VOLUME 4 | ISSUE 3

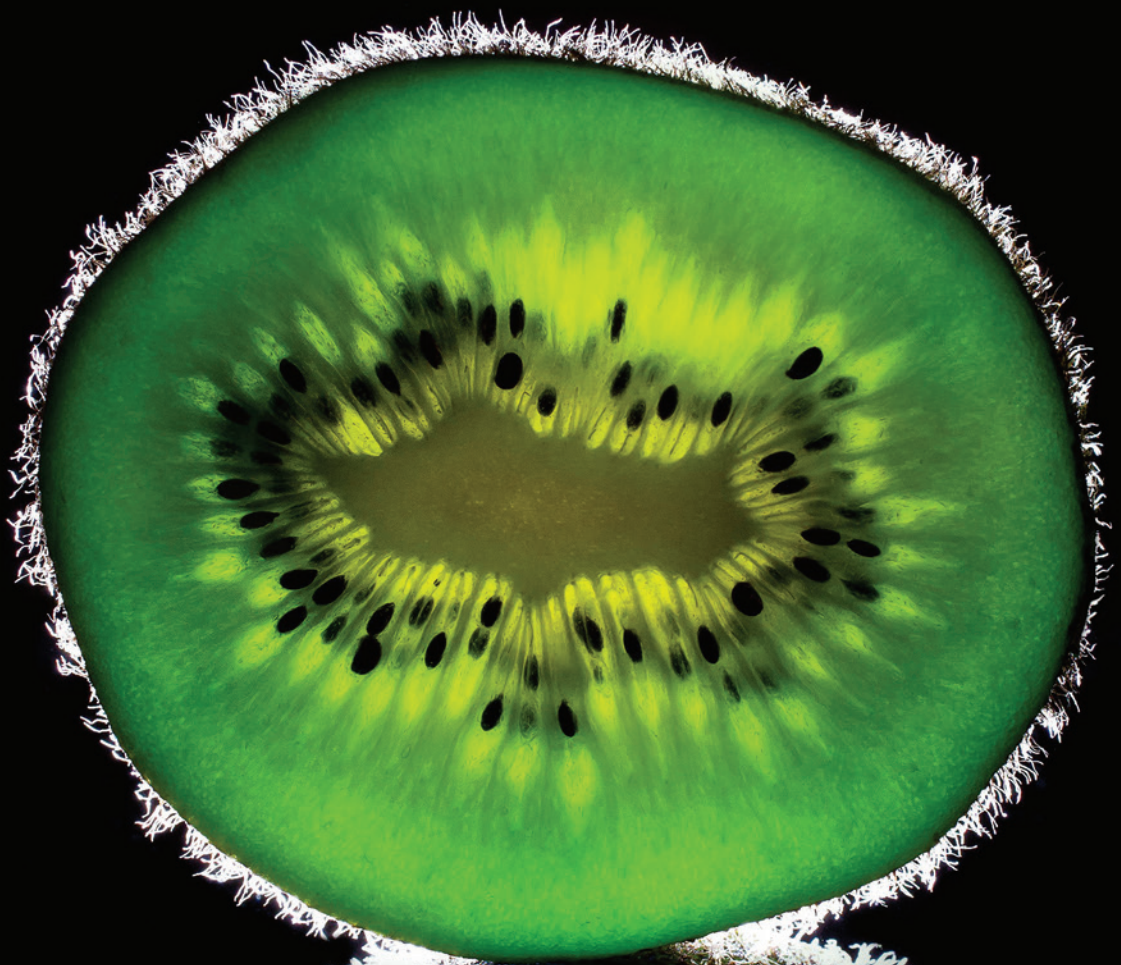
FALL 2016

techwire

CYBER STATE

California's security program evolves and predicts future threats.

Analytics see what you can't.
So you can see opportunities within.



How do you go beneath the surface of your data to reveal the hidden possibilities? Analytics. We help our clients use analytics to turn data into insight, insight into action and action into tangible results. It's just one of our Digital capabilities, along with Interactive, Mobility, Cloud and Security — everything you need to compete to win. That's high performance, delivered.

High performance. Delivered.

Accenture Analytics

Part of Accenture Digital

Strategy | Consulting | Digital | Technology | Operations

CONTENTS

BUSINESS, POLICY,
DIGITAL TRANSFORMATION

Publisher: **Alan Cox,** alanc@erepublic.com

EDITORIAL

Editor: **Bill Maile,** bill@techwire.net
Managing Editor: **Matt Williams,** matt@techwire.net
Chief Copy Editor: **Miriam Jones,** mjones@erepublic.com
Copy Editor: **Lauren Harrison,** lharrison@erepublic.com
Contributing Editor: **Elaine Pittman,** epittman@erepublic.com
Editorial Assistant: **Ryan McCauley,** rmccauley@erepublic.com
Contributing Writers: **Dorsey Griffith, Brooke Edwards Staggs, Samantha Young**

DESIGN

Chief Design Officer: **Kelly Martinelli,** kmartinelli@erepublic.com
Graphic Designer Pubs: **Erin Molina,** emolina@erepublic.com
Sr. Designer Custom: **Crystal Hopson,** chopson@erepublic.com
Production Director: **Stephan Widmaier,** swidm@erepublic.com
Production Manager: production@erepublic.com

PUBLISHING

Sr. Dir. of Sales Operations: **Andrea Kleinbardt,** akleinbardt@erepublic.com
Business Development: **Maggie Ransier,** mransier@erepublic.com
Custom Media
Managing Editor: **Jeana Bigham,** jbigham@erepublic.com
Dir. of Web Marketing: **Zach Presnall,** zpresnall@erepublic.com
Web Advertising Mgr: **Adam Fowler,** afowler@erepublic.com
Subscription Coord.: **Eenie Yang,** subscriptions@erepublic.com

CORPORATE

CEO: **Dennis McKenna,** dmckenna@erepublic.com
President: **Cathilea Robinett,** crobinett@erepublic.com
CAO: **Lisa Bernard,** lbernard@erepublic.com
CFO: **Paul Harney,** pharney@erepublic.com
Executive VP: **Alan Cox,** alanc@erepublic.com
Chief Content Officer: **Paul Taylor,** ptaylor@erepublic.com
Deputy Chief Content Officer: **Steve Towns** stowns@govtech.com
VP Research: **Todd Sander,** tsander@erepublic.com

Article submissions should be sent to the attention of the Managing Editor. Reprints of all articles in this issue and past issues are available (500 minimum). Please direct inquiries for reprints and licensing to Wright's Media: (877) 652-5295, sales@wrightsmedia.com.

Subscription Information: Requests for subscriptions may be directed to Subscription Coordinator by phone or fax to the numbers below. You can also subscribe online at **www.techwire.net.**

100 Blue Ravine Rd. Folsom, CA 95630
Phone: (916) 932-1300 Fax: (916) 932-1470

Printed in the USA.

A division of e.Republic

techwire.net

Bill Maile, Editor

TechWire Celebrates 5 Years

This fall we are celebrating a major milestone — five years in publication! In September 2011, I launched *TechWire* as a communications platform for the state IT community and the 10,000 professionals who support California's digital infrastructure. For those who manage projects, databases, email systems, data centers and IT programs, what started as a website and weekly email newsletter has become a widely known, thriving source of daily news and information focused on California's annual $5 billion industry.

Elise Armitage, my communications intern at the California Technology Agency, and her college friend Ashley Nelson, both at the time graduate students and experienced journalists, helped me launch the site. We ran articles about large projects, policy initiatives, leadership changes, legislation and other important technology-related matters. Never before could industry professionals read about topics so closely connected to their work — we aimed to be a business journal exclusively for the government technology community that I learned about while I was working for the state.

