OpenSSL CONFERENCE

During a Breach

How Encryption Is Evaluated by Regulators, Insurers, and Counsel

Amanda McAllister Novak
Constangy, Brooks, Smith & Prophete LLP

13.10.2026

Ransomware Attacks

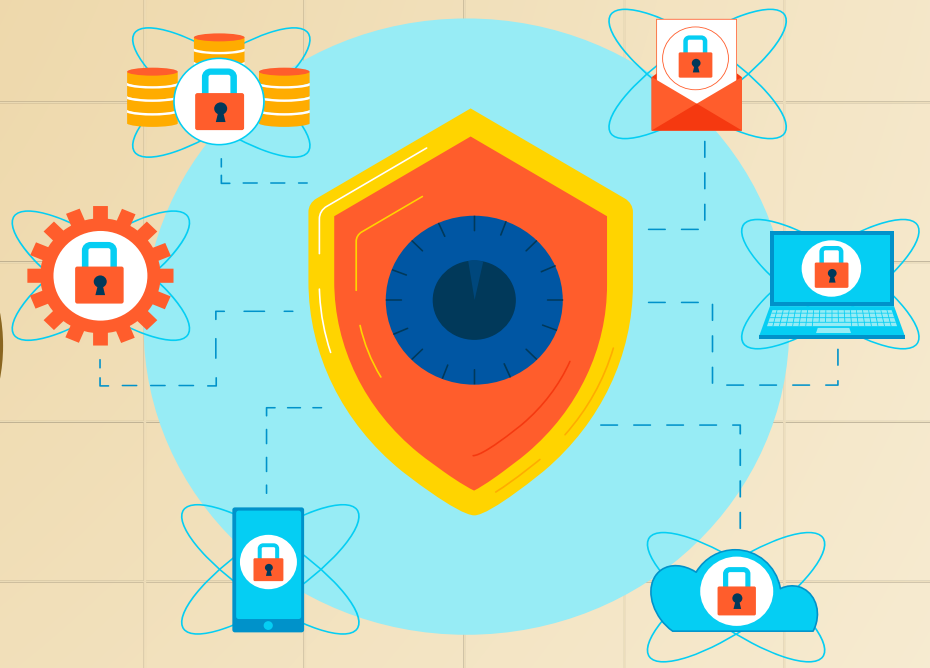
- **Full-scale Criminal Business Models**
  - Ransomware-as-a-service
  - Customized malicious code, credential stealing Trojans, stealthy attack tools
  - Press releases, shaming sites, outreach to leverage payment
  - Aggressive communication and secondary attacks
- **Effective execution of attacks**
  - Multiple attack vectors – phishing, RDP, unpatched vulnerabilities
  - Legitimate applications used for malicious purposes
  - Deletion of backup data
  - Theft of sensitive data before encryption

Phases of an Incident: Technical

01 **Preparation**
Establish and test response procedures, responsibilities, and evidence preservation before an incident.

02 **Detection & Analysis**
Review alerts and other evidence to determine whether an incident occurred and assess its scope and impact.

03 **Containment**
Limit the attacker's access and prevent further spread or data loss while preserving relevant evidence.



04 **Eradication**
Remove malicious access and artifacts, and address the weaknesses that allowed the attacker into the environment.

05 **Recovery**
Restore affected systems safely, validate operations, and monitor for renewed compromise.

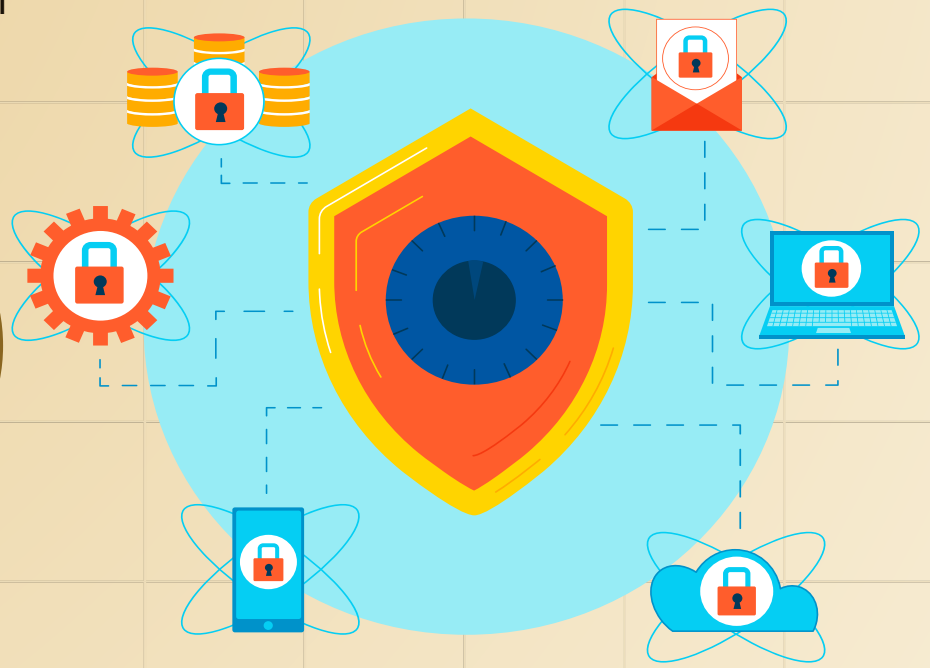
06 **Post-Incident Activity**
Review the response, document lessons learned, and improve procedures and security controls.

