Category
State CIO Special Recognition

State
California

Contact
Amy Tong
Chief Information Officer
California Department of Technology
Amy.Tong@State.Ca.Gov
916-319-9223

Project Initiation/Completion
December 2016 – December 2017

Executive Summary

Hacking, *Malware*, *Phishing*, *Ransomware*, *Denial of Service*, *Brute Force Attack*…just a few of the terms that have become common place within the cyber world in just a few short years. Hardly a day goes by that a private or public sector entity has not made the news for their information technology (IT) security…unfortunately the publicity is not positive. From small business to the largest Fortune 500 companies, the effects of cybercrime are far-reaching and costly. These costs are not just financial. Breaches and service disruptions have a devastating impact on the trust of the constituents we support – the stakes could not be higher.

In response, California has taken a unique collaborative whole of government approach to the ongoing threats that face the State's assets with ***California's Cybersecurity 4-Core partnership.*** The partnership is between the California Department of Technology (CDT), the California Governor's Office of Emergency Services (Cal OES) - California Cybersecurity Integration Center (Cal-CSIC), the California Highway Patrol (CHP) and the California Military Department (CMD). **Each of the core partners plays a distinct and critical role in the detection and protection of the state cybersecurity assets and data.**

The launch of CDT's statewide Security Operations Center (SOC) is the most recent addition to California's cyber defenses and is believed to be one of the few SOCs of its type in state government within the United States. What started as a vision in December of 2016 quickly became reality July 2017 with the launch of this new and critically beneficial capability. The SOC monitors the California Government Enterprise Network (CGEN), California's Wide Area Network that traverses the state, while interacting with the 4-Core partners in the exchange of critical cyber intelligence to defend the state's critical infrastructure and data.

Cal OES (Cal-CSIC) recently released the California Joint Cyber Incident Communications Framework, which clearly articulates the coordinated process for communicating and reporting cyber incidents to all state, local, tribal, territorial and private sector organizations once they occur. Additionally, the Cal-CSIC released the California Joint Cyber Incident Response Guide to assist all California entities, both public and private, to understand the identification, reporting and recovery procedures adopted by the state of California. This is a step-by-step "How to" Guide that any entity can use as a foundation to develop their own Cybersecurity Incident Response Plan should they become victim of a cyberattack.

Each of California's Cybersecurity 4-Core teams specialize in individual areas of cybersecurity response and expertise to strengthen the state's cybersecurity posture while communicating between each other and with external partners across the country. The specific cybersecurity capacities for each of the partners are as follows;

California's Cybersecurity 4-Core

- **CDT** – Security Operations Center (SOC); Statewide Network Monitoring
- **Cal OES** – Cal-CSIC; Incident Response, Threat Intelligence and Analysis
- **CHP** – Computer-Related Crimes and IT Security Incident Investigation
- **CMD** – Independent Security Assessments (ISAs), technical security controls

Through proactive leadership, California continues to overcome information security challenges that threaten its technology infrastructure and vast information assets. These security programs continue to expand and mature to mitigate increasingly sophisticated cybersecurity threats as the 4-Core continue to expand the State's detection and protection capabilities through continuous improvement.

