Cybersecurity Awareness for Leaders

WSAC Leaders Conference
November 15, 2022

Dan Mann, CISSP
Cybersecurity Specialist, Center for Government Innovation

Center for Government Innovation

Office of the Washington State Auditor
Pat McCarthy

SAO's mission

Center for Government Innovation

About SAO

Center for Government Innovation

State Auditor
Pat McCarthy

- Non Audit Services
  - Center for Government Innovation
  - Technical Support
- Audit Services
  - Performance & IT audit
  - State & Local Audit

About the Center

Center for Government Innovation

We offer tools and services to help local governments solve problems and improve operations

- Customized Lean facilitations
- Team-building & leadership workshops
- Financial Intelligence Tool (FIT)
- Online resource library of best practices
- Technical advice & training videos
- #BeCyberSmart resources

Today's agenda

Center for Government Innovation

- What hackers want from your county
- Cybersecurity incidents in the news
- Your role in cybersecurity
- Q&A
- Available resources

What hackers want from your county

How hackers attack your IT system

Center for Government Innovation

Phishing:

Hacker sends fraudulent message designed to trick a person into revealing sensitive information

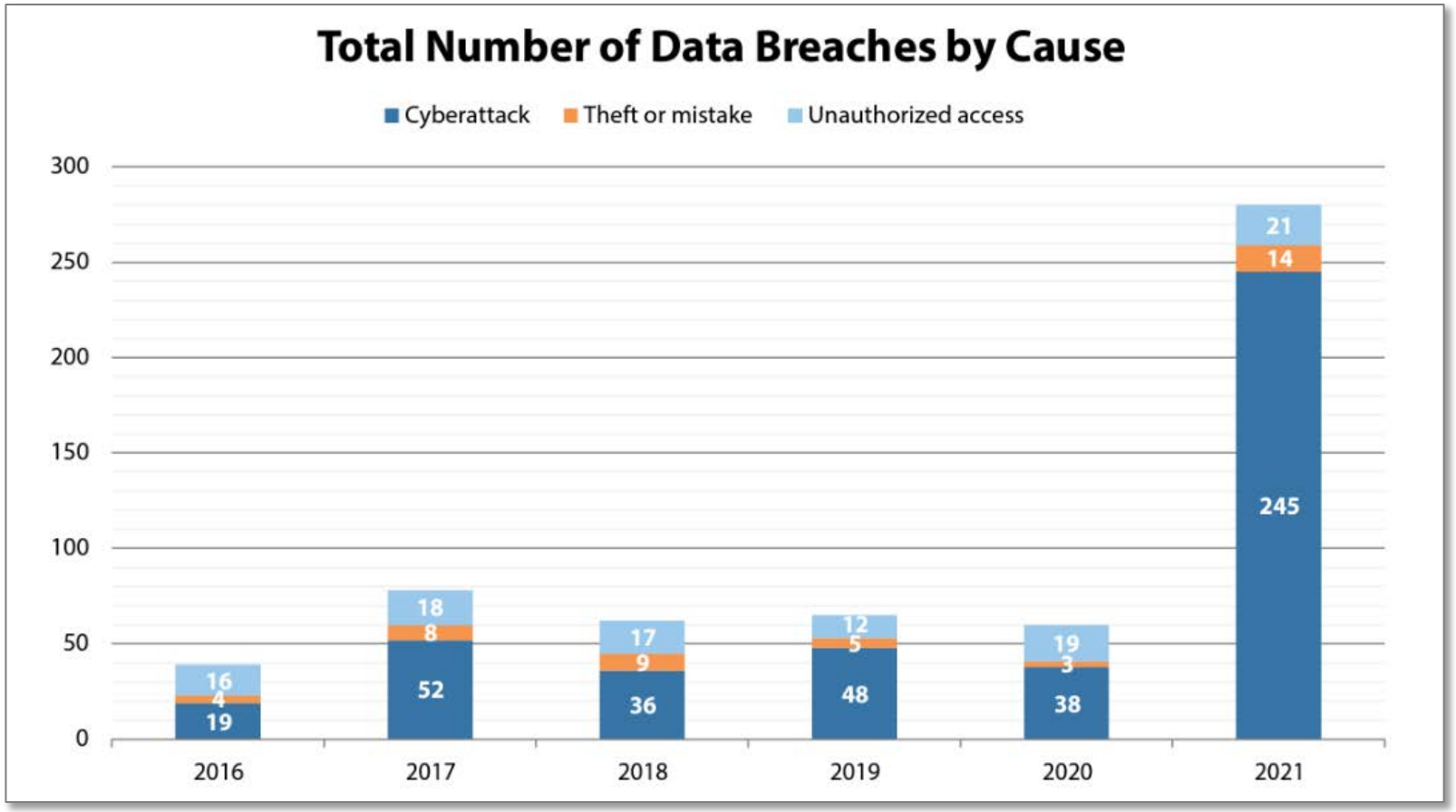
How hackers attack your county

Center for Government Innovation

Ransomware:

A type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid

Cyber incidents in Washington



Cybersecurity incidents in the news…

Center for Government Innovation

Headline:

"County back online after cyberattack"

Methow Valley News, Jan. 27 2021

Cybersecurity incidents in the news…

Center for Government Innovation

Headline:

"Data breach limits services at Whatcom County Libraries"

KGMI NewsTalk Radio, June 28, 2022

Improving your county's cyber hygiene

Center for Government Innovation

Set the tone for the organization

Budget for cybersecurity

Adopt cybersecurity policies and put into practice

Incident Response and Recovery Planning

Tone at the top

- Ensure strong internal controls are in place
- Talk about cybersecurity at meetings

Education & training

Center for Government Innovation

- Appointed & elected officials
- Employees
- Contractors
- Interns

IT security staffing

- Share expertise with neighboring governments
- Work with vendors:
  - Security assessments
  - Network monitoring
- Consider internships

At the end of the day…

Budgeting for cybersecurity

Center for Government Innovation

"How much cybersecurity is enough? Enough is enough."

- Kelly Handerhan, CISSP

Cybersecurity risk assessment

Center for Government Innovation

- **Identify information**
  Where is it maintained and who has access?
- **Assess vulnerability**
  What are the potential risks, exposures and areas for improvement?
- **Create actionable plan**
  How will you address weaknesses?

Adequately fund cybersecurity

Center for Government Innovation

- Align funding to assessment priorities
- Consider current and future needs
- Include IT cybersecurity training

What about cyber insurance?

Can cover:

- Cost of restoring data
- Legal liabilities

Cybersecurity policies

- Email
- File sharing
- Internet
- Laptops
- Remote access
- Social media
- Use of personal mobile devices

Preventing a cybersecurity breach

Center for Government Innovation

- Password management
- Multifactor authentication
- Encryption

Ensure vendors are included

Center for Government Innovation

Require vendors to:

- Comply with data security laws
- Provide security documentation
- Promptly report potential cyber incidents
- Cooperate in incident investigations

Incident response and recovery planning

Center for Government Innovation

Develop written plans that:

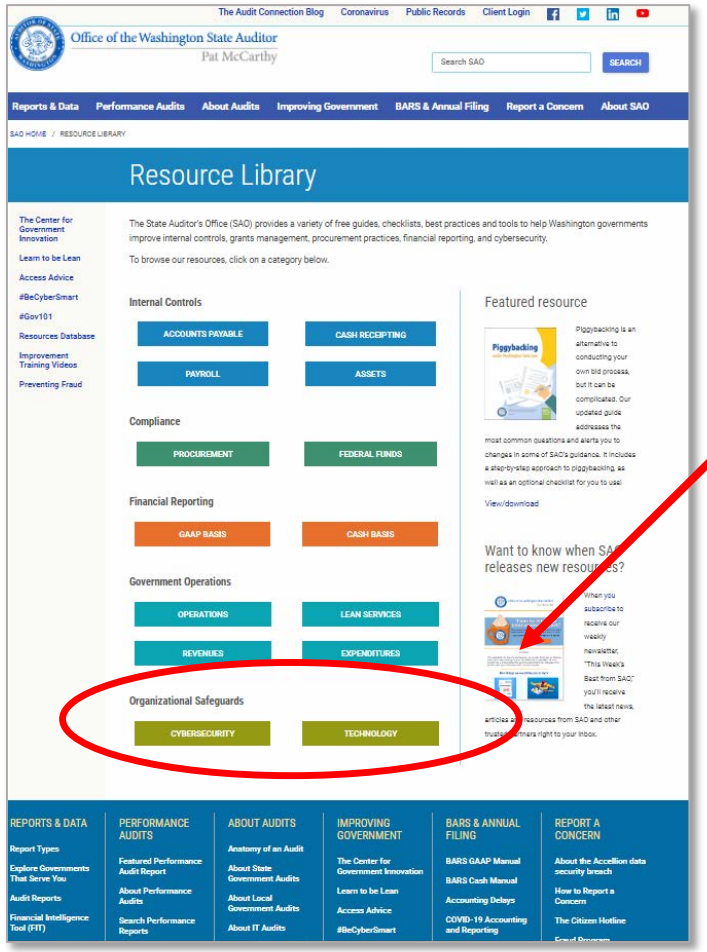
- Document a step-by-step plan to determine nature and extent
- Specify actions to take
- Identify key roles for employees, vendors, stakeholders

Questions

Center for Government Innovation

SAO's Resource Library

Center for Government Innovation



Browse cybersecurity resources

26

#BeCyberSmart resources

Center for Government Innovation

Improve your cybersecurity without breaking your budget

Center for Government Innovation

Office of the Washington State Auditor Pat McCarthy

Balancing the many needs and budget priorities of your local government is challenging and finding dollars for cybersecurity programs may seem monumental. Would you be surprised to learn there are tools you can use at little to no cost? Here, we have rounded up some of the best resources available to help you improve your cybersecurity posture.

