MARKET TRENDS REPORT

Combating Cyberattacks:

How SOCs Protect State & Local Governments

Introduction

When citizens give their data to state and local governments, they expect it will stay safe and protected from cyberthreats. But the list of cybersecurity challenges faced by state and local agencies continues to grow.

First, agencies have limited budgets and resources available for cybersecurity. The National Association of State Chief Information Officers (NASCIO) reported in 2018 that only 1-2% of state enterprise IT budgets were allocated to cybersecurity. This suggests that yearly budget increases aren't keeping up with increasingly sophisticated threats and new tools and solutions to stop them.

Next, state and local organizations often have trouble convincing their citizens and leaders that cybersecurity is a top priority worthy of major spending. Finally, these agencies often lack the expertise and manpower to adequately address this issue. Collectively, these concerns put state and local governments at a huge disadvantage in their ability to thwart cybercriminals.

Fortunately, security operations centers (SOCs) can help state and local agencies advance their cybersecurity efforts. A SOC is a centralized unit that deals with security issues on an organizational and technical basis. Inside agencies, SOCs are hubs where IT staff can closely monitor networks for problems using the latest data processing technology.

Despite their usefulness, building and maintaining a SOC is often a non-starter for resource-strapped IT teams. SOCs require a major investment in money, personnel and time, all of which are often in short supply for state and local governments.

Thankfully, SOC-as-a-service can meet agencies' needs without committing them to an on-premise SOC. SOC-as-a-service combines a subscription-based software solution with external assistance from dedicated security experts. This arrangement fiercely guards agencies' data while filling in their asset and talent gaps.

GovLoop partnered with Arctic Wolf, a SOC-as-a-service provider, on this report about how SOC-as-a-service can strengthen agencies' cybersecurity. The following pages explain how to maximize SOC-as-a-service's potential. We also list best practices for improving agencies' compliance with security regulations using SOC-as-a-service. For additional insights, we interviewed Dinah Davis, Vice President of Research and Development (R&D), at Arctic Wolf, and Benny Hsieh, Cupertino, California's IT Manager, Infrastructure.

BY THE NUMBERS

State and Local Cybersecurity Today

47%

of local governments said they experienced cyberattacks daily, with 28% saying they occurred at least hourly.

33%

of local governments said they experienced more cybersecurity attacks, breaches and incidents than in the year before.

11%

of local governments said their average citizen wasn't aware of the need for cybersecurity.

172

ransomware attacks affecting state and local governments have been reported since 2013. Ransomware is malicious software that blocks access to an IT system or threatens to publish private data unless a ransom is paid.

52%

of state chief information security officers (CISOs) said that an insufficient cybersecurity budget was the top barrier to an effective cybersecurity program.

50%

of state CISOs said that inadequate cybersecurity staffing was the top barrier to an effective cybersecurity program.

"Historically, cybersecurity in local governments was usually not a high-priority item, and it might not be something for which staff had training. What's more, even if you wanted to bring in more security, a city might not have had the funds readily available at the time."

- Benny Hsieh, Cupertino, CA
IT Manager, Infrastructure

THE CHALLENGE

Today's Complicated Cybersecurity Landscape

Cybersecurity becomes more complicated for state and local agencies as scores of problems threaten to overwhelm them every day. It's an uphill battle driven by the scarce budgets, resources, talent and stakeholder buy-in available to agencies.

For agencies, cybersecurity is also a multi-front war. Agencies that can't protect their infrastructure, for example, risk crippling disruptions to such valuable citizen services as electricity and emergency first responders.

"If those infrastructures go down, the entire social fabric of these communities disappears," said Dinah Davis, Vice President of Research and Development (R&D) at Arctic Wolf. Davis also noted that resuming normal operations can take weeks or months.

Agencies additionally handle vast amounts of personally identifiable information (PII), a fact that makes them attractive targets for cybercriminals. When attackers are successful, they can cause major headaches for agencies, including financial damages.

"The risk of having a person's data stolen from a government organization is high," Davis said. "They probably have the most PII data anywhere. It puts them at high risk of having their citizens' identities stolen."

Even worse, many agencies are falling behind in their response to current cyberthreats. For instance, take the money that agencies spend to help prevent cybersecurity incidents. The public often demands accountability into such spending, but agencies can become so bogged down with documenting their cybersecurity budgets that they find themselves devoting less time and fewer resources to what matters most — defending against actual threats. Ultimately, agencies can't tackle danger as quickly if they're buried under budget reports.

Despite this, agencies must find a balance. Meanwhile, the threat from bad actors is only growing. In August 2019, Texas learned this the hard way when 22 government entities there – mostly local governments – were hit by a ransomware attack. For state and local governments without a plan for countering such predicaments, the fallout can be immense.

Solution: SOC-as-a-Service

Surrounded by cyberthreats, many agencies are turning to SOCs for safety. Traditionally, SOCs serve as cybersecurity command centers. They involve data processing, IT staff and security monitoring in one centralized location.

