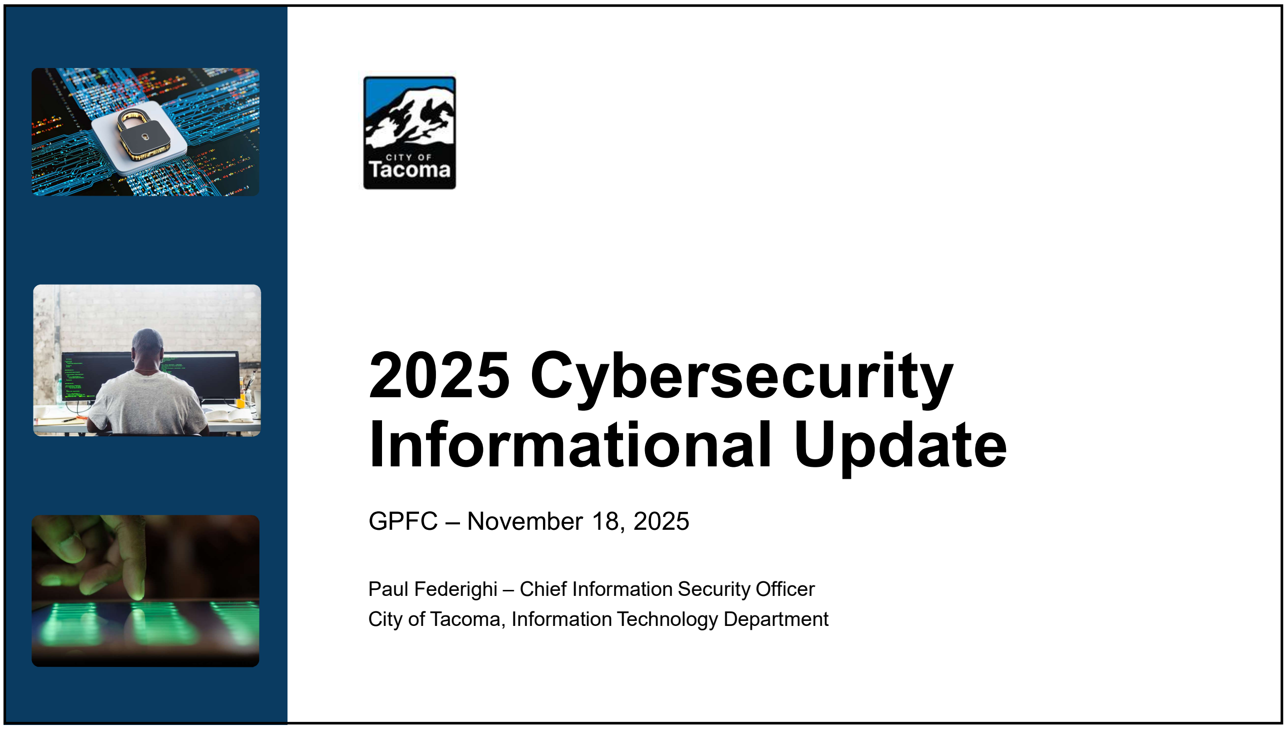
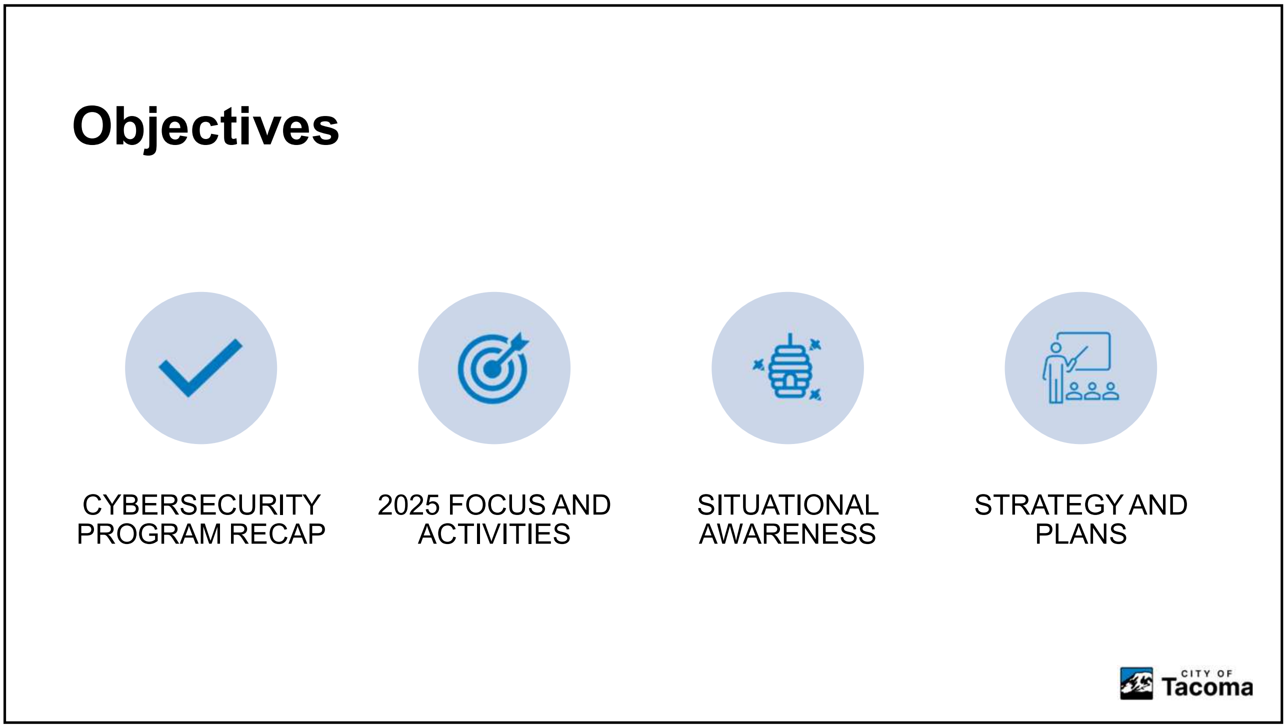


