



CENTER FOR
DIGITAL
GOVERNMENT®



Cybersecurity Transformed: From Social Engineering to Quantum

Sean McSpaden, Senior Fellow

Center for Digital Government

Center for Public Sector AI

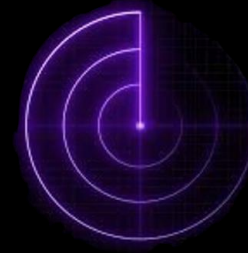
smcspaden@centerdigitalgov.com



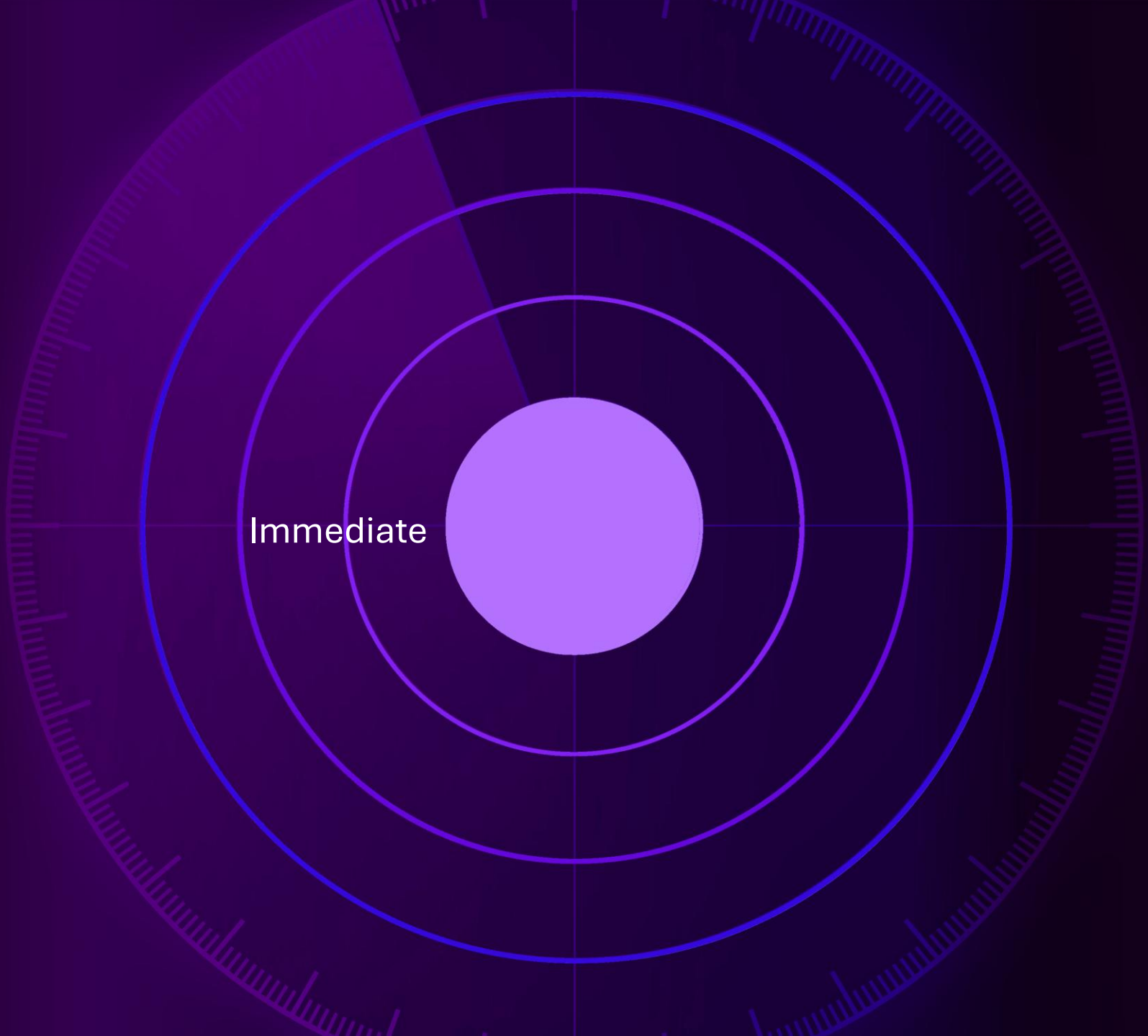
Agenda

- The 2025 Cybersecurity Radar
- Example Case Studies & Major Cyber Themes (101-style)
- Actions to Take