"The idea of a security operations center is to install technology that allows you to monitor what is happening in your organization 24/7," Davis said. "To properly manage your SOC you need to constantly update the rules and technology to stay one step ahead of the hackers."

Although highly valuable, building and maintaining your own SOC has significant drawbacks. For starters, creating SOCs is costly. Even agencies that can afford SOCs can struggle to staff them.

"The organizational lift is very strong," Davis said. "Many security engineers need six-figure salaries. That talent isn't widely available."

Davis said that although some agencies can field five-person SOCs, a staff of seven is best for 24/7 operations. The high cost in manpower and technology has prompted many agencies to adopt SOC-as-a-service.

"SOC-as-a-service is when you use a third party for your SOC," she said. "They provide the people, the technology and the eyes on the screen to make sure everything in your environment is being monitored."

SOC-as-a-service reduces the burden on agencies by assisting their workers with cybersecurity monitoring and by helping upgrade each agency's security practices, procedures and tools.

BEST PRACTICES

Starting SOC-as-a-Service

1. Evaluate your environment

Agencies that don't understand their cybersecurity environments aren't equipped to defend them. In contrast, agencies that frequently survey their IT landscape will see both potential problems and insights they can share with partners. SOC-as-a-service providers can help agencies notice every detail of their IT environment. Take software, for example. Providers can determine whether agencies have the latest product upgrades and security patches. This ensures they have the latest protections while filling in their security gaps.

2. Make your monitoring count

SOCs monitor an agency's entire IT landscape, so picking the right staff for one is critical. SOC staffers are responsible for their agency's applications, databases, networks and more. It's a long list that requires careful analysis, surveillance and safekeeping.

Regrettably, not all SOC-as-a-service providers are equal. Although many SOC-as-a-service providers promise 24/7 assistance, some don't truly provide services around the clock. Subsequently, agencies should exercise caution and test how long potential providers can sustain uninterrupted coverage.

Agencies looking for SOC-as-a-service providers also shouldn't ignore the customer experience (CX). SOC-as-a-service works best when it meshes seamlessly with an agency's current operations, so finding the best fit for both parties is crucial.

Initially, agencies should weigh how their workers mesh with a provider's account team. Over time, teams that can't coexist will struggle to reach common goals.

3. Don't wait to deploy

Installing SOCs is often time-consuming because it requires large amounts of equipment and personnel to get them up and running. The energy and time spent on SOC setup can wear public servants down and leave their agencies pinching pennies.

Furthermore, the gap between when agencies do and don't have a SOC can leave them exposed to cyberthreats. While constructing SOCs, agencies might suffer cybersecurity incidents that cost them money and infuriate citizens.

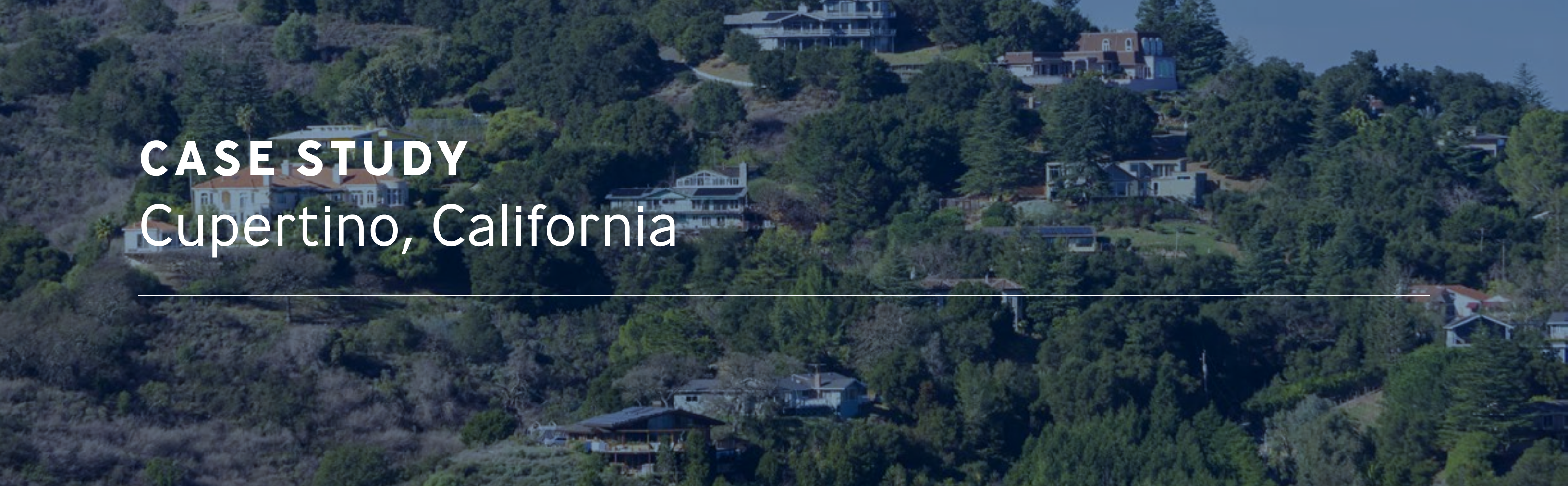
The right SOC-as-a-service provider can alleviate these concerns by quickly aiding agencies. These providers shoulder most of the burden of installing SOCs, letting agencies focus on their missions. By deploying SOCs quickly, they also minimize their agency's cybersecurity vulnerabilities.

