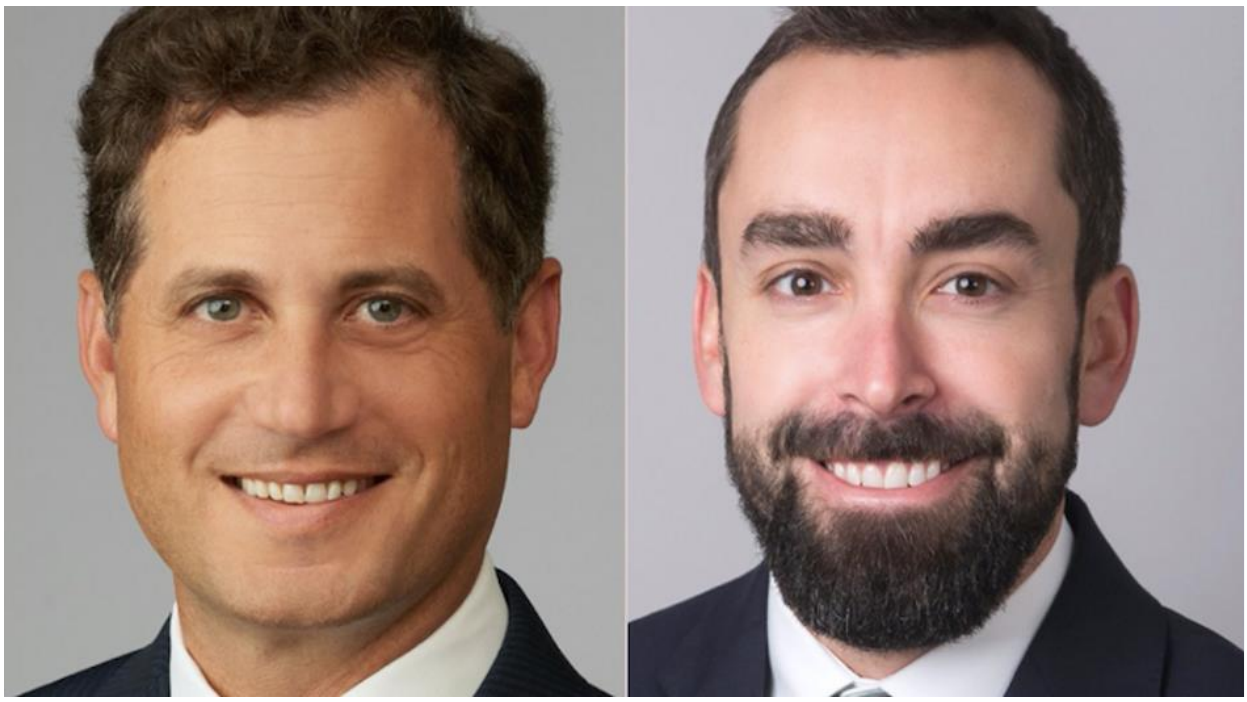
GIR Global Investigations Review

JUST SANCTIONS

Should companies cooperate with law enforcement during ransomware attacks?

08 October 2021



David Burns and Brian Williamson

Gibson Dunn & Crutcher's David Burns and Brian Williamson argue why companies have plenty to gain from reporting ransomware attacks to the US government.

Ransomware attacks have grown exponentially in recent years. Once a niche headache for industry and law enforcement, they have advanced into an acute national security, health and safety threat with profound consequences for all

First published on the *Global Investigations Review* website, 08 October 2021.

manner of organisations. Ransomware actors are becoming bolder and increasingly targeting larger organisations and making higher ransom demands. This year alone witnessed an explosion of high-profile attacks, including the well-publicised attack against Colonial Pipeline, which caused a run on gas stations, an increase in pump prices, and overall public angst. Attacks against the energy grid, water treatment facilities, a nuclear plant, or other critical assets are nightmare scenarios that keep law enforcement, national security, and private sector personnel up at night.