2025 Cybersecurity Informational Update

GPFC – November 18, 2025

Paul Federighi – Chief Information Security Officer
City of Tacoma, Information Technology Department

1

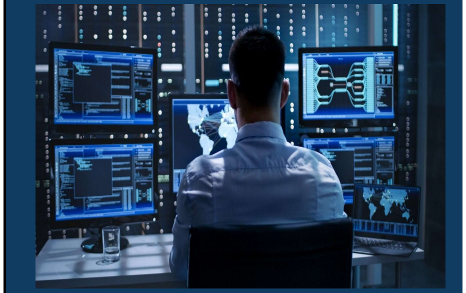


Objectives

- CYBERSECURITY PROGRAM RECAP
- 2025 FOCUS AND ACTIVITIES
- SITUATIONAL AWARENESS
- STRATEGY AND PLANS

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

CITY OF Tacoma

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

CITY OF Tacoma

4

2025 Cybersecurity-Related Projects

Completed

- Windows 11 Upgrade
- Criminal Justice MFA
- IT Asset Inventory
- Next Generation Firewall Upgrade
- Password Strength and Protection Standard
- Vulnerability Management Standard
- Cybersecurity Incident Response Plan (Phase 1)
- Annual Cybersecurity Awareness Training

In-flight

- M365 Sensitive Document Security
- M365 Document Classification and Labeling
- M365 3rd Party App Permission Cleanup
- Cybersecurity Incident Response Plan Phase 2

