Municipal Finance Institute 2025 Presentation

Incident Response and Crisis Management

SPEAKERS

Angelina Graves, Assistant City Manager	*City of Pico Rivera*
Jessica Alcaraz, Deputy Director of Administrative Services	*City of Pico Rivera*
Mohammad Ahmed, CEO	*Infinity Technologies*
Travis Nichols, Cyber Security Team Lead	*CalOES JRIC Representative*

Session Overview

WHY INCIDENT RESPONSE MATTERS TO MUNICIPALITIES

- Municipalities are increasingly targeted by ransomware, data breaches, and system outages.
- Cyber incidents threaten not just IT systems — but also budgets, credit ratings, and public trust.
- This session empowers finance leaders to lead confidently in cyber crisis scenarios.

Incident Response: A Financial Imperative

- A delayed or disorganized response can multiply financial losses and reputational damage.

- Finance leaders are critical in:
  - Approving emergency expenditures
  - Communicating with auditors and the public
  - Ensuring continuity of payroll, billing, and essential services

- Real-world California case studies show that proactive planning saves millions.

Case Study | City of Pico Rivera's Cybersecurity

BUILDING A RESILIENT CYBER RESPONSE FRAMEWORK

1. **IT Assessment Conducted** to identify vulnerabilities and system gaps.
2. **Cybersecurity Incident Response Plan (CSIRP)** developed and tailored to municipal operations.
3. **Third-Party Audits** by two independent entities validated the plan's strength and readiness.
4. **Incident Response Tabletop Exercise** held to test cross-departmental coordination.
5. **Continuous Refinement** underway to adapt to evolving threats and lessons learned.

Top Cybersecurity Best Practices for Municipalities

1. Establish a Cybersecurity Governance Framework

- Assign clear roles and responsibilities: Ensure executive leadership (e.g., City Manager, CIO, CISO) is accountable for cybersecurity oversight.
- Adopt a formal cybersecurity policy: Use frameworks like NIST, CIS Controls, or AICPA's SOC for Cybersecurity to guide policy development.

2. Conduct Regular Cybersecurity Risk Assessments

- Use tools like the GAO Cybersecurity Program Audit Guide or CISA's Cyber Resilience Review to evaluate vulnerabilities and readiness.
- Include cybersecurity in the internal control environment reviewed during financial audits.

3. Implement Strong Access Controls

- Enforce multi-factor authentication (MFA) for all critical systems.
- Apply least privilege principles to limit access to sensitive financial and operational data.

4. Prioritize Employee Training and Awareness

- Conduct mandatory cybersecurity training for all staff, especially those handling financial systems.

CONTINUED...

Top Cybersecurity Best Practices for Municipalities

5. Maintain and Test an Incident Response Plan (IRP)

- Develop a written IRP and conduct tabletop exercises regularly.
- Ensure the IRP includes financial system recovery protocols and reporting procedures.

6. Ensure Regular Backups and Patch Management

- Automate backups of financial and operational data and store them offline.
- Apply software updates and security patches promptly across all systems.

7. Monitor and Audit IT Systems

- Use continuous monitoring tools to detect anomalies.
- Include cybersecurity controls in annual financial audits or performance audits.

8. Cyber Insurance and Legal Preparedness

- Evaluate and obtain cyber liability insurance.
- Understand legal obligations for breach notification and data protection.

Lessons Learned from Real-World Breaches

- Case studies and examples from municipal / government incidents.
- Common pitfalls and how to avoid them.
- Best practices municipalities can adopt today.

Overview of Cybersecurity Risks

- **Vulnerabilities in Local Governments**
  - Local governments often use outdated systems lacking modern security, increasing cyberattack risk.
- **Common Cyberattack Vectors**
  - Phishing, ransomware, and data breaches are prevalent threats targeting government entities.
- **Impacts on Public Services**
  - Cyberattacks disrupt critical services like law enforcement, libraries, and utilities, harming communities.
- **Financial and Trust Consequences**
  - Responding to attacks strains budgets and erodes public trust in government reliability.

