A Byte of Prevention

By Rob Roque

As stewards of public data, finance officers must understand the significance of cyber threats, including the large costs governments face in recovering lost data, restoring public trust, and otherwise recovering from a breach.

All local governments are potential targets for cybercrime, a risk that intensifies as victims increasingly pay ransoms to regain access to their hijacked technologies. It can be tempting to pay up because hacks are disruptive, damaging, and embarrassing — and expensive. As stewards of (often sensitive) public data, finance officers must understand the significance of this threat, including the large costs governments face in recovering lost data, restoring public trust, and otherwise recovering from a breach.

Finance officers can implement simple and inexpensive strategies that address people, process, and technology to protect their organizations from cyber threats without conducting a costly cybersecurity assessment. Many of the recommendations below address the weakest link in cybersecurity: the human factor.

EMPLOYEE AWARENESS

Most breaches begin with an e-mail or file attachment. Employees in the finance department are likely targets because they have frequent transactions with vendors and access to business systems. To mitigate this threat, governments should train employees to:

- Be suspicious.
- Be wary of e-mails asking them to change their usernames or passwords.
- Double-check the sender's e-mail address before opening or downloading an attachment.
- Follow the government's compliance business processes when vendors request changes to electronic payment and bank account information (e.g., accounts payable) and staff members (e.g., direct deposit). These procedures are often "out-of-band" (i.e., not done by e-mail) and are therefore likely to expose wrongful requests.
- Check the sender's website address before entering or sending sensitive data.
- Periodically check the public website *haveibeenpwned.com* to see if their e-mail addresses and passwords have been exposed. If so, employees should report the breach and change passwords for the accounts listed.

Actions Governments Can Take:

- Conduct training for all members of the finance staff; online training videos provide a low-cost or free option.
- Avoid posting e-mail addresses on websites, if allowed by law.
- Remind employees frequently about the potential for cyber threats.
- Make sure employees know where to report suspicious incidents, and praise proactive behavior.

PATCH DIGITAL SERVICES

Software patches typically include security updates and fixes for vulnerabilities, so as part of cyber security awareness, teach employees about the value of updating all their devices promptly, including computers, laptops, and smart devices. Ideally, the updates should be pushed to all devices through a central server, but if this isn't possible, schedule updates to run automatically during the day (this can be done during workers' lunch periods to minimize downtime). Be sure to restart the device after a patch has been installed. Because employees' personal devices can't be monitored and updated, their use should be prohibited or limited. Many organizations offer a "guest" network that is separate from the business network to accommodate personal devices.

Actions Governments Can Take:

- Ensure that all devices are updated.
- Do not allow personal devices on government networks.

ANTI-VIRUS SOFTWARE

Every computer should have anti-virus software installed, and updates should be set to "automatic" so the software always includes the latest virus definitions. Some anti-virus software allows multiple tiers of scanning. Active scanning reviews all files that are downloaded, changed, or compressed. Some software also monitors website activity. The most thorough option — full scanning of the machine, which includes scanning all programs, hidden system files, and inactive files — should be conducted at least monthly. Device performance will diminish during a full-system scan, and the amount of time it takes to run a full scan varies depending on how much storage the machine has. However, active scanning is preferred to passive scanning, which is designed not to interfere with network activity but isn't as thorough. Always unplug your computer from the network and run a full scan if you suspect that your computing device is compromised.

Actions Governments Can Take:

- Install anti-virus software on all computing devices and run a full scan at least monthly.
- Make sure anti-virus software is updated regularly.
- Get an anti-virus update and scan mobile devices before they connect to the network.

Software patches typically include security updates and fixes for vulnerabilities, so as part of cyber security awareness, teach employees about the value of updating all their devices promptly.

VIRTUAL PRIVATE NETWORK

Many people now work from home or other locations, and technology assets must be secured when operated from remote sites. Workers often use the wi-fi at public locations such as coffee shops, airports, and hotels, but most of these access points are "open," which means that no security credentials are required to log in. These are inviting places for criminals to scour the network for sensitive data, since data transmission is unencrypted. One way to protect users is to use a virtual private network 9VPN0, which encrypts data and sends it through an established tunnel that can only be accessed from an encrypted key at both ends. Remote workers should only transact business through VPN tunnels. Business systems can be restricted to activity originating from secured networks, including VPN tunnels.

Actions Governments Can Take:

- Give all remote workers VPN access.
- Only use unsecured public wireless networks through a VPN, which can be set up by your IT administrators or outsourced to third parties.

PASSWORD SECURITY

Cyber criminals use many techniques to gather passwords, including collecting information about your security questions, which they can use to unlock accounts. To help protect against this kind of crime, enforce the use of strong security passwords throughout the organization. The password should consist of at least one capital letter, a number, and a symbol, and a minimum length should be specified. Employees should also be taught to consider their online actions outside of the workplace. For example, think before answering and sharing those "friendly" surveys on social media accounts. The answers, which may be publically available, can be used to guess the answers to your security questions for recovering passwords — giving cyber criminals access.

Actions Governments Can Take:

- Develop a policy for strong passwords.

- Train employees about safe social media practices.

