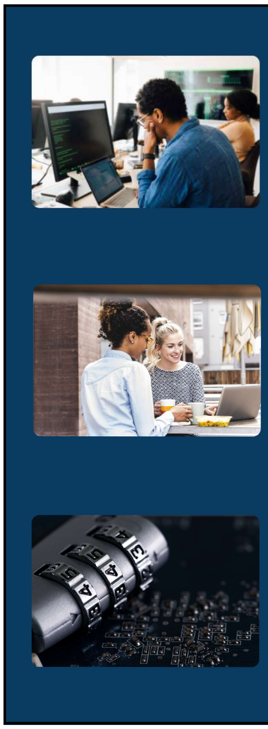


Cybersecurity Informational Update

City of Tacoma, Information Technology Department

Government Performance and Finance Committee

November 19, 2024

1

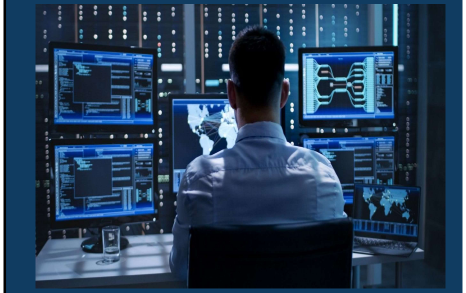
Objectives

CYBERSECURITY PROGRAM RECAP

CURRENT FOCUS AND ACTIVITIES

2

Information Assurance Program Recap



Security Assurance

- architecture
- engineering
- procurement and implementation assistance

Security Operations

- situational awareness
- event handling
- incident response
- threat hunting
- vulnerability management

Compliance Coordination

- compliance standards SME
- assessment and audit technical coordination
- policy/standards development

Readiness and Resilience

- awareness
- education
- practice
- planning

3

Other Program Features

Aligned with recognized standards and best practices

- National Institute for Standards and Technology Cybersecurity Framework (NIST CSF)
- Center for Internet Security Critical Security Controls (CIS CSC)