CASE STUDIES OF CYBER INCIDENTS

Solano County Ransomware Attack

CASE STUDY - APRIL 2024

Impact on Library Services

Ransomware attack disabled computers, phones, and Wi-Fi, halting library operations for months.

Ransom Demand and Threats

Hackers demanded $100,000 ransom and threatened to release stolen data if unpaid.

Challenges for Local Governments

Incident reveals vulnerabilities in public infrastructure and limited cyber preparedness in government.

Need for Incident Response

Prolonged downtime highlights importance of strong response plans and backup systems.

San Bernardino County Sheriff's Office Attack

CASE STUDY - APRIL 2023

Phishing Attack Vector

Attackers used a disguised phishing email to infiltrate the sheriff's office network.

Severe Data Loss

Five years of critical data was lost due to ransomware encryption.

Federal Response Effort

FBI and NSA intervened promptly to address the cybersecurity breach.

Preventative Measures

The attack highlights the importance of cybersecurity training and threat detection.

City of Oakland

CASE STUDY - 2023

Incident Overview

In 2023, Oakland faced a major data breach exposing thousands of city workers' sensitive information.

Causes of Breach

Budget limits and limited IT resources weakened cybersecurity defenses in Oakland.

Consequences and Risks

The breach led to reputational damage and potential legal liabilities for the city government.

Cybersecurity Importance

Investing in modern infrastructure, audits, and training is vital to protect public data.

CYBERSECURITY VULNERABILITIES IN LOCAL GOVERNMENT

Why Local Governments Are Vulnerable

Aging IT Infrastructure

Many local governments use outdated systems lacking modern security features, increasing their risk.

Critical Municipal Services

Essential services like water and emergency response rely on vulnerable technology that must be protected.

Sensitive Data Storage

Local governments store large volumes of personal, financial, and law enforcement data attracting cyberattacks.

Cybersecurity Training Gaps

Lack of employee training increases human error risks like phishing and weak passwords.

COMMON CYBERSECURITY PITFALLS

Typical Mistakes in Cybersecurity Strategy

Outdated Systems Risk

Relying on legacy systems increases vulnerability to modern cyberthreats and causes integration issues.

Neglected Human Factor

Ignoring employee training results in poor password habits and susceptibility to phishing attacks.

Poor User Experience

Cumbersome security tools lead users to bypass security measures, reducing overall protection.

Lack of Incident Plan

Absence of formal incident response plans causes delayed reactions and more damage during cyber incidents.

UNDERSTANDING CYBER THREATS

Most Common Cyber Threats

Ransomware Attacks

Malicious actors encrypt data and demand payment to restore access. These attacks have caused costly city disruptions.

Phishing and Social Engineering

Attackers impersonate trusted entities to steal credentials or deliver malware through deception.

Data Breaches

Sensitive personal and financial information is exposed or sold, risking privacy and security.

Infrastructure and IoT Attacks

Emerging threats target smart city tech, risking public safety and causing service disruptions.

PREVENTATIVE MEASURES

How to Avoid Cyber Attacks

Multi-Factor Authentication

MFA adds an extra layer of security to user accounts, reducing unauthorized access risks.

Regular Software Updates

Patching and updates close vulnerabilities and prevent attackers from exploiting known weaknesses.

Poor User Experience

Security Operations Center as a Service enables continuous monitoring and rapid incident response.

Employee Training and Response

Training programs reduce human error and incident response plans ensure quick recovery from attacks.

STRATEGIC RECOMMENDATIONS

Best Practices & Recommendations

Framework Alignment

Aligning with frameworks like NIST provides a structured approach to managing cyber risks.

Continuous Monitoring

Real-time monitoring and threat detection minimize damage and reduce downtime.

Public-Private Partnerships

Collaborations enhance threat intelligence sharing and access to advanced security technologies.

