

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 government's cybersecurity success.

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



Office of the Washington State Auditor
Pat McCarthy

Last updated November 2025

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 guide gives you a place to start.

1 Include cyber risks when performing entity-wide risk assessments

It is essential 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 (IT) 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 how the government will respond if 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 government-wide risk assessment. In particular, we recommend evaluating the risk and impact of a cyberattack on your critical infrastructure (such as emergency communications or water/wastewater treatment) or software applications (such as financial management software).

Here is a resource to consider:

[Services of the Multi-State Information and Analysis Center](#)



2

Develop and maintain policies and standards for your government related to cybersecurity

After gaining a basic education about cyber risks, leadership should work with the IT 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 leadership staff can also reach out to elected officials to better understand what their cyber security priorities are when making policies. Similarly, elected officials can work with local government leadership staff to clarify cybersecurity priorities, asking:

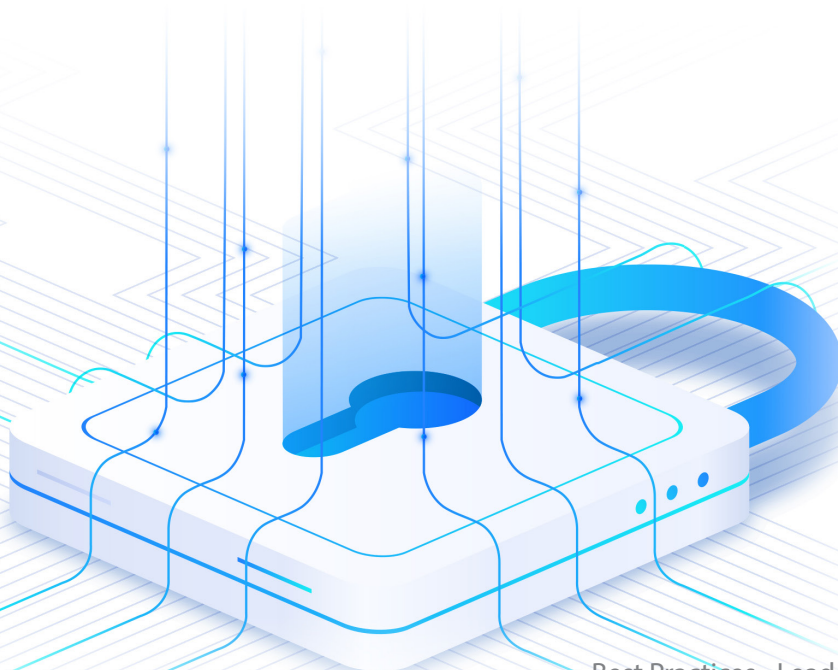
- What is the impact of a data breach?
- What are some compliance and regulatory requirements?
- What are the cyber risks?

- 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 it 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 \(CIS\)](#)
- [National Institute of Standards and Technology: Standards, guidelines, and best practices](#)
- [SAO's It Starts with Policy: A guide to jump-starting your cybersecurity program](#)



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 government. 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.

For additional best practices and questions leaders should address about cyber risks, refer to the CISA blog [“Questions Every CEO Should Ask About Cyber Risks.”](#)

sao.wa.gov/Be**CyberSmart**

Sources:

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

**Center for
Government
Innovation**