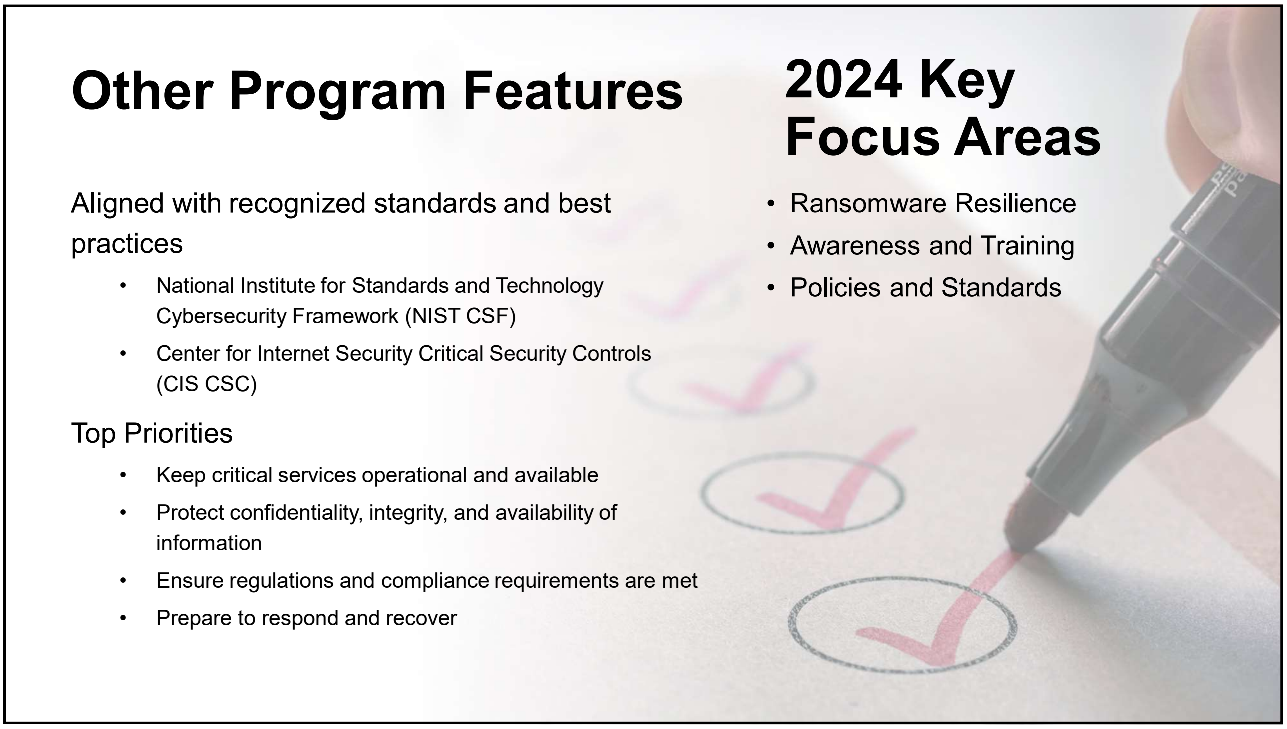
Top Priorities

- Keep critical services operational and available
- Protect confidentiality, integrity, and availability of information
- Ensure regulations and compliance requirements are met
- Prepare to respond and recover

2024 Key Focus Areas

- Ransomware Resilience
- Awareness and Training
- Policies and Standards

4



Other Program Features

Aligned with recognized standards and best practices

- National Institute for Standards and Technology Cybersecurity Framework (NIST CSF)
- Center for Internet Security Critical Security Controls (CIS CSC)

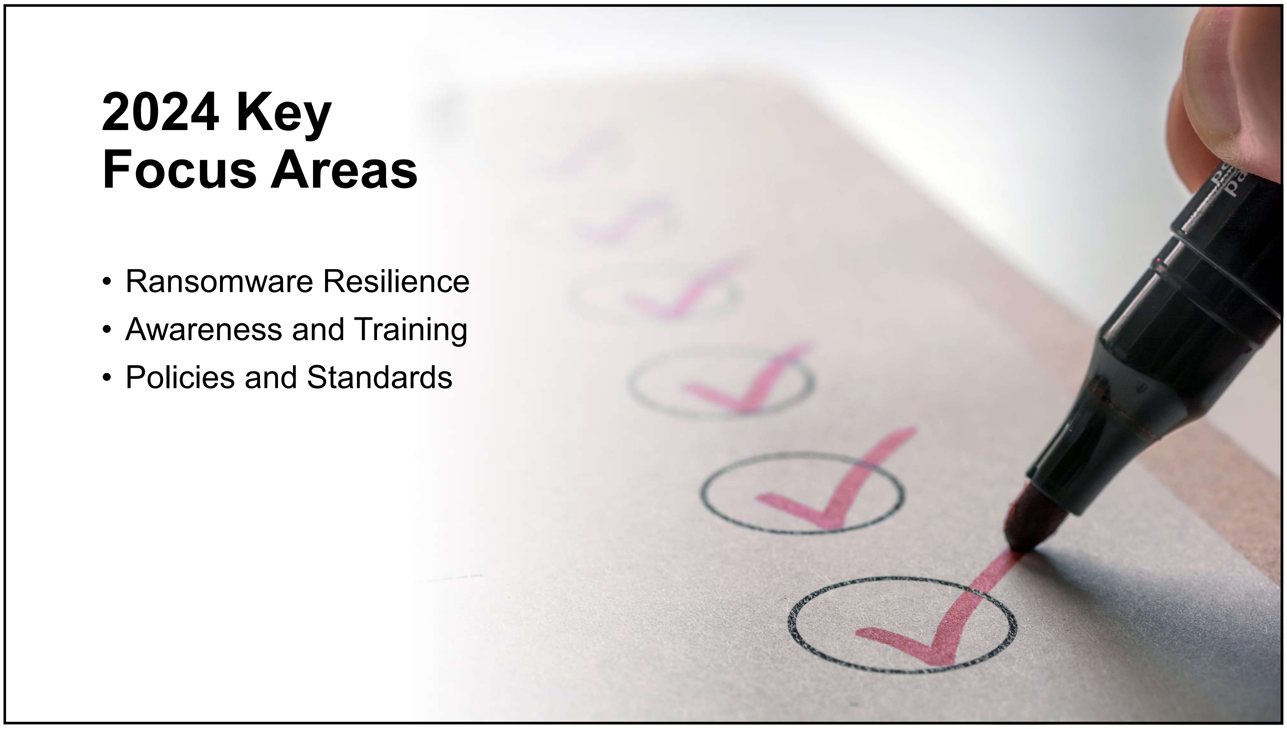
Top Priorities

- Keep critical services operational and available
- Protect confidentiality, integrity, and availability of information
- Ensure regulations and compliance requirements are met
- Prepare to respond and recover

2024 Key Focus Areas

- Ransomware Resilience
- Awareness and Training
- Policies and Standards

5



2024 Key Focus Areas

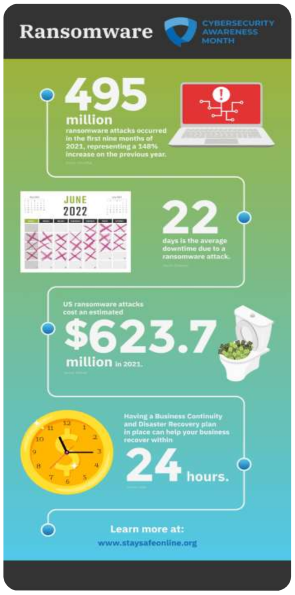
- Ransomware Resilience
- Awareness and Training
- Policies and Standards

6

Why Focus on Ransomware?

Ransomware continues to be a high-risk concern

- 49 attacks on Washington local governments in 2023*
- Average downtime experienced after an attack is 22 days**
- Average recovery cost for state and local governments is $2.83M, excluding any ransom payments***



Ransomware

CYBERSECURITY AWARENESS MONTH

495 million ransomware attacks occurred in the first nine months of 2021, representing a 148% increase on the previous year.

22 days is the average downtime due to a ransomware attack.

US ransomware attacks cost an estimated $623.7 million in 2021.

Having a Business Continuity and Disaster Recovery plan in place can help your business recover within 24 hours.

Learn more at: www.staysafeonline.org

*WA State OAG 2023 Data Breach Report
**Statistica U.S. average length of downtime after a ransomware attack 2022
***Sophos State of Ransomware in State and Local Government 2024

CITY OF Tacoma

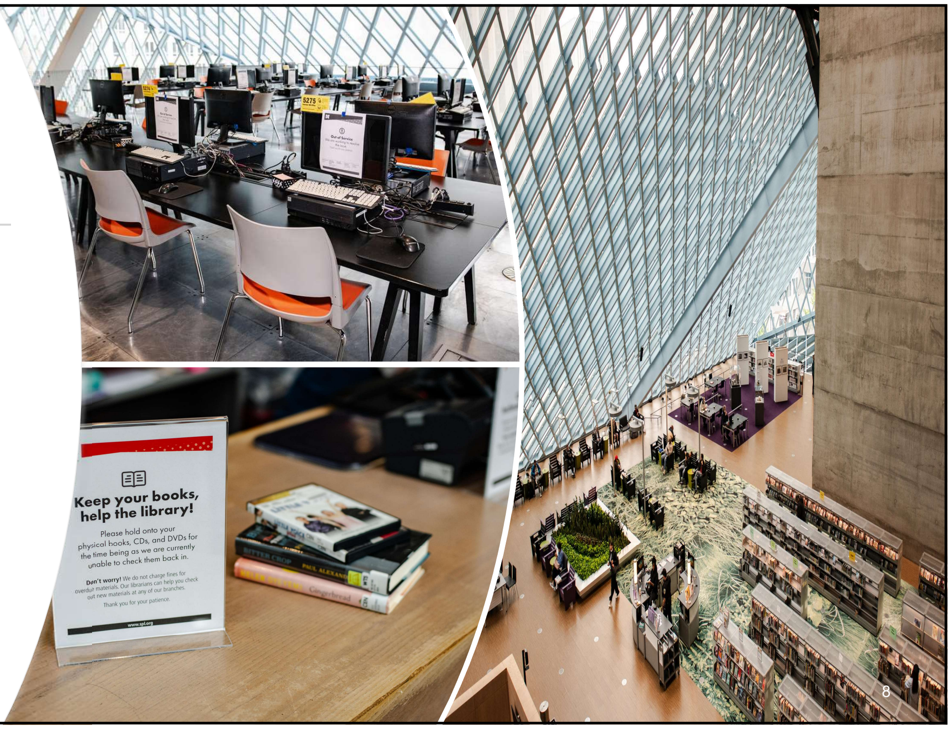
May 29th Seattle Public Library Ransomware Attack

All systems impacted including:

- Website
- Payroll
- Catalog, loaning, and check-in
- Public access computers & WiFi

Employee PII stolen

5-month recovery effort


Keep your books, help the library!
Please hold onto your physical books, CDs, and DVDs for the time being as we are currently unable to check them back in.
Don't worry! We do not charge fines for overdue materials. Our librarians can help you check out new materials at any of our branches.
Thank you for your patience.
www.spl.org

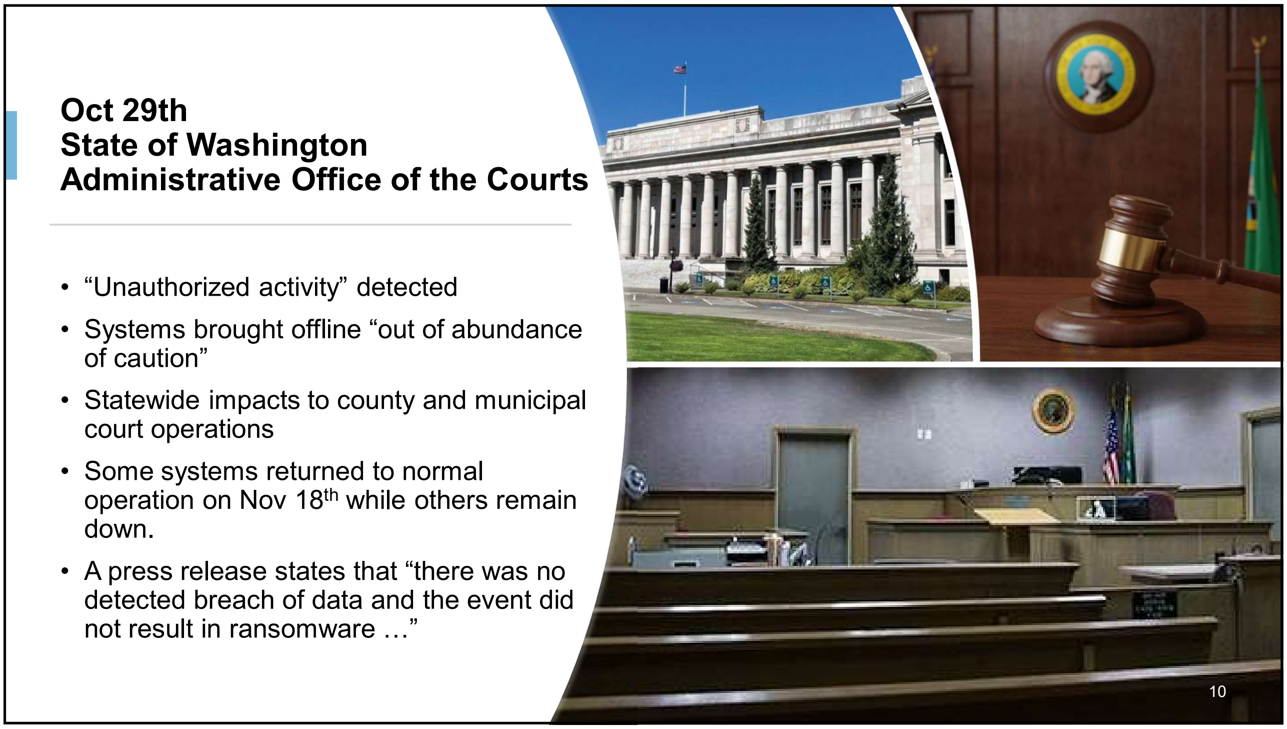
Aug 24th Port of Seattle Ransomware Attack

Major airport operations affected including:

- baggage handling
- check-in kiosks
- ticketing
- Wi-Fi
- passenger display boards

Some non-critical systems remain down after 6 weeks.

TSA Pre✓
4 Security Checkpoint
to all Gates
Due to the Port of Seattle Internet outage our check-in system is down



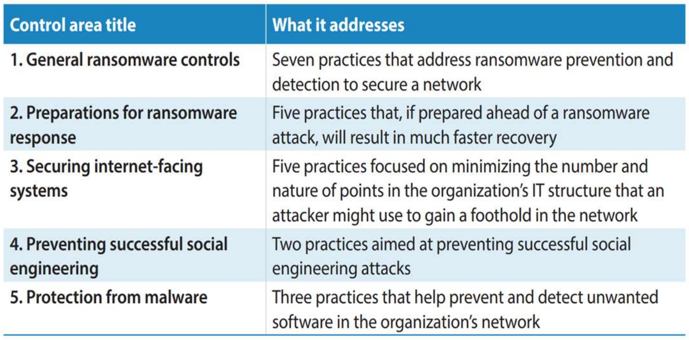
Oct 29th State of Washington Administrative Office of the Courts

- "Unauthorized activity" detected
- Systems brought offline "out of abundance of caution"
- Statewide impacts to county and municipal court operations
- Some systems returned to normal operation on Nov 18th while others remain down.
- A press release states that "there was no detected breach of data and the event did not result in ransomware …"

SAO Ransomware Resilience Audit

Voluntary assessment

Measure ability to withstand a ransomware attack



Control area title	What it addresses
1. General ransomware controls	Seven practices that address ransomware prevention and detection to secure a network
2. Preparations for ransomware response	Five practices that, if prepared ahead of a ransomware attack, will result in much faster recovery
3. Securing internet-facing systems	Five practices focused on minimizing the number and nature of points in the organization's IT structure that an attacker might use to gain a foothold in the network
4. Preventing successful social engineering	Two practices aimed at preventing successful social engineering attacks
5. Protection from malware	Three practices that help prevent and detect unwanted software in the organization's network

11

Assessment Results

- Majority of controls fully or partially implemented
- 10 recommendations for improvement
- No unknown gaps
- All captured and prioritized on cybersecurity workplan

12

Cybersecurity Awareness Training Helps Prevent Ransomware Attacks

69% of state and local government ransomware attacks can be traced back to poor cyber hygiene

- Weak passwords
- Compromised credentials
- Malicious links and attachments
- Phishing and other social engineering
- Unpatched software and systems

CITY OF Tacoma

13

Cybersecurity Awareness Training Info

New courses for 2024. Required for all technology users including employees, contractors, interns, and temps.

Progress as of Nov 15, 2024

TPU (Aug 1 – Oct 31 training period)

- % completion - **100%**

City Gen Government (Sept 16 – Nov 30 training period)

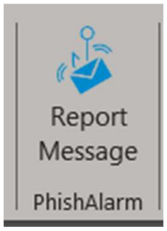
- % completion – **80%**

CITY OF Tacoma

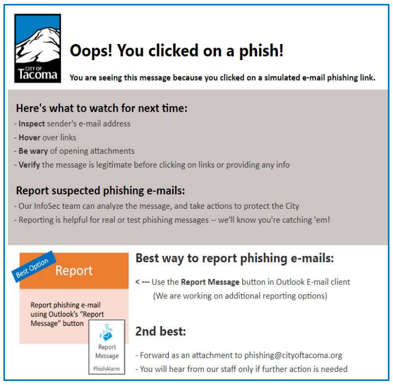
14

Training Goals

Report Suspicious Emails



Practice Phishing Message Recognition



Oops! You clicked on a phish!

You are seeing this message because you clicked on a simulated e-mail phishing link.

Here's what to watch for next time:

- **Inspect** sender's e-mail address
- **Hover** over links
- **Be wary** of opening attachments
- **Verify** the message is legitimate before clicking on links or providing any info

Report suspected phishing e-mails:

- Our InfoSec team can analyze the message, and take actions to protect the City
- Reporting is helpful for real or test phishing messages -- we'll know you're catching 'em!