Workforce Training

Investing in training ensures IT teams can handle evolving cybersecurity threats.

Summary and Call to Action

Cybersecurity Importance

Local governments handle sensitive data and must prioritize cybersecurity to protect public services.

Identified Threats

Key vulnerabilities and common cybersecurity threats facing municipalities have been highlighted.

Strategic Recommendations

Implement proactive measures and leverage state resources and partnerships to strengthen defenses.

Call to Action

Foster a security culture and adopt best practices at all organizational levels.

INSIGHT AND RECOMMENDATIONS

Key Lessons Learned

System Vulnerabilities

Outdated systems and limited budgets increase local governments' exposure to cyberattacks.

Centralized Cybersecurity Services

24/7 monitoring and threat detection improve resilience through centralized SOCaaS.

Incident Response and Backups

Planning and regular backups minimize downtime and prevent data loss during attacks.

Employee Training and Insurance

Training prevents phishing attacks; cyber insurance mitigates financial risks.

Recommendations for Local Governments

1. Invest in Modern Infrastructure

Local governments should upgrade cybersecurity infrastructure to defend against evolving threats effectively.

2. Employee Training Programs

Comprehensive training equips employees to recognize and respond to cyber threats responsibly.

3. Utilize State-Supported Services

Leveraging services like SOCaaS offers scalable, cost-effective cybersecurity protection.

4. Implement Technical Controls

Patch management and network segmentation reduce breach risks and limit attack impacts.

Coordination with State and Federal Agencies During Incidents

- Role of Cal OES and federal support structures
- Funding, compliance, and reporting obligations
- Communication channels and collaboration in crisis
- Threat Sharing (Anomaly)
- Regional Cyber Coalition (JRIC AOR No Cost Anomaly sharing to other cities)

CAL-CSIC 101

OVERALL TLP RATING: TLP: CLEAR

Briefed by:
Travis Nichols, Cyber Advisory Team Lead

Date:
10, December 2025

Agenda

- Cal-CSIC Mission, Vision and Tasks
- California Fusion Centers
- Cal-CSIC Structure
- Cyber Threat Intelligence Branch
- Cyber Operations Branch
- Mission Support Branch
- State & Local Cybersecurity Grant Program
- California Cybersecurity Task Force
- Q&A / Discussion

Mission

CAL-CSIC

Reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in the state.

Vision

CAL-CSIC

Through cohesive partnerships for sharing critical threat intelligence, providing premier advisory services and dynamic incident response, as well as delivering industry leading training, the Cal-CSIC empowers California to defend against evolving cyber threats while prioritizing sectors that provide the greatest public, governmental, and economic value.