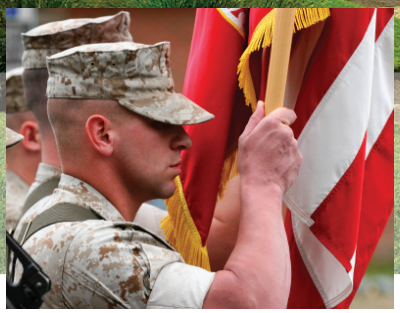
In March 2012, we launched our quarterly printed magazine, which kicked off a period of steady expansion that would eventually include adding contributing writers such as former FCC Commissioner Rachelle Chong and former Assemblymember Lloyd Levine. We were also fortunate to have on the team CALinnovates Executive Director Mike Montgomery, veteran AP reporter Samantha Young and tech journalist Matt Williams. Williams currently serves as *TechWire's* managing editor.

While a lot of the ground work was laid during the first year, we have steadily grown our coverage over time, with regular in-depth features and high-quality journalism. In 2014, *TechWire* was acquired by e.Republic Inc., the Folsom-based publisher of *Government Technology* and *Governing*, both respected national publications. With more customers to support our platform and an award-winning design team that creates stunning magazines, each issue of *TechWire* is better than the previous.

So where do we go from here? I hope it is safe to say that *TechWire* has reached a level of sustainability that will allow the platform to grow and last over time. Despite the rapidly changing publishing industry, I believe there is still a distinct place for traditional information gathering to serve a vested audience of business people, policy-makers and information technology professionals.

We have come a long way in five years but none of it would have been possible without a tremendous amount of community support in both the private and public sectors. I appreciate all of the feedback and tips that have helped us improve and mature. Our success is truly a reflection of you, our readers, and the credibility you have given us.

Thank you for tuning in over the years.



ens-inc

5th Annual Veterans Day Golf Tournament

Giving Back to Veterans

LINCOLN HILLS GOLF CLUB

plus...

2016 IT EXPO

Join us on Veterans Day, November 11

Our country has lost many brave service men and women, and many more have returned wounded, and struggling to acclimate back to civilian life. In one way or another, the sacrifices of these service men and women have touched all of our lives.

As a company whose executive management team is comprised of veterans, we feel it is important to remember and recognize those coming home from foreign wars and risking their lives for our country.

All donations from this event will go toward helping veterans with disabilities, as well as mental health and family services for them and their loved ones.

Sponsor this event! www.ens-inc.com

REGISTER • SPONSOR • PRESENT AT IT EXPO

www.ens-inc.com/events/135/

For more information, please contact the ENS-Inc Golf Event Team at golf@ens-inc.com.

Enterprise Networking Solutions, Inc
3054 Fite Circle #106, Sacramento, CA 95827
(916) 369-7567
www.ens-inc.com

virtualization • cloud integration • business continuity • migration/consolidation

IT Agility, Efficiency, Protection

Your Datacenter. Your Cloud. Reliable Customer Service.

Building a vital IT infrastructure through virtualization and cloud integration, then securing that infrastructure with a solid plan for business continuity and disaster recovery, gives you the confidence your organization requires to focus on the business of the bottom line.

With the expertise and innovation of our highly-skilled architects and engineers, the oversight of ITIL and PMP-certified Project Managers, and a passion for customer service, ENS-Inc develops and deploys proven reliable and scalable technology solutions on time, on budget, and within scope... *and then provides the onsite training and knowledge transfer to empower success!*

ens-inc
enterprise networking solutions inc

BBB ACCREDITED BUSINESS

CMAS Approved Contractor — DGS California Multiple Award Schedules — CMAS

CA.GOV California Certified Small Business

WSCA Western States Contracting Alliance

CA.GOV IT Consulting Master Services Agreement

DVBE OPTIONS

E-Rate For Schools and Libraries

CalPERS Spring Fed Pool

BILL FOSTER

Keith Tresh, CIO of the California High Speed Rail Authority, calls Cal-CSIC the "gel to help the state move in the right direction" on cybersecurity.

By Dorsey Griffith

Cyber Defense

Key agencies are collaborating across the state to fight against threats.

As the most populous state with the nation's largest economy, California also has the most to lose at the hands of cybercriminals bent on crippling critical infrastructure, shutting down essential services or stealing the private data of millions of people.

In an effort to prevent and respond to these threats, state information security officials are designing and implementing systems and policies to meet the growing and ever-changing demands.

"This is an ongoing and evolving threat," said Danjel Bout, assistant director for response at the California Office of Emergency Services (Cal OES). "If the expectation is we are going to solve it, I wouldn't be optimistic, but I am certain we are going to put in place the best practices in the world to address cyberthreats."

Prodded by anxious lawmakers and guided by legislative and executive mandates and federal initiatives, state agencies and departments across a range of disciplines are gradually building California's cybersecurity systems.

The focus: threat monitoring and incident response, as well as prevention and education.

Leading the threat monitoring and incident response is the California Cybersecurity Integration Center, or Cal-CSIC for short, which joins several state government agencies including Cal OES, the California Highway Patrol (CHP) and the Department of Technology (CDT), together with federal agencies such as the FBI and the Department of Homeland Security. California is a volunteer partner with the National Cybersecurity Communications Integration Center's Cyber Hygiene Program, for example, with a goal to get a broader picture of the state's cybervulnerabilities, measure performance of cyberdefense and help develop long-term strategies.

Cal-CSIC, which launched a few months ago, also engages academic institutions, tribal governments, utilities and key private companies like Verizon Communications Inc., which puts together a *Data Breach Investigations Report* that provides state information security officials with insights into national trends and risks.

Set up through an executive order in 2015 to be the "central organizing hub" of the state's cybersecurity activities, Cal-CSIC has the potential to be a cybersecurity game changer for California, said Keith Tresh, CIO of the state High Speed Rail Authority and former chief information security officer at CDT.

"Cal-CSIC is going to be something the state agencies can tap into and ... be the gel to help the state move in the right direction," he said.

Cal-CSIC is co-located with the California State Threat Assessment System, an arrangement made to better connect law enforcement, the intelligence community and the state's fusion centers, which, Bout said, "help our local and federal partners by looking at the threat environment and ensuring coordination and information sharing to increase the overall security of California."

Also at the table are representatives from the CHP, which is closely aligned with the FBI on many cybercrime investigations.

"When state departments make a notification about a crime, my unit collects evidence and does follow-up to track down the bad guys and hold them accountable," said Scott Howland, the CHP's CIO and chief of its Information Management Division.

Each member of Howland's nine-person investigations team is federally sworn, allowing them to partner with federal law enforcement to investigate and solve cases.

"While my computer crimes investigation unit is in Sacramento, we are statewide, and I can reach out for additional assistance," he said. "We use personnel across the state and tap into the FBI and other law enforcement agencies across the nation to solve these crimes."

The greatest challenge for law enforcement, Howland said, is that while California may be the target of cybercrime, the attacks can come from anywhere.

"With a property crime, the suspects show up at a physical location, you collect evidence from there and the suspect starts in your geographic proximity," he said. "With cybercrime, a suspect can commit a crime in California from China or Arizona. They could be anywhere, and that adds to the challenge of tracking them down."

> "With cybercrime, a suspect can commit a crime in California from China or Arizona. They could be anywhere, and that adds to the challenge of tracking them down.

Meanwhile, the state Attorney General's Office collects information about data breaches involving more than 500 people from businesses and governmental bodies. The office issues an annual breach report, enforces state data breach laws, and recommends policies and procedures that entities can use to enhance protections against data theft.

On the prevention and education side, the California Military Department, which had previously conducted state department cybersecurity assessments as part of a pilot program, is following a legislative mandate to conduct assessments of at least 35 state agencies annually.

Assessors use the National Institute of Standards and Technology's Cybersecurity Framework to evaluate different areas at each agency, such as their protection of communications and website functions, to find gaps and recommend fixes, said Col. Darrin L. Bender, director of external affairs at the department. They also can draw upon the Department of Defense resources to assess state vulnerabilities and help individual agencies reduce their risk of cyberattacks.

As of mid-July, the department had conducted five of the mandated 35 assessments, he said. "We are at the very beginning, the starting line," said Bender. "We have the remaining assessments scheduled, and we are on track to get them done before the end of the year."

For its part, the CDT works internally through its Office of Information Security to conduct audits of each department to determine compliance with state requirements and policies like use of passwords and handling of records.