Best Option

Report

Report phishing e-mail using Outlook's "Report Message" button

Best way to report phishing e-mails:

< --- Use the **Report Message** button in Outlook E-mail client
(We are working on additional reporting options)

2nd best:

- Forward as an attachment to phishing@cityoftacoma.org
- You will hear from our staff only if further action is needed

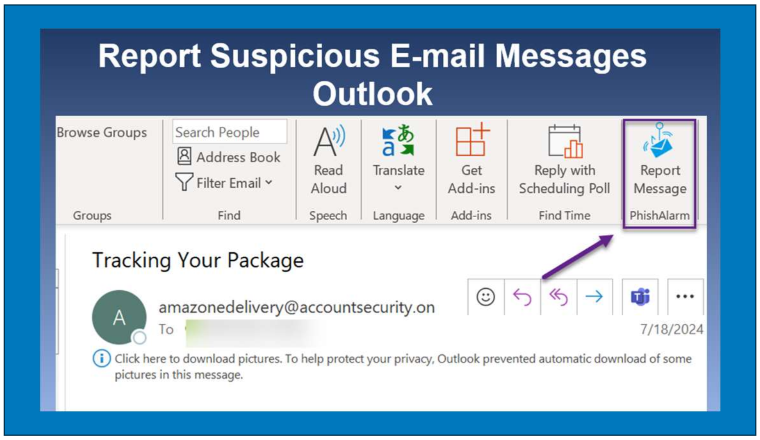
Inform about Policy and Standards Updates

Name	Quick Facts
Technology Acceptable Use	Updated in 2024
Use of Generative AI ML Systems	Added in 2024
Mobile Device Policy	Updated in 2024
Information Classification	Added in 2024
Technology Incident Response	Added in 2024
Password Strength & Protection	Updated in 2024

CITY OF Tacoma

15

Training Goal: Report Suspicious Emails



Report Suspicious E-mail Messages Outlook

Tracking Your Package

amazonedelivery@accountsecurity.on

To [redacted]

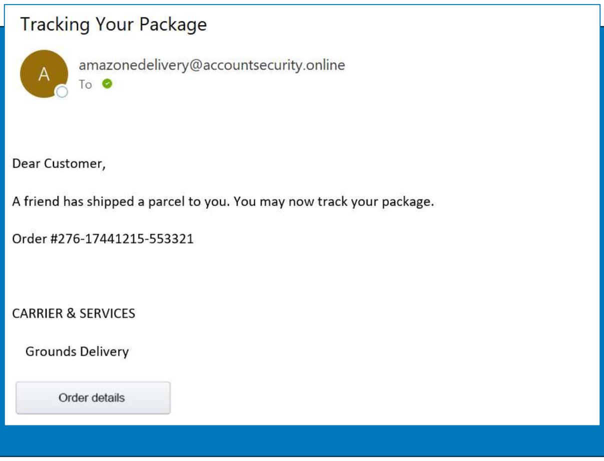
7/18/2024

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

CITY OF Tacoma

16

Training Goal: Recognize Phishing Messages Through Practice



Tracking Your Package

amazonedelivery@accountsecurity.online
To

Dear Customer,

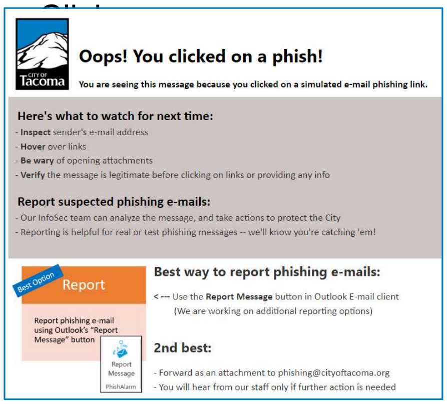
A friend has shipped a parcel to you. You may now track your package.

Order #276-17441215-553321

CARRIER & SERVICES

Grounds Delivery

Education Page for



Oops! You clicked on a phish!

You are seeing this message because you clicked on a simulated e-mail phishing link.

Here's what to watch for next time:

- **Inspect** sender's e-mail address
- **Hover** over links
- **Be wary** of opening attachments
- **Verify** the message is legitimate before clicking on links or providing any info

Report suspected phishing e-mails:

- Our InfoSec team can analyze the message, and take actions to protect the City
- Reporting is helpful for real or test phishing messages -- we'll know you're catching 'em!

