The Ransom of American Towns

Reports of yet another government entity being attacked by ransomware seem to appear in the news so often, it feels like reading the lyrics to Johnny Cash's "I've Been Everywhere." While the ransomware epidemic has targeted large metropolitan areas such as Atlanta (March 2018) and Baltimore (May 2019), smaller community infrastructures appear to be the latest lucrative sweet spot for cybercriminal activities.

The City of Atlanta opted not to pay a $50,000 ransom and subsequently spent an estimated $2.6 million on recovery efforts related to incident response, digital forensics, overtime, and crisis communications. Following the City of Atlanta's lead, the City of Baltimore also opted against paying a ransom, and early estimates indicated a recovery price tag of $10 million in addition to $8 million in lost revenue.

Alternatively, a number of small town municipalities have opted to pay hundreds of thousands of dollars to cyber attackers in the hope of receiving the encryption keys to restore hostage data. While cybercriminals will characteristically search for any Internet-facing system with a known vulnerability, these criminals may have found the perfect victim in small-town America. With these successful payouts, criminal enterprises are sure to return to ring the bell on these cash cows.

Closed for Business

While the true number of public and private sector victims of these attacks may never be known, we do know the following towns recently paid a ransom to recover lost data. As of mid-July, over 22 municipalities have been infected with ransomware in 2019 alone.

Municipality	State	Population	Ransom Paid
Riviera Beach City	Florida	34,000	$600,000
Lake City	Florida	12,000	$500,000
Key Biscayne	Florida	13,000	$600,000
Jackson County	Georgia	70,000	$400,000
LaPorte County	Indiana	110.000	$130,000
Midland	Ontario (CA)	17,000	$50,000
Wasaga Beach	Ontario (CA)	21,000	$35,000

Recently, in an unprecedented response, the State of Louisiana recently declared a state of disaster due to ongoing cyber-attacks across three parish school districts.

You Must Choose, But Choose Wisely

Law enforcement discourages victims from paying any ransom to criminals; however, once a municipality's data is held hostage, the decision to not pay the ransom will require serious financial analysis and ethical evaluation to protect the interest of stakeholders, employees, and taxpayers.

Recently, the **US Conference of Mayors unanimously adopted a formal resolution not to pay any ransom demands** to cybercriminals for ransomware attacks. While this is a noble cause, in some cases, the cost of recovery – especially without valid, recoverable backups – far outweighs the cost of paying the ransom. For example, the City of Baltimore's recovery bill has run up over $18 million thus far.

Paying the ransom has other known consequences, such as potentially not getting your data back despite having paid the ransom (**1 in 5 victims that pay do not receive the decryption key**).

Victims that choose not to pay a ransom will make panic-driven reactionary investments in remediation at premium fees. Sound stewards of tax dollars should consider risk assessment principles when determining cybersecurity budgets, weighing the cost of security systems, control benefits offered, and remediation of potential threats. In other words, those in charge of cybersecurity decisions should be pleading for better cybersecurity controls before something bad happens. The current ransomware epidemic and the potential impact of not taking action should be Example #1.

Municipalities and governmental agencies must commit budgetary funds to upgrade antiquated infrastructures and security before it's too late. In many cases, unfortunately, no action will be taken until a catastrophic cyber attack forces change. Failing to take action will result in a new wave of headlines reporting about municipalities being forced to file for bankruptcy protection because of these events (and ultimately taxpayers) will be forced to bail struggling agencies out.

Mitigating the Impact of an Attack

Ransomware attacks can target any system with Internet access or email capabilities. Attack successes are typically due to a trifecta of poor user awareness, failed patch management procedures, and excessive user access privileges; all factors that can be prevented through proper security awareness and management. At any business, those charged with cybersecurity management should consider the following steps to mitigate the impact of ransomware:

1. **Develop a bulletproof patch management program** designed to communicate a clear patch management process, including the identification, implementation, and testing of patches or updates to computers, servers, network hardware, and software applications. In addition, procedures should outline a process for documenting patch exceptions, as well as procedures for rolling-back implemented updates or patches that cause operational issues on the network or computing devices.
2. **Maintain World Class Backups (3-2-1 rule)** keeping at least three (3) copies of your data, and store two (2) backup copies on different storage media, with one (1) copy of your backup data located offsite.
3. Retain a "cold," separate, air-gapped backup copy physically isolated from the Internet. If ransomware affects your backups, this air-gapped backup may be your saving grace, but you don't want it to be months old.
4. **Plan to fail well (Incident Response).** Think through different cybersecurity incidents (like ransomware), proactively mitigate threats and train staff on recovering from worst-case scenarios. Discover gaps and exceptions in your environment and adjust plans accordingly.
5. **Train and test your people.** Waiting for a crisis to occur before testing your plan is a guarantee for failure. Tabletop testing and phishing awareness campaigns are critical to empowering your staff to follow proper response procedures and increasing your chances of successful recovery.

The bottom line when it comes to **incident response planning** is that the return on investment will far outweigh the expense and lost public trust when faced with buying Bitcoin or rebuilding from ground zero. No one remembers the Great Missouri Earthquake in New Madrid, Missouri, on December 3, 1990, because it never happened, but the region had prepared and performed mock drills for months. Plan for the worst, and hope for the best. You will be attacked by ransomware within the next twelve months. Remember, for a ransomware attack to be effective, someone inside your network will have to click a link or download an attachment from an email. Have you trained your people?

This is where your Incident Response Plan begins. What will be your first step?

Written by: Shane Daniel
Senior Information Security Consultant - SBS CyberSecurity, LLC