1. **Multi-State Information Sharing and Analysis Center (MS-ISAC) offers free membership with many benefits**

   As a local government, this is your key resource for cyber-threat prevention, protection, response and recovery! MS-ISAC is funded by the Department of Homeland Security, so it has many free and low-cost services, such as immediate help should you experience a cyber-incident. MS-ISAC's operations center is available 24/7, and offers free incident response services like emergency conference calls, mitigation recommendations and forensic analysis.

2. **Cybersecurity & Infrastructure Security Agency (CISA), a division of Homeland Security, offers services at no cost**

   CISA, a division of Homeland Security, offers free services to local governments including vulnerability scanning, phishing campaign assessment, and remote penetration testing. For a complete list of services, see https://www.cisa.gov/cyber-resource-hub.

3. **The Public Infrastructure Security Cyber Education System (PISCES) helps small local governments**

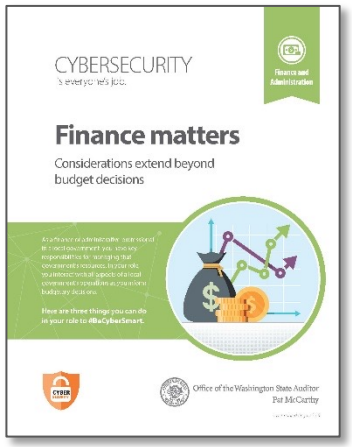
   PISCES connects small municipalities (fewer than 150 network users) with students who analyze live-streaming metadata, and perform network and threat analyses. CISA and Pacific Northwest National Laboratory support PISCES, and it started here in Washington.

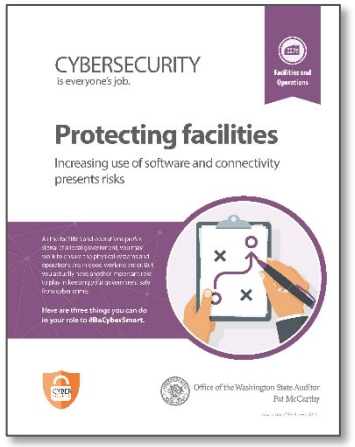
March 2022

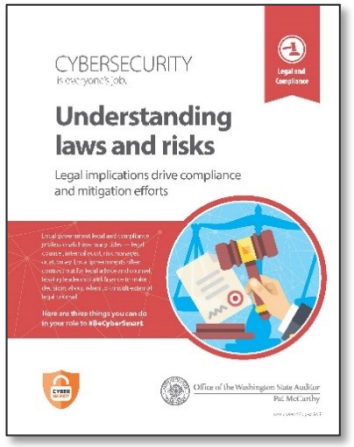
Provides links to free and low-cost tools, policy templates, resources and trainings

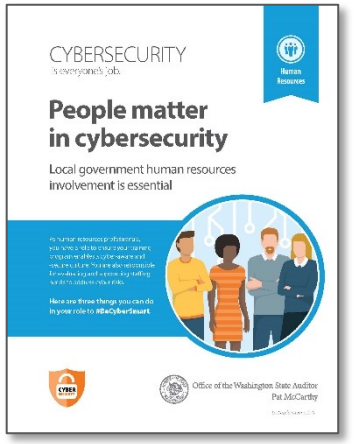
#BeCyberSmart resources by role

Center for Government Innovation









Subscribe to SAO's weekly e-newsletter

Center for Government Innovation

Office of the Washington State Auditor
Pat McCarthy

October is...
CYBERSECURITY AWARENESS MONTH
See Yourself in Cyber

Hello REBECCA!

This week, SAO recognizes Cybersecurity Awareness Month with helpful tips to keep your government's data secure, and we provide an update on the state's opioid lawsuit revenue. We also connect you to information on FDTA federal legislation that could affect your government if it issues debt. And don't forget to register for our annual BARS update webinars.

New things we would like you to know

What exactly is a data breach?

While data breaches at large companies often dominate the headlines, cybercriminals are

Your government has been hacked. How much is the public entitled to know?

When state and local government data has been

Two ways to sign up:

1. Via SAO's website at sao.wa.gov
2. Use the QR code below:

Contact information

Dan Mann, CISSP
Cybersecurity Specialist
Center for Government Innovation

For more information:

- Phone: 564-999-0818
- Email: center@sao.wa.gov
- Website: sao.wa.gov

Center for Government Innovation

Office of the Washington State Auditor
Pat McCarthy