CYBERSECURITY
is everyone's job.

Finance and Administration

Finance matters

Considerations extend beyond budget decisions

As a finance or administrative professional in a local government, you have key responsibilities for managing that government's resources. In your role, you interact with all aspects of a local government's operations as you inform budgetary decisions.

Here are three things you can do in your role to #BeCyberSmart.

Office of the Washington State Auditor
Pat McCarthy

Last updated August 2019

You have an essential role to play in keeping your government cyber-secure, through ensuring adequate funding of cybersecurity, addressing cyber-risks in the budget and within contracts, and keeping confidential information housed in financial management software secure.

1 Fund cybersecurity to enable its success

Preparing the budget requires you to consider many competing priorities and help make recommendations on how to spend limited resources. To help balance these demands in your local government, you should participate in an entity-wide risk assessment that also considers cybersecurity risks. The risk assessment can provide actionable information that can help you, as the finance professional, guide the government's leadership in prioritizing and balancing efforts to achieve operational goals and protect from risks.

A risk assessment can be an important tool to make budget recommendations based on the government's needs and priorities consistent with the direction of elected officials.

You can find more information on entity-wide risk assessments in the "Leadership and Planning" section of our #BeCyberSmart webpage.

Budget considerations include adequately funding cybersecurity. Also, make sure you gain an understanding of what cybersecurity investments your government has already made. This can help you recommend more effective areas for investment.

Additionally, consider training and awareness programs for all staff as part of funding your government's cybersecurity efforts. You should also consider software tools and training needs for IT staff as well as replacement costs for older, unsupported systems that might pose a risk.

2 Work with other departments to ensure third-party contracts include appropriate cybersecurity accountability clauses

Thinking about cybersecurity for your own local government is difficult, but have you considered all of the risks from third parties you rely on and share information with, such as contractors, vendors and government partners? These third parties can be a significant source of cybersecurity risk that could affect your government.

In your role as a finance professional in your local government, you are uniquely positioned to know most of the third parties a government interacts with. Are their cybersecurity controls and measures sufficient? How would you know if they were? You should work with Legal and Compliance and IT, as well as other departments, to ensure contracts include clauses that define measures or controls to address cybersecurity concerns. Some things you should also consider include:

- Requiring language that ensures compliance with local, state or federal regulations, or industry standards such as those required when accepting credit card payments (payment card industry guidelines). For an overview of PCI security standards, see www.pcisecuritystandards.org/pci_security/standards_overview

- Gaining an understanding about the third party's implementation of best practices to address cybersecurity. For example, the Center for Internet Security (CIS) Controls prioritize a set of actions to protect an organization and its data. For more on the CIS Controls, see www.cisecurity.org/controls/

- Requiring third parties to provide evidence they have actually implemented the controls referenced in contracts. Depending on risk levels, evidence could take the form of attestations, copies of cybersecurity-related policies, or a security audit.

- Addressing data breach notification protocols. Is the third party contractually required to notify you if a data breach occurs? If so, how soon? State law (RCW 42.56.590) requires notification to affected individuals and to the state Attorney General no more than 45 calendar days after a breach is discovered. To read the statute, go to apps.leg.wa.gov/RCW/default.aspx?cite=42.56.590

You can also reach out to other local governments for ideas and recommendations. Some associations, such as the Association of County and City Information Systems (ACCIS), have contract templates or questionnaires that address third-party risk. To learn more about ACCIS, go to www.accis-wa.org/

3 Protect sensitive financial, legal and other confidential information

As a finance professional, some of the information you handle is part of public record, but you also have access to sensitive and confidential financial information that needs protection, such as employee Social Security numbers and bank accounts. This kind of information poses real cybersecurity risks, and you should take steps to protect it:

- Ensure all finance staff understand what information is confidential and share only what is absolutely required by a data request. You can find out more information about creating specific policies to address which information is and is not confidential in the "Legal and Compliance" section of our #BeCyberSmart webpage.

- Protect sensitive information when it must be shared, using best practices such as transferring such information securely and/or using encryption methods.

- Protect your financial management system to prevent unauthorized access and service disruption, such as using strong passphrases and multi-factor authentication. SAO recommends multi-factor authentication be used for any online system that contains confidential information. The CIS has some good information on multi-factor authentication, available at www.cisecurity.org/newsletter/securing-online-accounts-with-multi-factor-authentication/
- Minimize or eliminate unnecessary records when possible. Specifically, finance staff should ensure unnecessary records and data are destroyed in accordance with the State of Washington's Core Records Retention schedule.

Some of these recommendations can be implemented by finance staff without help from other departments in your government. Some will require you to work with your IT department to make sure they are implemented.

You have an important role to play

As a finance and administrative professional at a local government, you help guide budgetary and operational considerations. By starting with these three steps, and working with all departments in your organization, you can help improve your cybersecurity program.

Our Office also offers training at conferences on cybersecurity. For upcoming dates and times, visit

sao.wa.gov/BeCyberSmart

Sources:

Department of Homeland Security
National Institute of Standards and Technology
Center for Internet Security

Center for Government Innovation