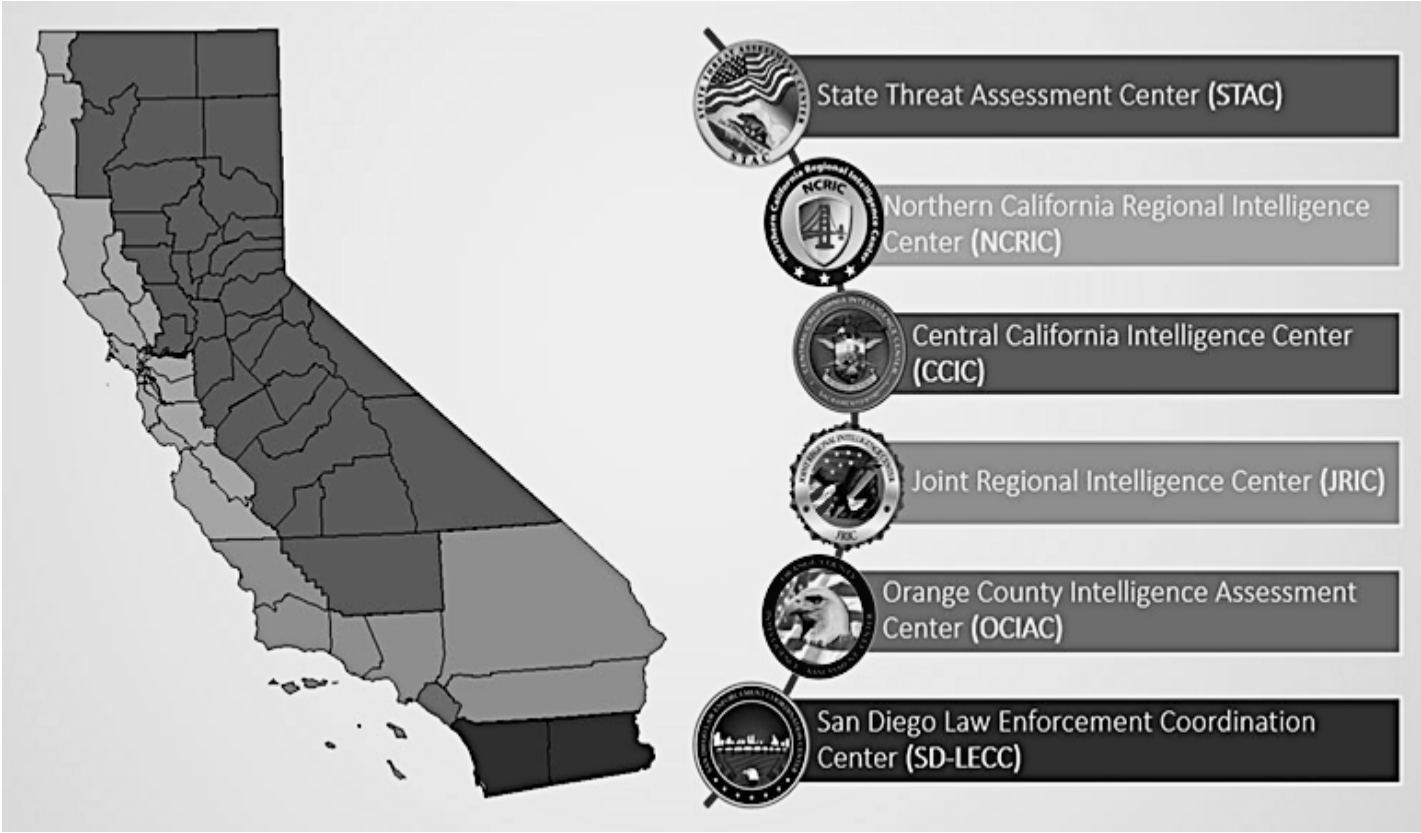
CAL-CSIC Tasks

CAL-CSIC: Four Core Pillars

CA Fusion Centers

What the Fusion Centers Offers:

- Local Relationship
- Quick Reaction Times
- Multi-Agency Support
- Federal Law Enforcement (DHS, FBI)
- Local Law Enforcement
- Intel Analysts
- Cal-CSIC



CAL-CSIC Structure

- Operations
- Cyber Threat Intelligence
- Mission Support

Cyber Threat Intelligence Branch

PREPARING THE CAL-CSIC & CALIFORNIA FOR THE FUTURE OF CYBER THREATS

- Collection Management
- Strategic Intelligence Reporting
- Threat Monitoring & Notification
- Vulnerability Awareness
- Incident Response Support

Cyber Operations Branch (OPS)

Conducts both proactive and reactive cybersecurity.

