ALM | LAW.COM

New York Law Journal

‘They’re Going To Take You’: Responding to a Ransomware Attack

By Sidhardha ‘Sid’ Kamaraju, Katherine Reilly and Aaron Wiltse

March 20, 2025

On Feb. 10, 2025, the Department of Justice unsealed a superseding indictment in *United States v. Berezhnoy*, 23-cr-459 (TDC) (D. Md.) (the “*Berezhnoy* Indictment”) and announced the arrest of the two Russian national defendants, in connection with a coordinated international effort to disrupt the cyber network to which the defendants allegedly belonged.

In the *Berezhnoy* indictment, the DOJ alleged a sweeping campaign of cyber-attacks by the defendants spanning more than five years. The defendants are alleged to have targeted a variety of victims, including auditing firms, healthcare companies, law firms, federal contractors, public school systems, a union, and a Native American tribe. In particular, the defendants are alleged to have hacked into the victims’ networks and used ransomware called Phobos to steal data, threatening to expose the stolen data to the public if the victims did not pay ransoms.

Ultimately, the defendants are alleged to have extorted their victims to make more than $16 million in ransom payments. The *Berezhnoy* indictment is a stark reminder of the threat that cyber-attacks and ransomware

pose to companies and organizations of all sizes and levels of sophistication.

While many companies now have some form of cyber-insurance, these policies often contain exclusions that can limit their benefits, leaving companies to bear significant financial costs after an attack. In addition, a data breach forces a company into a number of tough decisions.

What does the company have to disclose and when? Does it need to investigate? Should the company contact law enforcement, and if so, when? Should it pay the ransom? Each of these questions (and the many more that follow) requires balancing significant but often contradictory interests.

For example, law enforcement strongly discourages victim companies from paying ransoms to cyber-attackers, but companies facing significant hacks or the theft of important data may, practically, have little choice but to pay.

Moreover, paying a ransom could run afoul of U.S. sanctions laws, as many of the most prolific hackers have been sanctioned, thus preventing U.S. companies from legally dealing with them. Navigating these kinds of decisions requires the early involvement of counsel with the technical skill to comprehend not just the nature of any attack, but also companies' data storage plans and data privacy obligations, as well as with familiarity with the ways in which law enforcement investigates data breaches, and a deep understanding of U.S. sanctions regulations.

What To Say and When?

Of course, if the first time a company thinks about cybersecurity protections is after a hack, it's too late to meaningfully protect itself. Instead, companies have to think about these issues long before problems arise, including as part of their insurance coverage, IT infrastructure, staffing, and terms and policies. Unfortunately, history has shown that sometimes no amount of preparation is enough—an errant employee click on a questionable email can lead to catastrophe.

When a data breach happens, the victim has to make a number of big decisions, often very quickly and with limited information. First, the victim has to lock down its data as quickly as possible and assess the scope and origin of the attack.

Figuring out what happened will likely require some form of investigation—for example, in the early moments of an attack, the victim may not know if the threat is external or from inside, or even a combination of both. As with any form of internal investigation, the involvement of counsel is critical, in no small measure, because it can provide the protection of privilege.

At the same time, the victim may also be facing significant pressure to disclose the incident. For public companies, SEC regulations require them to disclose a data breach within four business days after the company determines the materiality of the incident (thankfully, and importantly, not from the incident itself).

Disclosure, however, may bring lawsuits, and delaying disclosure may just increase the pool of potential plaintiffs and amount of possible damages. Even for private companies, other regulations—like data privacy, health care, or consumer protection laws—may require them to disclose certain types of hacks. As a result, it's critical that the victims of a cyber-attack promptly seek legal guidance on how to investigate the incident and then how and when to disclose it.

The SEC does allow public companies to delay public disclosure of a cyber-attack if it would threaten national security or public safety—for example, in the case of a state-sponsored hack or an attack on critical infrastructure. But the regulations only allow that delay with a written certification from the Attorney General, which means contacting law enforcement.

While contacting law enforcement seems like a natural response to being the victim of a crime, that decision can be enormously complicated. Although law enforcement is certainly skilled at handling data breaches at this point, and has made advances in its understanding of the impact of an investigation on corporate victims, there's no doubt that a criminal investigation is likely to be very disruptive to the company's operations.

To understand the company's systems and what happened, law enforcement will most likely need a significant amount of time from certain company employees, including the IT and security staff. And to collect evidence appropriately,

federal investigators will almost invariably need to forensically image relevant servers, computers, or even cellphones.

Taking those devices offline for chunks of time can impose a real burden on the company and its employees. As a result, while notifying law enforcement may seem like the obvious choice to many, before doing so, the victim needs to consult with counsel with experience with these kinds of investigations so that the company can properly understand and manage the process as productively as possible.