Phases of an Incident: Legal

01 **Evaluation of potential data exposure**
What information could have been involved?

02 **Evaluation of actual data exposure**
What information was accessed or acquired?

03 **Evaluation of the types of data involved**
What information is regulated, and which legal frameworks apply?



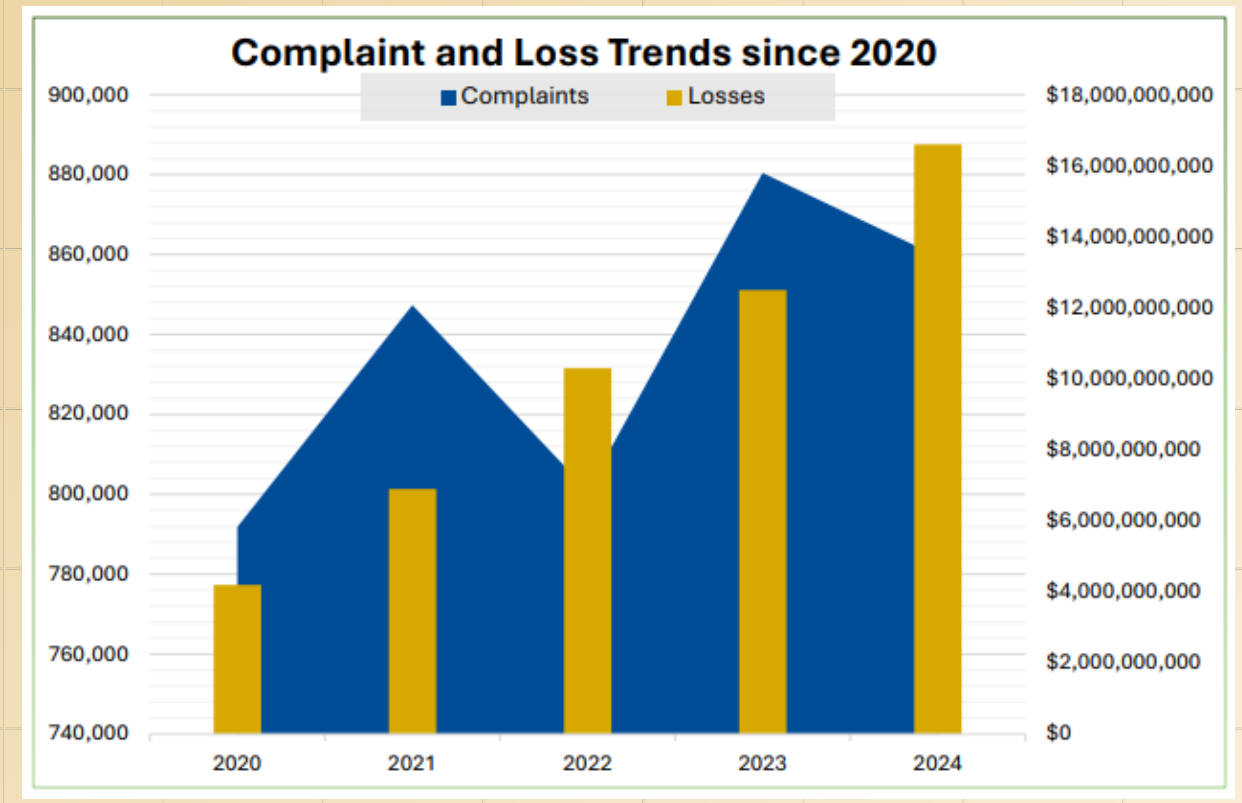
Contractual obligations **04**
What incident reporting duties do the agreements impose? Have they been triggered?

