Published on *The National Law Review* https://natlawreview.com

State And Local Governments Continue To Be Favorite Targets Of Cyberattacks

Article By:

Todd G. Vare

Jason A. Bernstein

Scott N. Godes

Brian J. McGinnis

Ransomware continues to threaten local governments around the country – and there is no end in sight. In mid-August this year, coordinated ransomware attacks reportedly struck local governments in 23 Texas towns. Texas is not alone. Recent ransomware attacks this year also hit state and local governmental entities in Florida, Georgia, Indiana, Louisiana and Maryland.

This update provides an overview of ransomware, the potential costs, and best practices when considering how to better protect against ransomware attacks.

What is Ransomware?

Ransomware is a type of malware or malicious software through which a hacker gains access to a computer or network and then encrypts computerized data, preventing the data owner from accessing their own files. Ransomware can be installed on data within a single computer or entire computer systems. It is common for all computers on a network to be affected as a result of infection of just one computer.

Cyberattackers frequently infiltrate their target computer systems through phishing emails from a known sender that are designed to look authentic. The phony email usually requests the recipient click on a link in or attachment to the email. Once the click occurs, the malware infects the computer system and allows the hacker to gain access not only to the recipient's computer, but also to the entire network to which that computer may be connected.

Once ransomware is installed, the data is "locked up" by the attacker until a ransom is paid, usually in bitcoin. In many cases, data owners are unable to unlock their data, and even law enforcement and the FBI may be unable to unlock the data without paying the ransom and obtaining the decryption key from the attackers. Even if the data owner pays the ransom, there is no guarantee that

the files will be unencrypted or recovered. And even if the data is recovered, attackers often leave software in the system that allows them to perform additional attacks.

The Cost of Ransomware – Not Just the Ransom

In many cases, ransomware causes significant damage to the data owner's computer and network systems. According to a report by Beazley, a global cyber risk and insurance company, ransomware attacks increased over 100% in the first quarter of 2019 compared to that same period in 2018. The average ransom payment during this period was approximately $225,000. The ransom payment, however, usually is the tip of the proverbial iceberg.

The ransom paid to these attackers does not account for the expense to data owners for the period of time in which their data is inaccessible – which is frequently an expense that is many times that of the ransom itself. The amount paid in ransom also does not account for the expense, time or resources needed to purge, repair or replace damaged hardware and software. For example, the City of Baltimore was reported to have approved $10 million to pay for recovery following a ransomware attack, after the city reportedly refused to pay a $76,000 ransom. Additionally, the City of Atlanta is reported to have paid some $18 million to recover after refusing to pay a ransom demand.

Not only does the data owner need protection against ransomware cyberattacks, but the data owner must exercise extreme caution in using third-party entities who advertise they can break the ransomware code and "unlock" the encrypted data – for a fee. Unfortunately, we have seen at least one recent instance where it is likely that such an entity contacted the ransomware hacker, paid the ransom and received the decryption key, and then charged the victim for the cost of the ransom plus an additional fee.

Questions to Ask About Protecting Against Ransomware Attacks

The increasing number of ransomware attacks is not expected to diminish anytime soon, as powerful software capable of installing these malware strains becomes more widely available, these attacks are only expected to get worse.

The potentially devastating effects of a ransomware attack make it clear that the best defense is a strong offense. Here are the questions your organization should consider to protect itself against ransomware and minimize the risk of a ransomware attack.

1. **Incident Response Plan:** Do we have an incident response plan (including responding to a ransomware attack) and have we practiced it? Have we tested this plan with tabletop exercises simulating events? How current are our other information security policies?

2. **Backups:** Do we back up all critical information? How frequently do we create these backups? Is data that is either critical or that changes frequently (e.g., email) backed up more often? Are the backups stored offline or on the cloud? Have we tested our ability to revert to backups during an incident? If we are hit with a ransomware attack, are our backups frequent enough to enable us to restore without unmanageable loss of data? Will our backups be affected by the ransomware? Are our providers able to provide backups in the way they promised? What happens if they cannot?

3. **Network Access:** Have we segregated and minimized access to critical data? Are we using VPNs for wireless network access? How secure is our remote access system? Are we using

two-factor authentication? Do we have an account lockout procedure?

4. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?

5. **Staff Training:** Have we trained staff to understand these attacks and how to recognize the phishing emails that can cause them? Have we trained staff on cybersecurity best practices?

6. **Vulnerability Patching:** Have we timely implemented appropriate patching of known system vulnerabilities?

7. **Application Whitelisting:** Do we allow only approved programs to run on our networks?

8. **Business Continuity:** Are we able to sustain key operations without access to certain systems? For how long? Have we tested this?

9. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

10. **Insurance Coverage:** Would our insurance carrier cover a ransomware event? Do we have insurance coverage for the costs of paying a ransom, hiring a forensic investigator, hiring legal counsel to coordinate the response, remediation, lost revenue, defending against and paying to resolve third-party claims, a customer resolution program, replacing hardware and software, and other expenses resulting from an attack?

11. **Third-Party Contracts:** How do we structure our contracts with vendors and other third-party partners? Do we have indemnification clauses that would address a ransomware event? What happens if one of our vendors or service providers suffers an attack? What are they contractually obligated to tell us and do for us?

National Law Review, Volume IX, Number 262