The threat is clear. The solution is not. Ransomware attacks will continue for the foreseeable future, and companies must be prepared to harden their systems against the attacks and minimise the damage after they occur. When cybercriminals penetrate a company's defences, corporate decision-makers must confront the critical question of whether to report the attack to law enforcement. Companies are often reluctant to proactively involve law enforcement in their affairs, for fear that attention will be turned on the company's own shortcomings or that interacting with law enforcement in the midst of a crisis will distract from core incident response efforts. At the same time, there are a number of significant benefits to working with law enforcement during an attack.

The threat

Although many attacks go unreported, the trajectory of known attacks is rising at an alarming rate with no signs of abatement. According to the FBI's Internet Crime Report, 2019 saw a 37% increase in reported ransomware attacks in the United States over 2018 and a 147% annual increase in associated losses over the same period. From 2019 to 2020, the FBI reported a 21% year-over-year increase in reported attacks, while the Department of Homeland Security reported a 300% increase over the same period. Global trends are almost certainly similar, with the German firm Statista reporting that in 2020 there were 304 million attacks worldwide, up 62% from 2019.

Many attacks are carried out by cybercriminal organisations based in Russia, with attacks also originating from China, Iran, North Korea, and elsewhere. Nation-state adversaries either directly support and cultivate ransomware actors and activities or, at the very least, permit ransomware activities to operate within their borders with impunity.

First published on the *Global Investigations Review* website, 08 October 2021.

In April 2021, for example, the Treasury Department issued new sanctions against Russia, drawing a direct connection between Russia's Federal Security Service (FSB) and ransomware actors, observing: "[T]o bolster its malicious cyber operations, the FSB cultivates and co-opts criminal hackers... enabling them to engage in disruptive ransomware attacks and phishing campaigns."

Lucrative extortion payments fuel these cyberattacks. Ransom payments incentivise further attacks and embolden criminal actors, creating a perverse cycle of escalating damage. They may also be used to finance terrorism, human trafficking, and weapons proliferation. It is also no coincidence that ransomware attacks have increased along with the prevalence of cryptocurrencies and crypto trading exchanges. As recent examples demonstrate, the size of ransom demands has grown to the millions and tens of millions of dollars: Colonial Pipeline was asked to pay $5 million, CNA Financial Corporation faced a $40 million demand, JMS was hit with an $11 million ransom, and Kaseya VSA was told to pay $70 million.

The decision whether to cooperate with law enforcement after an attack

The initial period after a ransomware attack is often chaotic. A number of important steps must be taken immediately, including assessing the nature and extent of the breach, determining system vulnerabilities, securing backups, and mitigating further damage. Cybersecurity incident response experts and legal counsel, internal and external, will be critical players during this time. Whether another critical player should be law enforcement has been the subject of much debate in the private sector.

There is a general reluctance within some quarters of corporate America to voluntarily involve law enforcement in a cyber event out of a fear that a victim company's own controls and conduct will come under scrutiny. Another concern is that the ensuing demands of agents and prosecutors will serve as a distraction to addressing the incident internally. Providing information to law enforcement also may create challenges in maintaining privilege over incident response findings in subsequent civil litigation. Finally, some companies see little upside in what is often viewed as the one-way information flow from the company to law enforcement.

First published on the *Global Investigations Review* website, 08 October 2021.

Not surprisingly, law enforcement authorities with jurisdiction over ransomware attacks, particularly the FBI, DHS, and Secret Service, encourage victim companies to report cyber incidents as early as possible. Law enforcement emphasises that it endeavours to minimise distraction and to "treat victims as victims." From the agencies' perspective, corporate reporting provides a more comprehensive view of the threat and its impact on victims and may help to deter future attacks.

Beyond corporate altruism, however, there are concrete benefits to reporting ransomware incidents. Law enforcement has deep experience and knowledge of cybercriminal gangs and malware variants from years of working on ransomware and cyber investigations. As a result, agencies may already have the decryption key to the operative malware. Indeed, there is reporting that at least one company paid a ransom demand to obtain a decryption code that the FBI already possessed.

Law enforcement does not support ransom payments because, among other reasons, they embolden adversaries and incentivise additional attacks. However, the government recognises that paying a ransom is a business decision that must be made in the best interests of corporate stakeholders. Nevertheless, the payment of a demand does not guarantee that cybercriminals will provide the decryption key to unlock a company's system or refrain from making subsequent extortion demands. Law enforcement may have actionable intelligence on the reputation and history of particular ransomware actors and may be able to provide information about whether actors will actually deliver a decryption key if a ransom payment is made. Such information could be extremely valuable during ransom negotiations.