Notification obligations **05**
Who must be notified, when, and how? What communications are needed?

Post-Notification Activity **06**
Respond to lawsuits and regulatory inquiries.

Cyber Crime Trends

- In 2024, the IC3 received a total of 859,532 complaints. Reported losses increased 33% from about $12.5 billion to $16.6 billion. Since 2000, IC3 has received more than 9 million complaints.



*FBI Internet Crime Report 2024

External Resources

BROKER

DIGITAL FORENSICS AND INCIDENT RESPONSE FIRM

CYBER INSURANCE CARRIER

DATA MINING VENDOR

OUTSIDE INCIDENT RESPONSE COUNSEL OR "BREACH COACH"

NOTIFICATION AND REMEDIATION SERVICES

PUBLIC RELATIONS FIRM

A Tale of Two Ransomware Attacks

- Two hypothetical U.S. healthcare organizations, Scylla and Charybdis, each hold records for approximately 100,000 patients across multiple U.S. states, as well as employee records.
- Both are subject to HIPAA.
- On Monday morning, both organizations discover that ransomware has disrupted their systems and find a ransom note.

ATTENTION!
Your network has been breached and all data was encrypted. Please contact us at:
[redacted].onion/

Login ID: [redacted]

! To access .onion websites download and install Tor Browser at:

[redacted] (Tor Browser is not related to us)

! To restore all your PCs and get your network working again, follow these instructions:

- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.

Please follow these simple rules to avoid data corruption:

- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption.

- Do not hire a recovery company. They can't decrypt without the key.
They also don't care about your business. They believe that they are
good negotiators, but it is not. They usually fail. So speak for yourself.

Waiting you in a chat.

Response and Investigation

- IT isolates affected systems while employees use downtime procedures.
- The organization engages counsel, its insurer, and forensic investigators.
- The recovery team assesses backups.
- The attacker claims to have exfiltrated an archive containing patient and employee information.

