CYBER security in 2021

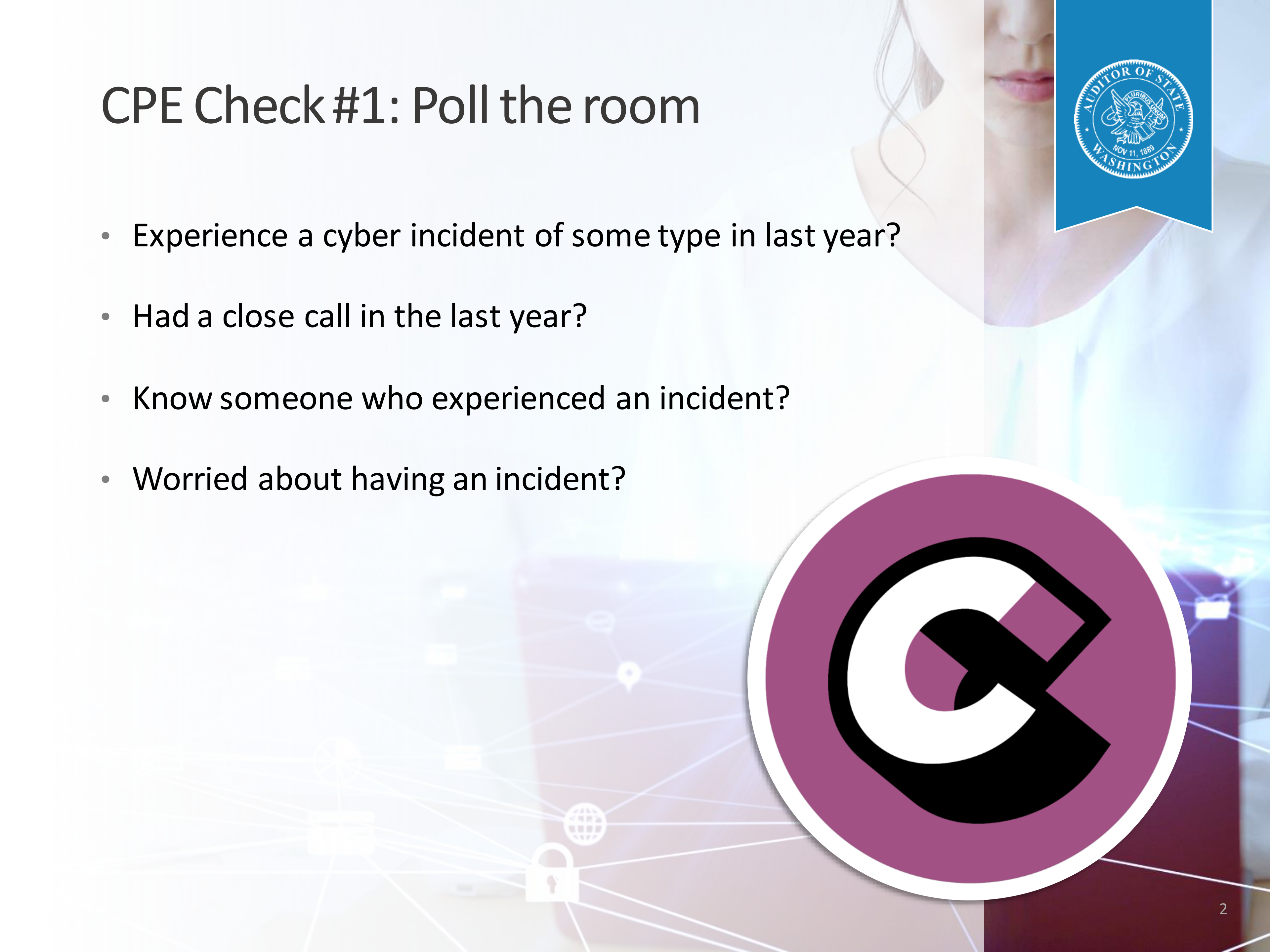
Puget Sound Finance Officers Association

