It Happened to Us

When it comes to cyber threats, many of us think it only happens to other people. Why would the “bad guys” even consider our municipality? Well, they will and they do! I am sharing with you the story of a Pennsylvania municipality that is a PennPRIME member and was attacked. Their story is not unique and we hear of situations like this regularly in cyber-security related reports. The manager wanted to ensure that other municipalities do not experience the same issues that their organization did. At their request, we are not sharing the municipality’s identity.

Bob Anspach, PennPRIME Director of Insurance Services

In March of this year our municipality was the target of a ransomware attack. Until that day, many of us did not fully understand what ransomware was and what the consequences can be. We received a crash course when employees arrived in their offices on a Monday morning and could not access the computer network and were told to immediately do a full shutdown of their computer. Many were somewhat excited at the prospect of having a day to take care of some of the “manual” tasks on which they wanted to catch up; except that the common refrain was “Oh wait, I need the computer to print the labels for those file folders” or “I need the computer to research the information for that report”, etc. You are never more aware of how much you rely on a computer until one is not available.

We do not have an on-staff IT person and, instead, utilize the services of a third party to provide IT services. The consultant at that time had a two-person staff with one person typically coming to the municipal offices twice per week for three to four hours on each visit. Monday was not the normal day for them to be in the offices and, therefore, they had to be called in on an emergency basis.

Fortunately, the consultant was able to isolate the ransomware, remove all files from the server, and restore the data via the most recent backup tapes. This may sound easy, but it was not, and the process consumed the entire day – a day of added expense for the provider’s time and a day of significantly reduced productivity for our office employees. The backup tapes were current through the night prior to the attack and, with it being a weekend and most offices being closed, there was minimal loss of new data. However, had there not been a current backup of data, the attack could have resulted in a devastating loss of data and the diminished ability to carry out the day-to-day operations of the municipality across all departments.

It was determined that the ransomware hit our system sometime between early Saturday evening when ambulance call information was successfully uploaded and Sunday morning when ambulance call information could not be uploaded.

According to the IT consultant, the attack originated in India and the demand was two bitcoins – the equivalent of $3000. While the municipality could have paid the ransom, there is no way to guarantee that the “key” to unlock the files would have been provided and paying the ransom may have made us a more likely target for future attacks.
It Happened to Us

We were fortunate that no information was taken (exfiltrated). Had it been, the municipality would have faced major expenditures to meet the requirements of applicable law (think Target and Home Depot).

The ransomware attack was a rude wake-up call that made us very aware of just how vulnerable our computer network was. While there are many on staff who are adept at using technology, we do not have anyone who “speaks the language” of computers. We relied on the IT provider to keep the system operational and, we believed, secure. That provider had been servicing the system for over a decade and, unfortunately, it became evident that they, perhaps, had not stayed fully up-to-date with training, particularly in internet security.

Prior municipal management apparently stressed the need for the consultants to operate within a given budget. Therefore, a few new computers, some new software, and software updates were purchased each year and, as we learned, the rest were “band-aid” fixes. When the current municipal manager came on board, it was thought that all was in order when, in reality, the consultants were not educating us as to what was necessary in order to keep the network secure and in proper working order. Their philosophy seems to have been to do what they could with what they had and hope that the band-aids held.

It was realized that we need to do more to educate ourselves to the extent that we can understand what is needed to operate a robust network and to ensure that there are sufficient cybersecurity measures in place. The Municipal Manager and another staff member attended a cybersecurity presentation and, as a result of information gained and contacts made, a new IT consulting firm was ultimately selected. The new firm has a full (growing) staff that monitors systems and is available 24/7. One of our council members is “tech savvy” and was invaluable in making the determination to move to a new provider and also in terminating the services of the prior provider.

At present, the new IT provider is in the process of resuscitating our network as it was one step away from needing to be rebuilt from the ground up. That dire state resulted in a risk assessment score of 96% - high scores are not what you want to see in this instance. This provider is working very closely with our staff to educate us and to keep us informed of what is being done and what needs to be accomplished to ensure the efficient operation and security of the municipality’s computer network. Fortunately, our city council recognized the need and authorized additional expenditures to bring our system to where it needs to be.

The lesson to be taken from our experience is that computers and other technology are wonderful tools. However, they can be vulnerable to outside threats and in this rapidly evolving field it is essential that municipalities be aware of threats to the security of their computer network and take steps to ensure that the proper measures to maintain their systems and to provide for their security are in place. Deferred maintenance in this area has the potential to result in disastrous consequences.

*PennPRIME Comment: PennPRIME takes this risk seriously and has added Cyber & Technology Liability Coverage for the Liability Trust Members.*