Bond Case Briefs

Municipal Finance Law Since 1971

Paying a Hacker's Ransom Shouldn't Be a Crime.

A federal law outlawing the practice would be a very bad idea.

I recently suggested that Baltimore might perhaps consider giving in to ransomware demands by unknown hackers who so cleverly froze the city's computer network last month that much of it remains inaccessible. Then came last week's news that the much smaller city of Riviera Beach, Florida, agreed to pay $600,000 to get its own computer services unlocked. This entirely rational act has led to considerable online criticism — including an editorial in the Washington Post demanding "a federal law banning ransomware payments."

Well.

Let me suggest, as gently as possible, that this is a very bad idea. I'm not pro-ransomware; but I'm very much in favor of leaving difficult and complex decisions to those entrusted with making them.

To begin with, it's not entirely clear whether there actually is a crisis. News stories keep insisting that ransomware attacks targeting cities are on the rise, but without official data it's hard to tell. A May 2019 blog post from Recorded Future, a cybersecurity firm, found 46 attacks on 2016, 38 in 2017, 53 in 2018, and 21 during the first four months of 2019. Each attack imposes terrible costs, but these numbers hardly signal an epidemic.

Corporations, because they have the deepest pockets, remain the major targets. Nevertheless, as corporate security improves, it's only logical for hackers to try extorting other entities. Cities are an obvious target in large part because they're notoriously terrible at protecting their systems. For those whose protection systems are weak — or for that matter who can't get their employees to stop clicking on unsafe links while at work — ransomware attacks will only get worse.

Getting locked out of your own systems until you pay a hacker a bunch of bitcoins might seem like punishment enough for those with sloppy cybersecurity. So what's the argument for adding legal penalties when the target, out of options, decides that the path of least resistance is to give the hackers what they seek? Here's the Post: "Morally, taxpayer money should not be used to reward criminal enterprises. Practically, if cities collectively stop providing that reward, hackers may pack up their keyboards. Every dollar — or, more accurately, every bitcoin — that cities turn over to cybercriminals encourages them to continue attacking, and it also gives them the resources to do so more effectively and more often."

Each of these claims may be correct.1 But while they might add up to an argument against the wisdom of paying ransom, they don't explain why the target shouldn't be allowed to pay if it would rather regain control of its own systems than stand up and make a point. Security consultants concede that situations may arise in which paying the ransom makes the most sense.

Yes, giving in to demands generates more demands. And we can all hope for stronger spines — not only in the leaders of cities whose computers have been hijacked, but also in college administrators and presidential contenders and social media companies, all of whom too often display the

distressing habit of yielding to the mob. In so doing they must surely encourage more mobs. But much as I might wish they'd more often stand up and fight back, I hardly want to make it illegal for them to give in.

It's fine to articulate a strong principle against yielding to extortion; as I have pointed out, frequent and clear articulation of this principle by those in positions of power might in and of itself serve as a deterrent. But principle is different from law, and by keeping them separate, we enable those who must actually make the decisions to weigh any of 100 factors that those drafting a statute can never take into account.

Consider, by analogy, the oft-stated principle that the U.S. does not negotiate with terrorists. Leaders repeat this rule time and again, but the rule does not actually mean what it says, because at times the U.S. does negotiate with terrorists. The existence of a strongly articulated and often repeated principle isn't hypocrisy; instead, it exerts strong pressure on decision makers to keep the exceptions rare. Still, those exceptions will arise, and we leave the determination to the judgment of the political actors of any given moment.

Surely the same rationale should be applied to municipal leaders (or corporate leaders or anyone else) who face a ransomware demand. Refusing to pay is often admirable. It's not at all clear, however, that it's the right answer in every case. The target might have a variety of perfectly sensible reasons for giving in, such as the expense in time and money. Citizens of a municipality that has been targeted can hardly be expected to bear the costs of someone else's principle.

Hijacking a computer system belonging to someone else is an outrageous violation of property and privacy rights. Such acts are prohibited under any number of federal statutes, including the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, and under a growing number of state enactments.2

But all these many laws punish only the hackers who seek to extort money from people or entities in return for giving back the target's own property — practical control over the hijacked system. None of them purport to punish the targets for how they choose to respond.

When one is facing extortion, it's often brave and admirable to stand up voluntarily to the demands of the extorter. It's wrong and overbearing to require such bravery by law.

1. OK, maybe not the implication that taxpayer funds (that is, monies held by governments) are more precious than, say, private funds.
2. Even in the absence of any special laws, to break into someone else's system would clearly constitute common law trespass, and perhaps common law conversion as well.

Bloomberg Opinion

By Stephen L. Carter

June 25, 2019, 6:00 AM PDT

Stephen L. Carter is a Bloomberg Opinion columnist. He is a professor of law at Yale University and was a clerk to U.S. Supreme Court Justice Thurgood Marshall. His novels include "The Emperor of Ocean Park," and his latest nonfiction book is "Invisible: The Forgotten Story of the Black Woman Lawyer Who Took Down America's Most Powerful Mobster."

Follow @StepCarter on Twitter