Office of the Washington State Auditor
Pat McCarthy

Peg Bodin
Assistant Director of IT Audit

Sunia Laulile
Sr. IT Security Specialist

March 10, 2021



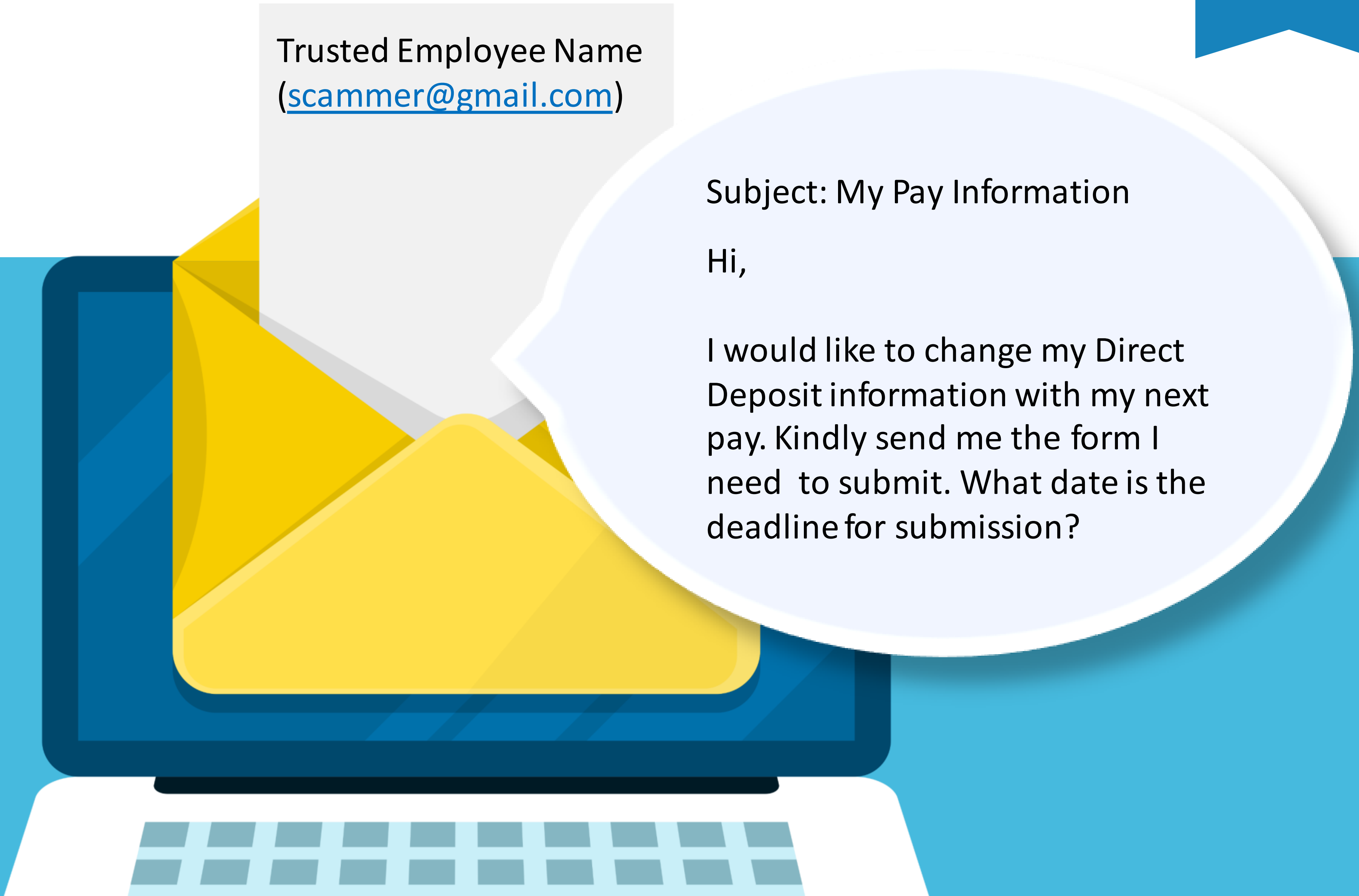
CPE Check #1: Poll the room

- Experience a cyber incident of some type in last year?
- Had a close call in the last year?
- Know someone who experienced an incident?
- Worried about having an incident?