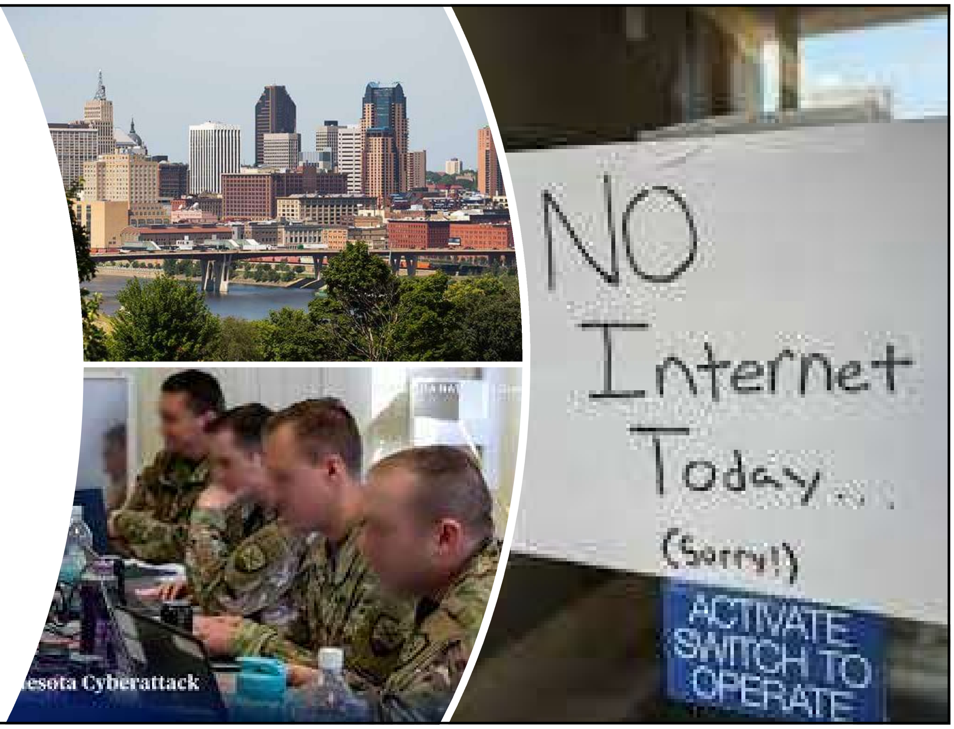
CITY OF Tacoma

5

July 25, 2025 City of St. Paul, MN Ransomware Attack

City services significantly disrupted, including phones, online payments and other digital systems.

- Interlock ransomware gang claims over 66,000 files stolen. Some files released to the public after city refuses to pay ransom
- Minnesota National Guard activated to provide cybersecurity support.
- As of 9/8 some systems are still being recovered

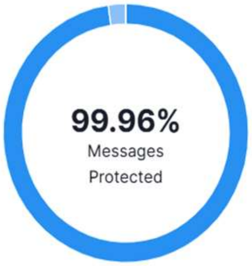


6

City of Tacoma Data

Protection effectiveness

July -October 2025



Message Protection	Volume (% of total)
● Pre-Delivery Protected	29,558 (97.7%)
● Post-Delivery Protected	680 (2.2%)
● Potentially Exposed	13 (0%)
Total	**30,251 (100%)**

