

Solutions for
state and local
government.

OCTOBER/NOVEMBER 2016

INSIDE:

All Together Now:
New partners round
out the security team.

Cyber and the Law

Do elected leaders
grasp the size of
the threat?

OUT OF THE

SHADOWS

**CYBERSECURITY CLAIMS ITS RIGHTFUL PLACE
AT THE CENTER OF THE CONVERSATION.**

PLUS:

How to survive
when you can't
afford a CISO.



50% of surveyed legislators say their state has an **inadequate number** of cybersecurity personnel.

Learn more by downloading a complimentary copy
of the cybersecurity policy guide at:
governing.com/cyberguide

Produced by:

GOVERNING
INSTITUTE



AT&T

NATIONAL
CYBERSECURITY
ALLIANCE

COVER STORY

18 / Massive Connectedness

Public safety now sits alongside IT as formal structures emerge to take on cyberthreats.

By Adam Stone

24 / Cyber Exposure

More governments are protecting their IT assets with cyberinsurance. Here's what you need to know when considering a policy.

By Robert Lemos

30 / Legislating Cybersecurity

State lawmakers begin to recognize their responsibilities with cyberthreats.

By David Rath

36 / Scaling Down Security

A smaller staff and a smaller budget don't lessen the cybersecurity burden. Here's how cyberleaders at the local level are approaching today's threats.

By Lisa Kopochinski

42 / Erasing Human Error

Can security awareness training change behavior and reduce risk?

By Tod Newcombe



MIKE GERAGHTY,
DIRECTOR, NEW JERSEY
CYBERSECURITY AND
COMMUNICATIONS
INTEGRATION CELL.

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

EDITORIAL

GT Editor: **Noelle Knell**, nknell@govtech.com
 Managing Editor: **Elaine Pittman**, epittman@govtech.com
 Web Editor & Photographer: **Jessica Mulholland**, jmulholland@govtech.com
 Assistant News Editor: **Eyragn Eidam**, eeidam@govtech.com
 Chief Copy Editor: **Miriam Jones**, mjones@govtech.com
 Copy Editor: **Lauren Harrison**, lharrison@govtech.com
 Senior Editor: **Tod Newcombe**, tnewcombe@govtech.com
 Staff Writers: **Ben Miller**, bmiller@govtech.com
Jason Shueh, jshueh@govtech.com
Colin Wood, cwood@govtech.com
 Contributing Writers: **Lisa Kopchinski**, **Robert Lemos**,
David Rath, **Adam Stone**
 Editorial Assistant: **Ryan McCauley**, rmccauley@govtech.com

DESIGN

Chief Design Officer: **Kelly Martinelli**, kmartinelli@govtech.com
 Graphic Designer Pubs: **Kimi Rinchak**, krinchak@govtech.com
 Senior Designer Custom: **Crystal Hopson**, chopson@govtech.com
 Production Director: **Stephan Widmaier**, swidm@govtech.com
 Production Manager: production@govtech.com

PUBLISHING

VPs OF STRATEGIC ACCOUNTS:

Kim Frame, kframe@govtech.com
Stacy Ward-Probst, sward@govtech.com
Arlene Boeger, aboeger@govtech.com
Shelley Ballard, sballard@govtech.com
Karen Hardison, khardison@govtech.com

SALES DIRECTORS:

Melissa Sellers, msellers@govtech.com
Tracy Meisler, tmeisler@govtech.com
Audrey Young, ayoung@govtech.com
Lara Roebbelen, lroebbelen@govtech.com
Carmen Mendoza, cmendoza@govtech.com
Deanne Stupek, dstupek@govtech.com
Lynn Gallagher, lgallagher@govtech.com
Kelly Schieding, kschieding@govtech.com

ACCOUNT EXECUTIVES:

Paul Dangberg, pauld@govtech.com
Christine Childs, cchilds@govtech.com
Rebecca Regrut, rregrut@govtech.com

BUS. DEV. MANAGER:

Lindsey Albery, lalbery@govtech.com
Kathryn Nichols, knichols@govtech.com

SR. SALES ADMINISTRATOR:

Kelly Kashuba, kkashuba@govtech.com

SALES ADMINISTRATORS:

Alexis Hart, ahart@govtech.com
Jamie Barger, jbarger@govtech.com
Jane Mandel, jmandel@govtech.com
Morgan Rothenbaum, mrothenbaum@govtech.com
Ashley Flynn, aflynn@govtech.com