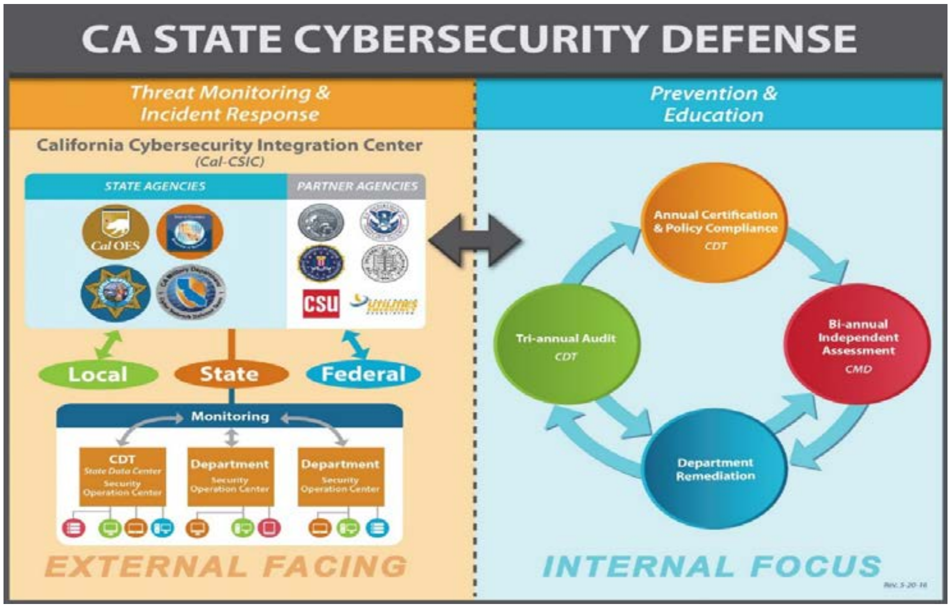
Business Problem

California is home to nearly 40 million people, has the 5th largest economy in the world, and has nearly 140 different state entities. The state's enterprise network (CGEN) provides the infrastructure support for these entities' critical data exchange in support of their services to the state's constituents which include highly sensitive data connected to health, safety, education, transportation, critical infrastructure, and the economy. This data is entrusted by the public to the state to be kept confidential and safe. Providing security to this infrastructure and its critical assets is no small task in today's environment of constantly evolving cyber threats.

The CGEN is the main pipeline into the state's datacenter, which houses the multitude of applications that support the state – Health and Human Services, Department of Motor Vehicles, Public Safety, and other highly critical systems to state government and its constituents. Malicious attackers from all over the world are constantly scanning the network to discover vulnerabilities. Intrusion detection and prevention technologies have long been an integral defense to these attempts, but the ability to immediately identify issues and communicate with our state partners within the Cybersecurity Information Center (Cal-CSIC), California Highway Patrol (CHP) and the Military Department (CMD) was not present.

The world of cyber terrorism is ever evolving and communication is critical in defending the state assets. Delays in communicating significant cyber information with our critical partners allows the bad actors to have an advantage in damaging state assets. As mentioned previously, this not only incurs monetary costs to the state, but perhaps even more importantly damages the trust of the constituency we support. As we move to provide more public services online it is of the upmost importance to ensure public trust in utilizing those services. Restoring public trust is not an easy task and as service providers it is the highest importance.

Cybersecurity is a team effort. The significant uptick of reliance on the CGEN network for core defensive protections by our state entities highlights the continued critical importance of the 4-Core partners to the overall defensive strategy. The multitude of state entities relying on the safety and security of the data traversing the state on the enterprise network and increasingly malicious activities, the OIS and 4-Core partners realized the importance of strengthening the security around the state's network.



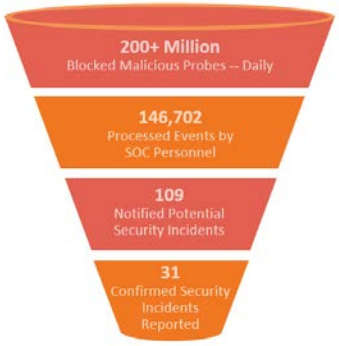
CA STATE CYBERSECURITY DEFENSE
Threat Monitoring & Incident Response
Prevention & Education
California Cybersecurity Integration Center (Cal-CSIC)
STATE AGENCIES
PARTNER AGENCIES
Cal OES
CSU
Local
State
Federal
Monitoring
CDT State Data Center Security Operation Center
Department Security Operation Center
Department Security Operation Center
EXTERNAL FACING
Annual Certification & Policy Compliance CDT
Bi-annual Independent Assessment CMD
Department Remediation
Tri-annual Audit CDT
INTERNAL FOCUS
Rev. 5-20-16

At the time, each entity was charged with monitoring their individual levels of security. As you can imagine this was a challenge with nearly 140 entities with varying levels of security expertise, staffing, and funding to support the tasks. It was imperative to take action to both break down these silos as well as address the massive threat to the state by utilizing a "whole of government" approach.

This approach matriculated into the 4-Core partnership, which was modeled after the Federal Department of Homeland Security – Department of Defense – and Federal Bureau of Investigations strategy. The plan leveraged the individual unique jurisdictional areas for each of the 4-Core team and utilized the California Compliance and Security Incident Reporting System (Cal-CSIRS) which was developed to facilitate the rapid reporting and notification of computer-related crimes and information IT security incidents by state agencies. The Cal-CSIRS system provides notifications to the CHP Emergency Notification and Tactical Alert Center (ENTAC) and the Computer Crimes Investigation Unit (CCIU).

