Our world today can be a scary place, especially when we look at the role of technology in our everyday lives. People use technology for just about everything today, including managing their finances, protecting their property, or simply starting their car. There is an app for everything, or so they say, but are the apps secure enough to make sure that no one steals our identities or our hard-earned money? Will our personal information be protected, or are we willing to accept the risk in order to have an easier way of life?

These questions are top of mind for most people—and governments have these same questions, coupled with the necessity of managing technologies that provide services for the betterment of their citizens. Many of these services, like those provided by law enforcement, are crucial to saving lives every day. Governments rely on technology, but they also have limited funding for developing these technologies. Funding priorities do not always put cybersecurity at the top of the list, prompting the “bad actors” of the world to prey on those that are less protected. The harsh reality is that the battle against cyber criminals may change over and over, but it will never end.

The Latest Scourge
The latest scourge on government technology is the emboldened process of locking up technology resources and forcing governments to pay a ransom, better known as ransomware. The criminals harvest information from unsuspecting government workers by using phishing scams or by simply providing inviting but malicious links. They prey on the technically weak because they can. Local governments have moved up the list of organizations targeted by criminals because in many cases they are the weak and because of their lack of funding coupled with limited cyber protections.

These criminals are often characterized as misguided 16-year-olds working out of their parents’ basements when in reality, they are part of organized crime and/or nation-states that see cybercrime as a way to crush the finances of their enemies. They often use mechanized attacks that pound on government systems relentlessly, sometimes reaching into the millions of attempts. They look for holes left as governments frequently change their systems to keep up with the needs of the organization. In fact, the ransomware phenomena represents an estimated $7.5 billion enterprise, making criminals wealthy beyond belief. Data published by the MIT Technology Review illustrates the level of impact ransomware is having on governments across the nation. The study estimates that approximately 966 government agencies were affected in 2019, along with 89 universities and 1,233 individual schools.

“Most American local governments do a poor job practicing cybersecurity,” according to a study by the University of Maryland. This study also found that a little more than one-third of governments did not know how frequently security incidents occurred, and that approximately two-thirds of governments did not know how often their systems were breached. A cyber criminal could in fact be buried within a target’s systems for hundreds of days before striking. The lack of awareness by government is exactly what the criminals count on and is why it is not “if” a government will be successfully attacked, but “when.”

The harsh reality is that the battle against cyber criminals may change over and over, but it will never end.

Fast and Furious
These attacks are coming at a rate so fast and furious that governments cannot keep up. Governments of all sizes, especially local governments, are ill-equipped to handle the problem, especially with many budgets declining annually. Services are adversely affected by ransomware. For example, some governments recently saw their 911 systems go down, failures of computer-aided dispatch, website crashes, and phone system malfunctions, along with the severe financial impact of paying ransoms or recovering systems.

Many organizations will focus on technology but soon realize that ransomware is predominantly a “people” problem. According to some estimates, more than 80 percent of attacks are people-related—to put it simply, they are caused by the questionable behavior of people. And governments are aware that the problem is a priority, but the funding doesn’t always get to where it needs to go. Data gathered by the Center for Digital Government show that cybersecurity is the top priority for states, cities, and counties. At the
Be Ready When \textit{(Not If)} You’re Hit with a Cyber Attack

BY PHIL BERTOLINI
same time, many governments have not invested in the training needed to ensure that employees do not fall prey to phishing attacks and social engineering. Many cybersecurity experts agree that a high percentage of cyber incidents could be avoided if people did not click on malicious links or open attachments from people they do not know.

The realization that it is impossible to close every hole is a difficult pill to swallow. Every government technology professional has a sinking feeling in the pit of their stomach when they feel good about closing one hole, only to have a criminal exploit another. This battle is being waged in every organization worldwide, and the price tag continues to rise. Governments have invested millions of dollars into protecting their systems, knowing it isn’t enough.

Ransomware can be an expensive problem when criminals ask for payment in Bitcoin, a cryptocurrency, for tens of thousands—should not hundreds of thousands—of dollars. And the costs do not stop there. Once a ransom is paid, measures must be taken to make sure that the same thing doesn’t happen again. Applying measures after an attack can be exponentially more expensive than measures that are strategically implemented before an attack.

Every government technology professional has a sinking feeling in the pit of their stomach when they feel good about closing one hole, only to have a criminal exploit another. This battle is being waged in every organization worldwide, and the price tag continues to rise.

The Pre-Work

As with any aspect of physical disasters or emergency issues, recovery is much easier and less costly if the government effectively prepares for the problem in advance. Properly funding advanced preparation is a key component of any successful cybersecurity program. The financial impact of ransomware can also vary, depending on the decisions made during the crisis itself. The unknown financial impact is real, but it can be mitigated if government technology professionals take the necessary steps and implement the proper controls before the attack. Several “pre-work” components can greatly benefit government if they are made a priority. Resiliency, disaster recovery, business continuity recovery, and data protection are key.
Backups have been at the forefront of preparedness for many years, and this kind of planning is even more important today. If plans are not exercised regularly, though, they become stagnant and may fail during the time of crisis. Currently, disaster recovery has mainly been used as a technical effort to ensure that data can be restored with minimal loss to the business. When you wrap business continuity recovery into the plan, a government can ensure that the business of government continues even if the technology is compromised.

Local governments weren’t able to perform several services after recent attacks, which directly affected citizens. It is one thing to back up the data, but it’s another to have the infrastructure, the applications, and the processes ready to make use of the data in the event of a successful attack. Everything wraps up into government’s need to be resilient. Older versions of recovery plans focused mainly on physical disasters, but the cyber criminals have forced everyone into a serious discussion about how to maintain the integrity of their digital capabilities—or suffer financial loss coupled with reputational loss.

