CYBERSECURITY
is everyone's job.

Leadership and Planning

Leading the way

Cybersecurity considerations for local government leadership

Local government leaders have many titles — elected official, Commissioner, Councilmember, Mayor, Administrator, Chief, City or County Manager and more. No matter your title, you play a key role in ensuring your organization's cybersecurity success.

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

CYBER SECURITY

Office of the Washington State Auditor
Pat McCarthy

Last updated June 2019

As part of your government's leadership team, you oversee the management of cyber-related risks, prioritize and fund cybersecurity programs, and set a cultural tone to create a cyber-aware workplace. Leaders can develop a cyber-aware culture through education and applying best practices. This document gives you a place to start.

1 Include cyber risks when performing entity-wide risk assessments

It is vitally important to conduct risk assessments for your government to identify threats and system weaknesses. Cyber risks aren't a separate and mysterious realm only for information technology staff to worry about. Leaders need to understand the organizational impacts of cyber incidents, what could be done to reduce the impacts of cyber incidents, and know how the government will respond in the event they occur.

There are many more risks to government operations than there are resources available to deal with them. A risk assessment helps you identify and prioritize those risks and plan for how to address the most important ones. Cyber risks are a very significant risk that should be considered in your agency-wide risk assessment. In particular, we recommend evaluating the risk and impact of a cyber attack on your critical infrastructure (such as emergency communications or water/sewer treatment) or software applications (such as financial management software).

Here is a resource to consider:

Multi-State Information and Analysis Center:
https://www.cisecurity.org/ms-isac/services/

2 Develop and maintain policies and standards for your organization related to cybersecurity

After gaining a basic education about cyber risks, leadership should work with the information technology and legal and compliance staff to establish and implement policies. The policies should broadly address organizational security risks, as well as cyber risks. For example, a county might have policies to restrict the public's access to certain facilities, and a policy to specifically address cyber risks that is designed to protect sensitive data.

Local government executive management can also reach out to elected officials to better understand what their cybersecurity priorities are when making policies. Similarly, elected officials can work with local government leadership staff to clarify cybersecurity priorities, asking: what is the impact of a data breach; what are some compliance and regulatory requirements; what are the cyber risks; what is our decision-making process during an

emergency; what kind of insurance coverage is required for cyber incidents? This information can help leadership further refine policies and prepare for future cyber risks. Ideally, the government's policy would ultimately reflect the standards the government chooses to follow. There are several best practice frameworks for cybersecurity.

Here are a few resources to consider:

Best practice for cybersecurity from Center for Internet Security (CIS): https://www.cisecurity.org/controls/

National Institute of Standards and Technology: Standards, guidelines, and best practices: https://www.nist.gov/cyberframework/new-framework

3 Adequately fund cybersecurity

Cybersecurity investments are crucial. Leaders are in the best position to advocate for financial support for those investments, including paying for people, systems or contracted services. The amount of investment should align with the needs and priorities established as a part of the above-mentioned risk assessment process. Leaders should weigh both current and future financial needs in determining cybersecurity spending.

You have an important role to play

As a leader, you help set the tone and cultural direction of your organization. By starting with these three steps, and ensuring the departments within your government work together on these issues, you are on your way to improving your cybersecurity program.

Department of Homeland Security - Questions every CEO should ask about cyber risks:

https://www.us-cert.gov/ncas/tips/ST18-007

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