Ransomware gangs get paid off as officials struggle for fix

21 June 2021, by Frank Bajak

In this Nov. 20, 2020, file photo a U.S. Department of Homeland Security plaque is displayed a podium as international passengers arrive at Miami international Airport where they are screened by U.S. Customs and Border Protection in Miami. The damned-if-you-pay-damned-if-you-don't dilemma on ransomware payments has left U.S. officials fumbling about how to respond. While the Biden administration "strongly discourages" paying, it recognizes that failing to pay would be suicidal for some victims. Credit: AP Photo/Lynne Sladky, File

If your business falls victim to ransomware and you want simple advice on whether to pay the criminals, don't expect much help from the U.S. government. The answer is apt to be: It depends.

"It is the position of the U.S. government that we strongly discourage the payment of ransoms," Eric Goldstein, a top cybersecurity official in the Department of Homeland Security, told a congressional hearing last week.

But paying carries no penalties and refusing would be almost suicidal for many companies, especially the small and medium-sized. Too many are unprepared. The consequences could also be dire for the nation itself. Recent high-profile extortive attacks led to runs on East Coast gas stations and threatened meat supplies.

Although the Biden administration has made battling ransomware crime a national security priority, public officials are fumbling over how to respond to the ransom payment dilemma. In an initial step, bipartisan legislation in the works would mandate immediate federal reporting of ransomware attacks to assist response, help identify the authors and even recoup ransoms, as the FBI did with most of the $4.4 million that Colonial Pipeline recently paid.

Without additional action soon, however, experts say ransoms will continue to skyrocket, financing better criminal intelligence-gathering and tools that only worsen the global crime wave.

President Joe Biden got no assurances from Russian President Vladimir Putin in Geneva last week that cybercriminals behind the attacks won't continue to enjoy safe harbor in Russia. At minimum, Putin's security services tolerate them. At worst, they are working together.

Energy Secretary Jennifer Granholm said this month that she is in favor of banning payments. "But I don't know whether Congress or the president is" in favor, she said.

And as Goldstein reminded lawmakers, paying doesn't guarantee that you'll get your data back or that sensitive stolen files won't end up for sale in darknet criminal forums. Even if the ransomware crooks keep their word, you'll be financing their next round of attacks. And you may just get hit again.

In April, the then-top national security official in the Justice Department, John Demers, was lukewarm toward banning payments, saying it could put "us in a more adversarial posture vis-à-vis the victims, which is not where we want to be."

Perhaps most vehement about a payment ban are those who know ransomware criminals best—cybersecurity threat responders.

Lior Div, CEO of Boston-based Cybereason, considers them digital-age terrorists. "It is terrorism in a different form, a very modern one."

In this Oct. 19, 2020, file photo Assistant Attorney General for the National Security Division John Demers takes a question from a reporter via teleconference at a news conference at the Department of Justice in Washington. The damned-if-you-pay-damned-if-you-don't dilemma on ransomware payments has left U.S. officials fumbling about how to respond. In April, the then-top national security official in the Justice Department, John Demers, was lukewarm toward banning payments, saying it could put "us in a more adversarial posture vis-à-vis the victims, which is not where we want to be." Credit: AP Photo/Andrew Harnik, Pool

A 2015 British law prohibits U.K.-based insurance firms from reimbursing companies for the payment of terrorism ransoms, a model some believe should be applied universally to ransomware payments.

"Ultimately, the terrorists stopped kidnapping people because they realized that they weren't going to get paid," said Adrian Nish, threat intelligence chief at BAE Systems.

U.S. law prohibits material support for terrorists, but the Justice Department in 2015 waived the threat of criminal prosecution for citizens who pay terrorist ransoms.

"There's a reason why that's a policy in terrorism cases: You give too much power to the adversary," said Brandon Valeriano, a Marine Corps University scholar and senior adviser to the Cyberspace Solarium Commission, a bipartisan body created by Congress.

Some ransomware victims have taken principled stands against payments, the human costs be damned. One is the University of Vermont Health Network, where the bill for recovery and lost services after an October attack was upwards of $63 million.