CITY OF Tacoma

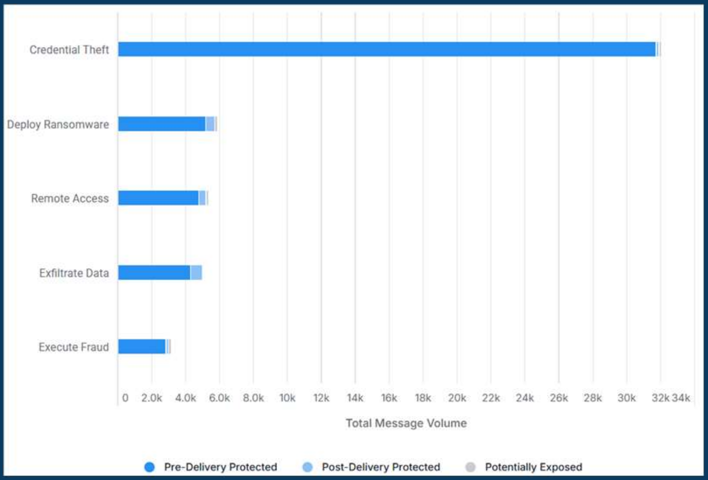
7

City of Tacoma Data

Threat Objectives

July -October 2025

Top 5 Threat Objectives



CITY OF Tacoma

8

Data Breach Impact

Average Cost of a Data Breach = $168* per record

- 280,000 customer records = $47,040,000

Cost contributors

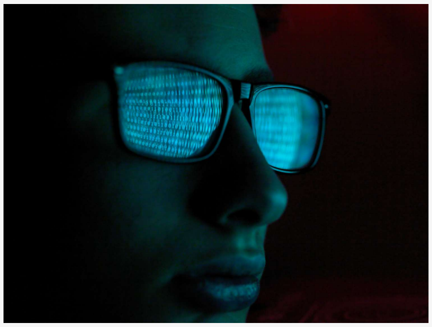
- Detection and escalation (forensics, crisis management, overtime)
- Post-breach response (credit monitoring, legal support)
- Notification (communication to affected parties)
- Regulatory/Compliance (fines, fees)
- Lost opportunity (resource diversion)

* IBM, “Cost of a Data Breach Report 2025”

CITY OF Tacoma

9

Cybersecurity Trends



Social Engineering

the #1 threat vector

- Phishing
- Smishing
- Vishing

Vulnerabilities

#2 and rising

- Missing software patches/updates
- End of support apps and equipment
- App proliferation

