Bond Case Briefs

Municipal Finance Law Since 1971

How Can City Governments Protect Themselves Against Ransomware Attacks?

The most recent incident in a series of ransomware attacks on American cities and municipalities happened in May in Baltimore. The hackers locked multiple systems such as emails, voicemail, and the parking fines database. The debacle delayed the sales of about 1500 homes in the city. Hackers have demanded over $100,000 in bitcoins in order to release these files, which has been declined by Baltimore's mayor.

Ransomware attacks have quickly become a preferred method of hacking with the emergence of bitcoins and other cryptocurrencies that enable hackers to receive their ransom without being tracked and identified. The popularity of cryptocurrency has soared in the recent years with fluctuations in their value. As these currencies become more mainstream, so does the incentive of hackers to make a quick buck through ransomware attacks. As I had warned before, we should expect ransomware attacks to become more frequent as cryptocurrency becomes more popular.

The bad news is that once a computer system is hacked with ransomware the options are very limited. The first option is to pay the ransom. While this is the quickest way to release the files, law enforcement officials strictly advise against it, simply because paying the ransom invites future attacks. Once the hackers know that an organization pays the ransom, they will repeat their attacks for more money. The other option is to refuse the payment. While this solution reduces the chances of future attacks, it will impose significant costs on the organization as it may take weeks or even months to remove all the malicious software from the computer systems.

The good news is, although there is not much to do once a system is attacked with ransomware, it is very easy to significantly reduce the chances of being attacked. While even the most secure computer systems could be hacked as there is no security technology that guarantees 100% protection against threats, implementing the most basic security solutions could significantly reduce the chances of experiencing a ransomware attack.

Most such attacks are not targeted, but opportunistic. Hackers look for organizations and businesses that seem more vulnerable than others. The ones that have neglected to set basic security standards in place are more likely to be targeted for ransomware attacks. The process is very similar to burglaries in which the criminals do not target a specific home, but rather cruise neighborhoods to find houses that do not seem to have security systems.

The best defense against ransomware attacks is putting basic security safeguards in place. It will most likely dissuade hackers that are after a quick buck and are not motivated to spend time hacking into a secure system while there are easier targets out there.

The critical services provided by government agencies make them attractive targets for ransomware attacks. In the case of Baltimore, the attack halted home sales and water bill payments. Due to the sensitivity and urgency of services that government agencies provide to the public, cities cannot afford to leave their computer systems suspended for prolonged periods. Hackers are more likely to

attack city governments, assuming that cities will be desperate to release their files and pay the demanded ransom.

As I have discussed earlier, compared to private organizations, government agencies usually have less resources to invest in information security technologies. Old and fragmented computer systems exacerbate this problem, since older systems are much more difficult and expensive to maintain than newer ones. Despite these difficulties, all levels of government should invest in upgrading security technologies to reasonable levels, or else many more agencies will soon become victims of ransomware attacks in the future.

The Brookings Institute

by Niam Yaraghi

Tuesday, June 11, 2019