COVINGTON

Ransomware in 2026: Evolving Threats and Regulatory Pressures

January 20, 2026

This article original published in *Dow Jones Risk Journal*

The ransomware landscape is constantly evolving. Over the past year, threat actors have focused on large, deep-pocketed targets in the hopes of extracting larger payments, and

governments are instituting new ransom payment disclosure requirements and other barriers in the hopes of chilling payments. In 2026, decisions made during a ransomware incident will continue to carry regulatory, legal and reputational consequences.

Understanding the current risks and trends is critical to shaping a response strategy that protects both compliance and business continuity.

Threat actors focus on 'big game hunting'

Ransomware incidents affected a range of industries across the globe in 2025. In the U.K. alone, the percentage of businesses experiencing a ransom incident doubled in the past year. Yet while attacks have continued, ransom payment rates have declined over the last year.

Some companies might choose not to pay because of improved backup and restoration processes, which allow systems to be brought back online without making a payment. Others might decline to pay on the theory that there has been a broader desensitization to data breaches, and they don't want to risk perpetuating the ransomware ecosystem by paying the "bad guy."

Although the percentage of companies paying a ransom has declined, companies reported receiving ransom demands scaled to their annual revenue, or that increased when threat actors believed a company would be willing to pay more. This trend suggests that some ransomware threat actors might be moving toward a "big game hunting" strategy, which focuses on a smaller number of more lucrative targets. Companies could be targeted because their size and profits suggest they have the funds to pay a ransom, or because they operate in an industry or a function (such as certain service provider/vendor roles) with access to more sensitive and regulated data. In particular, the U.S. financial services and healthcare industries reported the highest total amount of ransom paid between 2022 and 2024 compared with other industries—even though these industries didn't report the most ransomware incidents. This suggests that highly regulated companies, or those with more sensitive data, might face an elevated risk from ransomware threat actors.

New regulatory and legal considerations for ransomware response

In both the U.S. and the U.K., new and proposed legislation seeks to ban or limit ransom payments, or require disclosures (and, in some cases, justifications) when payments are made. For example, companies regulated by the New York State Department of Financial Services are required to report serious cybersecurity incidents within 72 hours, ransomware payments within 24 hours, and provide justifications of ransomware payments within 30 days. Several U.S. states, including North Carolina and Florida, also have laws that prohibit public entities from paying ransoms. The extent of U.S. reporting requirements for ransomware incidents is likely to expand significantly in 2026, as the U.S. Cybersecurity and Infrastructure Security Agency plans to publish a rule requiring a variety of entities across 16 critical infrastructure sectors to report covered cyber incidents within 72 hours of discovery and covered ransom payments within 24 hours. Outside of the U.S., the U.K. Home Office has proposed a ban on ransomware payments for public sector entities and owners and operators of critical infrastructure, along with mandatory incident reporting within 72 hours for any victims of ransomware. Interestingly, the U.K. government has estimated that over half of U.K. businesses have a "no ransomware payment" policy—an increase from 2024—which could be driven by shifting national policy.

Litigation impacts from ransomware payments

While laws and regulations might discourage ransom payments through prohibitions or reporting requirements, litigation considerations may sometimes counsel in favor of making payments in data breach cases. Following the Supreme Court's 2021 decision in *TransUnion v. Ramirez*, courts across the U.S. have grappled with what constitutes sufficient "concrete harm" to sustain a data breach-related lawsuit. In particular, some courts have held that the posting of data on the dark web may constitute sufficient harm to confer standing on the individual to sue. If paying a ransom prevents personal information from being posted on the dark web, and thus prevents sufficient harm to confer standing in federal courts, some companies might choose to pay to reduce litigation risk.

Evolving your ransomware response in 2026

If your company faces a ransomware incident in 2026, the appropriate response will likely depend on the unique facts and circumstances of your particular incident, including the types of data affected, the nature of your company's operations, your company's ability to recover quickly, and the current state of the legal environment. But no matter the context, you can reduce risk by preparing for a potential ransomware incident in advance, having a plan for how to respond, and lining up third parties to assist. Steps to consider taking include the following:

- First, shore up your defenses: identify your highest-risk and most business-critical systems and data (sometimes referred to as a "crown jewels" assessment) and evaluate the measures protecting them, including protections specific to ransomware incidents (such as ensuring that backups are available and protected).
- Second, evaluate your incident response, business continuity, and disaster recovery plans to account for the most recent changes in the cyber threat landscape and any unique company-specific risks or legal requirements.
- Third, test your plans for responding to a ransomware incident via a tabletop exercise to identify key risks and decision points and assess whether your plans will function smoothly during an incident.

- Fourth, evaluate your cybersecurity insurance to ensure that you have appropriate coverage that would apply to a ransomware incident as well as other common cybersecurity incidents that you might face, such as business email compromises.
- Finally, build relationships in advance of an actual incident with key third parties that you might need support from when an incident occurs, such as outside legal counsel, incident response vendors, and law enforcement personnel.

Editor's Note: Micaela McMurrough is a partner in Covington & Burling LLP's New York office and co-chair of the firm's global and multidisciplinary Technology Group. Caleb Skeath is a partner in Covington's Washington office who advises clients on a range of cybersecurity incident response and compliance issues. Miranda Rutherford is an associate in the firm's Palo Alto, Calif., office and a member of the Data Privacy and Cybersecurity practice.

If you have any questions concerning the material discussed in this article, please contact the following members of our Cybersecurity practice:

Micaela McMurrough	+1 212 841 1242	mmcmurrough@cov.com
Caleb Skeath	+1 202 662 5119	cskeath@cov.com
Miranda Rutherford	+1 650 632 4745	mrutherford@cov.com