Agenda

- ACH Scams Update
- Ransomware
- Vendor Management
- #BeCyberSmart
- Fraud Reporting

Anatomy of the ACH fraud



Trusted Employee Name (scammer@gmail.com)

Subject: My Pay Information

Hi,

I would like to change my Direct Deposit information with my next pay. Kindly send me the form I need to submit. What date is the deadline for submission?

The High-Tech Solution

Another Way the ACH Fraud Is Initiated

System compromise

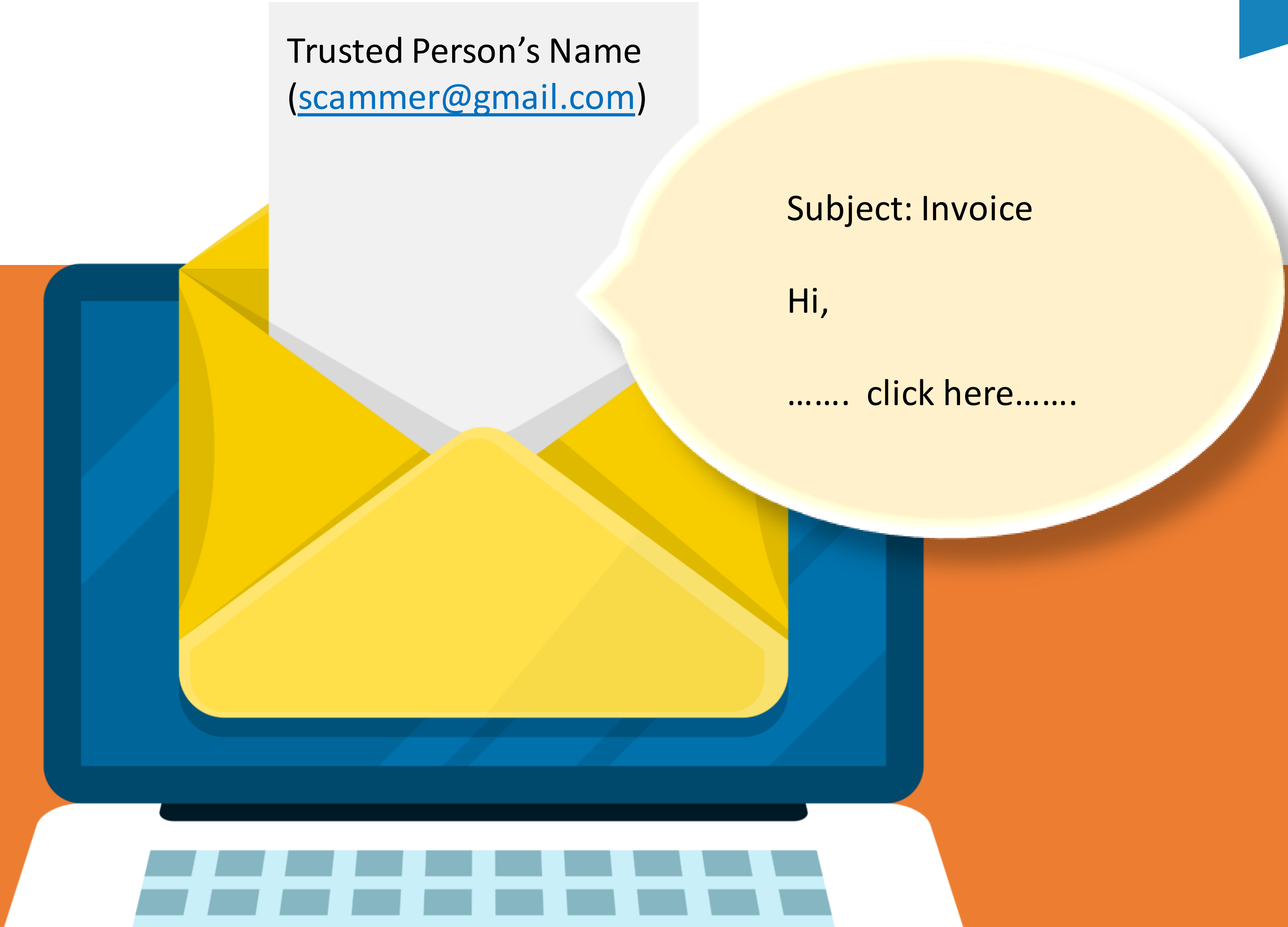
- Email or network
- Risk extends beyond ACH loss
- Difficult investigation
- Fraud is still easily prevented but…