ADMINISTRATIVE ACCESS CONTROLS

Limit the number of administrator accounts used for your business systems as much as possible. If many administrator (or even super user) accounts are needed, try to separate access as much as possible. That way, if one administrator's username and password is stolen, the entire system isn't compromised. Administrators should use strong passwords and multi-factor authorization.

Actions Governments Can Take:

- Identify, track, and actively manage the administrator rights to all critical applications.
- Implement multi-factor authentication for all administrator accounts (network as well as cloud).

> Develop policies and procedures governing the general use of technology and safe handling of data, and make these policies as important as your financial procedures and internal controls.

PHYSICAL SECURITY

Secure your devices. Activate time-out functions on business application logins so the session logs out after a defined amount of inactive time; this limits the number of tries a criminal gets to hack the machine. Take advantage of biometric features (such as finger print readers and facial recognition functions) on smart devices. Actively manage laptops and smart devices so the information on them can be erased if the device is lost or stolen. Consider implementing anti-theft peripherals like cable locks and anti-theft software on remote devices. These deterrents can keep criminals from being able to locate data or use the device.

Actions Governments Can Take:

- Consider activating biometric security on mobile devices. (This may not be feasible for all devices for public safety reasons.)
- Actively manage all mobile devices (e.g., by using a mobile device or enterprise manager).
- Consider using anti-theft software on mobile devices.

BACK-UP AND DISASTER RECOVERY

Always back up applications and data, preferably at off-site locations that are separate from your operating network. Many technology companies provide this type of service. Minimum outsourcing services store data, while comprehensive disaster recovery centers maintain mirror images of all critical back-up systems and data. At the very least, back-up data should be physically separated from production systems and made inaccessible from the Internet when data aren't being actively backed up or restored. Sensitive data should be encrypted at all times and in all locations, including the cloud and hosted data centers — and even backup sites.

Actions Governments Can Take:

1. Develop back-up and disaster recovery procedures.
2. Ensure that all sensitive data are encrypted.

POLICIES AND PROCEDURES

Develop policies and procedures governing the general use of technology and safe handling of data, and make these policies as important as your financial procedures and internal controls. Consider including general processes for when a breach occurs, including three sets of procedures: 1) what staff members are expected to do as "first responders"; 2) what the "incident response team" members should do; and 3) the communications your public information office should make. The list of items that should be considered can be daunting; however, it is feasible if you follow one of the security standards such as the National Institute for Standards and Technology Cybersecurity Framework (nist.gov/cyberframework).

Actions Governments Can Take:

- Develop policies and procedures that address the general use of technology and safe handling of data.
- Conduct regular exercises to prepare for responding to cyber threats, which should be part of regular disaster recovery training.

CONSIDER PURCHASING CYBER INSURANCE

Comprehensive cyber insurance is designed to help organizations recover most costs related to a cyber breach. Although coverage can vary, most cover costs associated with:

1) hardware replacement; 2) professional services (e.g., restoration and cyber forensics); 3) penalties imposed by regulatory agencies for infraction; 4) protecting third parties (e.g., credit card protection); and 5) cyber ransom. Be careful about the protection you are purchasing. For example, some insurance companies don't cover breaches associated with outsourced systems, so make sure your outsourcer has the appropriate insurance. Pay attention to contract requirements. Most cyber insurance providers require their customers to follow a minimum set of security standards and procedures. Include communications with your insurer as part of your attack response plan. Prices vary widely based on the size of your organization, the sensitivity of your system, and the security standards you have in place. Your underwriter can provide an assessment of your cyber security risk.

Actions Governments Can Take:

- Check with your insurance provider about cyber insurance offerings.
- Consider having your underwriter conduct a cyber-security risk assessment, or conduct your own risk assessment following the National Institute for Standards and Technology Cybersecurity Framework guidelines (nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf).

CONCLUSIONS

It is popularly noted that there are three types of organizations: those that have been hacked; those that are being hacked; and those that will be hacked. If that does not scare you, look at one of the live cyber-attack maps (https://norse-corp.com/map) to see live Internet criminal activities. This article outlines actions that individuals can implement without extensive technical knowledge and for minimal cost. GFOA recommends that organizations consider adding these practices to internal training programs and review how well they are implemented each year. Always coordinate these activities with your IT organization, if you have one. Consider contacting outside resources such as the FBI Division on Cyber Crime (fbi.gov/investigate/cyber) to provide guidance on how your organization can prevent becoming a victim.

Other Resources

- FBI Division on Cyber Crime (https://www.fbi.gov/investigate/cyber)
- Homeland Security — CISA (https://www.dhs.gov/cisa/combating-cyber-crime)
- Interpol (interpol.int/en/Crimes/Cybercrime)
- National Institute of Standards and Technology (https://www.nist.gov/)

ROB ROQUE is the technology services manager for GFOA's Research and Consulting Center.

Thanks to Phil Bertolini, co-director, Center for Digital Government, e.Republic; Tom Ray, chief information security manager, City of Berkeley, California; Ryan M. Fernandes, director of technology services, Weston, Florida; and Jim St. Clair, chief technology officer, Dinocrates Group, for their contributions to this article.