized leadership using current legal, sanctions, insurance, operational, and investigative input.

Required decision inputs

- Is payment legally permitted after current sanctions and recipient due diligence?
- What do counsel, law enforcement, insurers, and contractual obligations require?
- Can clean recovery meet the operational deadline without payment?
- Has the attacker demonstrated a working decryptor or credible possession of data?
- What are the financial, safety, continuity, litigation, and reputational consequences of each option?
- Who is authorized to approve funds, the intermediary, the currency, and the accounting treatment?

If payment is authorized

- Use qualified counsel and a vetted payment intermediary.
- Document due diligence, approvals, communications, timing, exchange-rate exposure, and transaction details.
- Confirm receipt and collect promised deliverables, but continue investigation and recovery as though the attacker may fail to cooperate.
- Report or notify appropriate authorities and parties as required.

A decryptor is untrusted software supplied by the attacker who caused the incident. Test it accordingly.

PART V

Recover Without Reinfecting

Recovery restores trusted business capability. Copying old problems onto new hardware is not recovery.

Build a controlled recovery environment

- Preserve critical evidence and back up important configuration and data, including encrypted data when relevant.
- Use segmented recovery networks to separate forensic, build, validation, and production activity.
- Rebuild core network and security controls with trusted configurations and credentials.
- Enable monitoring and logging before restored systems return to production.
- Define a repeatable system-restoration process covering evidence, rebuild or cleaning, patching, credential reset, validation, malware checks, and monitoring.

Restore in dependency order

- Identity and domain services must be trusted before dependent systems authenticate against them.
- Network services, name resolution, time, certificates, security tooling, and management infrastructure may be prerequisites.
- Prioritize systems by business function, safety, dependencies, and validated recovery objectives—not by whoever complains first.
- Keep infected or uncertain systems isolated until disposition is clear.

Data Restoration and Decryption

Select the safest viable source

- Known-clean offline or immutable backups are preferable when they contain the required data and can be restored in time.
- Production remnants, replicated data, reconstructed records, and decrypted files may supplement recovery but require validation.
- Check backup age, integrity, malware risk, dependencies, and whether attacker access predates the backup.
- Move restored data through controlled staging. Scan, test, reconcile, and document before production use.

Using a decryptor

- Preserve original encrypted data before testing.
- Test on copies and representative file types, sizes, applications, and storage conditions.
- Run the tool in an isolated environment with monitoring.
- Measure speed, failures, corruption, naming changes, metadata loss, and operational impact.
- Verify file and application integrity after decryption; scan for malware before data returns to production.

Recovery is not the end

- Maintain monitoring for persistence, reinfection, credential misuse, and data publication.
- Support legal, regulatory, insurance, notification, customer, and litigation work that may continue after systems return.
- Run a post-incident review, assign corrective actions, fund them, and track them to closure.

PART VI

Reduce the Next Incident

Ransomware prevention is not one control. It is a security program with fewer blind spots and less attacker leverage.

Know the environment and its obligations

- Inventory systems, identities, data, cloud services, suppliers, dependencies, and administrative access.
- Classify critical data and business services. Define owners and recovery requirements.
- Track applicable laws, regulations, contracts, and insurance conditions with qualified legal input.
- Assess risk continuously and tie remediation to business consequence.

Reduce entry and expansion

- Use phishing-resistant authentication where possible, secure remote access, and remove unnecessary exposure.
- Patch based on exploitability, exposure, asset value, and active threat—not a ceremonial monthly percentage.
- Control privileged access, service accounts, secrets, lateral movement, and third-party connections.
- Deploy and operate endpoint, network, identity, email, cloud, and vulnerability controls with continuous monitoring.
- Threat-hunt for behaviors that preventive controls miss.

Operational Resilience

Backups that survive the incident

- Maintain multiple copies with offline or immutable protection and separate administrative credentials.
- Cover data, configurations, identity services, cloud resources, SaaS data, and critical infrastructure.
- Monitor backup jobs and unauthorized changes. Attackers appraise backups because defenders depend on them.
- Test restoration against real recovery-time and recovery-point objectives. A green backup dashboard is not a recovery test.

Reduce the value of stolen data

- Retain only what the organization needs and can defend.
- Restrict access by role and business need; review access and sharing continuously.
- Monitor large transfers, unusual destinations, archive creation, cloud sharing, and email forwarding.
- Use data-loss prevention as one layer. It does not replace inventory, access control, logging, or investigation.

Prepare the organization

- Maintain business continuity and disaster recovery plans aligned to the same dependencies.
- Exercise ransomware scenarios with technical teams, executives, legal, communications, finance, and business owners.
- Test decisions, communications, evidence access, credentials, vendor contacts, and recovery—not just whether the meeting finished on time.

PART VII

Operational Checklists

Keep these available outside the environment they are meant to recover.

Immediate response

- Activate incident response and appoint the incident manager.
- Move coordination to trusted communications.
- Confirm current malicious activity and operational impact.
- Engage required internal and external stakeholders.
- Preserve volatile evidence and start the decision timeline.
- Contain encryption, deletion, exfiltration, denial of service, and persistence.
- Reset and secure identities in a controlled order.
- Scope affected systems, accounts, data, locations, and suppliers.
- Define recovery priorities and build the isolated recovery environment.

Decision controls

- Record who has authority for containment, shutdowns, evidence tradeoffs, communications, spending, negotiation, and payment.
- Separate confirmed facts, assumptions, risks, decisions, owners, and deadlines.
- Reassess strategy as evidence and operational conditions change.

Resources to Prepare in Advance

Plans	IR, crisis communications, business continuity, disaster recovery, evidence collection, restoration, and investigation procedures.
People	Named primary and backup owners for incident command, technical response, legal, finance, communications, recovery, and business decisions.
Contacts	After-hours contacts for leadership, counsel, insurer, forensic responder, negotiator, bank, vendors, PR, law enforcement, and regulators.
Access	Emergency credentials and methods for logging, EDR, SIEM, backups, network equipment, cloud, identity, servers, and endpoints.
Evidence	Source inventory, retention periods, collection procedures, preservation tools, and priorities approved with counsel.
Architecture	Current diagrams, asset and data inventories, dependencies, admin access, domain structure, configurations, and gold images.
Recovery	Prioritized business services, restoration order, clean build process, backup validation, and isolated recovery capacity.
Templates	Response strategy, status reports, decision log, internal notices, public statements, and regulator or insurer notifications.

If the response plan, contact list, credentials, and architecture diagrams are available only through the compromised environment, they are not response resources. They are hostages.

Program Readiness Checklist

Governance

- One owner is accountable for maintaining the extortion-response capability.
- Approval paths and decision authority are documented.
- Legal, regulatory, contractual, insurance, and notification requirements are reviewed regularly.
- Plans are updated after exercises, incidents, technology changes, and risk assessments.

Detection and response

- Critical telemetry is centralized, retained, protected, and monitored around the clock.
- EDR, NDR, identity, cloud, email, backup, and vulnerability signals feed actionable response processes.
- The organization can isolate systems, disable access, preserve evidence, and communicate without the primary environment.
- Outside response support is contracted or identified before the emergency.

Recovery

- Backups are segregated, protected, monitored, and restored in testing.
- System dependencies and business recovery order are documented and approved.
- Clean-build capability and emergency infrastructure are available.
- Exercises include loss of identity, email, remote access, backups, cloud control, and third-party services.

Final rule

Assume the attacker has read the same playbooks. The advantage comes from knowing your environment, detecting earlier, making controlled decisions, and practicing recovery before the clock starts.