CENSA® Council for Emerging National Security Affairs

CENSA Report:
Strategies for Preventing Ransomware Attacks on U.S. Local Governments

April 2021

Scott Vlachos, CENSA Fellow

BACKGROUND

Ransomware attacks are on the rise in the U.S., with municipal governments as a favored target for hackers. Poor information technology (IT) security infrastructure and a readiness to pay have caused local governments to be the most ransomed organization type since 2019.[1] Unlike large city and state governments, small county governments often lack the resources to upgrade their technology, employ full-time cybersecurity personnel, or hire external support from private IT security firms. Even with free toolkits, resources, and training plans provided by federal agencies, municipalities still struggle to prevent or overcome ransomware attacks. Some even fall victim to multiple attacks, only to pay the ransom each time as it is comparatively cheaper than the cost of repairing the damage.

In order to reduce ransomware attacks, further legislative action is needed to increase cybersecurity funding to troubled governments, spread awareness of the resources available to municipalities, attract more cybersecurity personnel, and create a centralized cybersecurity response system for each state.

ANALYSIS

Although ransomware is an old form of cyberattack, it has gained newfound popularity due to improved hacker strategies that increase the probability of success. Attackers no longer require coding literacy or advanced technical expertise to infect a device with ransomware. Hackers also distribute ready-made toolkits to novices in exchange for a percentage of the earnings, further fueling the frequency of ransomware infections and increasing the global pool of attackers. Additionally, more local governments are transitioning to digital tools to interface with their constituents, leaving them more susceptible to attacks.

The rising popularity of cryptocurrency as a means for ransom further incentivizes hackers, providing them with a layer of identity protection. While transactions are recorded in a public traceable ledger, known as blockchain, it is increasingly difficult for law enforcement to track a ransom payment across the network. Attackers typically move their payments across thousands of different transactions, sometimes with the aid from software, which mixes the cryptocurrency into smaller transactions with non-associated parties to launder the ransom.

Governments that choose to pay the ransom will likely never recover their money. Despite this, many vulnerable municipalities continue to pay in order to end disruption to vital services,

[1] According to research conducted by the IT security firm Barracuda Networks: https://blog.barracuda.com/2020/08/27/threat-spotlight-ransomware/

prevent private data from being publicly leaked, and to recover access to sensitive data. Payment incentivizes recurring attacks, as shown by the example of Cornelia, Georgia, which was the victim of four separate cyberattacks since 2019.

On the other hand, municipal governments that can afford to pay for cybersecurity protection and expensive system backups are typically able to refuse ransom demands and can instead opt to restore their databases and services to backups prior to the cyber intrusion.

Unfortunately, many municipalities cannot afford robust cybersecurity. Most contend with limited IT budgets, are encumbered by demands to upgrade technology, and have few external support options. Local governments often apply for grants through the Homeland Security Grant Program, which mandates that 7.5% of awards are spent on cybersecurity. This funding alone is not enough to make significant improvements in key problem areas. Municipalities struggle to attract cybersecurity specialists, who often flock to more lucrative positions in the private sector. As a result, many governments employ part-time cybersecurity staff which divide their attention between security and other IT duties. Dedicated cybersecurity personnel are required to consistently maintain security systems, provide red-team threat analysis, and ensure an immediate response to attacks.

Another issue affecting both cybersecurity and funding is that not all states utilize a centralized system for communication and support. This can result in redundant technology purchases and a sluggish response against compromised software found throughout a state’s various agencies. Furthermore, funding for IT is not always guaranteed by the state government, such as in Nevada, where the chief information officer’s (CIO) division accrues funding by selling services to other agencies. Nevada’s CIO, additionally, is not a member of the governor’s cabinet, which hampers efforts to prioritize the state’s cybersecurity agenda.

RECENT LEGISLATIVE INITIATIVES

The National Defense Authorization Act for Fiscal Year 2021 (NDAA) addressed many concerns for municipal governments struggling with cybersecurity. Under the act, states are assigned cybersecurity coordinators to facilitate communication between the federal government and non-federal entities. These coordinators assist state and local governments by serving as liaisons between federal agencies and states, supporting training and exercises designed to expedite recovery from cyber-attacks, and assisting in the development of cybersecurity plans.

Despite the progress made by the bill, state and municipal funding for cybersecurity was not addressed and remains a major issue. While the NDAA does touch upon cybersecurity personnel shortages, it does not provide a plan to attract new workers specifically to state and local governments. Its goal is to strengthen the national cybersecurity workforce pipeline by supporting cyber education at the elementary and secondary levels.

RECOMMENDATIONS

The following is a list of recommendations for Congress to aid states in improving their cybersecurity:

1. Create an annual cybersecurity grant program for state and local governments. This dedicated funding will help these governments improve their cybersecurity infrastructure. More funding is also instrumental in attracting cyber specialists. A similar proposition exists in the State and Local Cybersecurity Act, which provides $400 million to the Department of Homeland Security to award state and local governments. The framework for this bill can serve as a guideline for future grant legislation.

2. Mandate the creation of an exhaustive catalogue of all openly available federal toolkits, resources, and programs, and require its circulation throughout all states and municipalities. Many ransomware victims learn the existence of federal resources after suffering an attack. Publicizing this comprehensive directory will fortify cyber defenses and improve response times to cyber threats.

3. Implement new measures to attract and retain cybersecurity professionals for state and local government positions. This can be achieved by: (1) Increasing funding to the CyberCorps: Scholarship for Service program, which provides scholarships for cyber-related studies in exchange for government employment upon graduation; (2) Instituting cybersecurity rotational programs that move employees through different positions and cycle through municipal postings; (3) Establishing more public-private partnerships like the Cybersecurity Talent Initiative, but designed specifically for state and local government work placement.

4. Mandate a centralized cybersecurity response system in each state. This centralized system will allow for faster response times during a cyber-attack, access to common services and tools for all municipalities, and strengthened information-sharing and coordination capabilities within the state. Each state must additionally ensure that the CIO is a member of the governor's cabinet, so cybersecurity concerns are prioritized.

This report is the product of a policy working group sponsored by the Council for Emerging National Security Affairs. The views and policy recommendations are the authors' own and do not reflect an official position of CENSA or its board members. The author is a policy and technical expert affiliated with the companies mentioned in this report.