"We are working to educate the departments on what they need to do to step up their efforts on cybersecurity," said Amy Tong, CDT's director. Taken together with the Military Department's assessments, she said, it's a way to help departments be more ready — not only from the technological perspective, but also from a people and process perspective.

Playing a key advisory role over all of California's cyberdefense activities is Gov. Jerry Brown's Cybersecurity Task Force, first convened in 2013 under OES and CDT. The task force pulls together security experts from government, universities and laboratories, and major corporations and technology companies to advise senior administration officials on all cybersecurity issues.

The High Speed Rail Authority's Tresh said the state's responsiveness has come full circle in the past few years to focus on building a solid cybersecurity response system.

"Government as a whole is very aware and very concerned about today, tomorrow and the future," he said. "We have made some great strides. It's like guerrilla warfare. It's hard to catch up, but we are trying to get ahead of the game."

CYBER STATE

California's cybersecurity program is evolving with more threats, policies and stakeholders.

BY SAMANTHA YOUNG

When Gov. Jerry Brown created a cybersecurity task force, he positioned California at the forefront of state efforts to protect sensitive information and critical infrastructure.

Three years later, California has earned praise for its work — bringing together government, academia, technology experts and the private sector to identify vulnerabilities statewide and to require that state workers undergo cybertraining.

But the Brown administration also has garnered criticism for its fragmented approach, lack of accountability, and slowness to identify and assess vulnerabilities.

In 2015, a blistering state auditor report questioned California's cyber-readiness and faulted the Department of Technology for failing to ensure that state entities had complied with mandated security protocols. State agencies reported that the security rules were confusing and they had little help from the state's top IT department.

JESSICA MULHOLLAND

> "There is no 100 percent guarantee to cyberprotection. It's an evolving and complex threat that is going to continue to proliferate.
>
> – Mark Ghilarducci, director of the Governor's Office of Emergency Services

Earlier this year, the state chief information security officer, Michele Robinson, stepped down after tough questioning by lawmakers, and Department of Technology Director Carlos Ramos resigned to pursue a career in the private sector.

"We were definitely not where we needed to be," said Assemblymember Jacqui Irwin, D-Thousand Oaks, who serves as chair of the Assembly Select Committee on Cybersecurity. "I don't think it had really been prioritized in California."

Irwin and other lawmakers have called on the Brown administration to account for cybersecurity spending and deliver a blueprint for how it plans to protect the state's critical infrastructure and respond should there be an attack. In response, Brown's staff has met with lawmakers and provided tours of a new cybersecurity integration center — part of a concerted effort to educate lawmakers about the work being done.

Both the legislative and executive branches have expressed mutual concern that a security breach in California, the nation's most populous state and seventh-largest economy in the world, could expose confidential information or disrupt essential services like the water supply or electric power. Breaches at the Pentagon, the White House, California hospitals, universities, retailers and the Democratic National Committee have underscored California's vulnerability.

"There is no 100 percent guarantee to cyberprotection," said Mark Ghilarducci, director of the Governor's Office of Emergency Services (Cal OES). "It's an evolving and complex threat that is going to continue to proliferate."

By far, the biggest structural change in cybersecurity defense this year was the launch of the California Cybersecurity Integration Center (Cal-CSIC), an entity embedded at the State Threat Assessment Center that is intended to foster collaboration among the various state agencies that oversee cybersecurity.

Representatives from Cal OES, the Department of Technology, the California Highway Patrol, the state Attorney General and the California Military Department now work side by side at the center, in a secure room at OES headquarters outside of Sacramento, where they share classified information about potential threats and gaps, and collaborate on cyberstrategy.

The California Cybersecurity Integration Center was established to foster collaboration among the state agencies that oversee cybersecurity.

"They were all doing a good job, but they were doing it under their own authorities," said Ghilarducci, who as California's homeland security adviser has overseen the launch of the center. "Now it's a much more cohesive way. Everybody is under one roof."

Modeled after the National Cybersecurity and Communications Integration Center, Cal-CSIC was created after Brown last year issued an executive order declaring that the increasing number and complexity of cyberattacks demanded "heightened levels of coordination," not just within state government but also across local and tribal governments, private companies and academic institutions.

His order came a week after the critical state auditor report, which found California had weaknesses that "leave some of the state's sensitive data vulnerable to unauthorized use, disclosure or disruption."

Earlier this year, state lawmakers pointed to the report as evidence that the state's cybersecurity was in disarray, with one member accusing the Department of Technology of "falling down on the job." Others were frustrated at the lack of a plan should any of California's critical infrastructure be hijacked by hackers.

Ramos, who served as the Department of Technology chief at the time, defended

CALOES.CA.GOV

the administration in a recent interview, calling the report "incomplete" and one that "didn't paint an adequate picture of all the efforts that have gone on." He added that the auditor did not share the surveys or methodologies that supported her findings.

Lawmakers also held a cybersecurity legislative hearing six months after the report, leading several key administration officials to complain that lawmakers were simply out to get headlines or, as Ghilarducci described, conduct "political theater."

For example, administration officials say, work was already underway to launch the Cal-CSIC in hopes of providing leadership, coordination and information. Whether the work was already underway, or as Irwin believes, moved forward after legislative scrutiny, the progress has been welcomed by lawmakers.

"I've seen a big change," Irwin said. "We don't want an environment of the Legislature versus the administration. We want to make sure we work together to get things really going for the state."

Despite the growing pains in California's cybersecurity mission, its recent efforts, coupled with its first-in-the-nation data breach identification law passed in the early 2000s, have positioned California ahead other states, said Francesca Spidalieri, a senior fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy at Salve Regina University.

"When you compare California to the other states and how immature and unprepared they are, that's when you can give California a better score," said Spidalieri, who wrote a November 2015 report titled *State of the States on Cybersecurity*. "California is the example everybody looks at."

There's still room for improvement, however, she found. In her report, Spidalieri said California's cybersecurity efforts remain decentralized and lack a clear leader to coordinate the many cyberefforts across state government.

With the formation of Cal-CSIC, Ghilarducci has emerged as the key public face for state cybersecurity efforts. He's testified before Congress, and he reviewed agency cybersecurity budget requests — like equipment upgrades or security assessments — submitted this year to the Department of Finance. As a rule, departments were instructed to first spend their money on security assessments, he said.

In spite of Ghilarducci's more prominent role, administration officials have been careful to describe the state's cybermission as a collaboration and partnership across government. Duties for cybersecurity remain spread throughout state government, and each of California's 151 agencies, departments and commissions is responsible for implementing the required security policies, upgrading equipment and reporting any hacked systems.

To help them, the Department of Technology has increased its consultation with agencies and departments to prioritize and implement security improvements, said Amy Tong, California's state CIO and Department of Technology director.

"The administration has given us great support," said Tong, who was appointed to the role in June. "It is a priority of the administration to have a highlighted focus on that."

In addition, the Department of Technology and Cal OES are working with the California Military Department to perform independent network security assessments of at least 35 state agencies per year — a mandate the Legislature imposed last year with the passage of AB 670.

Meanwhile, work is underway at Cal-CSIC to complete an assessment by this fall of California's vulnerabilities, and technological and infrastructure needs so that lawmakers and policymakers are better informed about what it will take to "make a more resilient and capable California," said Danjel Bout, assistant director for response at Cal OES.

"One of the early efforts we've identified is to address the scope of threats that face us," Bout said. "We're trying to do a careful assessment because one of the dangers is to ask for something without understanding the full scope."

Cyber Trends

By Brooke Edwards Staggs

Experts share strategies for staying on top of security solutions.

Two days after WikiLeaks published thousands of emails this summer that had been hacked from the Democratic National Committee, Debbie Wasserman Schultz announced she'd be resigning from her position as chairwoman. And one day after the scope of the federal Office of Personnel Management breach became public in 2015, Director Katherine Archuleta stepped down from her post.

For those working in politics and government, a security breach can be a career killer.

"It's that old saying," said Agnes Kirk, chief information security officer of Washington state. "An attacker only has to be successful once. A defender has to be successful every time."

Breaches are happening more often, with a particular spike in ransomware attacks, according to Dan Lohrmann, chief strategist for Security Mentor and former chief security officer of Michigan. Part of the reason is that there are simply more connected systems to hack, he said. Also, the threat actors — from nation states like Russia to individual criminals — are getting more sophisticated.