CPE Check #2

Your Worst Nightmare

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost

Anatomy of a Ransomware Attack



Trusted Person's Name
(scammer@gmail.com)

Subject: Invoice

Hi,

……. click here…….

The Unwanted Houseguest

Gain entrance

- Email (most often)
- Unannounced guest

We’re in!

Dropper (small)

Look around

- Admin access
- Passwords
- Unpatched systems

Call home

The Difficult Goodbye

Stay awhile

Additional unwanted houseguests (malware)

Extract information

- Confidential data
- Passwords

Lock

- Encrypt

Threaten

Operational Standstill

One government's experience:

- Every server encrypted
- Backup partially encrypted
- Additional malware
- Data extracted?

Actions for a Finance Officer

- Read IC3 Ransomware Fact Sheet
- Ask your IT if they limit RDP access from the internet
- Ask your IT if software updates are occurring for ALL software

Actions for a Finance Officer

- Ask about backup and recovery
- Consider how you protect confidential and critical operations and processes.
    - Password?
    - Multi-factor authentication?
- Develop an incident response plan

CPE Check #3

We all need a little help

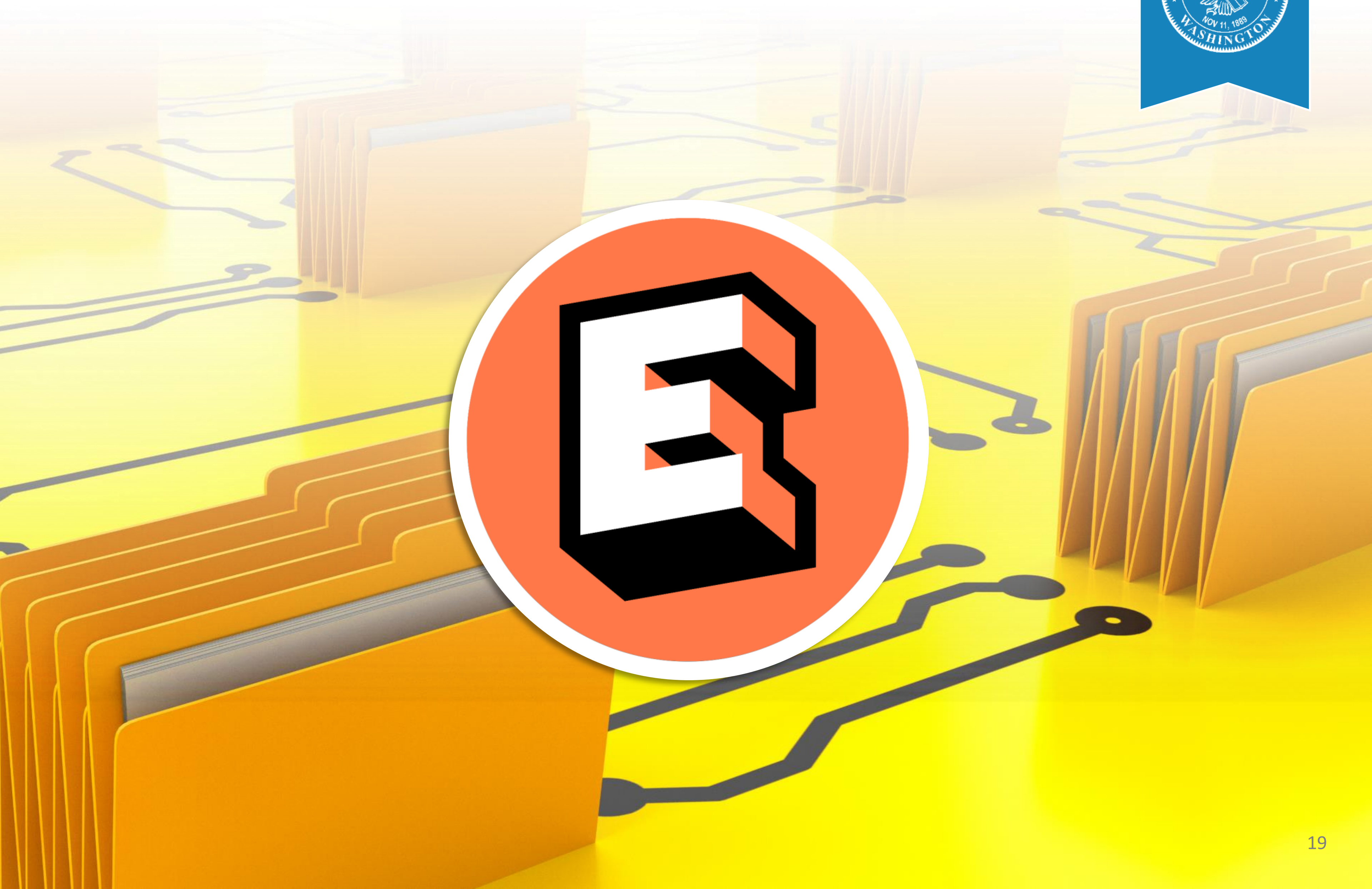
What can go wrong?

