The Cybersecurity 202: This Florida city just paid hackers a huge ransom. Is that better or worse for taxpayers?

By Joseph Marks

THE KEY

A small Florida city paid an extraordinary $600,000 in ransom this week to hackers who had locked up the city’s computer systems -- highlighting an increasingly common dilemma for city leaders across the country.

Cities have been hit with an increase in ransomware attacks in recent years since tight budgets have left them with outdated and hackable computer systems. But paying the ransoms to reverse the attack means putting money -- taxpayer money -- into the hands of nefarious hacking groups who probably will use it to target other victims.

If they refuse to pay up, though, they could be saddled with an even bigger bill to get their cities back online. And they may have to deal with lasting consequences -- like in Baltimore, where city leaders decided against paying the ransom and still hasn’t restored all its city services six weeks after a devastating attack.

“When you pay the ransom, you’re making the bad guys better,” says Allan Liska, a threat intelligence analyst at cybersecurity firm Recorded Future. “But, from a strictly business perspective, sometimes you have to pay the ransom because the cost of not paying it is going to be much, much more.”

But cities, of course, are not just businesses - they have citizens who don't want their tax dollars wasted and leaders who want to get re-elected. Given there are taxpayer costs to either choice, this is both a practical and moral question for city leaders.

“It’s their constituents’ money and it’s taxpayer money, so that’s very different,” Liska tells me.

Not to mention, there could also be career and electoral consequences for city officials who don't stand up to bad guys. “No politician wants to go on record as having paid a ransom to a cybercriminal,” Liska said.

Already on Thursday, the payout had registered in Washington, where Sen. Marco Rubio (R-Fla.) said he’s working on ways the federal government can help.
A study from Recorded Future found that cities are actually slightly less likely to pay off ransomware hackers than other victims. Just 17 percent of the cities struck with ransomware in the study paid compared with about 45 percent of ransomware victims overall.

That figure could change, though, as city officials draw lessons from major ransomware attacks in cities that didn't pay. In Baltimore, officials expect to pay about $18 million after refusing to pay a ransom demand of just about $70,000, and a 2018 attack in Atlanta cost the city about $2.6 million to recover from.

In the case of Riviera Beach, Fla., the city suffered through three weeks during which city workers couldn’t access their email accounts and emergency dispatchers couldn’t log calls into computers, my colleague Rachel Siegel reported. Ultimately, the city council voted unanimously to pay the hackers 65 bitcoin, which amounts to about $592,000.

Price tags like that are bound to make city officials think twice about whether they can refuse a ransom demand, Joe Hall, chief technologist at the Center for Democracy and Technology, told me.

“You’d think the incentive would be to pay as little as possible,” he said.

Ransom payments and ransomware recovery costs are sometimes covered by insurance, but insurance rarely covers all the costs and a big payout will raise cities’ insurance rates.

Another lesson cities are hopefully taking from the Baltimore, Atlanta and Riviera Beach examples, however, is that they should be better protecting their computer systems against hackers before the ransomware strikes, Tad McGalliard, director of research and policy at the International City/County Management Association, told me.

That includes installing basic protections such as guarding against phishing emails and requiring extra verification before people can access computer systems, he said. It also includes making sure that all the city’s vital records are backed up somewhere offline where hackers can’t seize them and lock them up.

“We’re likely to see a continuing increase in ransomware attacks on local governments, but I hope we also see local governments taking note of this and doing everything in their power to bulk up their cyber defenses,” McGalliard said.
PINGED: Iranian hackers are scaling up attacks on U.S. government agencies while conflict mounts between the nations over Iran’s nuclear program, Andy Greenberg at Wired reports. None of the attacks appear to have been successful yet, but the attackers’ targets include the Energy Department and its federal research facilities, according to researchers at the cybersecurity firm Dragos.

“We’re probably headed for a place very, very soon, where the days of aggressive Iranian activity are likely to return. If we’re trading blows with them in the Gulf, I don’t see them holding back,” John Hultquist, director of threat intelligence at FireEye, told Wired.