4. Don't stall on SIEM

Security information and event management (SIEM) products provide real-time analysis of security alerts generated by applications and network hardware. These tools combine security information management (SIM) and security event management (SEM) into one protective shield for agencies.

SOCs typically include the appliances, software and managed services that comprise SIEMs. SIEMs are valuable for agencies, as they log security data and generate reports that prove they're compliant with all applicable security standards. Despite this, fine-tuning SIEMs to an agency's specific needs is difficult. It's a process that can last weeks or even months and quickly eat up a budget.

Quality SOC-as-a-service providers, however, overcome these obstacles through their experience and expertise with SIEMs. These providers leverage artificial intelligence (AI) tools overseen by talented security analysts to distinguish false-positive alerts from the true threats amid billions of data observations. AI involves machines mimicking such human cognitive functions as learning and reasoning. Overall, this strategy ensures agencies are better protected at a more affordable cost.



CASE STUDY
Cupertino, California

Benny Hsieh has managed Cupertino, California's IT infrastructure for about two years and has already seen its cyberthreats landscape dramatically change.

"It's always a cat-and-mouse game in terms of cybersecurity," he said. "We're seeing more social engineering cyberthreats. It's bad actors impersonating email accounts and phone numbers to try and get access to information."

Hsieh said that Cupertino's IT department quickly realized partnering with a SOC-as-a-service provider could address its two biggest problems: money and expertise.

First, pairing with a SOC-as-a-service provider saves Cupertino money that would normally go to activities such as repairing its IT defenses.

"Having a SOC-as-a-service provider allows us to more easily budget what we do on our end for security," he said. It has also helped Cupertino bring more cybersecurity knowledge to its IT department without hiring and training new staff.

"Working with a SOC-as-a-service provider, you have access to someone who does security professionally," Hsieh said.

Ultimately, Cupertino picked Arctic Wolf as its SOC-as-a-service provider. Cupertino's IT department now meets with Arctic Wolf's security team monthly to discuss potential vulnerabilities, including recent internet traffic, security patches and unusual activity logs. Together, this combination works to keep Cupertino's networks safe 24/7.

HOW ARCTIC WOLF HELPS

SOC-as-a-service providers such as Arctic Wolf can give agencies a tireless cybersecurity partner. These providers lend help with both human expertise and machines, easing the strain that cybersecurity often places on agencies.

Consider the average IT team. No matter its size, unexpected challenges can always leave it needing help. Enter Arctic Wolf and other providers, which can boost an agency's team by providing security experts who multiply their manpower.

"A lot of times our security engineers become close friends with the people on your network," Davis said. "We do like to build a strong relationship with our primary contacts in the network."

Arctic Wolf typically provides agencies with at least two security engineers who help with 24/7 security coverage. After that, the company's hybrid AI lightens the load further.

Hybrid AI features machines that learn from complex rules created by a provider's security engineers. These rules can be customized for any agency's unique mission. For instance, hybrid AI can recognize new types of ransomware minutes after an attack, helping law enforcement agencies identify them faster.

"We're letting your IT people sleep at night," Davis said. "Working with a cybersecurity partner like Arctic Wolf means state and local security teams no longer have to go it alone."

Learn more here: Arctic Wolf's SOC-as-a-Service

CONCLUSION

Because they have valuable data, state and local agencies will always be prime targets for cyberattacks. Although security threats are always evolving, agencies are expected to respond accordingly despite limited budgets, resources and workforces.

SOCs can help make cybersecurity a fair fight. They provide a centralized command center for agencies to continuously watch for and respond to cyberthreats. But these installations are expensive, and the talent to staff them isn't widely available.

SOC-as-a-service solves both issues by having a third party manage an agency's SOC. It's an arrangement that gives agencies the same peace of mind SOCs provide at a fraction of the effort and cost.

ABOUT ARCTIC WOLF

Arctic Wolf Networks delivers the industry-leading security operations center (SOC)-as-a-service that redefines the economics of cybersecurity. Arctic Wolf™ Managed Detection and Response and Managed Risk services are anchored by the Arctic Wolf Concierge Security™ Team who provides custom threat hunting, alerting, and reporting. The Arctic Wolf purpose-built, cloud-based SOC-as-a-service offers 24×7 monitoring, risk management, threat detection, and response.

For more information about Arctic Wolf,
visit arcticwolf.com

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop