Ransomware on the Rise: The Expanding Role of Legal Counsel in Incident Response

Client Alert | 8 min read | 10.23.25

Ransomware attacks continue to evolve in frequency, sophistication, and impact. Threat actors are now leveraging artificial intelligence to enhance phishing campaigns, automate data exfiltration, and execute double extortion schemes—where data is both encrypted and stolen for leverage.

A recent report from **ThreatDown** underscores the accelerating pace of ransomware attacks against businesses, with implications for organizations across sectors. Specifically, they point to heightened risks in health care, retail, and critical infrastructure.

Against this backdrop, companies need to prepare for the increasing number and sophistication of attacks. In particular, companies need to focus on preparations to mitigate legal, regulatory, and contractual risk, and they should have counsel ready to assist in coordinating and managing the technical response and ultimately limiting reputational harm.

Key Findings From ThreatDown Report

- From July 2024 to June 2025, ransomware incidents rose 25 percent. February 2025 alone recorded 1,000 known attacks—the highest monthly total on record.
- 41 new ransomware groups reportedly emerged in the past year, pushing the number of active groups past 60 for the first time.
- 42 countries experienced their first reported ransomware attack during the period from July 2024 to June 2025, reflecting the spread of ransomware beyond traditional geographies.
- The U.S. remains a primary target with 3,030 incidents reported from July 2024 to June 2025—more than double the total of all other countries combined.

Popular Targets of Ransomware Attacks

While health care entities continues to be a prime target for ransomware, enterprises in the retail and critical infrastructure sectors have also faced particularly damaging attacks. Ransomware incidents in these three sectors now routinely disrupt operations, compromise data, and create cascading effects.

- **Health care**. Health care organizations store vast amounts of highly sensitive personal and medical data. Hospitals, health insurance companies, payors, and clinics rely on constant access to patient records and systems. For example, the June 2024 **Synnovis** attack in the United Kingdom caused severe diagnostic delays, harming 170 patients and causing one of the first deaths officially linked to a ransomware attack. In

the United States, the July 2024 attack on **McLaren Health Care** affected 750,000 patient records in Michigan, while the May 2025 attack on **Kettering Health** disrupted 14 hospitals across Ohio.

- **Retail**. Retailers store significant amounts of payment information and personal data. Disruption can halt sales and lead to immediate financial losses. Major retailers, such as **Marks & Spencer**, the **Co-operative Group**, and **Harrods** faced attacks that caused major financial losses, data theft affecting millions of customers, and sustained reputational harm. The April 2025 attack on Marks & Spencer resulted in $300 million in lost profits, along with a $930 million decrease in market value. The **Co-operative Group** attack in April 2025 resulted in the theft of customer data from all 6.5 million members and cost the company at least **$206 million** in lost revenue. Likewise, the **Harrods** May 2025 attack exposed 430,000 customer records.

- **Critical Infrastructure**. Attacks against U.S. electrical companies and steel manufacturers also illustrate how ransomware can quickly escalate into a public safety and national security concern. For example, an attack in October 2025 on the **San Bernard Electric Cooperative** affected approximately 3,900 miles of electrical distribution lines and serves approximately 28,000 households in eight counties across Texas. Likewise, an attack on **Karnes Electric Cooperative** that same month affected nearly 5,000 miles of lines that serve 23,000 households in twelve counties across Texas.

Preparation and Coordination in Response to an Attack

Legal counsel's role during a ransomware incident should extend beyond crisis management. From preparation to post-incident response, legal counsel can help organizations navigate an increasingly complex legal environment, maintain privilege, and make defensible and well-documented decisions.

1. Preparing for an Incident

Before a ransomware incident, legal counsel plays a critical role in helping organizations prepare. This includes by assisting with drafting incident response plans, conducting tabletop exercises, and ensuring compliance with data protection and breach notification laws. Legal counsel can review contracts and cyber insurance policies to clarify coverage, liability, and reporting obligations, as well as coordinate pre-incident relationships with approved vendors. Legal counsel can also advise on data handling obligations and legal risks that may attach to certain types of data, such as sensitive data, controlled unclassified information, or personal health information, as well as prepare policies and procedures and provide training that mitigate risk. Additionally, legal counsel can design broad data governance and retention policies, coordinate across organizational teams, and advise on obligations an organization may have before an attack occurs.

2. Coordinating the Incident Response

When victims detect a ransomware incident, rapid response is critical. Legal counsel can help lead the incident response effort to ensure that legal advice related to the incident is sought and obtained under attorney-client and/or attorney work-product privilege. To this end, counsel can engage, coordinate and properly document agreements among key stakeholders, including, as appropriate, the internal information technology and information security teams, external forensics, and crisis communications advisors. Similarly, counsel can help facilitate and oversee the preservation of evidence, determine the scope of compromise, including coordinating the assessment of what information was affected (e.g., sensitive or regulated information, whether data exfiltration occurred), and manage communications around the incident, including any legally required notifications.