Ireland, too, refused to negotiate when its national health care service was hit last month.

Five weeks on, health care information technology in the nation of 5 million remains badly hobbled. Cancer treatments are only partially restored, email service patchy, digital patient records largely inaccessible. People jam emergency rooms for lab and diagnostic tests because their primary care doctors can't order them. As of Thursday, 42% of the system's 4,000 computer servers still had not been decrypted.

The criminals turned over the software decryption key a week after the attack—following an unusual offer by the Russian Embassy to "help with the investigation"—but the recovery has been a painful slog.

"A decryption key is not a magic wand or switch that can suddenly reverse the damage," said Brian Honan, a top Irish cybersecurity consultant. Every machine recovered must be tested to ensure it's infection-free.

Data indicate that most ransomware victims pay. The insurer Hiscox says just over 58% of its afflicted customers pay, while leading cyber insurance broker Marsh McLennan put the figure at roughly 60% for its affected U.S. and Canadian clients.

But paying doesn't guarantee anything near full recovery. On average, ransom-payers got back just

65% of the encrypted data, leaving more than a third inaccessible, while 29% said they got only half of the data back, the cybersecurity firm Sophos found in a survey of 5,400 IT decision-makers from 30 countries.

In this May 11, 2021 file photo Energy Secretary Jennifer Granholm speaks during a press briefing at the White House in Washington. The damned-if-you-pay-damned-if-you-don't dilemma on ransomware payments has left U.S. officials fumbling about how to respond. While the Biden administration "strongly discourages" paying, it recognizes that failing to pay would be suicidal for some victims. Granholm said this month that she is in favor of banning payments. "But I don't know whether Congress or the president is." Credit: AP Photo/Evan Vucci, File

In a survey of nearly 1,300 security professionals, Cybereason found that 4 in 5 businesses that chose to pay ransoms suffered a second ransomware attack.

That calculus notwithstanding, deep-pocketed businesses with insurance protection tend to pay up.

Colonial Pipeline almost immediately paid last month to get fuel flowing back to the U.S. East Coast—before determining whether its data backups were robust enough to avoid payment. Later, meat-processing goliath JBS paid $11 million to avoid potentially interrupting U.S. meat supply, though its data backups also proved adequate to get its plants back online before serious damage.

It's not clear if concern about stolen data being dumped online influenced the decision of either company to pay.

Colonial would not say if fears of the 100 gigabytes of stolen data ending up in the public eye factored into the decision by CEO Joseph Blount to pay. JBS spokesperson Cameron Bruett said "our analysis showed no company data was exfiltrated." He would not say if the criminals claimed in their ransom note to have stolen data.

Irish authorities were fully aware of the risks. The criminals claim to have stolen 700 gigabytes of data. As yet, it has not surfaced online.

Public exposure of such data can lead to lawsuits or lost investor confidence, which makes it manna for criminals. One ransomware gang seeking to extort a major U.S. corporation published a nude photo of the chief executive's adult son on its leak site last week.

Rep. Carolyn Maloney, chair of the House Committee on Oversight and Reform, has asked in written requests to know more about the JBS and Colonial cases as well as CNA Insurance. Bloomberg News reported that CNA Insurance surrendered $40 million to ransomware criminals in March. The New York Democrat said, "Congress needs to take a hard look at how to break this vicious cycle."

Recognizing a lack of support for a ransom ban, Senate Intelligence Committee Chair Mark Warner, D-Va., and other lawmakers want at least to compel greater transparency from ransomware victims, who often don't report attacks.

They are drafting a bill to make the reporting of breaches and ransom payments mandatory. They would need to be reported within 24 hours of detection, with the executive branch deciding on a case-by-case basis whether to make the information public.

But that won't protect unprepared victims from potentially going bankrupt if they don't pay. For that, various proposals have been put forward to provide financial assistance.

The Senate this month approved legislation that would establish a special cyber response and recovery fund to provide direct support to the most vulnerable private and public organizations hit by major cyberattacks and breaches.