

ACWA 2026 SPRING CONFERENCE

Why the Current Cyber Posture Is Failing **Public Sector Agencies**

And What True Cyber Defense Looks Like

Frank Ury

VP, Santa Margarita Water District

SHIFTING FROM PERIMETER DEFENSE TO CONTINUOUS BREACH RESPONSE

About



Frank Ury

- VP, Santa Margarita Water District
- 20 yrs public service | 30+ yrs IT leadership
- Former Councilmember & Mayor, Mission Viejo
- Senior roles at DXC, HP Enterprise, Intel
- OC Transportation Authority | SCAG Big Data
- Catholic Charities OC — Board Member
- BSEE Notre Dame | MSEE USC | MBA UC Irvine

OCTA Ransomware Attack

February 4, 2016 | Orange County Transportation Authority

88

Servers
Compromised

\$700K

Taxpayer
Cost

60 hrs

Systems
Down



Transparency Failures

- Attack described publicly as "technical problems"
- No public disclosure for six months
- \$218K in emergency contracts with no public discussion



Systemic Weaknesses

- Grand jury: IT staff "largely untrained"
- Outdated job classifications for cyber talent
- No cybersecurity strategic plan at time of attack
- No audit schedule for third-party vendors

Sources: OC Register (Aug 2016) | Voice of OC (Aug 2016) | OC Grand Jury Report (Jun 2017)

Cybersecurity in 2026: The Numbers Don't Lie

\$10.22M

Avg US Breach Cost
2.3x world average

\$10.5T

Global Annual Loss
Projected 2025

241

Days to Detect
& Contain



Top Attack Vectors

- Phishing — 49% of businesses targeted
- Stolen credentials — 80% of breaches
- Ransomware — attacks tripled YoY
- Supply chain attacks doubled in early 2025



Nation-State Threats to CA

- Iran — targeting water & energy
- China — persistent espionage (Volt Typhoon)
- Russia — hacktivist proxies, OT attacks
- AI-orchestrated espionage now documented

The Cost of Inaction — Time / Event Horizon

\$10.22M

US Avg
Breach Cost

241 days

Avg to Detect
& Contain

-80 days

With
Security AI

25%

Are
Ransomware

-\$1.76M

Savings
with AI

Key Insight

Organizations that deploy security AI and automation save an average of \$1.76M per breach and detect threats 80 days faster. The data is clear: proactive, AI-augmented defense dramatically reduces both cost and exposure time. Every day without continuous monitoring is a day of compounding risk.

The Traditional Model

X

Outdated. Reactive. Failing.

- X Hardening perimeters to prevent initial compromise
- X One-time investments in defensive walls
- X Reactive posture — respond only after detection
- X IT and OT security managed in separate silos
- X Security treated as a technical issue, not operational risk



MTTD (Mean Time to Detect) and MTTR (Mean Time to Respond) — now the leading indicators of cyber resilience.

The Assume Breach Model



Proactive. Continuous. Resilient.

- ✓ Breaches are inevitable — focus on rapid detection
- ✓ Continuous, adaptive, enterprise-wide risk management
- ✓ Proactive posture — hunt for threats before they act
- ✓ Integrated IT and OT security governance
- ✓ Cybersecurity as operational risk, board-level oversight

MTTD (Mean Time to Detect) and MTTR (Mean Time to Respond) — now the leading indicators of cyber resilience.



SOUND FAMILIAR?

The Most Dangerous Mindsets in Cybersecurity



"We're Fine"

The most expensive phrase in cybersecurity. Oakland, OCTA, Oldsmar all thought they were fine.



False Positive Overload

When every alert is noise, real threats get buried. Alert fatigue is the #1 reason breaches go undetected for 241 days.



California Depends on You

Water, transportation, public services — every city in this room runs infrastructure millions depend on.



So What Does True Cyber Defense Look Like?

From alert volume to outcomes. From reactive monitoring to active defense.

The Mindset Shift

Continuous Breach Detection & Automation



Critical Thinking

Don't listen to third parties blindly. Question the model. Challenge assumptions.



Test Your Security

Run pen tests. Validate your controls actually work. Trust but verify.



Military Mindset

Hunt door-to-door. Don't wait for alerts. Proactive threat hunting continuously.



Be an Illusionist

Deploy deceptions and lures to trick attackers into revealing themselves.

Create an environment where the threat actor bumps into something. Detect once inside. Validate. Isolate. Respond.

6 Active Defense Strategies

Building cyber defense with outcomes, not noise

01 Strong Outer Shell

MFA, patching, NGFW, email/web filtering. Block commodity noise so analysts can focus on real threats.

02 Post-Breach Malware Detection

EDR + NDR across endpoints, network, cloud, OT, mobile. Multiple independent detection layers.

03 Human Adversary Detection

Deceptions, lures, moving-target defense. Expose lateral movement. Zero false positives by design.

04 Forensics Capability

Full packet capture. Reconstruct attacks completely. Preserve endpoint, network, and SIEM evidence.

