County Government
Cyber Security Programs

CSAC FINANCE CORPORATION

The Cyber Security Challenge

In 2016, SecurityScorecard analyzed and graded the current security postures of 600 local, state, and federal government organizations, each with more than 1,000 public-facing IP addresses, to determine their security hygiene. The report found that among 60% of local government “low performers” received an ‘F’ in Network security, 50% received an ‘F’ in Software Patching Cadence and 30% received an ‘F’ in IP Reputation (Malware). When compared to the cyber security performance of 17 other major industries, government (local, state, and federal) ranked at the bottom of all major performers.

Cyber security is a growing problem for counties as they have privileged access into large state and federal systems, which makes them a target to be leveraged in a larger attack.

The challenge is that counties are not funded, equipped, or staffed to properly confront this growing risk. Reduced budgets coupled with a growing need for cyber security has created a “perfect storm” for hackers to prey on the weak link in the chain to gain access into a treasure trove of information at the State and Federal level. Additionally, the State and Federal Government have not provided any subsidized programs to ease pressure of addressing the need for enhanced cyber security programs.

McAfee Lab’s 2016 Threats Prediction Report warns that nation-state attackers could target physical infrastructures through digital means, government-targeting ransomware will be on the upswing, and exploiting employees will continue to be a mainstay target for attackers.

County government must not only address the risks and vulnerabilities that led to its most recent breaches; it must also evolve to combat the new security risks each new year brings.

Sources:
1. 2016 US Gov Cybersecurity Report
2. McAfee Labs Threats Report 2016

Local Government ranked at the bottom in cyber security posture

How Does AB 259 Impact Your County?

On January 1, 2017, California's data breach notification laws became even tougher on county government with AB 259 taking effect. Under the amended law, counties and California businesses will be forced to rethink their approach to cyber security as the assembly bill holds them liable for breaches where the county was leveraged in the cyber attack.

SECTION 1.

Section 1798.29 of the Civil Code is amended to read:

(a) An agency that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following discovery or notification of the breach in the disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) An agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

If the agency providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (g).

AB259 was introduced in 2015 and is becoming increasingly relevant given the surge of cyber attacks.

Recent California County Cyber Attacks:
Sacramento County –
Date of Breach - 8.8.2015
Reported Date - 8.26.2016

San Diego County -
Date of Breach - 12.17.2015
Reported Date - 1.26.2016

Los Angeles County -
Date of Breach - Unknown
Reported Date - 4.29.2015

Tulare County Health & Human Services Agency -
Date of Breach - 3.19.2015
Reported Date - 4.6.2015

Sources:
1. Office of the Attorney General - State of CA Department of Justice
2. Lai, J. T. (2016, October 5). California Expands Data Breach Notification Law | Lexology.

Why is Your County at Risk?

Sources:
1. 2014 Data Breach Investigation Report
2. Matarrese, A. (2016, May 4). Local Governments: Attractive Targets for cybercriminals - GovTech.com

Local governments are attractive targets, in part because they're connected to state and federal systems. This access presents significant risk to the counties as they have less resources to protect the county against nation states that are targeting the State and Federal systems. There is an estimated 39 Nation State-Sponsored Cyber Syndicates that are well funded and outpace county IT departments.

Due to budget constraints, many local government agencies are still using traditional practices to keep their network secure. The traditional approach to IT security is based on the notion that you can keep threats out using passwords, firewalls, and other border defenses to stop unauthorized access. However, this approach is flawed as attackers are getting more sophisticated in their methods and just about anyone can purchase cyber technology products and services needed for malicious purposes.

During the recession, many local governments looked toward their IT departments as a place to cut back on headcount. Insufficient staffing and lack of qualified IT security resources puts local government at even a greater risk of being a cyber attack victim. In a 2015 report, the National Association of State Chief Information Officers surveyed IT chiefs from 48 states, and about 92% of respondents said pay prevented them from attracting and keeping talent, and that was for state governments.

Perhaps the greatest threat to local government is the most underestimated type of attack - the insider threat. According to the 2014 Data Breach Investigation Report, 72% of insider incidents had financial motives. Employees, partners, vendors, or anyone with access to your network is capable of launching an attack causing significant damage. The real challenge here is being able to identify these attacks in real time.

CSAC’s IT Security Program

CSAC’s IT Security Program for County Government represents a strong partnership in which CSAC’s Business Partner, Synoptek, provides the technology and security expertise to achieve higher levels of cybersecurity readiness. Synoptek helps the counties incorporate the people, tools, and procedures that lead to a more secure IT framework.

Advantages of CSAC & Synoptek’s IT Security program:

- Global Threat Visibility to manage risk more effectively across every application, end-user, device, and data asset within your organization

- 24x7 Security Monitoring across all devices with teams of security analysts identify incidents, investigate, triage and remediate

- Ongoing comprehensive actionable intelligence reports prepared by cyber security specialists to focus on the most critical threats to your business

- Access to industry leading cyber security experts (all US-based)

County governments now face a new wave of dynamic attackers who are using adaptable technology and stealth techniques that can change very quickly. Synoptek works with county governments to analyze their information environments on an ongoing basis to detect anomalous activity before it develops into a complex breach.

For the first time, Synoptek has developed an adaptive approach to defending counties from cyber attacks by focusing on detecting threats from within at an early stage of its attack life cycle.

> “They want to take your network down, they want to delay, destroy, degrade, or deny your information.”
>
> General Michael Hayden, former CIA director

A Multi-layered Approach to Cyber Security

Hackers have to be nimble and stay under the “radar” in order to see their objective through. As the State and Federal agencies tighten down their defenses against cyber-attacks, it forces the hacker to work from the bottom-up rather than the top-down. This growing problem can be addressed by leveraging Cyber Security programs provided by Synoptek’s Security Services.

Synoptek’s has several programs ranging from End-User training and threat education, End-Point Security, Network Security, as well as Cyber Security Advisory.

Network Anomaly Detection Program

Synoptek’s cyber security analysts look at the core of your network, using world-class technology that uses machine self-learning and probabilistic mathematics. Immediately after installation, the appliance begins modeling normal activity and detects abnormalities occurring in real-time. By looking at this data, Synoptek’s security analysts are able to take action on any active security incidents to prevent the infliction of serious damage. Counties will also receive a weekly Threat Intelligence Report, outlining any risks and recommended remedial action.

End-User Training - the Human Firewall Program

Synoptek provides monthly cyber security training for all of your users as part of their IT Security program. Counties must ensure that they’re not just investing in technology, but also nurturing a security-conscious environment. Synoptek’s human firewall program has three main components: educating the employee, minimizing human error, and getting ahead of new threats. The main objective of a human firewall is to raise the awareness of your staff to such an extent that they become a solid line of defense against attempts to compromise your systems. This training helps your users stay on top of threats - like phishing attacks, malware, and Trojans.

Web Content Filtering Program

Synoptek’s Web Content Filtering program blocks your employee’s access to content and websites related to malware, drive-by downloads, mobile threats, and phishing attempts. Synoptek’s Web Content Filter also detects and contains advanced attacks before they can cause damage to your devices. This program uses big-data analytics and machine learning to automate protection against both known and unknown threats. Because no new hardware or software is required, deploying Synoptek’s Web Content Filtering Program is fast and non-intrusive to your staff.

Company Background

Synoptek was founded in Irvine, CA in 2001 and provides world-class strategic IT leadership and IT operational support for customers around the world.

Synoptek has established a core competency in Local government IT projects and operations. Over the past decade, Synoptek has been responsible for the protection of critical data assets for County Government and Municipalities.

During this time, they have protected large and complex environments from sophisticated cyber threats including: insider attacks, malware mercenaries, and attacks on critical infrastructure.

Synoptek has a diverse team of over 475 IT professionals, who protect information environments and detect emerging threats within them 24x7. This gives the team and the customer the opportunity to proactively defend against active cyber-attacks.

Synoptek can extend your county IT department's capacity to protect applications, computing, and network infrastructure with advanced security solutions that are easy to implement, fully managed and do not require large upfront investments.

In 2017, Synoptek was globally recognized for many industry awards, including: #20 on the Top 100 Cloud Services Providers list, #4 on MSPMentor's Top 501 total-service-provider list, and received three accolades for customer service through the 2017 ACE Awards.

Synoptek is headquartered in Irvine, CA with offices in San Francisco, CA; Sacramento, CA; San Diego, CA; Las Vegas, NV; Boise, ID; Denver, CO; Marlborough, MA; Pittsford, NY; New Brunswick, Canada and Raleigh, SC.

A Data Breach in a County Government IT environment can be a huge public safety issue

For more information contact :

itsecurity@csacfc.org