"It's one of the few areas where what worked a month ago may not be the same problem you're trying to solve today," Kirk said.

High-profile breaches have shifted cyberconcerns from being the responsibility of siloed security teams to a top priority of government leaders. So while attacks are getting worse, Kirk said more attention is being paid to how agencies can prevent, detect and respond to them.

The vendor community routinely reaches out to government officials to sell the latest solutions, offering software aimed at blocking ransomware or deceiving bad actors. But it can be tough for public agencies to prioritize and decide which solutions merit an investment.

"A lot of people are looking for silver bullets," said Dave Damato, chief security officer of Tanium. "In reality, what we see — and this has been a cycle over the years — is that a new technology is released, it's effective for a short period of time, and then attackers understand and adapt to the technology, leaving customers searching for the next greatest thing."

An example, he said, are intrusion prevention systems. They were very useful 10 years ago. But soon, Damato

said, attackers found ways to get around them.

"A series of tried and tested security controls together are much more effective than attempting to beat attackers by buying the latest and greatest solution to detect a very singular use case like malware or lateral movement or whatever the specific attack of the day happens to be," Damato said. "The organizations that are the most successful in defending their environments, the ones that don't have incidents, are the ones that are following basic principles."

That includes practicing cyberhygiene, like activating firewalls and regularly patching all programs. It includes doing a thorough risk assessment, having strategic defense and response plans, and regularly testing those plans for vulnerabilities. And it includes taking a "least privilege" approach, allowing users to only access information that's necessary for them to do their jobs.

"They say on average 80 percent of the threats that hit government could have been avoided if people had done things that were known fixes," Lohrmann said.

Another key is training everyone to take responsibility for his or her own digital footprint, Kirk said. A receptionist, she pointed out, is the first line of defense in phone phishing scams, with end user errors the No. 1 source of most breaches.

"A few years ago, security was an IT problem," said Kirk. "Today, we're trying to create awareness that security is everybody's responsibility."

Before agencies buy new solutions, Damato said they should be sure they're taking advantage of capabilities baked into technology they already own. Many operating systems now come embedded with effective security tools, he pointed out, such as the application whitelisting built into Windows 10.

If governments discover they're not using some solutions in their portfolios, said Lance Dubsky, chief security strategist for FireEye, they can harvest those funds to buy technology that's evolved with the environment.

When it comes to new purchases, Damato said agencies should share notes on what works rather than rely on staged demos or which vendors can write the best proposals. But here are four cybersecurity technology solutions that many experts agree merit attention.

ENDPOINT DETECTION AND RESPONSE

Intrusion detection systems leave agencies always trailing the bad guys because they require analysts who observe attacks and generate defenses that are sent out to clients.

"You've got to use math on your side here so we can scale against the threats," said Ryan Gillis, vice president of cybersecurity strategy and global policy at Palo Alto Networks.

That's where endpoint detection and response software comes into play. These solutions constantly find and act on both identified and zero-day threats by tracking anomalies in behavior to find early hints of breaches. A solution from Palo Alto Networks, for example, generates 1.1 million new prevention measures every week.

"Having real-time visibility into all of your endpoints is extremely important for the government," Damato said. "The most successful organizations at preventing breaches are those that are able to detect them and respond to them within an hour."

SECURITY ORCHESTRATION AND AUTOMATION

Government systems often include a mix of solutions that were purchased independently and don't communicate well with each other, Dubsky said. That's a challenge for security professionals to manage.

"The fundamental problem that we've faced in cybersecurity for a long time is discrete individual products to solve one problem and then putting the onus on the network defender to figure out how to make all of those different things work together," Gillis said. "And the result has been manual defense generally against automated attacks, which is unsustainable."

Experts say it's worth investing in security orchestration and automation technologies, which integrate diverse systems so defenses are coordinated from a security operations center. And Gillis said that integration should be extended to incorporate the Internet of Things and cloud technologies.

CLOUD ACCESS SECURITY BROKERS

While most experts agree that government systems will never migrate entirely to the cloud, the trend is in that direction. The cloud presents its own set of data privacy issues since it requires an element of trust in a third-party provider.

Workers often now take matters in their own hands by jumping on cheap cloud solutions. Handing data over to the likes of FreeChinaStorage.com isn't a wise idea, but Lohrmann said he's seen it happen.

"You can't just throw the baby out with the bath water," said Lohrmann. "You need to be innovative."

Training is key here, but so are cloud access security brokers. These software tools act as gatekeepers, monitoring systems and confirming that security protocols are still in place as information moves to the cloud.

THREAT INTELLIGENCE SHARING

As security solutions detect threats, Lubsky said it's crucial for that data to be fed back into the systems so they can adjust and share any learning.

"The future of protecting an enterprise depends on being able to use machine learning or machine-to-machine speed when it comes to developing signatures and adjusting profiles so that the organization stays protected," he said.

Sharing threat intelligence across agencies is also important, Kirk said, with automated systems that send actionable information between governments.

"We'll never eliminate the human factor," she said. "But there's so much information and there are so many attacks that come in that you couldn't possibly respond with just human intervention. So we've really appreciated the new technologies that have come out."

Shell Culp is a principal with Almirante Partners and the chief innovation officer for Stewards of Change Institute. Her passion for performance improvement in government also makes her a champion of interoperability, open data and organizational change management.

SHUTTERSTOCK.COM

Security Considerations

Factors that have little to do with technology sometimes make the difference between success and failure.

By Shell Culp

Constituents should have high expectations of government. Agencies should also inspire confidence in people that they're up to the job.

When we think about cybersecurity, we should rightly expect that government will diligently protect citizen data, such as the sensitive information we not-so-voluntarily provide to the departments of Motor Vehicles, Social Services and Public Health. Cybersecurity cuts across all of the public sector and is fundamental for people to trust their government.

There are a number of factors that shape the government technology ecosystem related to infrastructure, data and applications. Although many of these emerging concerns have little to do with technology, they could profoundly impact privacy, confidentiality and security.

Interoperability

As we consider the work of delivering citizen-centered services across departments, such as serving homeless veterans or feeding hungry children, having access to data is fundamental to understanding the effectiveness of programs, what services families are using, who is eligible and what could work better.

When programs consider interoperability and sharing data, staff members often first bring up concerns about privacy and confidentiality. In some cases, these discussions quickly result in agreed-upon approaches for identifying and solving problems, such as who can see what data. But it's rare to find common ground

between departments with different missions and responsibilities around protecting sensitive information.

The more likely scenario is interoperability will have to be carefully planned and executed to maintain forward progress and make everyone comfortable about the idea of sharing data.

For instance, after many years of identifying data that would help foster kids get psychotropic prescriptions, and in spite of a "competitive demonstration project" a few years ago that showed California exactly how the vendor community would solve the problem in real time, interoperability of systems that "serve" this vulnerable population remains elusive.

Again, most of this process doesn't involve technology; rather, it's more about nudging people to help them understand the power of sharing and developing, and finding ways to break down the barriers of opposition.

Some healthy angst about privacy and confidentiality will certainly occur. It's key to fuel these conversations early and often, to engage the naysayers on the path to "yes, we can share."

By designing interoperability as a part of programs, government can strike the right balance between data sharing and security.

The Notion of Agile

Agile is the new darling in government software development, and the federal government is encouraging states like California to consider the agile approach as a way to solve longstanding development issues that have plagued some projects. Although agile software development methods typically are conveyed as a way to avoid failure, agile projects can and do fail spectacularly. What isn't talked about as much is the role that leadership and the organizations themselves play in project failures.

When it comes to agile software development, security must be part of the agile methodology's "user stories" and should be managed and tagged as "features" in order to maintain proper focus on the importance of security, privacy and confidentiality. Similarly, "misuse" stories must be crafted and thread through the entire agile cycle. This is a significant process change for the security team, and it also creates pressure on the project team that's trying to remain small and nimble.

Maintaining an agile pace of development while including security considerations means process efficiency, which is itself a challenge for many public-sector organizations.