Best Option
Report
Report phishing e-mail using Outlook's "Report Message" button
Report Message
PhishAlarm

Best way to report phishing e-mails:

< --- Use the **Report Message** button in Outlook E-mail client
(We are working on additional reporting options)

2nd best:

- Forward as an attachment to phishing@cityoftacoma.org
- You will hear from our staff only if further action is needed

17

Training Goal: Understand Policy & Standards Updates

Policies, Standards, & Guidelines provide important direction and guidance to employees

Number	Name	Document Type	Quick Facts
#4.1	**Technology Acceptable Use**	Policy	Updated in 2024, training available
#4.1-GD-2	**Use of Generative AI ML Systems**	Guideline	Added in 2024, training available
#4.20	**Mobile Device Policy**	Policy	Updated in 2024, training available
#4.30	**Information Classification**	Policy	Added in 2024, training available
#4.40	**Technology Incident Response**	Policy	Added in 2024, training available
#4.50-ST-01	**Password Strength & Protection**	Standard	Updated in 2024, distributed to all staff, ongoing effort to implement & train - (one year estimated)

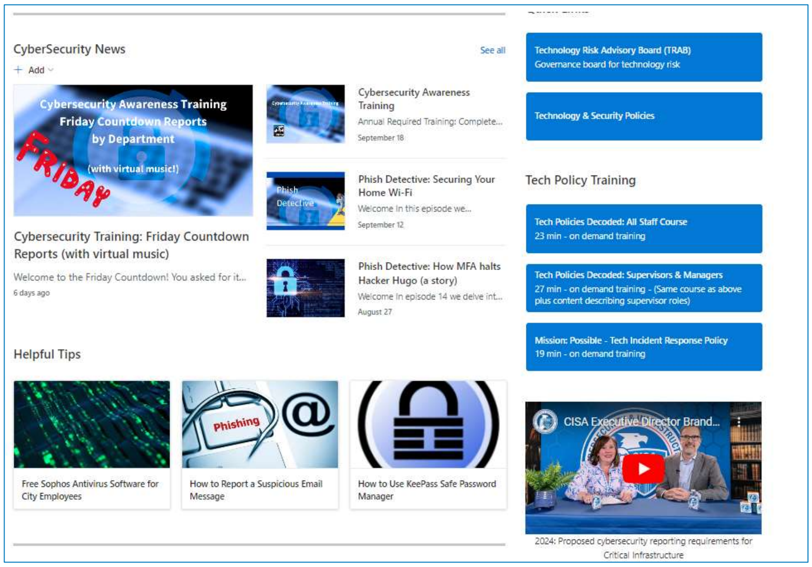
18

Resources: Tacoma Hub / Information Assurance Page

One Stop Shop for

- ✓Cybersecurity News
- ✓Policy Links
- ✓Policy Training Links
- ✓Phish Detective Articles
- ✓How-to Information

Information Assurance - Home (sharepoint.com)



CyberSecurity News

See all

+ Add

Cybersecurity Awareness Training Friday Countdown Reports by Department (with virtual music!) FRIDAY

Cybersecurity Training: Friday Countdown Reports (with virtual music)

Welcome to the Friday Countdown! You asked for it...

6 days ago

Cybersecurity Awareness Training

Annual Required Training: Complete...

September 18

Phish Detective: Securing Your Home Wi-Fi

Welcome In this episode we...

September 12

Phish Detective: How MFA halts Hacker Hugo (a story)

Welcome In episode 14 we delve int...

August 27

Helpful Tips

Free Sophos Antivirus Software for City Employees

How to Report a Suspicious Email Message

How to Use KeePass Safe Password Manager

Technology Risk Advisory Board (TRAB)
Governance board for technology risk

Technology & Security Policies

Tech Policy Training

Tech Policies Decoded: All Staff Course
23 min - on demand training

Tech Policies Decoded: Supervisors & Managers
27 min - on demand training - (Same course as above plus content describing supervisor roles)

Mission: Possible - Tech Incident Response Policy
19 min - on demand training

CISA Executive Director Brand...

2024: Proposed cybersecurity reporting requirements for Critical Infrastructure

19

Questions

20