- Extension of risk
- Unmonitored access
- Software / system design
- Age
- Default passwords

What can we do?

- Ask questions
- Show interest
- What are the challenges?

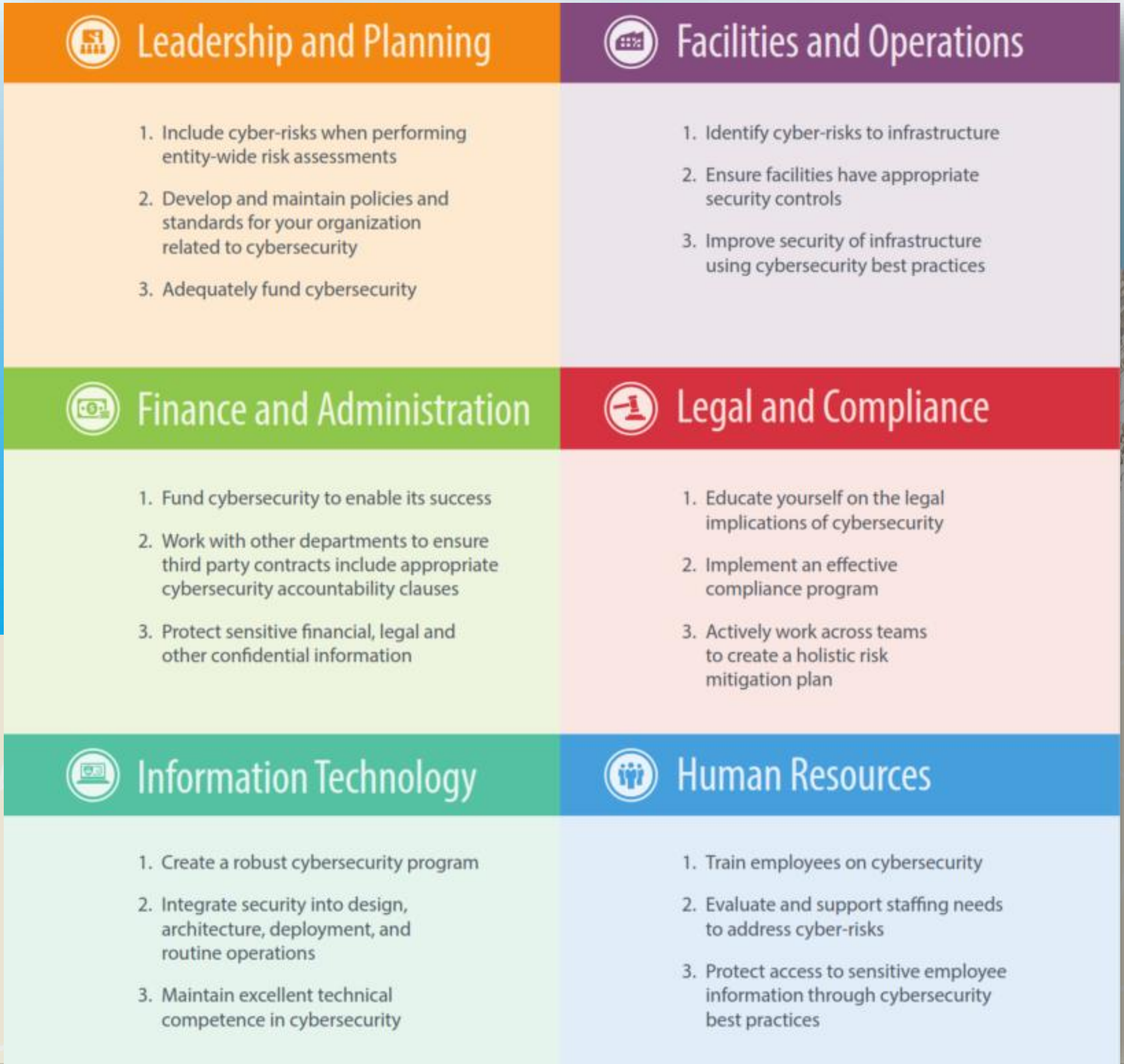
CPE Check #4



#BeCyberSmart Campaign

- Curated suite of cybersecurity resources for local government
- Customized by role in government
- Designed as a place for governments to start

#BeCyberSmart Initiaitve



Leadership and Planning

1. Include cyber-risks when performing entity-wide risk assessments
2. Develop and maintain policies and standards for your organization related to cybersecurity
3. Adequately fund cybersecurity

Facilities and Operations

1. Identify cyber-risks to infrastructure
2. Ensure facilities have appropriate security controls
3. Improve security of infrastructure using cybersecurity best practices

Finance and Administration

1. Fund cybersecurity to enable its success
2. Work with other departments to ensure third party contracts include appropriate cybersecurity accountability clauses
3. Protect sensitive financial, legal and other confidential information

Legal and Compliance

1. Educate yourself on the legal implications of cybersecurity
2. Implement an effective compliance program
3. Actively work across teams to create a holistic risk mitigation plan

Information Technology

1. Create a robust cybersecurity program
2. Integrate security into design, architecture, deployment, and routine operations
3. Maintain excellent technical competence in cybersecurity