A Scrum project working on a two-week sprint cycle can't really wait for a 30-day turnaround on a security review. It's better to have the security personnel embedded in the project so that security is designed and built in from the beginning.

Another challenge: Public-sector projects sometimes are much more complex than private-sector projects, and agencies must understand and prepare for the impacts of an agile project, which is radically different from a traditional approach.

And the reverse also is true. The agency has an enormous impact on the project, a factor that is routinely ignored. What if your agile teams need data, information or decisions from other parts of the organization that aren't operating in an agile fashion? What if middle managers want to exert influence over the resources they have provided to the project but don't quite understand agile methods — how will their fumblings affect the project? Will technology initiatives be able to force changes in organizations accustomed to legacy processes? Time will only tell as California embarks on a major project, the Child Welfare System, using agile methodologies.

While serving in government, I often said we need to pay attention to people and culture when scoping any kind of changes, especially interoperability projects that would revolutionize the way programs deliver services. Workforce is the elephant in the room; we can't realize progress, innovation or success without buy-in from the workforce. But we routinely pay little or no attention to the care and growth of employees.

Cybersecurity, therefore, must be part of the conversation from the beginning, while we remain diligent throughout to anticipate the sometimes vague factors that are critical to protecting our assets.

Tech Chairman

Q&A with California Legislative Technology and Innovation Technology Caucus Chairman Evan Low

ASMDC.ORG

By Samantha Young

Born and raised in Silicon Valley, Assemblymember Evan Low describes technology and innovation as second nature to him and his millennial generation. But that's just not the case with many members of the Legislature. So the Silicon Valley Democrat partnered with Assemblymember Ian Calderon, D-Whittier, to form a venue where lawmakers could learn about technology and share ideas.

When it launched in October 2015, the California Legislative Technology and Innovation Caucus had 11 members. It has grown to 30 lawmakers from both parties and houses. Its members include former teachers, attorneys, small business owners, a sheriff's captain, a dentist, a financial planner — just to name a few. The group comes together to discuss and debate legislation, and provides a forum for members to learn about various advancements in technology and the implications and opportunities for government.

Q: Why did you create the Tech Caucus?

I had bill where I had a senator asking, "What is Uber?" I was shocked, and it was very apparent to me we needed to start from the very basics. Our mission is to educate our legislators about what the tech and innovation economy is all about.

I want to ensure California continues to maintain its competitiveness, not only in the nation but worldwide. That we could replicate Silicon Valley, not just in Silicon Valley, but across the entire state.

Q: The Tech Caucus is a relatively new entity. How have you and your co-chair sought to raise the profile of the caucus and tech legislation in general?

Often times a piece of legislation is in response to a news article or in response to a constituent complaint. We want to ensure we have the tech expertise in the Legislature. It's not just about the sexy Googles and Facebooks of the world, but the biotech industry, shared economy, drones, cybersecurity, procurement, manufacturing, the health-care sphere and the agriculture community. There are so many issues to cover.

Q: How often do you hear from the tech industry about legislative issues? Is there a partnership there?

This is a member-driven caucus, and it's a forum for members and industry alike to have dialog and education about issues. For example, we're having conversations with the tech industry about its workers, holding the tech industry accountable, and making sure we have a diverse workforce. Ensuring we have a workforce that supports everybody, not just the engineers, but also the rank and file. That there are livable wages for its bus drivers and janitors.

Technology + Business Consulting for What Lies Ahead

What's IN Your Horizon?

Project Management
Waterfall, Agile

Process
BPR, OCM, Salesforce
Performance Measures

Security
Assessment, Mitigation

Big Data
Analytics, Visualization

Cloud
IaaS, PaaS, SaaS

Propoint

TECHNOLOGY, INC.

www.propoint-technology.com

Propoint is a proud participant at the upcoming

Project Delivery Summit 2016

November 1st, Sacramento Convention Center

Facebook, in particular, has taken a leadership role in this area.

We've passed a number of bills in the Legislature on paid family leave, paid vacation and minimum wage. As part of our conversation with the tech industry, we say we would be encouraged if they could pass these philosophies within their own workforce. This is by no means a rubberstamp for the industry.

Q: Government is often criticized for being slow to embrace technology. What has your experience been as a legislator?

I wholeheartedly agree. But, by default, government is designed to be slow and to have separation of powers. By default, innovation and an innovation economy is disruptive. It changes the status quo. The change is much more forward-thinking than the regulatory environment. So, by default, government is always going to be behind. I want to know how can we ensure the gap isn't that wide.

Q: Can you give any examples of how government remains behind others on a technology issue?

Driverless vehicles are a good example. Not too long ago, it was the case when an innovator had a conversation with the DMV. The DMV's response was, "We don't have anything in statute." Other states said, "Uber, Google, you want to have driverless vehicles? Come to our state."

We can provide a forum for state agencies to use and talk about the innovation economy. So if they say it's not in statute, we'll say that we'll work with legislation that will help.

Another example are drones. The use of drones is a new thing. We don't have the laws and regulations in place because they are so new. We defer to the [Federal Aviation Administration], and then there are local ordinances. What we saw in California was a patchwork of ordinances. Now we are discussing if it's in the best interest of the state to provide a foundation so we can have a baseline.

Low describes the Tech Caucus as a venue that allows for meaningful dialog around potential legislation.

ASMDC.ORG

Q: Neither you nor your co-chair came from the tech industry. In fact, very few members of your caucus have tech backgrounds. How does a group of lawmakers with such a diverse background come together to represent technology?

The tech industry is not monolithic. Facebook and Google will have differences of opinion, as will Apple. We are not monolithic. Everyone has expressed an interest in a particular area. You have different leaders with different skill sets. Our caucus tackles different sectors and different areas, and different individuals are interested in different areas, and we come together. It transcends more than "I want to be a member because tech and innovation is a sexy issue."

It's the largest caucus of its kind in the Legislature related to a specific issue. We are not a caucus in name only. We have priority legislation, we have meetings, and we engage with departments and agencies.

There's not a structure in the Legislature for something like this. In the committee process, you have a three- or five-minute testimony of opposition or support. There's not the opportunity to have thoughtful conversation because of the legislative deadlines. This provides a venue and real, meaningful dialog.

Q: The issue of encryption on mobile devices is one example you have cited as a place where your caucus shared different opinions. How so?

Assemblymember Jim Cooper, D-Elk Grove, believed it was in the best interest for law enforcement to get data from the devices. Because of the terrorist attack in San Bernardino, there was much conversation around why he believed that. He had the opportunity to talk about these issues and why he believed it was important. I had concerns understanding the legislative intent and its implications.

We had a thoughtful dialog about why this bill was introduced and helped strengthen it. Without the existence of the Tech Caucus, where else would we have a venue for discussion in a non-combative way? [Cooper's AB 1681 was held in the Assembly Privacy and Consumer Protection Committee.]

Q: What is in the future for the Tech Caucus?

Hopefully we will bring in new members. We will be visiting different conferences and meeting with industry to talk about computing and procurement. We will be talking about the things we can be doing to help California be that much stronger.

Driving Security

By Matt Williams

A tour of the DMV Security Operations Center.

The computer systems at California DMV contain what could be the biggest collection of personally identifiable information — names, addresses, credit card information, Social Security numbers — in all of state government. The DMV processes nearly 26 million drivers' licenses, about 7 million ID cards, and 34 million registrations for vehicles and vessels.

It's no wonder, then, that this trove of sensitive data and the DMV's website can be a tempting target for malicious hackers and other nefarious actors. For instance, in 2013 the DMV was notified of a suspected attack on its credit processing infrastructure. Although DMV officials later asserted after a forensic investigation that no breach occurred, the incident convinced the department's leadership to bolster its cyberpreparedness and response capabilities.

The result was the creation of DMV's Security Operations Center, a new facility where the overarching goals are to actively manage security threats, vulnerabilities and incidents; reduce the impact of security incidents; and increase the department's overall security posture.

At a secure location within an unidentified building, a team of analysts is busy at work using state-of-the-art tools to track Internet security logs and Web traffic; eradicate phishing campaigns; protect servers and critical infrastructure; and defend against other attack and intrusion vectors. They call the room the "SOC."