To Pay or Not To Pay?

Law enforcement will also discourage the victim of a cyber-attack from paying a ransom in exchange for relief. Unfortunately, sometimes that is simply not a viable business decision—the nature of the data stolen may be too valuable to risk its public disclosure or permanent loss, for example. But even once the victim has made the difficult decision to pay the ransom, that's not the end of the trouble—the victim still has to consider whether making that payment would violate U.S. sanctions.

Many of the organized and well known ransomware attackers are subject to OFAC "blocking" sanctions, which generally prohibit U.S. persons from engaging in transactions, directly or indirectly, with them. As a result, victims of ransomware attacks by sanctioned attackers may themselves be subject to liability for paying a ransom, and any entity that facilitates that payment (*e.g.*, banks or money services businesses) are also potentially subject to liability.

Moreover, U.S. law also prohibits conducting transactions for the purpose of evading U.S. sanctions, meaning that companies need to be very careful when considering how to structure ransom payments.

And, of course, ransomware attackers can be difficult to identify, making it nearly impossible in some instances to determine whether the recipient is a sanctioned person or entity. But ignorance of the attackers' identities or sanctioned status is no defense for a company seeking to pay a ransom. OFAC can impose civil penalties on a strict-liability basis, so victims and payment facilitators may be liable even if they had no reason to know that the attacker is a sanctioned entity.

Following an uptick in ransomware attacks over the course of the COVID-19 pandemic, OFAC issued guidance in October 2020 on the potential risks for victims and payment facilitators, and then updated that guidance in September 2021. OFAC does not give a blanket sanctions pass for victims of sanctioned attackers.

Instead, OFAC requires victims to seek a specific license, or authorization, from the agency, which it will review "on a case-by-case basis with a presumption of denial." In other words, victims who have decided to make a ransom payment must not only seek authorization from OFAC, they will likely face an uphill battle to get that authorization. And even if a company can compile a compelling case for a specific license, the bureaucratic process of applying and waiting for OFAC licensing costs precious time that the victim seeking to secure its data may not have.

The practical impact of the situation is that victims faced with ransom demands may have no choice but to pay ransoms without any comfort that they aren't violating U.S. sanctions laws. At that point, the question becomes how to best position the company should a sanctions violation occur and OFAC come calling. OFAC's guidance on these issues offer several indications about how a company facing an attack might protect itself.

One part of that equation is coming up with a process to best assure companies that they are not dealing with a sanctioned entity—contrary

to popular belief, a simple search of any names associated with the attacker may not be sufficient depending on the facts on the ground.

The attackers will likely hide their real identities and may well be associated with sanctioned persons or entities unknown to the victims. As a result, victims and payment facilitators should do what research they can, including relying on any evidence developed by an investigation about the attackers' identities, and should document that research.

As for payment facilitators, OFAC's guidance is the same as its guidance for all potential sanctions violations—companies are encouraged to "implement a risk-based compliance program to mitigate exposure to sanctions-related violations" that should "account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction."

The second element of the company's efforts to avoid OFAC penalties involves decisions about coordination with law enforcement—OFAC will credit companies for their "self-initiated and complete report of a ransomware attack to law enforcement" and "ongoing cooperation."

And, critically, the third part of the equation requires companies to take steps long before the data breach occurs. Specifically, with respect to cyber-attack victims, OFAC will consider "[m]eaningful steps taken to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices," such as "maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols."

Put simply, in the case of a ransom payment, OFAC is going to not only look at what the victim did in response to the attack, but also what they did to prepare for and prevent the attack.

Conclusion

At the end of the day, a ransomware attack is a harrowing prospect for any company. At each step of the way, companies would be wise to involve experienced counsel as early as possible.

Bringing in counsel when designing cybersecurity procedures and data storage plans, well before an attack, can help on the back-end, if the company is called one day to explain a ransomware payment to OFAC.

Working with counsel in the early days of a data breach can help ensure that any internal investigation or public disclosure is conducted in the safest way possible.

Counsel can also help if and when it comes to contacting law enforcement and can work to mitigate any disruption caused by the investigation. And, if a ransom has to be paid, counsel can work to minimize the risk that there's no insult added to the injury in the form of a sanctions violation and resulting penalties.

Even as law enforcement makes arrests and works to disrupt networks of ransomware attackers, companies would be wise to consider the increasing prevalence and sophistication of these attacks and prepare and plan for what to do if their systems come under attack.

Sidhardha 'Sid' Kamaraju *is the chair of Pryor Cashman's White Collar + Regulatory Enforcement Practice.* **Katherine Reilly** *is a partner in the White Collar + Regulatory Enforcement Practice.* **Aaron Wiltse** *is an associate in the firm's White Collar + Regulatory Enforcement Practice Practice.*