The Security Operations Center (SOC) utilizes intrusion detection and prevention technologies as well as other specialized technologies to monitor network traffic within CGEN. Each day the SOC blocks over 200 million malicious probes to the network, and has processed nearly 150,000 events, notified entities of over 110 potential security incidents, and detected and reported nearly 30 confirmed security incidents. Detecting and preventing these malicious attacks to the states assets has not only saved money from the fallout of potential breaches and loss of data but also helped ensure that the state remains a trusted entity in our citizens lives.

Malicious Activity Detected by the Security Operations Center Since Inception



The number of malicious activities detected by CDT's Security Operations Center (SOC) targeting the California Government Enterprise Network (CGEN) and other State IT systems

The **California Cybersecurity Integration Center** partnerships include other Federal, State and private sector partners including the Federal Bureau of Investigation (FBI) and the United States Department of Homeland Security (DHS) in addition to the 4-Core and are charged with the following tasks for the state:

1. Cyber Incident Response Coordination
2. California Automated Indicator Exchange
3. Phishing Email/Malware Analysis
4. Strengthen the state's cybersecurity strategy.

Each partner provides experts to the Cal-CSIC, which serves as the central organizing hub of the State's cybersecurity activities. The Cal-CSIC is co-located with the California State Threat Assessment Center (STAC), which serves as the State's primary fusion center with responsibility to protect the State from terrorist and other physical threats. With its core partners, the Cal-CSIC established multiple capabilities to accomplish its mission.

Collectively established by the 4-Core partners, the California Cybersecurity Integration Center (Cal-CSIC) is staffed with members from each of the partners to provide constant monitoring and active communications between CDT, OES, CHP, and CMD. Additional partners that either have a presence or work closely with the Cal-CSIC include; Federal Bureau of Investigations, the Department of Homeland Security, the California Department of Justice, the California State Universities (CSU), University of California (UC) system, Community Colleges, United States Coast Guard, Health & Human Services, the statewide Fusion Centers, and the California Utilities Emergency Association as well as other state and local governments and private sector entities such as statewide utilities, infrastructure and safety.

The Cal-CSIC is able to monitor in real-time global cyber threats; assess the potential impact to California's economy, critical infrastructure, and public and private sector networks statewide; then prioritize and alert affected entities. In less than two years of being operational, the Cal-CSIC—including its 4-Core agencies—has established itself as a national leader and example that other states are emulating.

The **California Military Department (CMD)** supports these efforts in several ways. The Cyber Network Defense (CND) Team, which is comprised of cybersecurity professionals is focused on providing the states Independent Security Assessments (ISA). These assessments provide a third-party view of the entity's current cybersecurity state and analyze the following foundational areas:

1. Host vulnerability assessments
2. System Hardening analysis
3. Firewall analysis
4. Phishing Susceptibility Testing
5. Network Penetration testing
6. Network Traffic Analysis for Indicators of Compromise

These areas of support complement the existing CND support missions to provide assist the Department of Defense, Federal, State, Local Government partners, and Critical Infrastructure providers to provide confidentiality, integrity, and availability of critical network infrastructure. In addition, the CMD team also provides support and assistance through established partnerships with cybersecurity vendors, academia, and government entities.

The CMD supports the Core-4 efforts by supplementing key positions within the SOC and Cal-CSIC with highly qualified analysts. The CMD currently provides SOC Analysts and Open-Source Cyber Threat Analysts. This effort leverages Department of Defense cyber training, civilian education, and civilian acquired skills to support 24X7 State cybersecurity operations. The CMD can also be called upon to provide incident response and recovery for Department of Defense, Federal, State, Local Government, and Critical Infrastructure partners.

The **California Highway Patrol (CHP)** has primary investigative authority for computer crimes against state agencies. The CHP's Computer Crimes Investigation Unit (CCIU) was formed with the primary mission of conducting investigations of criminal activity involving the State of California's computer assets. The unit not only provides service to and investigates cyber-crimes against state agencies and departments, but also delivers technical investigative support to the CHP's own Investigative Services Units, local area CHP offices and local police and sheriff's departments when requested.