With its low-slung fluorescent lights and rows of desks and cubicles, the center looks like a typical government office — except for the big-screen monitors mounted on one wall. The screens display real-time data from a variety of sources and systems, some of which DMV had at its disposal before the SOC went live in late 2015. Putting the tools all in one place, for the first time, is already paying dividends, officials say, because it now allows the security team to react more quickly, act proactively and find issues they wouldn't otherwise.

The analysts sometimes stand up from their desks and gather around one

From this undisclosed location, a team of analysts is using state-of-the-art tools to detect attempts to infiltrate the DMV's computer systems and deter other cyberthreats that could imperil Californians' personal data. Staff are working day and night from the secure facility, which officials say is the first of its kind in California state government.

PHOTOS FROM THE CALIFORNIA DMV

of the screens to collaborate and study what could be a new threat. Some of the analysts — the team will eventually grow to 16 people (their identities aren't readily public) — work during the day, others at night and some on swing shifts. The facility will be staffed around the clock, 24/7. In the SOC room, all of them access intelligence-based tools (the DMV will not disclose them publicly, either) that have been used in other settings, but rarely in government. The center's centralized view of the DMV's security landscape could be the first of its kind in California state government, the department says.

The state budget is funding the facility for the next two years. The DMV says its analysts already have rooted out cyberincidents at the SOC that are saving the department money or avoiding costs. So from purely a dollars-and-cents view, there likely will be at least some return on investment. But they concede it's difficult to put an exact value on enhancing the DMV's security posture as a whole. Officials say that it might make sense someday, if the SOC proves to have staying power, to bring in other state agencies and departments as customers, creating what could become a center of excellence.

From a wider perspective, the DMV says its Security Operations Center uses well established standards, practices and guidelines from the National Institute of Standards and Technology, Department of Homeland Security, and the White House, similar to how other SOCs have been formed around the country. The department also believes the SOC aligns with the executive order Gov. Jerry Brown issued last year to strengthen the state of California's cybersecurity coordination, as well as the federal Comprehensive National Cybersecurity Initiative.

"Moreover, we believe that we are positioning the SOC to integrate across the state government space as other facilities come online. Our goal is to function as a component of a statewide effort, sharing information, communicating real-time intelligence and working collaboratively to meet the threat against all state information assets and resources," the DMV said in a statement.

Policy Update

By Samantha Young

Cybersecurity took center stage in California's 2016 legislative session.

SHUTTERSTOCK.COM

Reports of government computers breached, state election databases penetrated, hospital networks held hostage by hackers and private retailers asking customers to change their passwords have been constant in 2016.

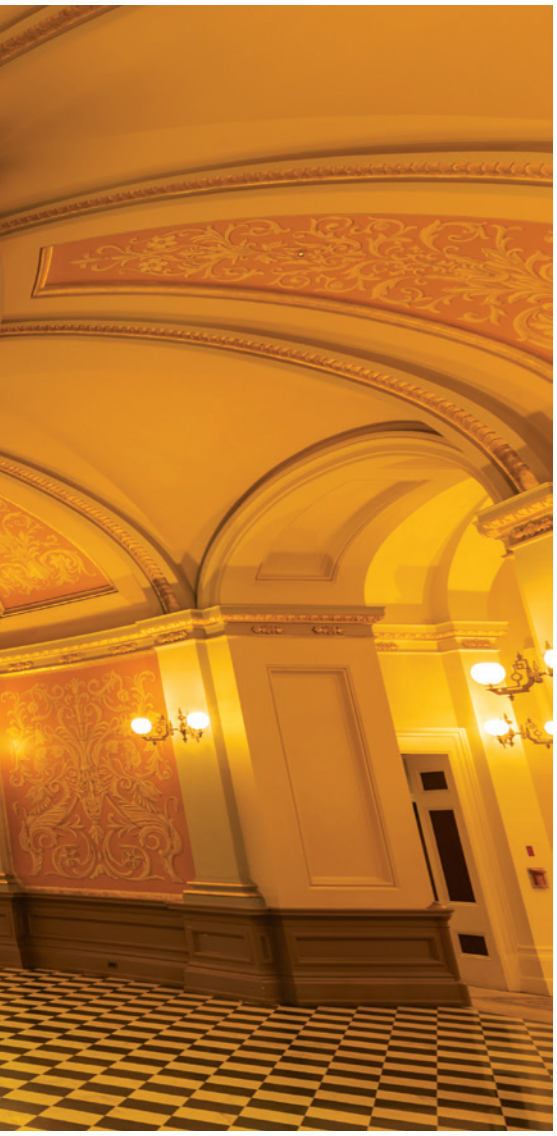
In this era of burgeoning cybercrime, California lawmakers this year have sent Gov. Jerry Brown a series of bills intended to bolster the state's cybersecurity and craft response plans should an attack occur.

"As we have seen just this week with breaches to election databases in Arizona and Illinois, states are under constant assault from cyberattacks," Kelly Hitt, director of state government affairs for California and Hawaii at CompTIA, said in an email to *TechWire* in late August.

"It is incumbent upon state governments, much like our member organizations, to secure their computer systems and networks to safeguard users' data," she said.

On the governor's desk are bills that seek to crack down on ransomware attacks, require government entities to inventory data that contain personal information, and mandate state agencies to report annual cybersecurity spending.

The Department of Technology could be tasked with crafting incident response standards that agencies must follow. AB 1841 by Assemblymember Jacqui



Irwin, D-Thousand Oaks, would require the standards be incorporated into the State Administrative Manual by 2018.

While a number of state agencies already have crafted incident response plans, some haven't had the money to implement them, said Srinivas Atluri, vice president of cybersecurity services at Anvaya Solutions Inc., based in Folsom.

"What this bill does now, it requires the plans and it will help the agencies get funding to formulate a recovery plan," said Atluri, whose company provides cybersecurity services to the public sector, utilities and private-sector organizations. "State agencies need to catch up to the security that's done in the private sector," he added.

The focus on cybersecurity comes amid reports of security breaches at the White House, U.S. health-care companies, the Democratic National Committee, universities and retailers. In August, the FBI disclosed it had discovered breaches of voter registration systems in Illinois and Arizona, and it urged states to beef up their computer systems ahead of the November election.

California lawmakers were especially sensitive to cyberissues after the state auditor reported many entities had weaknesses in their controls over information security, leaving some of the state's sensitive data "vulnerable to unauthorized use, disclosure or disruption." The report also faulted the Department of Technology for failing to ensure state entities had complied with mandated security protocols.

That led Sen. Bob Hertzberg, D-Van Nuys, to introduce legislation that would require state agencies to inventory all computerized data that contains personal information, a move security experts say is a critical step to both protecting IT assets and responding quickly in the event of a breach. State agencies hold records detailing the personal information of millions of Californians in their systems.

SB 1444 also calls for agencies to establish communication procedures between an incident response team, agency officials and individuals affected by a breach.

The state auditor report also triggered lawmaker curiosity about how much California spends on cybersecurity, an amount the administration could not provide earlier this year during a legislative hearing on cybersecurity. AB 2623 by Assemblymember Rich Gordon, D-Menlo Park, would require state agencies to report their information security spending to the Department of Technology every year.

In an effort to deter hackers in both the public and private sectors, lawmakers approved legislation that would make ransomware a crime of extortion under the state penal code. Under SB 1137, also by Hertzberg, hackers who render computer systems unusable until a ransom is paid could face a two- to four-year jail term and fine of up to $10,000.

While the identity of hackers can often be hard to trace, especially those overseas, security experts welcomed Hertzberg's push to classify ransomware as extortion.

"Just because it's hard to go after criminals, doesn't mean you shouldn't have something on the books," Atluri said.

Not all bills that sought to target cybercrime won approval from the Legislature.

Lawmakers earlier this year rejected AB 1881 by Assemblymember Ling Ling Chang, R-Diamond Bar, that would have required the state chief information security officer to develop baseline security controls for all agencies and departments under his or her jurisdiction.