3. Managing Regulatory and Notification Obligations

Legal counsel can evaluate whether notification obligations are triggered under U.S. federal or state law, General Data Protection Regulation (GDPR), and other international privacy frameworks. In some cases, this notification must shortly after the discovery of an incident. Meeting those required timelines mitigates potential liability, so it is important to know and understand what notices are required and when they need to be made.

The growing patchwork of privacy and cybersecurity regulations in the United States, such as the Securities and Exchange Commission's cybersecurity disclosure rules, the Federal Trade Commission Act, the Health Insurance Portability and Accountability Act (HIPAA), the Health Breach Notification Rule, and state breach notification laws, requires a fact-specific assessment of applicable legal requirements. For example, U.S. Department of **Health and Human Services guidance** on HIPAA and ransomware clarifies that when electronic protected health information is encrypted due to a ransomware attack, a breach is presumed to have occurred, and the only way to rebut this presumption is to perform a risk assessment and determine that there is a low probability that the protected health information has been compromised. No two ransomware attacks are identical, and each incident presents unique facts and legal considerations.

Legal counsel can determine notification thresholds and timelines, coordinate with data protection authorities, law enforcement, and other regulators, and draft or review notices to affected individuals, regulators, and business partners. Many breach notification laws and regulations also contain express documentation requirements, particularly where an organization experiences an incident but ultimately determines no reportable breach has occurred. Legal counsel can help ensure that adequate documentation is maintained to meet such requirements and support the organization's defense in future investigations or litigation.

4. Negotiating with Threat Actors and Advising on Payment Decisions

Engaging with a ransomware threat actor presents complex legal and compliance considerations. Legal counsel can help assess whether negotiation or payment is permissible under sanctions administered by the U.S. Office of Foreign Assets Control and anti-money laundering laws. In many cases, legal counsel can work with specialized ransom negotiators and cyber insurance carriers to evaluate options, advise companies, and document decision-making. Counsel can seek to preserve privilege, document deliberations, and engage law enforcement, if needed.

5. Managing Communications and Reputational Risk

Public perception following a ransomware event can have lasting implications. Legal counsel can partner with internal communications teams and public relations firms to craft accurate, compliant, and consistent messaging for stakeholders, employees, customers, and investors. Counsel can also help avoid premature or misleading disclosures that could expose the company to litigation or regulatory scrutiny.

6. Post-Incident Remediation and Litigation Readiness

After systems are restored, counsel can also help guide post-incident response, focusing on compliance, remediation, meeting contractual obligations, and managing litigation exposure. Regulatory investigations, class actions, and shareholder suits often follow major ransomware incidents. Legal counsel can also help

coordinate a “lessons learned” meeting to assess the organization’s response to the incident. Legal counsel can advise on and help implement appropriate corrective actions, such as training or policy updates.

7. Post-Incident Recovery of Losses from Third-Party Vendors

Responding to an incident costs money—from legal fees to forensic investigator fees, to remediation efforts, to ransomware payments, and regulatory fines. And this accounting does not even cover the direct and consequential business and reputational costs of a cybersecurity incident. Where the incident occurred due to a third-party vendor failing to meet its promises to protect your organization’s data under contract, legal counsel can assess whether there are claims under contract or tort to recover these losses and, if so, they can assist with efforts to recoup those losses.

Conclusion

Ransomware is not solely a technical or operational threat—it is also a legal and regulatory challenge that demands a coordinated response under the guidance of experienced counsel. Early involvement of legal counsel can preserve privilege, reduce liability, and help ensure that organizations emerge from an incident in the best possible position.

Crowell & Moring has extensive experience helping clients prepare for and manage their incident response efforts. We provide a coordinated approach to incident response and can help mitigate legal exposure while maintaining privilege, helping to chart a path with our clients through a crisis.

Contacts

Jason Johnson
Partner & CHS Managing Director
New York D | +1.212.530.1860
jjohnson@crowell.com

Neda M. Shaheen
Associate
She/Her/Hers

Washington, D.C. D | +1.202.624.2642
nshaheen@crowell.com

Jacob Canter
Counsel
He/Him/His

San Francisco D | +1.415.365.7210
jcanter@crowell.com

Brandon C. Ge
Counsel & CHS Director

He/Him/His

Washington, D.C. D | +1.202.624.2531
bge@crowell.com

