The Texas Lawbook

Free Speech, Due Process and Trial by Jury

Texas Municipalities and Ransomware: Can the Sheriff Surrender to the Outlaw?

July 11, 2019 | By PHILIP J. BEZANSON and DAVID B. SPRINGER

Ransomware attacks against government entities are on the rise. Three Florida towns were infected last month alone, and Texas municipalities are increasingly finding themselves between Scylla and Charybdis: pay ransom to hackers or lose data (or access to data) critical to the basic functions of modern cities. This dilemma has been widely discussed practically and abstractly, but there remains little official guidance as to whether a public entity in Texas can legally pay a ransom, even if it is the financially responsible thing to do.

In one example from earlier this year, on the morning of January 10, a ransomware attack plunged the municipal government of Del Rio, Texas, into a tech blackout. Hackers encrypted the city's data and demanded ransom for its release. City Hall employees resorted to working with pens, paper and typewriters to keep the local government functioning.

City officials faced a choice that has become familiar in the business world: lose your data or send Bitcoin to cyber-bandits. The Department of Justice estimates that four thousand ransomware attacks occur every day. Municipalities are frequent targets—at least 53 state and local systems were infected in 2018, up from 38 in 2017.

Del Rio decided that recovering the city's data was worth paying ransom. According to recent CyberEdge research, about 45 percent ransomware victims made a ransom payment. But government entities appear relatively less likely to pay. Another researcher found that "only 17.1 percent of state and local government entities that were hit definitely paid the ransom, and 70.4 percent of agencies confirmed that they did not pay the ransom." That trend might be changing, however, as two of the three Florida towns infected by ransomware last month opted to pay, as did Atlanta last year.

While valid legal and ethical concerns linger, the consequences of not surrendering to ransom demands can be dire, as some municipalities learned the hard way. A recent standoff over a $76,000 ransom set the city of Baltimore back $18 million. In 2017, a Dallas County police department lost years of evidence when they refused to meet their attackers' demands.

Using taxpayer dollars to pay off criminals may not sound Texas tough. But ransomware payments are something of a legal wild west—there is little to no law explicitly governing how to respond to such a demand. This gap in the law makes it possible that a Texas municipality might resist paying ransom to free their data, even if payment is the more financially prudent option.

State Law

Of known ransomware incidents involving Texas municipalities, Del Rio appears to be the only one who has opted to pay, and under state law, they were likely empowered to do so. House Bill 9 in the Texas legislature's 2017 session criminalized ransomware, but neither the statute nor its legislative history discuss ransom payment.

Other Texas laws that address public payments to private entities probably do not prohibit ransom payments. Art. XI Sec. 3 and Art. III Sec. 52 of the Texas Constitution prohibit grants of public funds to private corporations or associations. These provisions do not, however, prohibit all municipal associations with private entities.

In Barrington v. Cokinos, the Texas Supreme Court held that municipalities can pay private corporations and associations "for the direct accomplishment of a legitimate public and municipal purpose." 338 S.W.2d 133 (Tex. 1960). The Texas Attorney General's office has agreed with this reading on several occasions, advising, for example, that payments in the context of county officials' attendance at a conference, publishing notices in privately owned newspapers, and covering medical expenses of an injured public school student are constitutionally permissible expenditures. *See* 24 Tex. Reg. 5617 (Jul. 23, 1999); Tex. Att'y Gen. op. GA-0076 (2003).

The same logic used by the Texas Supreme Court and the Attorney General's office, namely that payments made to private parties in the public interest do not violate the Constitution,

likely extends to ransom payments. Paying ransom could might also be constitutionally legitimized as emergency expenditure under Texas Local Government Code Sec. 102.009(c), which authorizes out-of-budget payments in cases of "grave public necessity to meet an unusual and unforeseen condition."

Federal Law

Most cyber crime directed at U.S. targets originates from abroad, particularly Russia and Eastern Europe, and nation-states are the fastest growing group of cyber-attackers. Of attacks on local and state bodies identified in one study, six came from Iran, four from North Korea, and three from Russia and Eastern Europe.

There is no federal law explicitly prohibiting ransomware victims from paying a ransom. Yet the FBI strongly discourages paying and a thicket a federal laws and regulations could render payments illegal. For example, a payment could be prohibited if the payer knows the payee is on an Office of Foreign Assets Control ("OFAC") sanction list, to which some hackers and hacking groups have recently been added.

Further complicating the issue, victims often do not know the true identity of a ransom recipient, and in some cases, may not even know a ransom is being paid on their behalf. Reporting from ProPublica suggests that some local agencies have engaged cybersecurity firms to decrypt hostage data, but instead of decrypting ransomware, the firms simply paid the ransom—effectively profiting off of long-term, symbiotic relationships with hackers.

Municipalities are likely protected against tort suits for engaging with sanctioned entities through official immunity, however, which protects government employees and their governmental employer for discretionary, good faith acts within the scope of the employee's authority. See *Univ. of Hous. v. Clark*, 38 S.W.3d 578, 580 (Tex. 2000). But a municipality is of course subject to enforcement actions from the federal government. *Marshall v. A & M Consol. Indep. Sch. Dist.*, 605 F.2d 186, 188 (5th Cir. 1979).

How Municipalities Should Respond to an Attack

Though the data is incomplete and exercises of prosecutorial discretion could change rapidly, the federal government has generally not prosecuted people who make ransom payments. For that reason and others discussed in this article, it seems unlikely that federal or state law enforcement would take action against a municipality for paying ransom. But legal concerns aside, municipal bodies should still think twice before using public funds to rescue data from criminals' clutches.

Ransom payments are problematic from a policy perspective. First, the more frequently victims pay, the more emboldened hackers become. And while most financially motivated ransomware attackers do release systems after being paid, it's also possible that paying ransom is wholly ineffective to free captive data.

Further, governments risk blowback from their constituents—both as a principled "law and order" issue and in terms of decreased public trust in institutions. As the authors have noted before, that decreased trust can have direct financial consequences such as credit ratings downgrades and more difficult bond elections. For example, a private company recently became the first to see its credit outlook downgraded due to cyber issues.

Advance preparation is also key—namely data backup, redundant systems, a practiced response plan, and insurance. Ideally, municipalities would have sufficient insurance and redundant backups to mitigate the need for using taxpayer money to pay ransom. Lake City, one of the Florida towns recently hit by ransomware, saved $450,000 in taxpayer money by using insurance to pay the bulk of their ransomware payment.

A written response plan, that is regularly updated and practiced, is a relatively low-cost but high-impact preparatory step. A cyber-incident playbook that contains a notification checklist of security, state and federal law enforcement, insurance, and legal contacts is a valuable resource in the early hours of an incident. Response plans should ensure stakeholders can securely communicate if normal communication platforms like email are unavailable. Municipalities should also identify and consider how to wall-off or create a backup copy of that data in case the city has to work offline

As part of that notifications process, municipalities should also carefully follow data breach notification requirements dictated by Section 205.010 of the Texas Local Government Code, which incorporates Section 521.053 of the Texas Business & Commerce Code.

Finally, municipalities would likely welcome state legislation or a clear statement of policy on this issue, resolving a complex and somewhat murky legal question from an already complex and time-constrained decision-making process.

Philip J. Bezanson is a partner at Bracewell LLP. **David B. Springer** is an associate at Bracewell LLP. **Claire Cahoon**, a Bracewell LLP summer associate and rising 3L at SMU Dedman School of Law, made many valuable contributions to this article.