Although less likely, working with law enforcement also puts the government in the best position to claw back a ransom payment after it is made. Following the Colonial Pipeline attack, the Department of Justice and FBI announced the seizure of 63.7 bitcoins valued at approximately $2.3 million (out of the $5 million total payment reportedly made by the company). The clawback was accomplished by a seizure warrant for funds representing the proceeds of the ransom payment to individuals in the DarkSide ransomware group. Following another attack, in January 2021, the government recovered almost $500,000 in proceeds connected to the NetWalker ransomware actors.

First published on the *Global Investigations Review* website, 08 October 2021.

Companies that make or facilitate ransomware payments also may risk violating sanctions regulations, including transactions with sanctioned persons or to comprehensively sanctioned jurisdictions. On 21 September, the Treasury Department announced a "set of actions focused on disrupting criminal networks and virtual currency exchanges responsible for laundering ransoms," in addition to encouraging cybersecurity efforts in the private sector and increasing ransomware reporting to US government agencies. The actions included the unprecedented step of designating Suex OTC, a cryptocurrency exchange known to have facilitated illicit proceeds from at least eight ransomware variants, to the Specially Designated Nationals List. Such action comes on the heels of an October 2020 warning from the Treasury Department's Office of Foreign Assets Control (OFAC) that "[c]ompanies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations." OFAC has designated numerous cybercriminal actors pursuant to its cyber-related sanctions authorities, including ransomware actors such as the Lazarus Group and Iranian nationals connected to the SamSam ransomware attacks.

In addition to criminal liability for willful violations of sanctions laws, there is strict liability for civil enforcement penalties – a person subject to US jurisdiction may be held civilly liable even if he did not know or have reason to know he was engaging with a person who is subject to sanctions. Obtaining an OFAC licence would shield against such liability, however, the time pressures of the cyber crisis and its implications for the company often preclude such an approach. Further, OFAC has said that it will review licencing applications involving ransomware payments on a case-by-case basis with a presumption of denial.

Working with law enforcement at the early stages of a cyber incident, and before a ransom demand is paid, affords law enforcement the opportunity to provide information about the nature of the cybercriminals to bolster the victim's due diligence efforts to avoid sanctions violations. At the very least, OFAC's enforcement guidelines encourage self-reporting to and cooperation with law enforcement, considering them important factors in exercising its enforcement discretion.

First published on the *Global Investigations Review* website, 08 October 2021.

Similarly, if a payment is made to a prohibited party, advance reporting to and cooperation with law enforcement would be important factors the Department of Justice would consider in assessing whether to pursue a criminal investigation. And regulatory agencies, including the SEC, view reporting favourably.

Finally, in the aftermath of (and even during) a ransomware attack, there can be intense scrutiny by board members, shareholders, regulators, civil plaintiffs, and legislative bodies of the system vulnerabilities that permitted the attack, the control systems designed to mitigate damage, and the handling of the incident once it occurred. Early cooperation with law enforcement puts the company in the best position to demonstrate the seriousness of its response. It is no surprise that during congressional testimony, the CEO of Colonial Pipeline highlighted the company's cooperation with law enforcement: "We are deeply sorry for the impact that this attack had… We quietly and quickly worked with law enforcement in this matter from the start, which may have helped lead to the substantial recovery of funds announced by the DOJ this week." This statement provided a powerful public messaging advantage for a company in the spotlight during a crisis.

Conclusion

The ransomware crime spree and its threat to public and private entities is waxing, not waning. The cyber extortion schemes are simply too attractive to both criminal actors and foreign adversaries interested in profit and harm to the United States to stop. Organisations must undertake urgent steps to harden their cyber defences and prepare mitigation measures to minimise the likelihood of a successful attack, or at least the consequences. For those entities that do find themselves victim to a ransomware incident, serious consideration should be given to reporting the attack to law enforcement early in the process and cooperating going forward.

First published on the *Global Investigations Review* website, 08 October 2021.