Both FireEye and Dragos attributed the attack to APT33, a hacker group linked to the Iranian government.

PATCHED: A bipartisan pair of House lawmakers wants a government watchdog to measure how well the United States is working with other countries to combat cybercrime.

Despite a bevy of efforts to counter cybercrime across the State and Justice departments, the government has not “clearly articulated an inter-agency strategy with firm objectives as to what these efforts are aiming to achieve,” Reps. Eliot L. Engel (D-N.Y.) and Michael McCaul (R-Tex.), the top Democrat and Republican on the House Foreign Affairs Committee, wrote the Government Accountability Office.

The report should focus on the State Department’s cyber office, which has gone through jarring reorganizations during the past two years, as well as the U.S. government’s work with international organizations including the United Nations and Interpol.

PWNED: NASA’s Jet Propulsion Laboratory was hacked in April of 2018, allowing attackers to access a communications network used by multiple NASA spacecrafts, according to a government watchdog report out this week. The attack was serious enough to spook the Johnson Space Center into ceasing to share some data communications with the lab, fearing a breach could lead to more attacks on other technology infrastructure.

JPL did not follow a number of NASA cybersecurity protocols, according to the report from NASA’s inspector general. Even after security vulnerabilities were identified they “were not resolved for extended periods of time — sometimes longer than 180 days,” per the report. In addition to fixing the security weaknesses, investigators are ordering the NASA lab to introduce a new threat identification process to prevent more attacks.

If hackers got into JPL they could have a field day, information security analyst Mike Thompson tells Davey Winder at Forbes. “[NASA’s] depth of research and development includes patents covering cutting edge science that nation states would literally kill for,” he said. The lab was also the target of a China-based attack in 2012.
Nadler: Hope Hicks broke with Trump on accepting foreign dirt

Hicks “knew that the president’s statement was troubling” and “understood the president to be serious,” Nadler says.

Politico

The Drone Iran Shot Down Was a $220M Surveillance Monster

The Global Hawk can fly at an altitude of 55,000 feet and stay aloft for 30 hours straight.

Wired

Prosecutors rebut Roger Stone: U.S. caught Russian election hackers on its own

Trump ally has alleged the government relied solely on ‘an inconclusive and unsubstantiated report’ written by a cyber research firm.

Politico

Senate wants to boost oversight of Pentagon’s cyber activities

Several provisions in the Senate’s version of the annual defense policy bill aim to increase oversight of cyber activities in the Department of Defense, including a new two-star general officer to serve as the senior military adviser to cyber policy.

Fifth Domain

Email scammers use corporate consultant sites to find victims

They operate just like any other small business.

Axios
California experienced more data breaches than any other state in the past decade: report

California has suffered more data breaches and personal records exposed than any other state in the U.S. over the past decade, with almost 1,500 data breach incidents, a new report has found.

The Hill

Meds prescriptions for 78,000 patients left in a database with no password | ZDNet

Database containing 390,000 Vascepa prescriptions for 78,000 patients left open on the internet.

ZDNet

Dell quietly patched a SupportAssist vulnerability that affected millions of users - CyberScoop

Dell released a security advisory Thursday about a vulnerability in SupportAssist that could impact millions of machine running Microsoft Windows.

CyberScoop

Canadian lender Desjardins says personal data of 2.9 million...

Canadian lender Desjardins Group said on Thursday an unauthorized use of interna...

Reuters

— Coming Soon:

The House Administration Committee will mark up HR. 2722, the Securing America’s Federal Elections Act, on Friday at 9 a.m.
The House Homeland Security Committee will host a hearing on Artificial Intelligence and Counterterrorism on June 25 at 10 a.m.
The House Homeland Security Committee will bring in representatives from Facebook, Google, and Twitter to discuss their company’s efforts to address terror content and misinformation on June 26 at 10 a.m.

Joseph Marks