The CHP employs a multidisciplinary team of experienced trained investigators that are cyber forensic examiners and network security experts. The CCIU investigators are cross-sworn US Marshalls and are members of the Sacramento FBI Cyber Crimes Task Force. This Federal collaboration provides information sharing on an international level since suspects in cybercrimes can operate from anywhere in the world. The CHP also partners with the California Department of Justice's eCrimes Unit, Office of Digital Investigations, and Bureau of Forensic Sciences.

The most common types of cyber-crimes that CHP investigates includes the following:

1. Phishing
2. Email Scams
3. Disruption of Services
4. Network Intrusions
5. Theft of Personal Information
6. Employee misconduct
7. Other criminal investigations

As intelligence is developed during investigations, information is shared with the 4 core partners to allow for proactive activities to prevent further incidents and reduce the impact and spread of incidents. Cal-CSIC widely shares information like the indicators of compromise so other can implement proactive protective measures and the CDT SOC can use the information to protect California's CGEN network.

Significance

The 4-core partnership is the most critical element in counter cyber threats to the state's operational enterprise. The partners represent the first line of defense against all levels of threat ranging from organized criminal syndicates bent on stealing or holding data for ransom to advanced persistent threat nation states who are laying the ground work for something worse or stealing intellectual data for their own use. Following the tragic ransomware attacks against Colorado and Georgia this year it is readily apparent that not having "all hands on deck" when it comes to countering cyber-threats leaves one's citizens data and way of life open to attack from malicious actors.

It is also important to note that these partnerships do not just extend to state government entities but, through the CAL CSIC integration, to the Federal, Local, Educational and municipalities as well. Each partner has a role to play and if one is unable to fulfill their role the state is put at risk.

Impact

The effectiveness of the partnership is apparent through the success stories below;

The Security Operations Center (SOC) is one component within the Office of Information Security providing oversight for all cybersecurity activity across the executive branch as well as operates the SOC.

The **California Cybersecurity Integration Center** developed a vendor-agnostic machine to machine threat intelligence sharing solution that allows for real-time cyber threat intelligence sharing between the Cal-CSIC and its SLTTP partners. The system receives automated cyber threat indicators from over 70 cyber information-sharing partners, then distributions critical cyber threat information to over 630 California-based partner entities, all without human interaction.

The 630+ Cybersecurity Partners include:

- **Federal:** FBI, DHS ,DoD, National Cybersecurity & Communications Integration Center
- **State:** State Threat Assessment Center and all California Fusion Centers, UC/CSU/Community Colleges, State Agencies, Governor's Office of Business and Economic Development
- **Local:** Educational (K-12), Financial, Critical Infrastructure, Cities, Counties
- **Interstate:** New York, Michigan, Utah

In addition to this impressive feat, the CAL CSIC also recently;

1. Deployed a tactical team, at the request of another state who was impacted by a massive cyber-attack outage
2. Published the California Joint Cyber Incident Communications Framework and the California Joint Incident Response Guide, and
3. Is an active participant in multiple national exercises including North American Electric Reliability Cooperation's GridEX and the National Cyber Guard Prelude.

The **California Military Department** has had a tremendous impact across the state and has helped assess and identify gaps within its information security program. Specific achievements include conducting over 100 Independent Security Assessments and has analyzed over 56,000 hosts in the last two years for vulnerabilities. These actions have directly contributed to improving the state's phishing detection rate by 47% and reduced the number of harvested credentials by 49% across the enterprise.

The **California Highway Patrol's** proactive sharing of intelligence from criminal investigations has provided the state the ability to proactively respond to incidents and minimize the effects of cyber incidents. Before the 4-Core partnership, investigations were completed, but intelligence information was siloed and not used proactively. The identification and sharing of threats and indicators of compromise proactively while incidents are being investigated has helped the state more effectively respond to incidents and threats that have had the potential to grow significantly, but because of proactive information sharing were minimized. In 2017, state Departments reported 889 incidents in the California Compliance and Security Incident Reporting System (Cal-CSIRS), of which 76 resulted in criminal investigations by the CHP.

Each of California's Cybersecurity 4-Core teams specialize in individual areas of cybersecurity response and expertise to strengthen the state's cybersecurity posture while communicating between each other and with external partners across the country. These efforts have not only strengthened the State's cyber defenses, but continue to evolve with the ever-changing cyber threats targeted within the state, throughout the United States and the world.