Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Ransomware Scourge May Be Nearing Its Breaking Point

By **Ben Kochman**

Law360 (May 5, 2021, 9:56 PM EDT) -- New task forces convened by the U.S. Department of Justice and a cybersecurity-focused nonprofit are confronting the sobering reality of ransomware, which has become a constant menace to institutions of all types and one of the nation's top security threats.

Hospitals, schools, COVID-19 vaccine researchers and private businesses like law firms have all been targeted within the past year with such attacks, in which cybercriminals demand digital currency after freezing victims out of computer networks. Organized ransomware cartels, some of which have ties to foreign nation-states, are increasingly also extorting victims by threatening to publicly post their sensitive data, Justice Department officials say.

The tactics are working. The business of ransomware payments is booming, with victims forking over at least $350 million in 2020, according to the cryptocurrency data firm Chainalysis.

Many data breach responders believe that the true payment total is far larger, given the unknown number of incidents that are never reported. The global cost of ransomware attacks, which includes remediation efforts, was a whopping $20 billion in 2020, according to an estimate by information technology company PurpleSec.

The pace and scope of ransomware have spurred the DOJ to launch an internal task force, which officials say will target the wider ecosystem of attacks in a bid to shift the calculus out of criminals' favor.

"Ransomware can have devastating human and financial consequences," acting Deputy Attorney General John Carlin wrote in an April memo announcing the task force. He vowed to employ a mix of "criminal, civil and administrative actions for enforcement," including taking down servers used to spread ransomware and seizing criminals' "ill-gotten gains."

A panel of representatives from the technology industry, government and academia assembled by the nonprofit Institute for Security and Technology has also released suggestions for addressing ransomware, including mandating that victims report extortion payments to the government.

Making a dent in the ransomware scourge won't be easy. But here, cybersecurity attorneys share three ideas for priorities that governments and the private sector should set as they work to combat the issue.

Clarify If and When Victims Can Pay

Ransomware victims and third-party intermediaries like insurance companies have been criticized for funding future attacks by making extortion payments. But attorneys say it can make rational sense for some victims to pay the ransoms if doing so is far cheaper than the alternative of rebuilding their networks from scratch.

"On the one hand, paying ransoms is adding fuel to future attacks. But at the same time, for victims, not paying a ransom could mean extinction for their organization," said Michael Phillips, chief claims officer at cyber insurance firm Resilience and co-chair of the Institute for Security and Technology task force. "If that is the decision you are faced with, it's not really a choice."

The IST group did not reach a consensus on whether to ban ransomware payments outright, but the panel did make several other suggestions, including creating a "Ransomware Response Fund" to support victims that refuse to pay ransomware actors and subsidizing entities' efforts to shore up their IT defenses.

The panel also recommended that ransomware victims be required to report extortion payments to the government in exchange for a limited form of liability protection, including that the report cannot "form the basis for a regulatory or other enforcement action."

That suggestion comes after ransomware targets and the third-party companies that negotiate on their behalf were warned by the U.S. Department of Treasury in October that they may face stiff legal penalties for paying attackers that are under economic sanction — even if evidence tracing the criminals to a sanctioned entity only emerges after the fact.

"The department is wrestling with its need to enforce the law without chilling cooperation with victims who fear that despite their best efforts, they won't have certainty about who the payment is going to and are concerned about the potential liability because of sanctions laws," said Alex Iftimie, a former DOJ national security official from 2012 to 2019 who is now of counsel at Morrison & Foerster LLP.

Sway Nation-States to Stop Fostering Hackers

U.S. Department of Homeland Security Secretary Alejandro Mayorkas vowed in March to call out foreign nations that allow ransomware attackers to flourish within their borders, often out of the reach of the U.S. justice system.

Biden administration officials will need to figure out which diplomatic levers to push to effectively pressure those nations to crack down on ransomware gangs, including but not limited to sanctions, ex-government attorneys say.

"Sanctions are a possibility, and certainly prosecutions, but we are not going to prosecute our way out of this," said Luke Dembosky, co-head of the data strategy and security practice at Debevoise & Plimpton LLP and the former assistant attorney general in the Justice Department's National Security Division from October 2014 to March 2016.

"Most of these ransomware groups operate in places with little to no rule of law, where prospects for getting local cooperation for an arrest are dim," Dembosky added. "And who can doubt that certain corrupt officials are having their pockets lined by these organized criminal groups?"

After publicly calling out specific nation-states for failing to act, U.S. officials have a variety of tools at their disposal to escalate matters, including issuing sanctions and refusing to answer evidence requests made under mutual legal assistance treaties, Iftimie said.

"By being able to essentially keep a scorecard of what foreign jurisdictions are failing to do, you can continue putting this front and center in your discussions with those countries," the Morrison & Foerster attorney said. "There are ways of making those nation-states feel the pain for not doing anything to stop this activity from happening."

Regulate Cryptocurrency More Tightly

The IST task force is pushing for more efforts to trace ransomware payments by enacting transparency rules on a wide swath of the cryptocurrency industry, including not only currency exchanges but also crypto "kiosks" used to convert currency into cash and crypto "trading desks" that buy and sell digital coins.

Regulators "must designate clear enforcement bodies" to penalize cryptocurrency entities that don't report suspicious activity to authorities under existing know-your-customer laws, anti-money laundering laws and counter-terrorist financing laws, wrote members of the panel, which includes representatives from the FBI, DHS, the U.S. Secret Service and the New York Department of Financial Services.

The possibility of staying anonymous is a key feature of many digital currencies like Bitcoin, which uses blockchain technology to record every transaction in a publicly accessible ledger but does not require users to identify themselves if they are using what are known as self-hosted wallets. But having authorities know which cryptocurrency exchanges or wallets ransomware actors are using could prove helpful in tracing and even potentially clawing back ransom payments, cybersecurity attorneys say.

Given that the ransomware surge has affected countries all over the world, U.S. government officials should also make it a priority to "encourage other countries with less developed regulatory systems to similarly treat [crypto entities] as financial institutions subject to reporting requirements," said Behnam Dayanim, a partner at Paul Hastings LLP who advises fintech companies and heads the firm's privacy and cybersecurity practice.

"Responsible actors in the crypto industry understand and embrace" that some degree of regulation on the issue is appropriate, Dayanim added.

--Editing by Jill Coffey and Emily Kokoll.