They also held back AB 2595 by Assemblymember Eric Linder, R-Corona, that would have codified into law the California Cybersecurity Integration Center. The bill also would have required the Office of Emergency Services to develop a state cybersecurity strategy for California and authorize the office to administer federal homeland security grant funding.

And the state won't be administering a so-called "bug bounty" program where individuals who find network vulnerabilities could be eligible for a monetary reward. AB 2720 by Assemblymember Ed Chau, D-Monterey Park, sought to replicate programs used widely by the tech industry in an effort to fix bugs before they can be exploited by hackers.

Risks to 911 Systems

The governor's homeland security adviser warns of cyberthreats to next-gen 911.

By Samantha Young

SHUTTERSTOCK.COM

The move to an Internet-based 911 system in California comes with the promise of faster response times and the ability to send first responders valuable video and text messages. But it also carries a host of potential vulnerabilities that could disrupt emergency services.

"We need to keep in mind, that as we move forward, cybersecurity is a greater concern than ever before," California Office of Emergency Services (Cal OES) Director Mark Ghilarducci told a legislative panel in early August.

Ghilarducci delivered his comments before the Joint Legislative Committee on Emergency Management, which convened the two-hour hearing to examine California's move from its legacy 911 system, designed in 1980 for landline phones, to what is known as next-generation 911.

Like many other states, California is developing an Internet-protocol-based (IP) system intended to harness the latest technology and create a more efficient and effective emergency response network. The idea is that the growing number of wireless phone users could send digital information through the 911 network, via California's public safety answering points (PSAPs), to first responders.

The simple act of connecting the PSAPs over an IP platform brings a greater potential for a cyberattack, Ghilarducci told lawmakers. Such attacks are already occurring, he added.

For example, 911 callers who use a cellphone are routed through a mobile switching center rather than connected directly to a PSAP, allowing a hacker to potentially change the location of callers who need assistance, an act known as spoofing.

Other cyberintrusions that have plagued emergency services include instances where malicious actors use nonregistered burner phones to call in reports of an event to lure police response; flood the system with calls, preventing legitimate calls from getting answered; install malicious software known as ransomware onto computer systems; or insert themselves into the communications between callers and first responders and the PSAPs.

Recently a Bay Area agency was a victim of ransomware, Ghilarducci told lawmakers. He did not disclose the agency, and a Cal OES spokeswoman did not respond to *TechWire's* inquiry by the deadline.

"All of this doesn't mean that the next-gen 911 is ultimately unsecure," Ghilarducci said. "We do believe that proper training of staff and encryption of data and hardening of PSAPs and network data provider databases is going to be really important."

Specifically, Ghilarducci said it was critical the state partner with the private sector to address such cybersecurity threats and share information as California builds out its next-gen 911 system.

"Our communities and our citizenship should not be held hostage to cybersecurity threats that have the potential to cut them off from access to 911 and our law enforcement, fire and emergency medical first responders," Assemblymember Freddie Rodriguez, D-Pomona, said before he closed the hearing.

Rodriguez pledged to pursue legislation next year that would ensure reliable funding for deployment of a secure next-gen system, which is estimated at $900 million. That's money the state doesn't have in the dwindling account that pays for the current 911 network, upgrades and new equipment. Revenues collected in the State Emergency Telephone Number Account have fallen steadily since 2008 due to an outdated statutory fee designed for landline users.

Former Official Launches IT Consulting Business

Former Assemblymember and ex-Chico Mayor Rick Keene recently reopened his IT consulting business, with a focus on business development advocacy and procurement assistance for the C-suite and all levels of government. Keene served in the Assembly from 2001 to 2008, representing the 3rd District, whose boundaries in the north part of the state include Chico and parts of Butte and Colusa counties. "After three years of in-house business development work, I recently left SAS Institute to broaden my focus from assisting a single company to assisting multiple companies within the IT community to advance their technology solution footprint within California state government," said Keene.

Former State CIO Carlos Ramos Opens Tech Consulting Business

Former California CIO Carlos Ramos launched his own business focused on bringing leading-edge technology solutions to the public sector in May. His new venture, called Maestro Public Sector Strategies, is working with Silicon Valley companies that have keyed in on the commercial sector but haven't yet pursued business opportunities in government. Ramos, a resident of Elk Grove, Calif., said he's the principal of his business and is working with a few associates right now. He's targeting not just California state government but eventually the local, state and federal public sector across the country as well. Ramos said he sees his consultancy as being a bridge between Silicon Valley and state government.

California Hires First Chief Data Officer

LINKEDIN

California hired its first-ever chief data officer for state government, appointing 30-year-old Silicon Valley tech executive Zachary Townsend to the newly created position, the governor's office announced on June 30. Townsend, of San Francisco, will assume the role of chief data officer at the California Government Operations Agency. Townsend has been product management lead at payroll and health benefits company Gusto since 2016, according to the governor's office. He was director of product and channel management at Silicon Valley Bank from 2015 to 2016, co-founder and head of product at Standard Treasury from 2013 to 2015, and an affiliate at the Harvard University Berkman Klein Center for Internet and Society from 2013 to 2014.

SHUTTERSTOCK.COM

Secretary of State's Office Names CIO as New Projects Emerge

The California Secretary of State's Office has hired Rita Gass to the position of CIO. Her first day was June 13. For the past eight years Gass was the CIO of the California Conservation Corps. During her tenure there, the corps won an award in 2014 from the National Association of State Chief Information Officers for its rapid deployment of a cloud-based recruiting system. Gass has worked for the state for more than 20 years in positions such as network and system administrator for the California Franchise Tax Board (1999-2000), senior system engineer (2000-2004) and technical project manager for the California Energy Commission (2004-2008).

Senator Fighting Ransomware Hit with Cyberattack

A day after the state Senate approved legislation outlawing ransomware on May 31, the bill author's website was hacked. In a tweet the next day, Sen. Bob Hertzberg, D-Van Nuys, showed a screen shot of his hijacked Senate website. "All of our shared drive files have been encrypted with software typically used in ransomware attacks," Hertzberg spokesman Andrew LaMar wrote in an email to *TechWire*. "So we cannot access our shared files." The attack occurred between the evening of June 1 and the morning of June 2, he added. Lawmakers on the Tuesday before had unanimously approved legislation by Hertzberg that would make it a crime for anyone to knowingly put ransomware on a computer's system, network or data.

CHP Selects Vendor for Body-Worn Camera Pilot

The California Highway Patrol intends to award a contract for its body-worn camera project to Taser International Inc., according to state records released in June. CHP expects that the test will begin this summer. Prior legislation requires the CHP to develop a plan for implementing a body-worn camera pilot program. CHP will test the body cameras at field offices in Oakland and Stockton. At the conclusion of the pilot, CHP will send a report to the Legislature on the test's outcome, likely in late 2017 or early 2018. The Department of Finance is proposing to spend $919,000 on the pilot.

Integration and Beyond

Complex modernization programs require leadership across multiple stakeholders, expert navigation of requirements and experience managing a multi-vendor technology ecosystem. As a local IT partner for California with global scale, that's where CGI excels.

CGI brings the right combination of business understanding, systems integration skills, governance and domain expertise to our clients' most complex challenges. With deep expertise in both business and technology environments, clients trust CGI to deliver best fit integrated systems and applications — and so much more.

cgi.com/california

CGI

Experience the commitment®

CalVet IT System 'Flawed,' State Auditor Finds

A $28 million enterprise IT system developed for the California Department of Veterans Affairs (CalVet) has suffered from functionality issues and project management and oversight deficiencies, according to a report from the State Auditor released June 16. The Enterprise-Wide Veterans Home Information System was implemented beginning in mid-2012. The auditor recommended that CalVet define IT project management responsibilities for staff and establish a policy to use separate contractors for independent oversight functions on future IT projects. The auditor also recommended that the Department of Technology make changes to project oversight processes.