Identities and Permissions

attackers don’t break in, they log in

- Compromised credentials
- Privileged accounts
- Non-human accounts

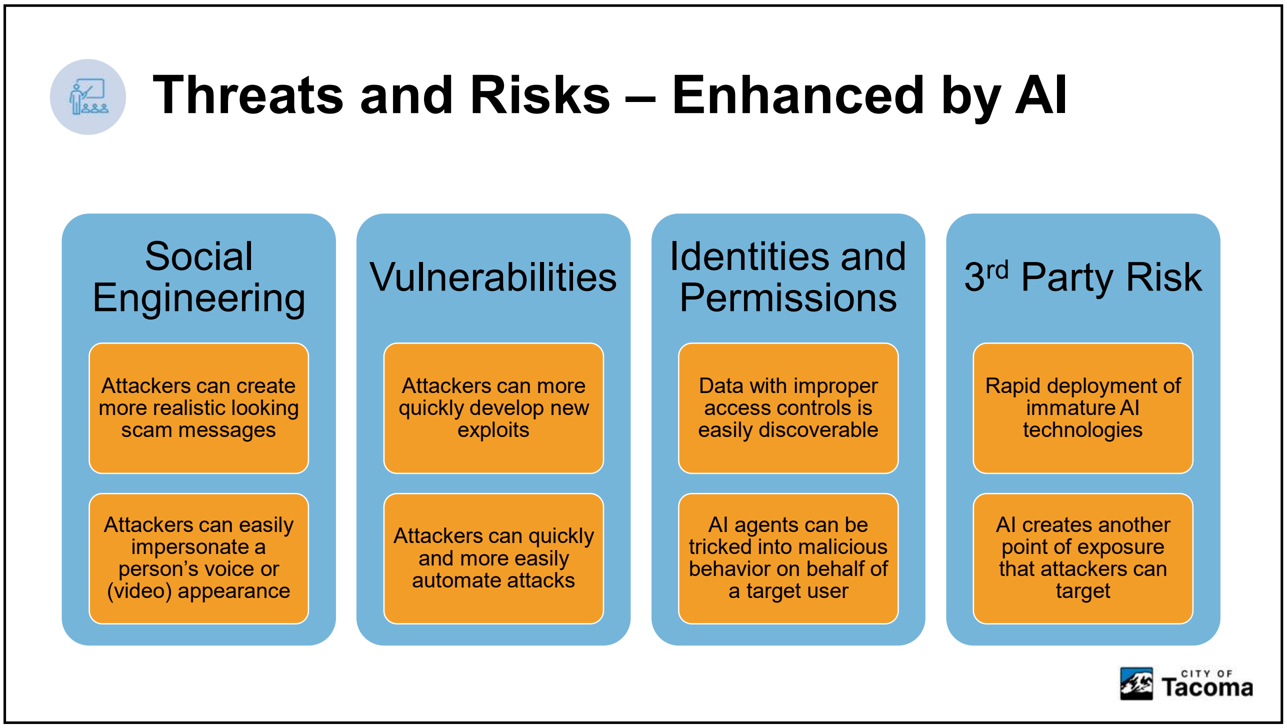
Third Party Risks

a chain is only as strong as the weakest link

- Supply chain breaches
- Contract accountability
- Code dependencies

CITY OF Tacoma

10



Threats and Risks – Enhanced by AI

Social Engineering

- Attackers can create more realistic looking scam messages
- Attackers can easily impersonate a person's voice or (video) appearance

Vulnerabilities

- Attackers can more quickly develop new exploits
- Attackers can quickly and more easily automate attacks

Identities and Permissions

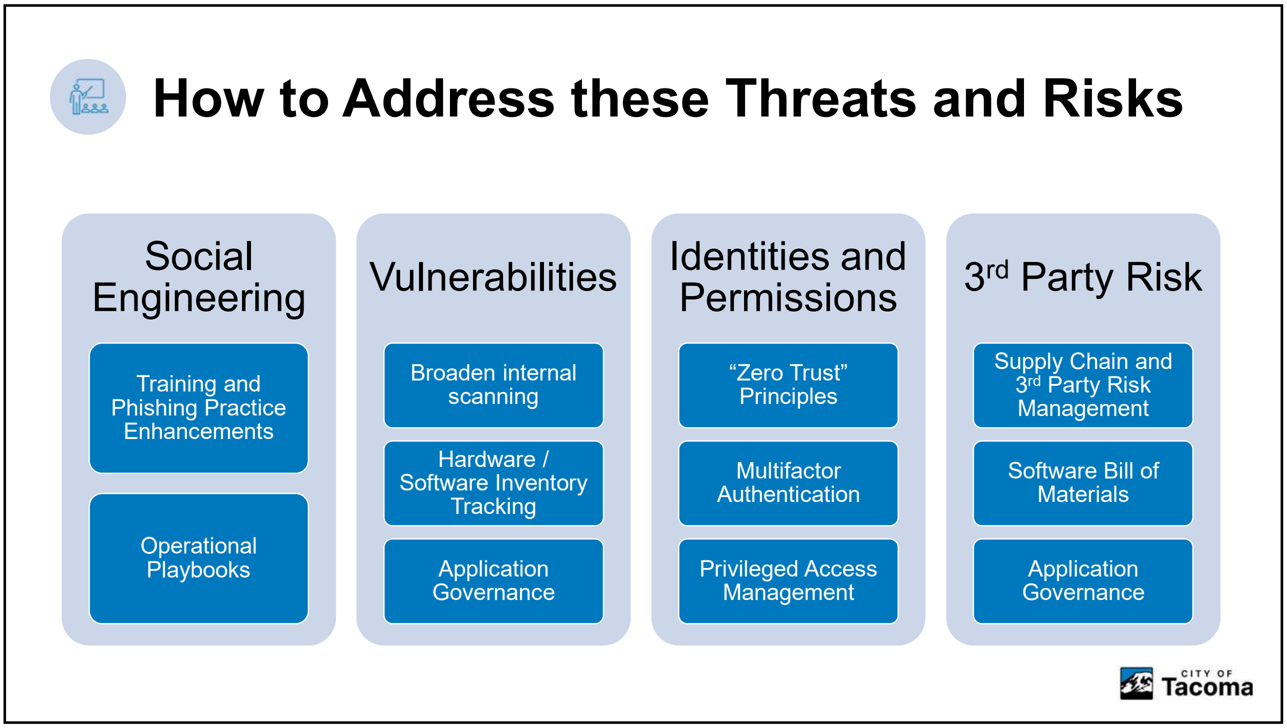
- Data with improper access controls is easily discoverable
- AI agents can be tricked into malicious behavior on behalf of a target user

3rd Party Risk

- Rapid deployment of immature AI technologies
- AI creates another point of exposure that attackers can target