The 2025 Cyber Radar



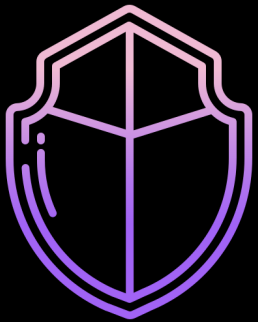






Immediate (0-1 years)

Cybersecurity & Identity Management



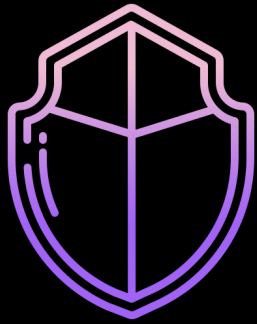
- **NEW** AI-Driven Security & Cyber Resilience
- **NEW** Passwordless Authentication
- **NEW** Zero Trust & Whole of State Cybersecurity Approaches
- Data Security & Privacy



1-2 Years



1-2 Years



Cybersecurity & Identity Management

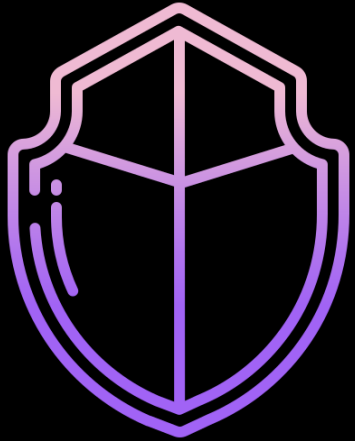
- **NEW** Decentralized Identity & Self-Sovereign Identity
- **NEW** Autonomous End-Point Management
- **NEW** Post-Quantum Cryptography
- Identity & Access Management Modernization



2-5 Years



2-5+ Years



Cybersecurity & Identity Management

- **NEW** Automated/AI Cross-Agency Incident Reporting
- **NEW** Disinformation Security
- Edge AI/Compute Resources
- Web3 Infrastructure

The 2025 Cyber Landscape



Mini Case Studies Topics

Social
Engineering

Ransomware

Endpoint
Protection

Cloud &
Identity
Security

Insider
Security /
Zero-Trust

Supply Chain
Security

Threat
Intelligence

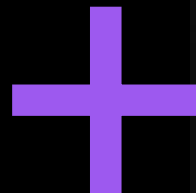
Shadow Apps /
AI / IT

Physical
Security

Post-Quantum
Security



**ANONYMIZED
CYBERSECURITY
CASE STUDY**



THE IMPACT

Case Study - **Social Engineering**



ANONYMIZED CYBERSECURITY CASE STUDY

An employee of **Agency A** received a phishing email disguised as a routine vendor request. After clicking a malicious link, attackers gained access to internal financial systems. The attackers exfiltrated budget planning documents and set up persistent access.



THE IMPACT

🛑 **Impact:** Data exfiltration,
2 weeks of remediation

💰 **Cost:** Estimated \$300,000 in
forensic investigation and system
hardening

Social Engineering – The Human Weak Link

What It Is (101):

- Manipulation of people to bypass security
- Phishing, pretexting, baiting, tailgating

Why It Matters for State/Local Gov:

- Clerks, finance staff, and elected officials are common targets
- AI-generated phishing emails are nearly undetectable
- Deepfake voicemails mimicking city managers or mayors

Action:

- Conduct mandatory phishing simulations quarterly
- Add voice authentication protocols for high-risk transactions
- Train staff to verify requests for sensitive information

May 8, 2024

FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence

SAN FRANCISCO—The FBI San Francisco division is warning individuals and businesses to be aware of the escalating threat posed by cyber criminals utilizing artificial intelligence (AI) tools to conduct sophisticated phishing/social engineering attacks and voice/video cloning scams. The announcement, made today from the RSA cybersecurity conference at the Moscone Center in San Francisco, coincides with the division's outreach efforts to include an FBI booth at the conference and participation in multiple conference panel sessions during the week of May 6, 2024.

AI provides augmented and enhanced capabilities to schemes that attackers already use and increases cyber-attack speed, scale, and automation. Cybercriminals are leveraging publicly available and custom-made AI tools to orchestrate highly targeted phishing campaigns, exploiting the trust of individuals and organizations alike. These AI-driven phishing attacks are characterized by their ability to craft convincing messages tailored to specific recipients and containing proper grammar and spelling, increasing the likelihood of successful deception and data theft.