Knowing that the response window for a cyber incident is very short, it is imperative to develop and exercise solid plans so decisions can be made at the time of the crisis. These plans should be developed using best practices from the governments that have successfully blazed the trail. Funding should also be allocated in advance to implement prioritized cyber controls that are based on best practices nationwide. Some governments may need cybersecurity assessments to create a baseline of cyber controls and procedures to work from. And of course, understanding everything cyber comes with a price tag.

A portion of the cyber spending should be focused on effectively educating employees on good cyber hygiene. As stated earlier, most ransomware attacks begin with human interaction: clicking on a malicious link or opening a malicious attachment. Governments need to implement mandatory education with measurable results. It is also good practice to test cyber knowledge regularly by phishing staff and by constantly reminding them of what can happen if they open the door to attackers.

Investigating and purchasing a cybersecurity insurance policy is always a good idea. Cyber insurance is a relatively new tool that governments can use to mitigate the financial impact of a cyber incident. This insurance doesn’t allow governments to ignore the necessary cybersecurity controls or avoid taking the proper steps for recovery and response. In fact, most cyber insurance providers will not provide coverage if certain controls and policies are not in place or being implemented.

The benefit of doing the necessary advance work is that when the incident happens—and it will—the government will be prepared to take the necessary steps to regain the technologies being ransomed by the attackers. A finance officer will be more prepared to justify the business decision to either pay the ransom or pay for the recovery if the necessary work is successfully completed in advance.

The Incident
The time has come, and the attackers have locked up the government’s technologies. They are demanding a ransom, or they’ll delete everything. Services will be affected, and the citizens will undoubtedly want to know why it happened. In reality, the first reaction of the government technology professional is to fix the problem immediately. Decisions will be made to either pay the ransom or recover from backups. The finance officer may or may not be looped into the situation, but they should be immediately because, one way or another, a financial decision will be made.
A common mistake governments make is closing ranks and keeping the problem internal because they're worried about public perception; however, the response window is short, and governments should instead call out for help as soon as they recognize the attack and receive the ransom communication. The Federal Bureau of Investigation, Multi-State Information Sharing and Analysis Center, and many state resources can be brought in to address the problem in the blink of an eye. Bringing neighboring government cyber professionals to the table has also been found to help in the short- and long-term. The ransoming criminals will not wait very long for a response before moving on to other prey.

This is not to say that they are honorable: there is no guarantee that the technologies will be unlocked if the ransom is paid. The government must make an immediate assessment of the impact of saying no to the ransom, although in many cases it will be a rough guess. In some instances, there is no way to tell what the costs will be if the criminals delete everything and a government must start rebuilding from scratch.

**The Recovery**

Immediately after the incident takes place, the business of recovery commences. Decisions need to be made, and the clock is ticking. Some governments will hire a technology firm to represent them during the crisis, which is a good solution, especially if it’s necessary to negotiate for the best deal possible, which allows the government to make a solid financial business decision. Some governments have agreed to pay a large ransom because their deductible for cyber insurance was $10,000, and recovering the technologies would have cost much more than the deductible. Right or wrong, the decision was based on dollars and cents.

If the proper pre-work was completed, the decision potentially could go in a different direction. If there is a clear understanding of the costs to recover from solid backups and the gap in data loss, then a decision may be made to deny the ransom and move forward. Again, this is a decision that should not be made without the proper facts in advance of the attack. Losing technologies to criminals can have a devastating effect on the entire organization, including the reputational damage incurred.

What do you plan to do if you lose everything? Maybe paying the ransom is a better financial decision at the time.

**Cyber attackers are looking for easy ways to penetrate defenses, so making your defenses more complicated will send these attackers on to easier prey.**

One state auditor recognized that their state was extremely behind on managing their cybersecurity program. The audit report delineated that the state had a “disregard for cybersecurity in state government” as a result of its lack of security policies and disaster recovery plans and not performing legally mandated risk assessments. One would surmise that if a ransomware attack took place, the decision may be to pay the ransom.

The decision to pay the ransom or not is not a simple one. This decision will be analyzed at all levels of government with the final business decision being made. Knowing the capabilities, plans and recovery options are very important. In the end, the decision to pay—or not—may be a purely financial exercise, which requires that the financial professional be involved from beginning to end.

**The Repeat**

Whether a government pays the ransom or not, it has to be prepared to close the holes that allowed the cyber criminal to gain access in the first place. If the government paid the ransom and successfully unlocked the technologies, all steps must be taken to make sure the same criminal cannot walk back in through the same doorway. As stated earlier, you will never close all the holes, and an attack will happen again. Priorities must be set and the proper funding must be provided to implement best practices for cybersecurity. Government technology professionals across the country have made cybersecurity a top priority, and finance officers need to do the same. Ransomware cost U.S. governments $7.5 billion in 2019, and that number is set to rise. The only way to battle this problem is to try to stay ahead of the attackers.

**The Bear in the Woods**

An anecdotal story highlights the struggle governments face when it comes to cybersecurity. A group of friends is standing in the woods around a campfire, enjoying each other’s company, when they hear a noise in the darkness. A large bear runs into the clearing and everyone scatters into the trees. One of the friends who is running away thinks: Do I need to run faster than the bear? And the answer is no, you just have to run faster than the slowest person in your group. (OK, maybe they weren’t the best of friends.)

If a government highly prioritizes cybersecurity, it will fund the necessary cyber controls and policies to make it faster than the slowest entity. Cyber attackers are looking for easy ways to penetrate defenses, so making your defenses more complicated will send these non-stop, potentially mechanized attackers on to easier prey—ideally in an industry other than government.

*Phil Bertolini* is co-director of the Center for Digital Government, e.Republic.