Cities Held for Ransom:
Why are public entities easy targets for cyber crime?

By Scott Schleicher, Underwriting Manager, Cyber & Technology Insurance

In May 2019, Baltimore found itself fighting off cyber crime -- a ransomware attack that hit the city – the second known cyber attack in 14 months. Business had come to a sudden halt as hackers took control of the city's computer systems, demanding $76,000 in cryptocurrency ransom.

In a bold move, the city refused to pay. Since then, city officials have been working hard to restore systems and employee access, which could take months and could cost over $18 million.

It was the first time Baltimore faced ransomware demands, it certainly was not the first time it had been attacked. In 2018, hackers disabled Baltimore's 911 dispatch system. However, there was no ransom demand. Instead, officials worked to isolate the threat and restore systems, which were down for 17 hours. The cost of recovering from that attack is still unknown.

Other cities have faced similar cyber-crime attacks. When Atlanta's municipal operation systems were breached in 2018, the ransom demand was for approximately $55,000 in Bitcoin. City officials hesitated, and hackers removed the payment portal, leaving Atlanta offline. The cost to recover is now expected to exceed $9.5 million.

No matter the size of the public entity, both ransoms and recovery costs are devastating, particularly in municipalities that have limited funds. Such was the case for the city of Leeds, Alabama, which was hit with a ransomware attack in 2018. Leeds, a city of just under 12,000 residents, was forced to pay $12,000 in cryptocurrency to regain control of its systems.

And yet the ransoms are just the beginning of the costs that public entities will face when hackers take control of company systems. The average cost for a business hit

with a ransomware attack is over $8.25 million and over 40 employee working hours spent on recovery.

Easy Prey

Why are public entities being targeted repeatedly by hackers? Because they are the perfect target. Many public entities, hamstrung by tight budgets and little funding available to spend on IT systems upgrades, do not have enough security measures in place to ward off a ransomware attack.

Statistics show that 44% of local governments face regular cyberattack threats, and 28% do not know how often they are attacked. More alarming is that 41% of those local governments surveyed do not know if they're systems have been breached.

Cybercriminals are aware that public entities are more vulnerable, too. Publicly announced ransomware attacks against state and local governments spiked in 2018 with 53 incidents recorded, a 39% increase over 2017. The first months of 2019 were equally active, showing no signs of the trend slowing.

No city is immune. Ransom demands of $250,000 or more are not uncommon in small municipalities. Should a town fail to pay by the stated deadline, ransoms will go up or, as in the case of Atlanta, payment options disappear, and towns are left with no recourse but to start over.

That is where the cost of a ransomware attack can go far beyond the initial ransom demand. Recovery is expensive: what public entities are compelled to pay for include:

- System recovery services or new systems
- Forensics investigations
- Recovery and remediation of any personal identifiable information
- Claims services and related expenses
- Improving system security, prevention, and response

The Evolution of Cyber Attacks

Even the most prepared public entity is still vulnerable to ransomware attacks. Because of the fast payout, ransomware attacks have become the method of choice for many

cybercriminals. Unlike cyberattacks of even five years ago, when main systems were the target and recovery was faster, ransomware attacks target everything.

Now, cyber thieves seek out both the systems and the servers where system backups are being stored. Once the backups are encrypted, public entities no longer are able to restore their systems. The only option is paying the ransom.

Thanks to the internet, ransomware attacks have become big business. Even inexperienced hackers can buy ransomware programs on the dark web and launch an attack. It has become a fast payout for hackers – there is no reselling of personal data needed, and little effort involved in extracting payment from organizations.

Protection and Recovery
In order to avoid both paying ransom and having systems breached, public entities of all sizes should be implementing cybersecurity measures. It need not be expensive, either. Many public entities can put affordable, basic cybersecurity protections in place with in the following ways:

Training
Train all employees on the dangers of phishing, and of accessing certain sites via the company internet during work hours. Retail sites are not always secure, and employees should understand how to identify sites and links that have little to no security. Also, employees should be trained in how to identify suspicious email and what steps to take when encountering one.

Robust Patch Management System
Your organization can reduce the chances of a ransomware attack by patching the known vulnerabilities. Establish a process by which your organization rolls out patches in a timely fashion.

Offline Backups
One of the easiest ways for public entities to recover quickly from any cyberattack is to keep all backups offline and out of the reach of cybercriminals. Storing to an offline location, an offsite location, or hiring a third-party backup service can keep your recovery data safe from attack.

Software Protection
Commercially available security software can help reduce the risk of a ransomware attack crippling your organization. While such software runs the gamut in terms of price and features, most public entities can find an affordable option that can bolster their cybersecurity.

Breach Response Planning

During a crisis is not the time to be making decisions on what to do next. Starting now, your organization should be working on a breach response plan. When a breach occurs, what are your first steps? Who will you call first? Who needs to be involved? What should you be doing as you await outside help? Having a plan in place can speed your recovery time significantly.

Cyber Insurance

At a minimum, small entities should be investing in cyber insurance that covers ransomware attacks. By working with a carrier that specializes in cybersecurity, public entities can get more bang for the buck. These insurance carriers give insureds access to forensics, recovery teams, and claims specialists as well as the knowledge and risk assessment that can help your organization recognize risks and help you create a response plan to complement your coverage.

As cybercriminals target the organizations most likely to have gaps in their cybersecurity, public entities are wise to look for ways to thwart cyber attacks and improve their approach to system security. Ransomware is more targeted and much more in use now than even five years ago. And the target is the smaller entity that may not be properly prepared.

Because they are such easy marks for cyber criminals, public entities large and small should be educating their employees, tightening their security, and planning how they will respond to a ransomware attack. Also, working with an insurance carrier that specializes in cybersecurity is an affordable way to protect the business and ensure that recovery services are in place should the unthinkable happen.

# # #

Scott Schleicher is underwriting manager in AXA XL's Cyber and Technology insurance business. His specialty is helping cities, municipalities and other public entities address their cyber risks. Reach out to Scott at scott.schleicher@axaxl.com.