Controller Reaches $59M Settlement with Tech Vendor over Failed Payroll System Modernization

California State Controller Betty Yee announced in June that her office reached an agreement with SAP Public Services Inc. that resolves lawsuits over the 21st-century statewide payroll modernization project known as MyCalPays. The state suspended the payroll project and terminated its $90 million contract with SAP in 2013 after a pilot demonstration was unsuccessful. Under the terms of the settlement, SAP will pay the State Controller's Office $59 million and also abandon its claims against the State Controller's Office amounting to about $23 million. The settlement stipulates that the State Controller's Office and SAP each do not admit any liability or fault concerning the claims and allegations made between them.

Sacramento's Innovation Fund Will Invest in Local Companies, Mayor Says

The city of Sacramento will invest in local companies and start a grant program as part of a multimillion-dollar plan to bolster the community's innovation economy, Mayor Kevin Johnson said in May. The city is going to invest $1 million in local companies this year, Johnson said. Selections will come from proposals submitted to a new mayoral tech council. The investments potentially could yield a profit for Sacramento that would be used to continually replenish the city's $10 million Innovation and Growth Fund. Sacramento also is launching a new grants program of up to $1.5 million called "RAILS." The acronym, which aligns with the city's railroad heritage, stands for Rapid Acceleration, Innovation and Leadership in Sacramento.

WWW.CALPERS.CA.GOV

Treasurer John Chiang Calls for IT Contracting Reforms

State Treasurer John Chiang said in June that California must build partnerships with the private sector to develop IT projects that are fair, efficient and effective. "We can't continue to have the same contracting process where the focus is on winning the bid and not staying focused on putting out an incredible product," Chiang told *TechWire* in a wide-ranging phone interview to discuss his 2018 gubernatorial bid. His comments came a day after the state reached a $59 million settlement with SAP Public Services Inc., ending lawsuits over the 21st-century statewide payroll modernization project known as MyCalPays.

California's Vendor Performance Scorecard Moving Forward

A vendor performance evaluation system that has been in the works the past two years appears to be moving forward despite the departure of state CIO Carlos Ramos. California says the initiative, which some have called a "scorecard," will be factored into future state IT procurements after a pilot occurs sometime in 2016. The Department of Technology is continuing to look for suitable IT projects to participate in the pilot. The Contractor Performance Evaluation Scorecard would measure five key performance indicators, included in the language of RFPs and signed contracts. Overall ratings would look at scope, schedule, quality and timeliness.

California's Early Adopters of Open Data Share Lessons Learned

The report, called *Making Open Data Work in California's State Government: Lessons from Early Adopters*, is available on the California State Library's GitHub page. The report brings together knowledge from people and organizations across state government, said Anne Neville, director of the California Research Bureau, which authored the report. The California State Library hosted a forum and panel discussion in June to share the report's findings. A video of the session is online.

State CIO Hopes for More Collaboration with Vendors

TechWire asked California's new state CIO, Amy Tong, on July 11, what she wants from the vendor community now that she's the director of the Department of Technology. "To sum it up, more collaboration. And I'm not saying that as just 'collaboration' as a buzzword. If you're looking at the whys of the [state's] move to agile, the focus on cybersecurity maturity, and the focus on oversight and the project management framework — and soliciting input on the vendor performance scorecard — at the end of the day what we're looking for is the state taking on more accountability in the delivery of technology solutions to state programs."

Ballot Measures Could Expand State Tech Projects

At least three measures that have qualified for California's Nov. 8 ballot could force the state to either broaden current IT systems or launch entirely new projects. Prop. 64 would allow adults to possess up to an ounce of cannabis and grow as many as six plants. The initiative would pose a major expansion of an IT system that California is in the beginning stage of developing to "track and trace" the movement of medical cannabis in the state. Two other ballot measures would expand technology: Prop. 54 would put in place a 72-hour wait period before a final vote on legislation after a bill is amended and require the Legislature to make audiovisual recordings of all its proceedings (except in closed session) and post them online. Prop. 63 "prohibits possession of large-capacity ammunition magazines, and requires their disposal ... destruction or removal from state." A new California Department of Justice database likely would result.

Amy Tong Appointed California CIO and Department of Technology Director


GOVTECH.COM

Amy Tong will stay on as California's state CIO and Department of Technology director after serving in an interim capacity for three months. Tong has been appointed to the position, Gov. Jerry Brown's office announced on June 30. Tong took over the state government's top tech post in March, when Carlos Ramos, who was appointed state CIO in June 2011, retired from state government and launched a consulting firm. She has worked in California state government for more than 20 years in positions of increasing responsibility. Tong was appointed deputy director of the Office of Systems Integration in July 2014 and previously was named the California State Lottery's deputy director of information technology services — its CIO — in December 2012.

11 Vendors Qualify for Pool of Agile Developers

The California Health and Human Services Agency has selected 11 vendors for a prequalified pool of agile developers eligible to work on the Child Welfare Services/Case Management System replacement and other projects, officials announced on July 13. The 11 vendors "all received assessments of 'highly qualified' based upon their submission of a functioning prototype, working source code and a narrative description of the technical approach used to create the prototype," the agency said. The selected vendors are Accenture, Binti Inc., Cambria Solutions, Case Commons, CivicActions, Deloitte, EngagePoint, Exygy, Oliver Wyman, Portland Webworks and Taborda Solutions. These firms will provide user-centered design and agile software development services.

Governor's Office Backs Precision Medicine Ideas Contest

The California Governor's Office of Planning and Research and the Governor's Office of Business and Economic Development (GO-Biz) are partnering with a Silicon Valley entrepreneurship organization to call for ideas that utilize precision medicine. The winning entrant in the Precision Medicine Impact Challenge will receive a $10,000 prize from Singularity University and an invite to present a prototype at the Exponential Medicine conference in San Diego this fall.

Child Welfare Services — New System Project Director Retiring

Child Welfare Services — New System (CWS-NS) Project Director Les Fujitani retired from state government at the end of August, he confirmed to *TechWire*. Fujitani has been the project director of CWS-NS for the past eight years, and he is the co-founder of a consulting firm specializing in IT employment services. Fujitani has worked in a variety of roles in the IT industry for more than 20 years. Duties of the CWS-NS project director include directing activities to procure and recruit design, development, implementation and DevOps services.

State Archives Digitizes Exhibits, Puts Them on Google

The California State Archives is partnering with Google to present some of its exhibits in digitized form to a worldwide audience online. Secretary of State Alex Padilla and the Google Cultural Institute announced the project in late June at the California Museum in Sacramento. The first three collections now available online feature California state parks, the California Secretary of State's office and campaign materials created by the nation's first political consulting firm.

State Selects Contractor for California Dental MMIS

In June, the Department of Health Care Services (DHCS) issued a notice of intent to award Hewlett Packard Enterprise for its competitive procurement on fiscal intermediary services for the Medi-Cal Dental Program. "DHCS intends for the selected proposer to take over the existing CD-MMIS [California Dental Medicaid Management Information System]," the department wrote in a Request for Proposal last year. A related bid for the California Dental Administrative Services Organization was awarded to Delta Dental, DHCS also announced on June 17. HP Enterprise and Delta Dental will coordinate on the project.

Deloitte.

PROGRESS

Risk powers progress.

Transforming state government to interact with citizens in real time, across multiple technology platforms, creates cyber risk. It's unavoidable. But it doesn't have to derail progress.

As a recognized leader in cybersecurity, we can help you navigate stakeholders and facilitate the evolution of your cyber risk program. Our Secure.Vigilant.Resilient.™ approach, coupled with new ways of engaging, can provide you with options to better manage cyber risk so you can focus on what matters. Let's make progress together.

Strategy & Governance

- Governance, Risk & Compliance Strategy and Implementation
- Enterprise Security Architecture
- Agency Governance
- Third Party Risk Management
- Privacy

Secure

- Identity & Access Management
- Enterprise Application Integrity
- Application Security
- Data Protection
- Infrastructure Security

Vigilant

- Security Operations Optimization
- Application Risk Monitoring
- Threat Intelligence & Analytics
- Vulnerability Management
- Outsourced Cyber Operations

Resilient

- Cyber Incident Response
- Cyber Simulation & War Gaming
- Technical Resilience

Learn more at: **www.deloitte.com/us/state**

FI$CaI READY

She's ready, are you?

Learn more at fiscalready.com

M Corp

THE-MCORP.COM