Human Resources

1. Train employees on cybersecurity
2. Evaluate and support staffing needs to address cyber-risks
3. Protect access to sensitive employee information through cybersecurity best practices

Cybersecurity for Finance and Administration

1 Fund cybersecurity to enable its success

2 Work with other departments to ensure third-party contracts include appropriate cybersecurity accountability clauses

3 Protect sensitive financial, legal and other confidential information

Additional Resources

- Center for Internet Security – CIS Controls
  www.cisecurity.org/controls/

- NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
  csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

- NIST 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organization https://doi.org/10.6028/NIST.SP.800-161

- Multi-State Information Sharing & Analysis Center (MS-ISAC)
  www.cisecurity.org/ms-isac/

Additional Resources

- SAO’s #BeCyberSmart Page
  [www.sao.wa.gov/becybersmart/]

- SAO’s Guidance on ACH Fraud
  [www.sao.wa.gov/where-are-your-payments-going-this-month/]

- SAO Guidance on when to report a cybersecurity issue
  Has your government experienced a cybersecurity issue? Here is when and how to report - Office of the Washington State Auditor

Fraud Reporting

- Fraudulent ACH payment
- Ransom payment
- System compromise

CPE Check #5

Questions

Information

Contact Peg Bodin,

Peggy.Bodin@sao.wa.gov

(564) 999-0965

Sunia Laulile

Sr. IT Security Specialist

Sunia.Laulile@sao.wa.gov

(564) 999-0963