In addition to traditional phishing tactics, malicious actors increasingly employ AI-powered voice and video cloning techniques to impersonate trusted individuals, such as family members, co-workers, or business partners. By manipulating and creating audio and visual content with unprecedented realism, these adversaries seek to deceive unsuspecting victims into divulging sensitive information or authorizing fraudulent transactions.

"As technology continues to evolve, so do cybercriminals' tactics. Attackers are leveraging AI to craft highly convincing voice or video messages and emails to enable fraud schemes against individuals and businesses alike," said FBI Special Agent in Charge Robert Tripp. "These sophisticated tactics can result in devastating financial losses, reputational damage, and compromise of sensitive data."

The FBI encourages individuals and businesses to mitigate the risks associated with AI-powered phishing and voice/video cloning by doing the following:

FBI Warns That Scammers Are Using Deepfakes to Apply for Sensitive Jobs

JULY 1, 2022

BLOG

WILMERHALE PRIVACY AND CYBERSECURITY LAW

SHARE AND DOWNLOAD



Authors



Jason C.
Chipman
PARTNER

 jason.chipman@wilmerhale.com

On June 28, 2022, the FBI issued a [Public Service Announcement](#) (PSA) warning that fraudsters are using deepfakes to impersonate job applicants during online interviews and employing stolen Personally Identifiable Information (PII) to apply for positions. Deepfakes are

Case Study - Ransomware



**ANONYMIZED
CYBERSECURITY
CASE STUDY**

This mid-sized city government, **Agency B**, was hit by a ransomware gang, shutting down all IT systems, including 911 dispatch, email, and online bill pay. The attackers demanded \$100,000 in cryptocurrency. The city refused to pay but spent heavily on recovery.



🛑 **Impact:** 3 weeks of service disruption, 911 delays, loss of public trust

💰 **Cost:** \$18.2 million in recovery and upgrades

Ransomware – A Crisis, Not a Trend

What It Is (101):

- Malware that encrypts files and demands payment for decryption
- Often enters via phishing, exposed RDP, or supply chain

Why It Matters for State/Local Gov:

- Small towns, counties, and school districts are prime targets
- Downtime hits critical services: 911, water, payroll, courts
- Increasingly tied to data theft and public extortion

Action:

- Maintain secure, offline backups and test restoration regularly
- Conduct tabletop exercises simulating ransomware scenarios
- Block common entry points: disable unused RDP, monitor VPN usage

Case Study – Endpoint Protection



ANONYMIZED CYBERSECURITY CASE STUDY

An unpatched laptop belonging to a remote employee of **Agency C** was compromised via a known VPN vulnerability. The device had local admin rights and stored cached credentials. Attackers used it as a foothold to pivot laterally through the agency's flat network, ultimately reaching finance and HR systems.



THE IMPACT

🛑 **Impact:** Exposure of employee tax info, rerouted vendor payments

💰 **Cost:** \$950,000 in financial fraud, endpoint overhaul, and network segmentation

Endpoint & Network Security – The Foundation

What It Is (101):

- Protecting laptops, phones, IoT devices, and internal networks
- Includes antivirus, firewalls, patching, VPNs

Why It Matters for State/Local Gov:

- Aging infrastructure and legacy systems create blind spots
- Smart city devices (cameras, traffic sensors) often lack security
- Public Wi-Fi and field-based workers increase risk

Action:

- Implement endpoint detection & response (EDR)
- Audit all connected devices annually (esp. IoT)
- Enforce strong configuration baselines

Case Study – Cloud & Identity Security



ANONYMIZED CYBERSECURITY CASE STUDY

Agency D migrated its document management system to a popular cloud storage service. A misconfigured sharing setting made thousands of files publicly accessible via a search engine. Documents included internal memos, budget drafts, and scanned personal IDs submitted for licenses.



