Bond Case Briefs

Municipal Finance Law Since 1971

Should Cities Ever Pay Ransom to Hackers?

Some say paying hackers to release hijacked data encourages more attacks. Others say it can be the responsible thing to do.

Cities across the U.S. face a growing threat from ransomware, where cybercriminals infiltrate computer systems and hijack data, vowing to delete critical files unless they receive payment.

It is difficult to say exactly how many such attacks have taken place in recent years, as there is no centralized agency that tracks them and many go unreported. But research firm Recorded Future says it has tracked 71 ransomware attacks against state and local governments so far this year, compared with 54 in 2018. (The firm counts a recent coordinated attack in Texas affecting 22 municipalities as a single incident.)

Once hackers have control of a city's files, local leaders have a decision to make: Do they pay the bounty in the hopes of resolving the problem quickly, or forge ahead with the time and expense of a disaster-recovery effort?

The Federal Bureau of Investigation advises against paying hackers, saying it only encourages more attacks, and the U.S. Conference of Mayors in July adopted a resolution opposing ransom payments.

But some security professionals say there may be times when municipalities have few options other than to pay, especially if the systems taken hostage are critical to public health and safety and can't be restored quickly.

Craig Shue, an associate professor of computer science and cybersecurity at Worcester Polytechnic Institute in Worcester, Mass., says there are cases where paying a ransom is reasonable. Frank Cilluffo, director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security, says it is always a bad idea.

YES: Sometimes, the benefits of paying a ransom outweigh the costs
By Craig Shue

Some cybersecurity experts oppose the payment of ransomware demands under any circumstance, saying it serves only to embolden hackers and spur more attacks. While those are credible concerns, there are clear cases where paying a ransom is the responsible, even morally ethical, thing for a local government to do.

When deciding what to do, municipal leaders need to look carefully at the costs and benefits and then take whatever action yields the greatest benefits to all. Under such a utilitarian analysis, to ethically pay a ransom, municipal leaders must be without any better options. Further, the benefits from the payment must meet or exceed the harm that paying a ransom incurs. Importantly, this analysis must include the harm to society, such as the risk that paying a ransom could fund more ransomware development or acts of terrorism.

Companies that have to send employees to potentially dangerous locations, where abduction is a real

risk, often perform similar calculations. Sometimes those calculations lead them—or the individuals themselves—to purchase kidnap-and-ransom insurance, recognizing that in some circumstances the best option may be to pay a ransom to preserve human life.

So under what circumstances might paying a ransom be a rational decision for a city or municipality?

Local governments manage information that is vital to keeping people safe. Losing control of data related to water safety, fire risks, emergency medical services or law enforcement could have immediate and significant consequences. If a local government must make a small ransom payment to save a person's life or many people's lives, or to protect public health, one could argue the benefit may outweigh the cost.

Local governments also keep vital records such as birth certificates, property deeds and court documents that citizens may need to prove identity, ownership of property or even child custody. Given the great harm associated with the loss of this data, attempting to recover the records quickly though a ransom payment may be the most ethical thing for local leaders to do.

Then there is data that local governments need to continue operating. If a municipality's financial records are encrypted in a ransomware attack, the government may not know what debt it owes or what funds it is entitled to collect. While trying to reconstruct these financial records from outside sources, the government may not be able to function. The cost of a ransom payment, in comparison, might seem small.

Unfortunately, hackers often set deadlines for ransoms to be paid, which may force leaders to make decisions with limited or imperfect knowledge. There also is the risk that paying the ransom won't work—that is, the payment won't result in the data being unlocked or it will lead to a demand for more money. But the alternative—simply banning ransomware payments outright—ignores the nuances of ransom decisions and eliminates flexibility for decision makers.

I agree with those who say that local governments should do everything in their power to be better prepared in case of an attack. For instance, some local governments have joined in a pledge to not pay ransomware demands. Such promises tell government employees that they must take appropriate precautions to ensure they can achieve their missions without ransomed data, through system backups or other disaster-recovery approaches. In effect, the city decides to treat the ransomware attack as equivalent to the attacker irrevocably deleting the data.

All local leaders should aspire to and achieve such a standard, as no-ransom pledges may discourage some attackers who specifically target local governments for payment. But the reality is that not all cities and towns have the resources to secure their data fully or rebuild their servers if attacked. System backups are complicated, requiring information-technology experts, and some local governments don't have IT people on staff and can't afford to hire them.

