ALM | LAW.COM

New York Law Journal

Ransomware: To Pay or Not To Pay

By Paul Greene
January 2, 2024

Ransomware can present an organization with an impossible choice, between losing access to, or control over, the organization's most sensitive data or funding an ever-growing criminal behemoth that has threatened and continues to threaten hospitals, schools, and critical infrastructure, not to mention private industry.

Yet often, an organization's options to avoid payment are limited, and attackers utilize tactics designed to create maximum pressure to ensure that payment is made. Aside from the business and ethical issues that arise when assessing whether to make a ransomware payment, legal considerations abound, and can increase both the complexity of decision making and of risk surrounding such a payment.

Because of this, an organization's troubles do not simply end, when it pays to unlock its encrypted data or obtain deletion of stolen data. Rather, making a ransomware payment can have repercussions that survive long after the underlying security incident has been resolved.

Payment of a ransomware ransom has become more common, because of the evolution of this form of attack, and because of the more widespread adoption of network extortion insurance coverage. In relation to attack tactics, modern ransomware attacks almost always involve so-called "double extortion," *i.e.*, encryption of the victim's systems and theft of data from those

systems, with the threat of releasing that data, usually on the dark web.

As data backup practices and endpoint protection solutions improve, organizations become more resistant to malicious encryption, because of increased ability to recover data from backup or to even stop ransomware deployment in its tracks. Backups do nothing to deter data theft, however, and attackers have pivoted to accentuate this aspect of their attack tactics.

Specifically, many ransomware attackers have dark-web "leak sites," where they advertise the victims they have compromised, and then post stolen data, if the ransom is not paid. The sites are well known in the security industry, such that news of a ransomware attack at an organization often breaks because the attacker has announced the attack on its leak site.

Generally, absent other applicable restrictions, making payment to a ransomware attacker to either obtain a decryption key or secure deletion of stolen data, or both, is legal in the United States.

As a matter of policy, government agencies have spoken about the importance of avoiding ransomware payments where possible, and the United States has recently made a pledge, as part of the International Counter Ransomware Initiative, to develop a joint policy statement that government agencies should not make ransomware payments. But government agencies, including law enforcement, can understand why an organization may have no other choice than to make a ransomware payment, and many organizations do just that.

The choice whether to make a ransomware payment is not consequence free as a legal matter, however. In September 2021, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) issued its "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (the Advisory).

In the Advisory, OFAC made clear that sanctions-list restrictions apply in full to ransomware payments. Stating first that "[t]he U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands," the Advisory went on to detail how making or facilitating ransomware payments, whether directly or on behalf of a third party, may violate OFAC restrictions. It is for this reason that ransomware payments facilitated through third parties funded by insurance are now preceded by an OFAC sanctions check.

In this regard, if an organization or individual makes a ransomware payment without an OFAC sanctions check, or if a vendor facilitates such a payment on behalf of an organization, all parties involved in making or facilitating such a payment run the risk of a civil penalty, even absent knowledge that the organization or third party was dealing with an OFAC-sanctioned attacker.

Even if an attacker is not on the OFAC sanctions list, the act of paying a ransom may lead to reporting duties. The recently amended Cybersecurity Requirements for Financial Services Companies in New York, 23 N.Y.C.R.R. Part 500 ("Part 500"), include a 24-hour reporting requirement upon any extortion payment made in relation to a defined "cybersecurity incident," which includes "deployment of ransomware within a material part of the covered entity's information systems." *See* 23 N.Y.C.R.R. §§500.1(g)(3) (amended definition of "cybersecurity incident" to include ransomware deployment); 500.17(c)(1) (notice to Commissioner required within "24 hours of the extortion payment").

Beyond this, Part 500 requires that the covered entity making the payment provide, within 30 days, "a written description of the reasons payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment and all diligence performed to ensure compliance with [OFAC restrictions.]" *See id*. §500.17(c)(2).

Such a reporting duty creates risk, of course, especially since the New York Department of Financial Services (NYSDFS) has yet to provide guidance on reasons that may justify a ransomware payment and what level of diligence is required to explore alternatives to payment.

Indeed, such guidance can often first appear in an enforcement proceeding or settlement, such as in a Consent Order issued by NYSDFS under Part 500, which is, of course, too late for the organization facing such enforcement.

Also, the decision whether to pay a ransom or not is often made while an organization's incident-response efforts are ongoing. Adding a reporting duty triggered within 24 hours of payment, before the decryption key may have even been received or deployed, creates the risk that an organization

will be dealing with inquiries from its regulators while it is attempting to contain and eradicate the threat underlying the incident.

For publicly traded companies, updated Securities and Exchange Commission ("SEC") reporting rules recently came into force, such that an organization having experienced a material cybersecurity incident must issue a Form 8-K report, detailing the nature and scope of the incident, and the potential impact on the organization. This report must be made within four business days of a determination of materiality. *See* SEC Form 8-K Item 1.05 *available at* https://www.sec.gov/files/form8-k.pdf.

Nothing in the updated SEC rules changes the materiality considerations currently in place, just because a cybersecurity incident is involved, however. And it may not be the payment itself that leads to a materiality determination.

Rather, as SEC chair Gary Gensler stated in relation to the new 8-K reporting requirements "[w]hether a company loses a factory in a fire—or millions of files in a cybersecurity incident—it may be material to investors." *See* SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, *available at* https://www.sec.gov/news/press-release/2023-139.

Lastly, in relation to data breach notification obligations, paying the ransom in a "double extortion" scenario, where personal information giving rise to a notification duty has been compromised, provides virtually no legal benefit, as state data breach notification statutes focus instead on unauthorized access to or acquisition of such personal information in the first instance, not remedial measures taken to potentially limit the impact on affected individuals.

Case in point, N.Y. Gen. Bus. Law §899-aa, which requires notice to all affected individuals and the New York State Attorney General if "private information was, or is reasonably believed to have been accessed or acquired by a person without valid authorization." *See* N.Y. Gen. Bus. Law §899-aa(2).

The factors given in §899-aa to determine unauthorized access or acquisition do not consider actions taken to minimize impact, such as securing return of the data or paying a ransom for assurances of deletion from the attacker. And, in this regard, organizations must remember that they are dealing with criminals, when paying for the deletion of stolen data. A promise by a criminal to delete stolen data upon payment may be central to that criminal's value proposition, but it is nonetheless a promise made by a criminal.

Ultimately, the decision whether to pay a network extortion ransom will be driven by the facts of the particular incident. In some cases, paying the ransom will be the valid business choice, and therefore best serve the victim and its stakeholders. In others, payment may be prohibited under OFAC restrictions or frowned upon by the organization's regulator or regulators.

Regardless of the circumstances, determining whether to make a ransomware payment is now also a legal determination, requiring appropriate time, consideration and due diligence. Organizations are best served by thinking about these issues in advance, as part of their incident response preparation activities, lest they make a mistake in the heat of incident response, and inadvertently increase risk to the organization by way of a payment intended to have the exact opposite effect.

Paul Greene *is partner and chair of the privacy and data security practice group at Harter Secrest & Emery. He can be reached at fgreene@hselaw.com.*