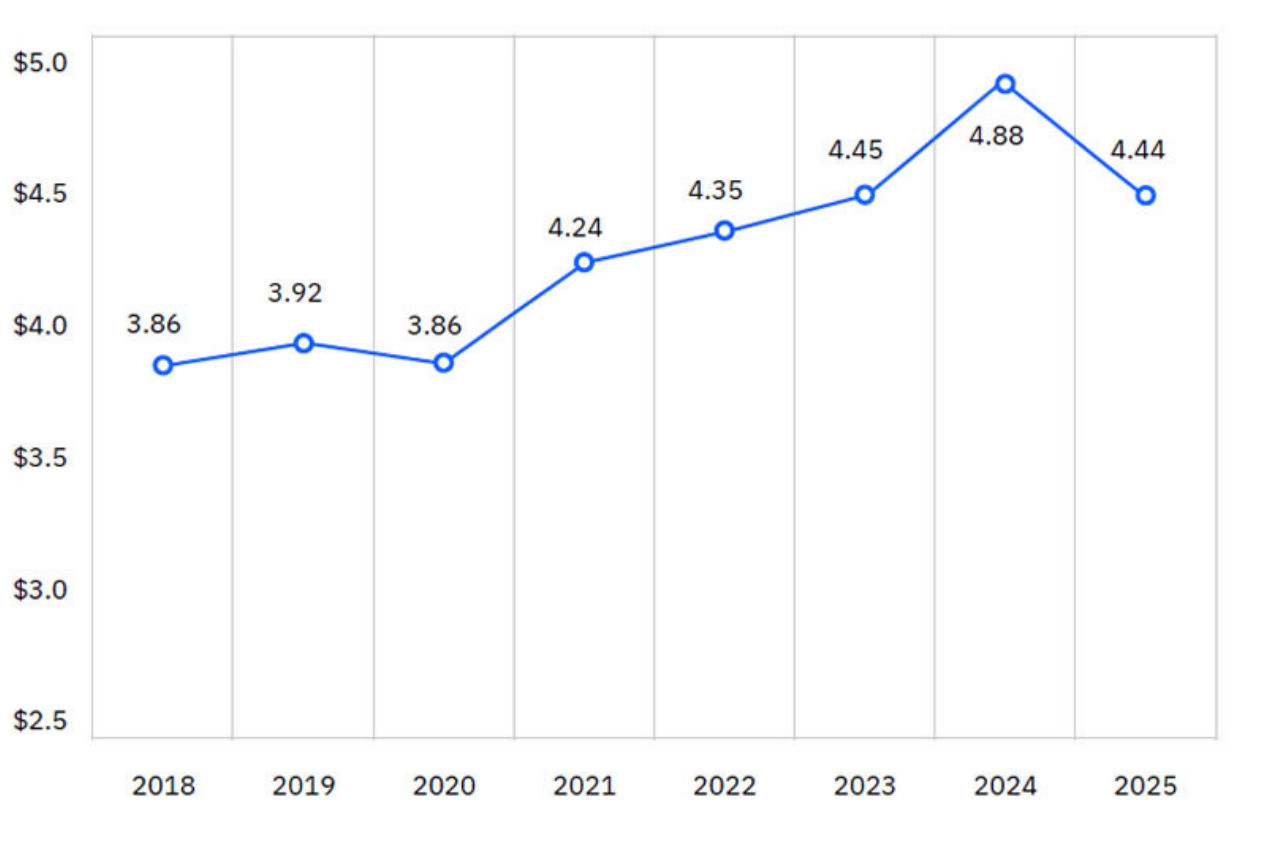
Scylla and Charybdis

Investigation finding	Scylla – No Reportable Breach	Charybdis – Reportable Breach
Stolen archive	The archive was encrypted before the attack.	Readable patient and employee records
Attacker's capability	The compromised account could copy only encrypted files, with no readable access or means of decryption.	The attacker provides readable files as proof of exfiltration.
Outcome	The investigation supports that no readable information was exposed.	The attacker publishes stolen data on the dark web after no ransom payment.

Charybdis's Notification Response

- Six-week data review, followed by intensive internal efforts for correction of gaps, duplicates, and missing addresses
- Coordination with more than 50 covered entities (and their legal counsel) under business associate agreements
- Approximately 90,000 patient notices, employee notices, call center support, and identity protection
- Substitute notice, media notification, and reports to OCR and applicable state regulators
- Regulatory investigations and class action lawsuits

Global Average Cost of a Data Breach



IBM's 2026 Report raised the average to a record $4.99 million.

Healthcare data breaches are the costliest out of all industries, with an average of $7.42 million

IBM 2025 Cost of a Data Breach Report; https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-2025/

Putting the Legal Pieces Together

- U.S. state breach statutes vary by residence, information type, and the nature of the compromise.
- Federal and sector-specific obligations may also apply.
- Encryption exceptions and risk assessments depend on the applicable law and investigation findings.

The Definition of Personal Information

Employee records	Patrick in Kansas	Lamar in Maryland
Exposed records	Name and readable medical information in electronic personnel records	Name and readable medical information in electronic personnel records
State definition	Medical information is not a listed element under the Kansas statute.	Name plus readable health information is covered by the Maryland statute.
Notification analysis	Likely **no** notification obligation.	Likely notification obligation.

Access v. Acquisition

Applicable trigger	Matthew in California	Baker in Florida
Readable name and Social Security number	Acquired, or reasonably believed to have been acquired, by an unauthorized person	Unauthorized access to electronic data containing personal information
Forensic question	What supports a conclusion of acquisition?	What information did the unauthorized actor access?

Where Does Encryption Fit In?

Employer subject to the state statute	Jordan in Wisconsin	Kyler in Minnesota
Affected information	Name and Social Security number	Name and Social Security number
Encryption analysis	Protected elements fall outside the definition if encrypted, redacted, or altered to be unreadable.	Protected data remains covered if the key, password, or other means to read or use it was also acquired.

Risk of Harm

- Some statutes allow an assessment that individual notification is unnecessary.
- The required investigation, harm standard, and procedural steps vary.
- Readable sensitive information stolen, threatened with disclosure, or published can make a favorable assessment difficult to support.

State Regulatory Reporting

Reporting approach	Example or implication
No general regulatory report	Some general state breach statutes, such as in Michigan, do not require one.
Numerical threshold	Texas: at least 250 residents requiring notice
Any affected resident requiring notice	New York: reporting can be required for one resident

HIPAA

- The Breach Notification Rule applies to unsecured protected health information.
- Encryption consistent with HHS guidance can remove information from that notification requirement if the means of decryption remains protected.
- For unsecured PHI, the assessment considers the information, recipient, actual acquisition or viewing, and mitigation.
- Ransomware's possession or control of PHI can trigger the breach presumption even without confirmed exfiltration.

