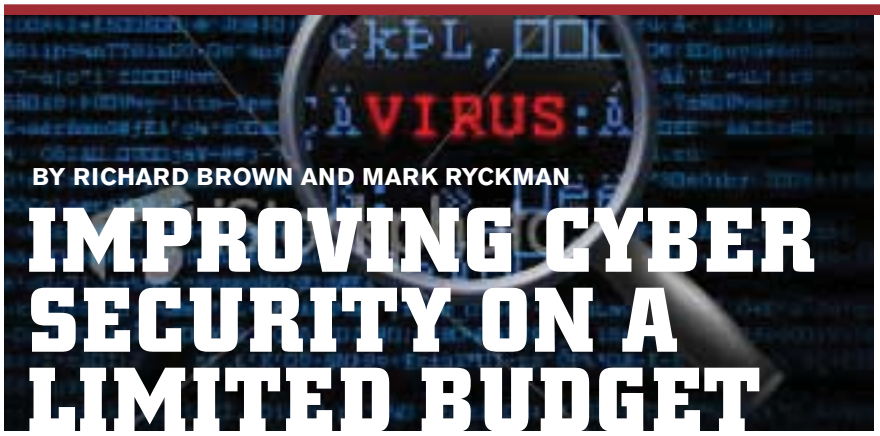

BY RICHARD BROWN AND MARK RYCKMAN

IMPROVING CYBER SECURITY ON A LIMITED BUDGET

You're in the middle of the workday, preparing for meetings and dealing with the normal demands of being a local government manager, when your administrative assistant informs you the computer server isn't operating. You inquire further, only to find out the server has been infected with a virus. You ask when the server will be operational again, but your one IT specialist doesn't know and is waiting for a computer vendor to arrive.

In the meantime, employees can't process tax receipts, issue purchase orders, take citizen inquiries, or carry out any of the other functions all employees have grown accustomed to providing. To compound the problem, citizens trying to access your local government's website start calling, and you begin fielding inquiries from members of the legislative body. It's only a matter of time before the media contact you.

How can this happen? Why are your systems being targeted? And what can you do to prevent a recurrence?

There are many motivations for cyber attacks. These attacks can be politically motivated, launched to steal financial information, or a means of vandalism. Regardless of the attacker's motivation, this method of attack can be attractive to criminals because cyber attacks are often less expensive than traditional methods, they can be operated from remote locations to hide the identities of the attackers, and there are no physical barriers to launching an attack. Their effects can hamper your operations, as in the example above, as well as slow your system performance or lead to the theft of information and funds.

But what can you do, with your limited budget, to prevent these attacks? When your resources are limited, IT often takes a backseat to other competing demands. Here are basic low-cost measures that will help you significantly reduce your system's vulnerability.

- Educate the organization. Explain to the legislative body, department heads, and all employees using electronic devices why cyber security is an important issue to your organization. For your policies on computer usage to be effective, you'll need buy-in from all levels.
- Install a firewall. A firewall is a device, usually a hardware add-on with periodic software updates, that prevents unauthorized access to your system while still allowing normal communications to take place. Basic firewalls can cost as little as $500.
- Regularly run anti-malware software. Malware stands for "malicious software." Malware can infiltrate your system through, for example, e-mails, Internet surfing, and downloading music files. There are various anti-malware programs that are free of charge, and commercial products are relatively inexpensive. It is important to keep the software updated and run it frequently to scan your system.
- Back up the data. Make sure your system can back up computer data at least nightly on a separate storage device. This is a low-cost way to ensure that, if you have a problem with your computer system, you can recover vital information and restore system settings.
- Have a strong password policy. Make sure you have a password policy in place that prohibits the sharing of passwords and requires they be changed periodically.
- Don't open unrecognized e-mail. Malware is often attached to e-mails. It is important not to open e-mails from senders you do not recognize. This sounds simple, but it is one of the hardest rules to follow because it requires discipline at the individual user level. When employees are busy, they may click open e-mails without first recognizing the sender.
- Limit employee Internet access. Employees can need access to the Internet to conduct research, to file applications, to access regulations and forms, and to contact other agencies. A myriad of job-related functions benefit from the Internet. But you should limit this access to the types of sites your employees need in order to perform their official duties and prohibit surfing the Internet for personal shopping, downloading music, and personal e-mail. Much of this can be accomplished through a strong Internet use policy, periodic monitoring of activity, and firewall settings.
- Install approved software applications only. Issue a list of approved software applications for each user. Your local government should have a software license covering each installation. Nonauthorized software should be prohibited from being installed.

Although these suggestions won't prohibit all attacks on your computer systems, they are a low-cost means of reducing your risk. PM

MARK RYCKMAN, ICMA-CM, city manager, Corning, New York, manager1@stny.rr.com and **RICHARD BROWN,** ICMA-CM, city manager, East Providence, Rhode Island, rbrown@cityofeastprov.com.