It isn't illegal to pay ransom in most cases, but local leaders should report such demands to law enforcement. They also should be transparent with their citizens; however, it may be prudent to decrypt ransomed data before public disclosure to avoid price increases or other demands from the ransomer.

Every organization hopes to avoid being the recipient of a ransom demand. But rather than simply condemn ransom payments universally, we owe these leaders advice on how to make rational, ethical decisions.

NO: Paying a ransom will only encourage more hackers to attack in the future
By Frank Cilluffo

From the early days of our republic, history has shown that paying ransom is a bad idea.

Consider the case of the Barbary pirates, when countries would make payments known as “tributes” to guarantee safe passage for ships through the Mediterranean. The practice gave rise to a vicious circle, wherein one payoff would simply spur another attack and demand, instead of securing passage. President Thomas Jefferson thus ended the payments after his inauguration in 1801, and set a precedent: Ransom wouldn’t be paid because it encourages more attacks and strengthens criminal groups.

The same logic holds true for ransomware demands today and is why states and local governments shouldn’t pay.

Already this year, dozens of local governments in the U.S. have fallen victim to ransomware, and the magnitude of the threat underscores why it must be eliminated altogether. This can only be done with a unified front across all sectors. While paying ransom is enticing as a quick fix, allowing institutions to forgo costs associated with system repair, it doesn’t get at the root of the problem—and may exacerbate it if systems are left insecure and vulnerable to more hacking. Compounding the problem is that only one-quarter of all ransomware attacks are reported, which inhibits law enforcement from fully assessing and responding to the problem.

Not paying ransom is comparable to the strategy used in terrorist hostage situations. International commitments forbid governments from making payments to terrorists because it encourages more kidnappings and higher amounts in the long run. It also finances international terrorist organizations, thereby increasing terrorist threats everywhere. Similarly, evidence points to ransomware payments going to state sponsors of terrorism, like North Korea and Iran, which then plow earnings back into their operations to improve and refine malware.

Paying ransomware demands therefore directly sabotages U.S. national security by funding our adversaries to perpetrate more sophisticated attacks—a gift that keeps on giving.

Like terrorism, ransomware endangers lives by threatening systems that exist to protect us. But even in the toughest of cases, local governments have to stand firm. Otherwise, we provide cybercriminals with an incentive to keep doing what they are doing, with the result being that many more lives may be lost or placed in jeopardy. What’s more, paying ransom doesn’t guarantee the return of the captured data. In fact, only about half of those who fell victim to attacks in 2017 were able to recover their data after paying the demand. A Kansas hospital in 2016, for example, paid the requested ransom—but then received an order for more money instead of the decryption key.

So, what can we do? Most important, local governments should focus on prevention and resilience. The best strategy for institutions is to act now to improve cybersecurity—before an attack occurs—thereby making the ransomware debate irrelevant. Establishing system backups and updating and patching software are both easier and cheaper than paying off criminals. In several notable cases, such as the attacks on San Francisco’s MTA and the city of Sarasota, Fla., ransom payments weren’t even considered because data and information systems were properly secured beforehand. This should be every organization’s goal.

It is also important for cities and states to communicate with law enforcement, as officials can facilitate the adoption of measures to be used both before and (if necessary) after an attack. The FBI increasingly has succeeded at identifying ransomware actors and indicators, which enables officials

to pinpoint vulnerabilities and help organizations deter hackers. But this can only happen if ransomware incidents are reported.

Establishing mechanisms through the Department of Homeland Security that provide aid and funding to local and state governments for cybersecurity and resiliency efforts would help support victims and alleviate the pressure to pay. Designating ransomware operators as transnational criminal organizations would provide officials with more tools and authority to prevent, deter and punish offenders.

While it's understandable for institutions to want to quickly regain access to data to maintain continuity of operations, it is essential to derail and deter the growing cycle of attacks through a unified front. This is a national emergency and we need to treat it like one.

Technology and the means to perpetrate crimes may change, but human nature remains consistent. From old crimes to new ones, the same thing holds true: Ransom and ransomware wouldn't exist if we didn't pay.

The Wall Street Journal

Sept. 17, 2019 10:02 pm ET

Dr. Shue is an associate professor of computer science and cybersecurity at Worcester Polytechnic Institute in Worcester, Mass. Email him at reports@wsj.com.

Mr. Cilluffo is the director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security. Email him at reports@wsj.com.