ALM | LAW.COM

New York Law Journal

To Pay or Not to Pay? Key Factors to Consider When Ransomware Strikes

By David R. Owen, Kenneth Ritz and Alexa Moses
May 2, 2023

On Dec, 8, 2022, a ransomware attack on the Metropolitan Opera in New York City crippled the company's computer systems enterprise-wide, including its website, box office and call center. As is typical with ransomware attacks, there was no warning and the timing during the key holiday season of performances was awful for the company. With employees and customers generally in the dark, the company was urgently faced with a very troublesome and dramatic question: should they resist the hacker's demands and go forward as best they could in the face of significant and uncertain technical and public relations challenges, or should they quickly capitulate and pay the hackers to release the systems … hopefully? The potential consequences for the Met from the incident were not small. And after weeks of frantic recovery efforts to restore crippled systems, the company was still selling seats at a hugely discounted $50, and still without full email function as late as Dec. 27.

Of course, the Met has plenty of company as a recent victim of ransomware, and it will certainly not be the last to face this dilemma at the worst possible time. While a large percentage of ransomware attacks go unreported, ransomware incidents continued unabated in 2022. According to cybersecurity firm Sophos's "The State of Ransomware 2022" report, the average reported ransom payment is up to $812,360, and the average total loss per incident $1.4 million, including business impact, security remediation, legal and compliance costs. In most cases, ransomware attacks simply use traditional hacking techniques to exploit security vulnerabilities to access company network systems.

Credit: whiteMocca/Shutterstock.com

While strong and up-to-date security is usually effective to stop most technical attacks, even the best security in the world can be defeated by attacking the more fallible human vulnerabilities. All it takes is a stray click on a well-crafted phishing email from someone with access, and the bad guys are in. Once inside, they will scramble the data they encounter with encryption and

jump to any attached systems to spread the infection as far and wide as possible. Employees are left with locked screens, no files and communication only by personal cellphone.

Management has to quickly figure out: What functionality do we still have? How quickly can we respond technically? How much do they want? What will it cost to say no?

The answers to these questions will vary depending on the kind of entity that gets hit, the extent of the infection and the hackers' demands. Given the prevalence of these attacks, response planning is vital so that decisions don't get made in the heat of the moment, without consideration to all the possible risks and consequences. While it might appear imprudent to make a payment to criminals without any assurance that they will actually provide a working decryption key, paying the ransom may (or may not) offer a better chance of quickly restoring functionality and recovering data. In fact, because the scam depends upon victims' expectations that the keys will be forthcoming upon payment, hackers have proven more reliable than one might expect in restoring functionality once payment has been made.

While management may recoil at the prospect of a six-figure ransom payment as extortionate and outrageous, any ransom demand should still be weighed against the costs of fighting the attack. In 2018, the City of Atlanta's public services were shut down by hackers who demanded $51,000 in order to restore access. The city refused, and according to the New York Times the cost to remediate turned out to be 300 times the original ransom demand. Likewise, in the spring of 2019, the city of Baltimore refused to pay hackers the $76,000 they demanded in ransom, opting instead to rebuild their entire infrastructure; according to the Baltimore Sun, this rebuild ended up costing $18.2 million when all was said and done.

While most companies these days carry cyber insurance coverage, it may not cover the ransom demand, or sub-limits may apply. Given the rapidly increasing cost of this coverage and underwriting challenges for the issuers, it may not be in the interest of the company to use the insurance to pay if the amount demanded is small. The hackers may discover the existence and scope of coverage as a result of the security breach, which can significantly affect ransom negotiation. Some firms have already begun to segregate their cyber insurance documentation in an effort to shield it in the event of a breach.

For most companies that interact directly with the public, being the victim of a ransomware attack can cause significant reputational damage and loss of business. Customers may lose trust in the hacked organizations or, if the ransom is paid, refuse to do business with organizations that would indirectly help fund further criminal activities. Good planning should consider the reputational and collateral consequences of a ransomware hack and the practical harm that may flow from business interruption and compromise of sensitive information. For ransomware attacks that hit critical infrastructure, lives may be threatened, and time may be of the essence in reestablishing essential services. For example, ransomware incidents have forced some hospitals to cease chemotherapy treatments, delay reporting of laboratory results and postpone important appointments. Ransomware incidents also have disrupted heating services and have caused gasoline and jet fuel shortages.

Other factors may weigh against making a quick payment. If systems have been hardened and restoration capabilities are sufficiently strong, the demand may be irrelevant. Technical solutions that provide a complete and relatively prompt restoration of corrupted systems can be very effective against ransomware, even in the event of a successful attack. Likewise, if the attack has been isolated and is not affecting any critical systems, it may be preferable to simply rebuild the affected noncritical systems. In the event of a successful attack, it is vital that additional remediation is undertaken to prevent similar attacks, and counsel engaged

to ensure that privacy and other legal obligations are addressed.

There is no guarantee that the hacker's decryption key solution will be fully effective and reliable, as the keys they send may be only partially effective or result in other system corruption. Making any payment to cybercriminals, especially a publicly-disclosed payment, may invite future attacks. Ransom payments go directly to criminals and are used to facilitate more cybercrimes and support larger criminal enterprises, including drug cartels with links to terrorism. While the FBI generally recommends that ransoms should not be paid in order to discourage the criminals, agents admitted at a 2015 cybersecurity conference that in most cases payment would be the best and only way to recover the files.

While most companies still choose to keep silent about ransomware payments, public disclosure rules and practices are evolving. Indeed, one indication of the scale of non-reporting came from the recent FBI takedown of the ransomware group Hive. According to FBI director Christopher Wray, only about 20% of Hive's victims reported the incident to government authorities, based on the information obtained. For public companies, an undisclosed material payment to hackers could violate expanded reporting rules under consideration by the SEC.

Companies considering whether to report ransom payments should bear in mind the possibility that an incident may be discovered by authorities well after the fact.

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has imposed sanctions against a number of foreign countries, entities and individuals believed to be perpetrating or facilitating cybercrime (e.g., the billion-dollar Russia-based Hydra, the largest darknet market left in the world, or Garantex, a virtual currency exchange), prohibiting U.S. persons from any transactions with these sanctioned parties. While the identity of ransomware perpetrators is typically uncertain, it remains unclear whether a good-faith ransom payment made to a sanctioned entity to avoid a threatened harm would draw enforcement scrutiny. Speaking to Congress in 2021, FBI officials recommended against banning ransomware payments, partly out of concern a ban would create additional extortion opportunities for successful hackers who could threaten to disclose the ransom payments to authorities after they were made. And although OFAC discourages ransomware payments due to the potential of sanctions violations and threatening of national security, OFAC would consider mitigating factors, such as the victim's existing cybersecurity program and its disclosure and cooperation with government authorities, in assessing whether to pursue any sanctions penalties or enforcement actions.

Ultimately, the best defense against ransomware is still good preparation, which includes complete and up-to-date technical defenses, a strong and fast recovery capability and, most importantly, regular employee training. Counsel should be involved in both the planning and implementation of incident response processes, and in communications to government authorities that are deemed necessary in the event of an attack. Finally, the key people involved in cyber incident response should collectively conduct regular implementation exercises, just like fire drills, so that the responsible people know their roles and what they need to think about when an unexpected lock appears on company computer screens at the worst possible time.

David R. Owen *is a partner in Cahill Gordon & Reindel's New York office, advising leading financial institutions and global corporations in connection with data privacy and cybersecurity matters.* **Kenneth Ritz** *and* **Alexa Moses** *are associates at the firm.*