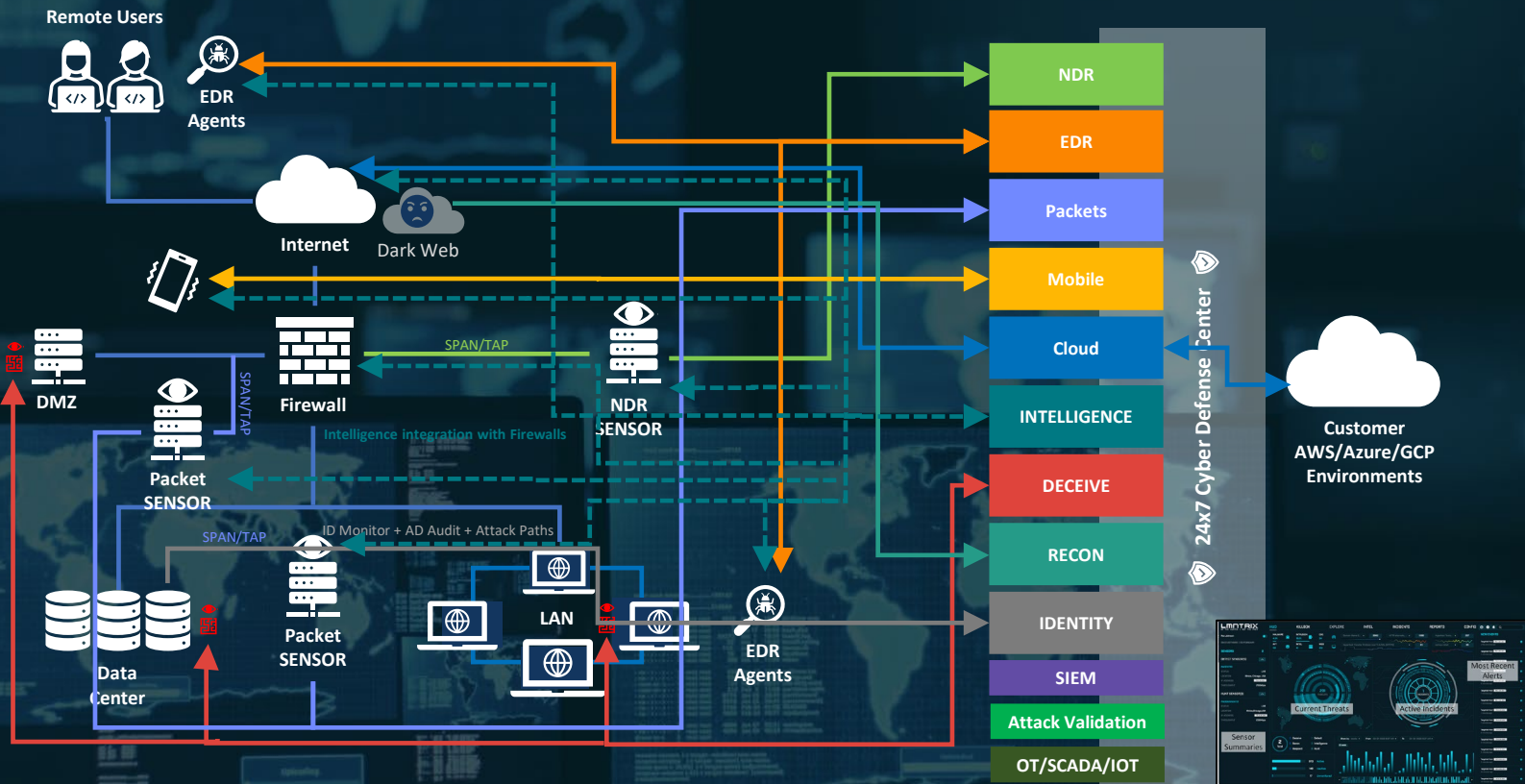
05 Assume Breach & Hunt

IOC hunts hourly. IOA behavioral hunts continuously. 200+ threat hunts mapped to MITRE ATT&CK.

06 Validate & Automate

Validate every threat. Auto-push intel to firewalls. Respond in seconds, not hours. Close the loop.

LMNTRIX XDR Platform



What Boards & Elected Officials Need to Understand



It's an Operational Risk

Cybersecurity is a core operational risk requiring the same governance as financial risk, safety, and infrastructure. Not just an IT problem.



Funding Must Be Continuous

One-time capital investments in firewalls are over. Defense needs ongoing operational funding — just like maintaining roads and bridges.



Accountability Is Shared

Technical teams, managers, and boards must all share understanding. Cross-training is essential. The OCTA grand jury made this clear.

Advanced Technologies for Resilient Defense: Remote Remediation, Host Isolation, and Continuous Threat Hunting are now table stakes.

Recommendations for Leadership

1

Adopt Assume-Breach Governance

Cybersecurity is an operational risk, not just technical. Board-level visibility and accountability.

2

Invest in Continuous Monitoring

MTTD and MTTR as core performance indicators. Target < 1 minute detection.

3

Prioritize Cross-Training

Ongoing dialogue between technical teams and boards. Break down the IT/OT silo.

4

Leverage Federal Partnerships & Grants

Shared intelligence, CISA resources, consortium efforts, and piggyback contracting.

5

Plan for Resilience, Not Just Defense

Cyber contingency plans for treatment plants, SCADA systems. Tabletop exercises quarterly.

Information security is managing risks to the confidentiality, integrity, and availability of information.

This is no longer an IT risk — it has business implications.

While organizations aren't in the business of securing information, they won't stay in business if they get it wrong.

Assume Breach. Hunt It Out.

Eliminate The Vulnerability.