THE IMPACT

🛑 **Impact:** Widespread data exposure, media scrutiny, and loss of public trust

💰 **Cost:** \$2.1 million in breach response, legal fees, and privacy settlement

Cloud Security & Identity – The Modern Perimeter

What It Is (101):

- Managing access to cloud apps and data
- Identity and Access Management (IAM), MFA, SSO

Why It Matters for State/Local Gov:

- Remote work and cloud adoption outpaced security policy
- Inter-agency access risks (justice, health, education data)
- Misconfigured cloud storage is a top breach cause

Action:

- Enforce MFA across all accounts (especially elected officials)
- Conduct cloud config reviews quarterly
- Centralize IAM across agencies with role-based controls

Case Study – Insider Security / Zero-Trust



**ANONYMIZED
CYBERSECURITY
CASE STUDY**

A recently laid-off contractor for **Agency E** retained access to internal HR systems due to a missed offboarding process. The individual downloaded confidential personnel records and later attempted extortion.



THE IMPACT

🛑 **Impact:** Exposure of sensitive employee data, potential legal action

💰 **Cost:** \$750,000 including legal settlement and IAM overhaul

Insider Threats – Not Just a Big Agency Problem

What It Is (101):

- Employees or contractors who intentionally or unintentionally cause harm
- Includes data leaks, sabotage, negligence

Why It Matters for State/Local Gov:

- High contractor turnover and lack of offboarding
- Sensitive citizen data held at DMV, housing, and courts
- Privileged access often goes unmonitored

Action:

- Automate user provisioning and de-provisioning
- Review and update privileged access policies and protocols
- Monitor for anomalous user behavior (UEBA)
- Create a clear insider threat response playbook

Case Study – Supply Chain Security




**ANONYMIZED
CYBERSECURITY
CASE STUDY**

Agency F was compromised through a third-party software update from a vendor that unknowingly distributed malware. Attackers used the backdoor to monitor internal communications and extract business and resident customer records.



THE IMPACT

 **Impact:** Loss of public trust, mandatory data breach notifications

 **Cost:** Estimated \$1.2 million in legal, audit, and containment expenses

Supply Chain Security – Trust But Verify

What It Is (101):

- Risk introduced via third-party software, hardware, or services
- Includes vulnerabilities, backdoors, and insecure integrations

Why It Matters for State/Local Gov:

- Many vendors used across agencies with little scrutiny
- Public safety tools (CAD, RMS), education platforms, and ERP systems at risk
- Recent breaches show attackers prefer supply chains to scale impact

Action:

- Require SBOMs (Software Bill of Materials) in procurements
- Vet vendors for security practices, not just price
- Monitor for unusual activity from vendor-linked accounts

Case Study – Threat Intelligence




ANONYMIZED CYBERSECURITY CASE STUDY

Agency G was notified via an ISAC alert that a known ransomware group was actively scanning for a specific vulnerability in their firewall brand. Because the agency lacked automated threat intelligence feeds and alerting, they didn't act in time. A week later, attackers exploited the exact vulnerability and encrypted critical records.



THE IMPACT

 **Impact:** Downtime in housing assistance systems, forced to pay ransom

 **Cost:** \$1.1 million in ransom, recovery, and threat hunting

Threat Intelligence – Seeing Around Corners

What It Is (101):

- Gathering and using information about current or future cyber threats
- Includes open-source intel, commercial feeds, and ISAC participation

Why It Matters for State/Local Gov:

- Threats change daily—local governments need early warnings
- Regional collaboration is key (multi-county or statewide sharing)
- Shared services and cross-agency alerts reduce blind spots

Action:

- Join MS-ISAC and actively consume/share threat reports
- Automate threat feeds into detection systems (SIEM)
- Establish a cross-jurisdictional intel-sharing framework

Case Study – Shadow Apps, AI, IT



**ANONYMIZED
CYBERSECURITY
CASE STUDY**

A department head at **Agency H** began using a free task management app (outside of IT's approval) to coordinate projects. Staff unknowingly uploaded sensitive client case files. Simultaneously, another team was using an AI chatbot to draft memos by pasting in internal briefings. The agency had no visibility or policies for either.



THE IMPACT

🛑 **Impact:** Client PII stored on unsecured third-party servers; public records violations risk

💰 **Cost:** \$250,000 in legal review, incident reporting, and SaaS filtering technology

Shadow IT, Shadow AI & Unapproved Apps – The Unseen Threat

What It Is (101):

- *Shadow IT*: Use of unauthorized hardware, software, or services outside IT's control
- *Shadow AI*: Staff using generative AI tools (like ChatGPT, Gemini) without security oversight
- *Shadow Apps*: Freemium SaaS tools (e.g., Trello, Dropbox, Canva) handling sensitive data

Why It Matters for State/Local Gov:

- Staff use AI tools to draft public statements, analyze case data, or summarize legal docs
- Sensitive citizen data copied into AI tools with unknown retention/privacy
- Risk of data leakage, compliance violations, and ethical concerns (bias, hallucinations)

Shadow IT, Shadow AI & Unapproved Apps – The Unseen Threat

Action:

- Inventory and monitor use of generative AI and unapproved SaaS
- Deploy data loss prevention (DLP) tools to flag sensitive data in AI/chat interfaces
- Publish an “approved AI use” policy: what’s okay, what’s not, and what must be reviewed.

