Hartford Courant

10/23/2018

Cities Must Pay For Cybersecurity, Not Ransoms

By MATTHEW KOZLOSKI

Last week, West Haven paid a $2,000 ransom to hackers to unlock its computer systems. In a statement from the city, the ransom was characterized as a “one-time fee.” The word-choice here reveals an oversimplified view of the reality of ransomware, a cyberattack in which hackers lock data and demand payment.

First, West Haven was lucky to regain access to its systems after paying the ransom. Fewer than a quarter of ransomware victims actually get their files back after paying up. More often, hackers pocket the money and leave the data scrambled.

The notion of a “one-time fee” also fails to account for reputation damage and loss of trust. A city like West Haven — which is already navigating difficult financial straights — needs to rally community support. A blunder like this undermines the momentum it was building.

While there isn’t any evidence at this point that information was leaked in the cyberattack, the truth is we won’t know for sure for years to come. Hackers often hang on to data until the heat dies down before they sell it on the dark web. Hopefully, the $2,000 payment spells the end of this issue. Only time will tell.

Finally, the FBI directly discourages victims of ransomware attacks from paying the ransom because doing so makes attacks like this a lucrative business. Although West Haven may have paid a “one-time fee,” in a sense, the hacker’s next victim is paying for their mistake as well.

It’s understandable that in its current strapped state, West Haven has not made modernizing its technology defenses a priority. However, the fact is that remediating a cyberattack comes at a much greater cost than preventing one in the first place. While the $2,000 ransom may seem relatively low, tracking how the attack happened, assessing the damage and shoring up defenses quickly is an expensive proposition. Just ask Lansing, Mich., which, even with insurance, paid $500,000 out of pocket for remediation after a 2016 ransomware attack (total cost: $2.4 million).

The best way to bounce back from ransomware is to have a strong backup system, something every organization needs for a number of reasons. The fact that West Haven paid the ransom suggests that there was no effective backup system in place. If that is the case, the city truly did not have a lot of options once the ransomware attack occurred.

Like most cyberattacks, ransomware usually gets into a system through user error. Someone opens an attachment they shouldn’t or clicks on a phony link and the ransomware spreads through the system. There are technologies that can recognize this and stop it from happening, but the most effective tool is user awareness and cybersecurity training.

The number of cyberattacks in the U.S. doubled in 2017. As recently as a few years ago, many organizations rightfully thought of themselves as not being on hackers' radar. That is no longer the case.

A few weeks ago, Arthur House, chief cybersecurity risk officer for Connecticut, told me, "Five or six years ago, you wouldn't have put 'cybersecurity' and 'municipality' on the same page. They are now, and they know it." In fact, cities make attractive targets for hackers because they can't abide having critical systems such as police and fire down for very long.

Because cyberattacks are inevitable, and no training or technology is 100 percent effective at preventing them, I don't fault West Haven for falling victim to a ransomware attack. That city officials found themselves in a position to have to pay the ransom, however, is frustrating. With proper backups, this situation is preventable.

If you're wondering if your town or organization is prepared for a ransomware attack like the one West Haven experienced, there's a simple test you can apply. Imagine that your systems are locked. What would you do? If you have a clear answer to this question, you're OK. If not, you have some work to do.

Matthew Kozloski is vice president of professional services at Kelser Corporation, a technology consulting firm based in Glastonbury.