CYBERSECURITY
is everyone's job.

Facilities and Operations

Protecting facilities

Increasing use of software and connectivity presents risks

As the facilities and operations professional at a local government, you may work to ensure the physical systems and operations are in good working order. But you actually have another important role to play in keeping your government safe from cyber crime.

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

Office of the Washington State Auditor
Pat McCarthy

Last updated September 2019

Facilities and Operations professionals in a local government have important responsibilities; telecommunications and building efficiency, maintenance, security and safety. You play an essential role in ensuring that government facilities stay safe and secure by identifying risks to infrastructure, ensuring facilities have appropriate security controls and improving security of infrastructure by advocating for cybersecurity best practices.

This guidance does not address responsibilities relating specifically to critical infrastructure, which has additional considerations and requirements for controls. If you want to learn more about critical infrastructure, the Department of Homeland Security has resources: www.dhs.gov/topic/critical-infrastructure-security

1 Identify cyber risks to infrastructure

You maintain facility operations as a key part of your job, but have you considered cybersecurity risks to facilities and operations? In all of the below cases, you need to partner with your IT department to address these risks.

Working closely with your IT department is key to addressing and mitigating many cybersecurity risks. For example, there may be security concerns related to outdated or unsupported software that manage facilities like heating, cooling, building security access and monitoring. Your IT department can help you make upgrades to equipment, and, if required, separate these functions from the rest of your local government's network.

Facilities also house critical IT equipment –this equipment should be safeguarded and protected with climate controlled environments, when needed.

Similarly, so-called "smart buildings" are a rapidly evolving trend; these involve internet connected devices that allow for remote monitoring and management of building subsystems such as lighting or heating. These types of devices that makeup smart buildings are commonly referred to as the "Internet of Things," or IoT. Building subsystems like smart cameras connected to the internet might leave you vulnerable to unauthorized access.

Connecting unauthorized personal devices to your local government's network can put facility-related systems at risk of malicious software infections. Your HR and IT departments can make sure local government staff are educated about the risks of connecting personal devices to the network.

Third-party vendors working with your local government shouldn't have more access to facilities and systems than what's needed to perform their service.

Checking for risks to your facility systems periodically is important. For example, network-connected hardware might be "orphaned," and have no one responsible for it. Additionally, you will need a process to back up important information contained in facilities management systems, and a response plan should an incident occur that affects facility-related systems and operations.

If you do not have internal expertise to identify these risks, you might want to find help in performing your risk assessment.

As a resource, there might be assistance at no-cost from the Department of Homeland Security:

www.us-cert.gov/resources/assessments

2 Ensure facilities have appropriate security controls

Have you thought about cybersecurity controls that might affect local government facilities' security or operation? As mentioned above, contracting with third party vendors that manage systems and support facility's operations can pose a risk, and it's important to restrict how and when a vendor can access the

system. The IT department can help you determine the cybersecurity controls that will prevent vendor misuse. In addition, partner with your legal and compliance staff ensure appropriate contract language is included to address cyber risks and enforce these controls.

Part of ensuring facilities have appropriate cybersecurity controls is also considering smart devices and systems. Again, you will need to engage your IT department to consider if IoT devices meet IT security requirements prior to purchase. You should also identify the IoT systems you already have and implement security controls where appropriate. For example, it is critical to change system defaults and generic passwords to prevent unauthorized access.

Here's a resource to learn more about IoT and smart buildings:

www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html

3 Improve security of infrastructure using cybersecurity best practices

The role of partnering with other departments in your local government to improve the security of your infrastructure can't be stressed enough. IT can help you identify your critical data and formulate a plan for backing it up, as mentioned above. You will then be better prepared to recover your data if you happen to experience a data-loss incident. Your HR department can help you create and implement cybersecurity trainings for new hires and existing facilities and operations staff. Staff should also be trained on the technologies they deploy so that they can better understand how to properly configure and secure it.

Resources for you on cybersecurity best practices related to IoT:

(CIS) www.cisecurity.org/blog/6-simple-tips-for-securing-iot-devices/

(CIS) www.cisecurity.org/press-release/cis-controls-internet-of-things-companion-guide/

You have an important role to play

As a Facilities and Operations professional, you help ensure the safety of government facilities. By starting with these three steps, you can help keep your government's facilities and systems secure from cyber-threats.

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