Case Study – Physical Security



**ANONYMIZED
CYBERSECURITY
CASE STUDY**

Attackers gained access to the water treatment control system of a regional utility, **Agency I**, through an internet-exposed interface. Although no damage occurred, attackers altered chemical levels temporarily.



THE IMPACT

 **Impact:** Public safety risk, emergency shutdown of OT systems

 **Cost:** \$400,000 in response, upgrades, and public communication

Operational Technology (OT) Security – The Physical Side

What It Is (101):

- OT includes water treatment, traffic systems, utilities
- Often managed separately from IT, with older protocols

Why It Matters for State/Local Gov:

- Many OT systems are directly connected to public safety
- Legacy SCADA systems rarely patched
- State-sponsored actors actively targeting infrastructure

Action:

- Conduct an OT/ICS security risk assessment
- Require network segmentation between IT and OT
- Establish joint IT-OT incident response plans

Case Study – Post-Quantum Security



ANONYMIZED
CYBERSECURITY
CASE STUDY

Between 2023 and 2025, **Agency J**, responsible for managing court records and police body cam footage—relied on standard RSA encryption for stored files and secure transmissions. Unknown to the agency, a foreign threat actor had been quietly exfiltrating encrypted backups during a supply chain compromise.

In 2028, with access to a quantum computer, the attacker decrypted those files—revealing sealed court records, confidential law enforcement evidence, and witness identities. The leak compromised active cases, put individuals at risk, and triggered lawsuits against the agency.

🛑 **Impact:** Criminal cases jeopardized, national headlines



THE IMPACT

💰 **Cost:** Priceless – legal fallout, public safety breaches, and irreparable loss of trust

🕒 **Warning:** The breach happened years before quantum was mainstream. The damage only became clear once decryption became possible.

Quantum & Post-Quantum Readiness

What It Is (101):

- Quantum computing could break current encryption standards
- Post-Quantum Cryptography (PQC) is the future-proof replacement

Why It Matters for State/Local Gov:

- Encrypted data stolen today can be decrypted tomorrow
- Vendors will begin requiring PQC readiness in procurement
- Elections, justice, and client data systems are high risk

Action:

- Inventory systems using public-key encryption
- Start conversations with vendors about PQC timelines
- Follow NIST's PQC standardization process

Where Do We Go From Here?

Key Takeaways – Securing the Public Sector in 2025

- **Cyber threats** are evolving faster than policies – AI, quantum, and ransomware are raising the stakes.
- **People remain the most common entry point** – Social engineering, insider threats, and shadow AI must be addressed with training and tooling.
- **Legacy systems = future risk** – Aging infrastructure is a soft target for attackers. Modernization must include cybersecurity by design.

Key Takeaways – Securing the Public Sector in 2025

- **Zero Trust and Post-Quantum Readiness aren't optional** – They're foundational for long-term resilience and vendor compliance.
- **You can't secure what you can't see** – From Shadow IT to unmanaged devices, visibility is step one.

Cybersecurity is a shared responsibility – Across agencies, vendors, and the community. Leadership matters.

INSIGHTS



Call for Entries Digital Government Experience Awards 2025

The Center for Digital Government invites nominations for its Government Experience Awards, taking digital government awards to the next level by recognizing improved government constituent/customer experience!

March 12, 2025



ANNOUNCING THE DIGITAL COUNTIES SURVEY 2025

January 22, 2025



Digital Cities Survey 2024 Winners Announced

November 05, 2024



Digital States Survey 2024 Results Announced

September 25, 2024



Government Experience Awards 2024 Winners Announced

September 18, 2024

PROGRAMS

Plug in Online at govtech.com/cdg



Thank you!



Connect with me



Sean McSpaden, Senior Fellow
Center for Digital Government
Center for Public Sector AI
smcspaden@centerdigitalgov.com