

## What's your biggest ongoing project?

As a CISO of an organization with 48,000 full-time employees, I am responsible for overall cybersecurity strategies and initiatives to protect city's critical digital assets supporting 4 million residents. Of the many accomplishments, the Integrated Security Operations Center (ISOC) is most noteworthy. The \$1.8 million facility consolidates all departmental cybersecurity into one central system, monitored 24/7 and incorporates advanced technologies such as a Security Operations/Incident Management System, Posture Dashboard, Alert Indicator, and Threat Analysis Platform. This provides real-time awareness of cyberthreats across all departments. In addition, the Threat Intelligence Portal (TIP) coordinates collaboration and response between city departments, the FBI, and Multi-State Information Sharing and Analysis Center (MS-ISAC). This partnership is critical to immediate threat resolution, provides early warning to state/federal agencies (to protect other municipalities) and rapid response capabilities. ISOC started with managing around 3 million citywide security events per week in 2015. Today around 1 billion security records per day are added to ISOC for correlation and analysis. In 2016, ISOC successfully detected and blocked 40 ransomware attacks and stopped about 49,000 botnets.

## What's the best cybersecurity decision you ever made?

The best cybersecurity decision I ever made is establishing the Cybersecurity Strategy based on the NIST CSF (Identify, Protect, Detect, Response and Recover).



## Rob Lloyd

**Chief Information Officer**  
**San Jose, California**

**We use cookies** to provide you with the best experience across all Scoop News Group websites. By using Scoop News Group websites, you consent to the use of cookies. [Learn more](#)

**GOT IT!**

CIO for the City of San Jose. I'm sharing the CISO role with one of our senior managers as we stand up our Information Security Office. I was previously CIO and CISO for City of Avondale, Arizona; CIO and utility director for City of Ashland, Oregon, and chief of information technologies for Colorado Parks and Wildlife.

### **What's your biggest ongoing project?**

In the realm of cybersecurity, it's standing up our Information Security Office. We've phased the work plan into three segments: immediate needs, maturity and excellence. It focuses on outcomes and spans building around a NIST CSF policy and processes; human-centered vigilance; contracting and purchasing standards; a cybersecurity-as-a-service model for maximum signal through the noise without an armada of hard-to-fill positions; vSOC; joint procurement with peer governments for cybersecurity services and contracts; talent development; intelligence sharing; and joint work with the cyber threat alliance we are a part of (ACTRA).

### **What's the best cybersecurity decision you ever made?**

The decision to be part of and contribute to ACTRA. In this environment, it takes a network to beat a network. The alliance is a group of major local government, federal, private sector, academia, and utility partners contending against the malicious actors across the globe. ACTRA gives us early insights, monitoring, cross-sector information sharing, a talent development channel, and a partnership for joint response if any of us runs into something dire. Organizations that stand alone will not survive, and allying was an early smart direction some of us made.

---

## **John MacMichael**

**Chief Information Security Officer**  
**Washington, D.C.**

**We use cookies** to provide you with the best experience across all Scoop News Group websites. By using Scoop News Group websites, you consent to the use of cookies. [Learn more](#)

**GOT IT!**