Financial-Sector Reporting

Regulatory report	FTC Safeguards Rule	New York DFS
Who reports	Covered financial institutions	Entities covered by the DFS cybersecurity regulation
Relevant trigger	Unauthorized acquisition of unencrypted customer information involving at least 500 consumers	Qualifying incidents, including ransomware deployed within a material part of the covered entity's systems
Reporting time	As soon as possible, no later than 30 days after discovery	As promptly as possible, no later than 72 hours after determining an incident occurred
Role of encryption	Information is treated as unencrypted if an unauthorized person accessed the key.	Encryption does not remove the ransomware reporting trigger.

GDPR

Controller's obligations	Article 33	Article 34
Recipient	Supervisory authority	Affected individuals
Threshold	Notice required unless the breach is unlikely to result in a risk to rights and freedoms	Communication required if the breach is likely to result in a high risk to rights and freedoms
Timing	Without undue delay and, where feasible, within 72 hours of awareness	Without undue delay
Role of encryption	Encryption informs the risk assessment. Availability and integrity also matter.	Article 34(3)(a) exempts communication if protective measures rendered the affected data unintelligible to unauthorized persons.

Lost in Translation

Connecting technical findings to legal decisions

- Containment and restoration proceed alongside forensic investigation and legal analysis.
- Counsel needs to understand what information was affected and how.
- The technical team and forensic investigators need to explain what information the attacker could access, whether it was readable, and what evidence supports those findings.

Preservation and Recovery

- Wiping or rebuilding systems can eliminate evidence relevant to the scope of the compromise.
- Preservation should be coordinated with containment and recovery from the beginning.
- Urgent operational and patient-care needs remain part of the response.
- For both organizations, the investigation examines when the archive was created, whether encryption protected it during the attack, and whether the attacker obtained any readable copies.

Questions About Encryption

- Was the affected information protected at the time of unauthorized access or acquisition?
- Did the attacker obtain encrypted files or readable information?
- Did the attacker obtain the means to decrypt the information?
- What evidence supports those answers?

The Attacker's Actual Access

- Encryption must be evaluated in the context of the incident.
- The investigation determines whether the attacker could read the affected information or obtain the means to decrypt it.
- Those findings inform counsel's notification and reporting analysis.

How Readability Affects Notification

Evidence of readable data	Only encrypted files acquired
Validate authenticity and the source of the records.	The investigation determines whether the information remained unreadable to the attacker.
The investigation determines the source and scope of the readable information the attacker obtained.	Investigators assess whether the attacker obtained the key or other means of decryption.
.An encryption exception does not protect information the attacker obtained in readable form	An encryption exception may remove notification obligations if the information remained unreadable and the attacker lacked the means to decrypt it.

Documenting the Conclusion

- HIPAA places the burden on the covered entity or business associate to demonstrate notification or explain why the event was not a breach.
- The legal analysis should record what was encrypted, what the attacker could access, and the evidence supporting the determination.
- People answering questions months later need a record of how the organization reached its decision.

Under the Microscope

The Regulatory Investigation

- A request for information can examine the security program before the attack, the response, and subsequent improvements.
- Questions may cover policies, risk assessments, remediation, training, and supporting records.

Encryption Policy and Practice

- The organization needs to explain how the policy operated in practice.
- Technical teams often hold the information counsel needs for a regulatory response.
- Records of implementation, exceptions, and remediation are easier to assemble before an incident and regulatory investigation.

Litigation

- Plaintiffs may question data protection, known weaknesses, and security representations.
- Regulatory inquiries and litigation can require substantial effort and resources.
- Evidence that information remained unreadable may strengthen defenses and reduce the potential class and settlement exposure.
- Encryption does not create blanket immunity, particularly for separate operational consequences.

Cyber Insurance

- Underwriting responses can affect pricing, limits, deductibles, and self-insured retentions.
- Technical personnel should verify what is encrypted and identify exceptions when preparing applications and renewals.
- The organization should retain the information supporting its answers.

Coverage Questions After a Loss

- An unencrypted archive raises questions about what the application asked, whether the answer was accurate when submitted, and whether the environment changed later.
- Depending on the law and policy, a material misrepresentation may support denial of coverage or rescission.
- A reservation of rights preserves identified coverage defenses while the facts develop.

Before That Monday Morning: Why Encryption Matters

Encryption protects people by keeping their sensitive information unreadable to an attacker.

It can also reduce notification obligations, response costs, and regulatory scrutiny and litigation exposure.

The organization needs evidence showing that those protections held during the attack.

Thank you!