CYBERSECURITY
is everyone's job.

Information Technology

At the core of cybersecurity

IT staff can help build, integrate and maintain a cybersecurity program

As an IT security professional in a local government, you are at the heart of your organization's cybersecurity efforts. You have a vital role to play in building, integrating and maintaining a cybersecurity program at your organization.

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

CYBER SECURITY

Office of the Washington State Auditor
Pat McCarthy

Last updated ***July*** *2023*

As an IT security professional in a local government, you are at the heart of your organization's cybersecurity efforts. Whether the IT department is large or small, you are an important IT resource to ensure your organization's cybersecurity success. In your IT role, you are responsible for creating a robust cybersecurity program, integrating it into everyday operations, and maintaining cybersecurity technical competence.

1 Create a robust cybersecurity program

Creating a robust cybersecurity program takes some thought. The program needs to address many considerations, like governance, risk management and oversight, threat intelligence and collaboration, internal and external resources, training and awareness, incident response, and more. A good cybersecurity program is also about relationships: Building key relationships will give you access to the resources you need to build and support the program. Cybersecurity is everyone's job, and engaging with other departments in your organization helps to build a successful cybersecurity program.

Additionally, look outside of your local government to collaborate with peers by joining a professional association like the Association of County and City Information Systems (ACCIS) or the Multi-State Information Sharing & Analysis Center (MS-ISAC).

You need to ensure that your government has appropriate controls, policies and procedures in place. These should incorporate a best-practice framework like that from the Center for Internet Security (CIS) or the National Institute of Standards and Technology (NIST).

Resources to help guide you:

(ACCIS) www.accis-wa.org

(MS-ISAC) www.cisecurity.org/ms-isac/

(CIS) www.cisecurity.org/controls/

(NIST) www.nist.gov/cyberframework/framework

2 Integrate security into design, architecture, deployment, and routine operations

Being cyber safe is not a destination – it is a journey. IT staff should regularly review and assess system security; identify risks, vulnerabilities and threats; and determine additional steps for your organization to improve cybersecurity.

When using software, whether developed in-house or by a contractor, ensure that best practices are followed. For example, Development and Operations (DevOps) is a best practice that includes security integration throughout software application development, testing, staging, and deployment. For more information about DevOps, visit: https://docs.microsoft.com/en-us/azure/devops/learn/what-is-devops

Additionally, you should work with your Finance, Administration, Legal and Compliance departments to ensure vendor contracts meet your cybersecurity expectations.

You could also consider using data encryption and multi-factor authentication to help departments in your government protect and securely share sensitive information.

Gain insight into the effectiveness of your cybersecurity efforts, such as using a vulnerability scanner to identify weaknesses in operating systems, applications, and network infrastructure.

You could also get an outside perspective by having a third party review some of your practices and controls.

Some resources to consider include:

https://www.cisecurity.org/insights/white-papers/cis-primer-securing-login-credentials

https://www.cisecurity.org/controls/continuous-vulnerability-management

(CIS) https://www.cisecurity.org/ms-isac/services/

3 Maintain excellent technical competence in cybersecurity

Knowledge, skills and abilities (KSAs) are essential to cybersecurity. Whether cybersecurity is your full-time job or just an additional duty, the ever-changing cybersecurity landscape means you must stay current with your training, education and certification. The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) provides additional information: https://niccs.cisa.gov/sites/default/files/documents/Cybersecurity_Workforce_Training_Guide_7.28.21_508c.pdf

Training budgets are sometimes strained. Local government employees are eligible to receive free technical training from the Department of Homeland Security online at https://fedvte.usalearning.gov/

Look for conferences and workshops or reach out to your peers to share their knowledge and experiences as ways to enhance your KSAs; some of the resources above offer such opportunities.

The role of IT is vital in addressing cybersecurity

As an IT professional at a local government, you are at the core of your organization's cybersecurity efforts. You must develop a cybersecurity program that leverages relationships throughout your organization and beyond and maintains the technical expertise that is essential for effective cybersecurity. By starting with these three steps, you are on your way to improving your local government's cybersecurity.

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