Digital Forensics & Incident Response

- Incident Response
- Digital Forensics
- IOC Feed to Intel

Cyber Advisory Team Services

- Program & Security Assessments
- Advisory Briefings & Threat Awareness
- External & Internal Vulnerability Scans
- Advocacy Support
- Remediation Roadmaps
- Attack Surface Management

CSIC Efforts to Improve Statewide Cybersecurity

Statewide Attack Surface Management Program

STRONGER TOGETHER

- Gain Unified visibility of internet-facing assets across California
- Receive early warnings about vulnerabilities before exploitation

ACTIONABLE SUPPORT

- Cal-CSIC and Fusion Centers provide overwatch for your AOR
- Receive prioritized alerts based on urgency and severity

AGENCY ROLE

- Provide entity contacts and asset inventory
- Validate alerts and act on remediations
- Partner with Fusion Centers and CSIC for ongoing security posture improvement

Intelligence Sharing via Threat Intelligence Platform

AUTOMATED INTELLIGENCE SHARING: INDICATOR OF COMPROMISE EXCHANGE

- Integrated into 9 different cyber defense tool types with capability for many more (Crowdstrike, Splunk, MS Sentinel, Cisco firewall, TAXII, API)
- Tracking 14,500 Malicious IOCs from Incident Response and CAL-CSIC collections in 2024
- ~ 130 different sources currently ingesting
- CDT integration supporting SOCAAS
- CAL-CSIC Curated Feed
- Over 200 active automated processes

Operational Technology (OT) & Industrial Cybersecurity Services

OUR FOCUS

- Network and Environment hardening for OT equipment
- Expansion from electric sector into water operations
- Organizational Evaluations

APPROACH

- Surveys: Cybersecurity & OT Infrastructure
- Analysis: Network Capture & Physical Walkthrough
- Out-of-band, zero production impact

OUTCOMES

- Asset inventory & vulnerability identification
- Malicious traffic detection
- Tailored remediation & hardening
- Sector-specific threat intelligence

Mission Support Branch

Provides Support, Services, and Tools to Achieve the Cal-CSICs Mission

- Partner Integration
- Information Technology Engineering
- Cyber Policy and Strategy Planning
- Facilities, System Engineering & Development
- Training Coordination
- Metrics Reporting & Governance
- Operational Technology Lab Support
- Business Administrative Support

Join the California Cybersecurity Task Force (CCTF)

Be part of California's prominent cybersecurity advisory body!

BENEFITS

- Shape California's cybersecurity initiatives
- Collaborate and network with California cybersecurity professionals

WHO CAN JOIN

Open to California cybersecurity professionals, including: Federal, State, Local, and tribal government, private industry, academia, and non-governmental organizations.

JOINING THE CCTF

Email calcsic@caloes.ca.gov and put [California Cybersecurity Task Force inquiry] in subject line.

State & Local Cybersecurity Grant Program (SLCGP)

- SLCGP provides funding to state, local, and territorial (SLT) governments to manage and reduce systemic cyber risk.
- Total funding available for fiscal year 2025: $4 million

For more information see:
https://www.caloes.ca.gov/SLCGP

Who's eligible?

6 U.S.C. § 101(13)

- Tribal Governments
- Other Public Entities
- Counties
- Cities
- Towns
- Rural Communities
- Unincorporated Towns
- Municipalities
- School Districts

RESOURCES

CONTACT INFO

Phone

(833) REPORT-1
(916) 636-2997

Cal-CSIC Main Email

calcsic@caloes.ca.gov

Location

10390 Peter A. McCuen
Building D
Mather, CA 95655

Cybersecurity Resources

- **Center for Internet Security (CIS) controls**: https://www.cisecurity.org/controls/cis-controls-list/
- **National Institute of Standards and Technology (NIST) Cyber-security Framework:** https://www.nist.gov/cyberframework
- **MITRE ATT&CK Framework:** https://attack.mitre.org/resources/getting-started/
- **Cal-CSIC Intel products and Monthly Threat Briefs**: https://www.caloes.ca.gov/cyber/
- **Security Operations Center as a Service (SOCaaS):** https://cdt.ca.gov/services/security-operations-center-as-a-service-socaas/
- **Cal-CSIC Website:** https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/california-cybersecurity-integration-center/

THANK YOU FOR YOUR TIME!

DATE: **10, December 2025**

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

Q&A

Resources

MUNICIPAL INCIDENT RESPONSE AND CYBERSECURITY READINESS

Thank You