CITY OF Tacoma

11



How to Address these Threats and Risks

Social Engineering

- Training and Phishing Practice Enhancements
- Operational Playbooks

Vulnerabilities

- Broaden internal scanning
- Hardware / Software Inventory Tracking
- Application Governance

Identities and Permissions

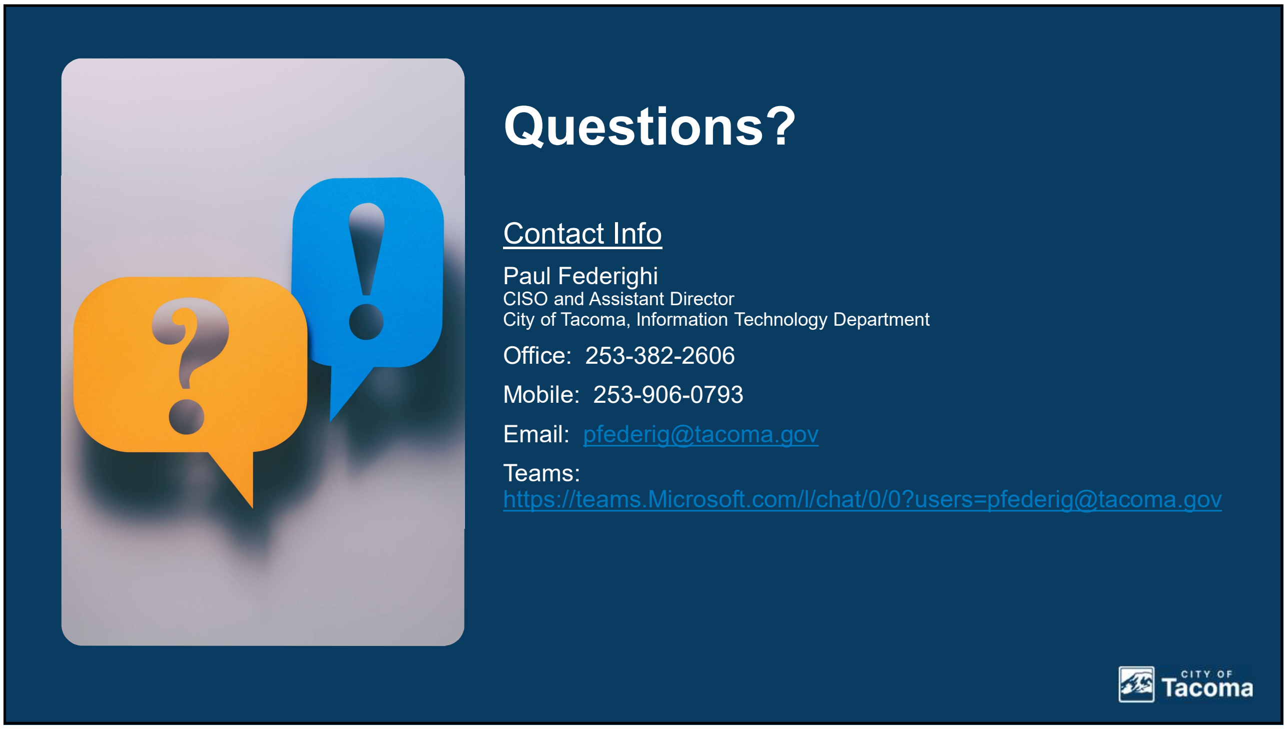
- "Zero Trust" Principles
- Multifactor Authentication
- Privileged Access Management

3rd Party Risk

- Supply Chain and 3rd Party Risk Management
- Software Bill of Materials
- Application Governance

CITY OF Tacoma

12



Questions?

Contact Info

Paul Federighi
CISO and Assistant Director
City of Tacoma, Information Technology Department

Office: 253-382-2606

Mobile: 253-906-0793

Email: pfederig@tacoma.gov

Teams:
https://teams.Microsoft.com/l/chat/0/0?users=pfederig@tacoma.gov

CITY OF Tacoma

13

14