Sr. Dir. of Sales Operations: **Andrea Kleinbardt**, akleinbardt@govtech.com

Custom Media

Managing Editor: **Jeana Bigham**, jbigham@govtech.com

Dir. of Web Marketing: **Zach Presnall**, zpresnall@govtech.com

Web Advertising Mgr: **Adam Fowler**, afowler@govtech.com

Subscription Coord: **Enie Yang**, subscriptions@govtech.com

CORPORATE

CEO: **Dennis McKenna**, dmckenna@govtech.com

President: **Cathilea Robinett**, crobinett@govtech.com

CAO: **Lisa Bernard**, lbernard@govtech.com

CFO: **Paul Harney**, pharney@govtech.com

Executive VP: **Alan Cox**, alancox@govtech.com

Chief Content Officer: **Paul Taylor**, ptaylor@govtech.com

Dep. Chief Content Ofc: **Steve Towns**, stowns@govtech.com

VP Research: **Todd Sander**, tsander@govtech.com

Government Technology is published by eRepublic Inc. Copyright 2016 by eRepublic Inc. All rights reserved. *Government Technology* is a registered trademark of eRepublic Inc. Opinions expressed by writers are not necessarily those of the publisher or editors.

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.govtech.com.

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

Printed in the USA.

40 / Who You Gonna Call?

Have a pressing cybersecurity question or unsure what to do after a breach has been detected? Here's a look at some of the key resources available to state and local agencies.

COLUMNS

5 Point of View

Cybersecurity remains a top priority for CIOs nationwide.

8 Becoming Data Smart

A five-point plan to cultivate citizen support.

10 Four Questions

Benny Chacko, CIO of the Los Angeles County Probation Department, on understanding your agency's unique business needs.

48 Cybersecurity Strategies

Data can help public agencies predict the future.

52 Data Points

The U.S. must take action before it falls too far behind in the race to build smart cities.

54 GovGirl on Social

Tips for making social media a team effort.

FOLLOW
US ON



NEWS

6 govtech.com/extra

Updates from *Government Technology's* daily online news service.

14 Big Picture

Key trends from the Digital States Survey.

50 Products

InFocus Corp's Mondopad
 Ultra, Spectra Logic's BlackPearl
 P storage, Xerox WorkCentre 3345 Printer

53 Spectrum

More research, more science,
 more technology.



IN OUR NEXT ISSUE:

Breaking Down 2016

A look at the most impactful tech stories and trends of the year.

Who Went Where?

Key personnel changes and how they affected the public sector.

Data Dive

Highlights from the Center for Digital Government's 2016 surveys.



Holding Steady at No. 1

One major takeaway from this year's Digital States Survey was near-universal agreement that cybersecurity is the top priority for CIOs. It was No. 1 on their minds when the Center for Digital Government last conducted the survey in 2014 too. That's why we devote this issue to covering several aspects of cybersecurity, and how state and local governments are working to get a handle on it. It's no longer necessary to prove that it's important. Everybody knows. Here are a few highlights from the stories in the pages that follow, easily supported by what's happening in so many other jurisdictions across the country.

You can't (and shouldn't) do it alone.

Much of our reporting underscores the fact that successful efforts stretch far outside of the offices of IT staff, even outside of government. Cyber and physical security continue to come together under the same umbrella, uniting a bigger group of stakeholders than in years past. Multifaceted coalitions are cropping up across the country.

Colorado's planned National Cyber Intelligence Center, announced last year by Gov. John Hickenlooper, is just one of many great examples. Partners include higher education, private industry, government and the military. CIOs and CISOs in broad endeavors like this now routinely sit across the table from emergency management staff and other law enforcement representatives — recognition that traditional one-dimensional approaches aren't effective against today's threats.


It takes money. Executive support is critical to any jurisdiction's cyber efforts. If the governor/county executive/mayor doesn't understand why cybersecurity deserves his or her attention, good luck

securing needed funding. But the growing chorus of organizations making the case for investments in cyber (e.Republic's Center for Digital Government, the National Governors Association, the National Conference of State Legislatures, NASCIO, etc.) along with more concerted efforts by state IT leaders to bend policymakers' ears on the subject is having an impact.

In Indiana, a \$15 million budget allocation was tied to cyber initiatives, some of which went toward the state's Information Sharing and Analysis Center, a Security Operations Center and a risk and compliance program. Minnesota Gov. Mark Dayton made a \$46 million budget request this year for agency-level security upgrades, breach response guidance and activities like tabletop exercises. This evidence is far from isolated.

Help is out there. As the field and the threats mature, so has development of standards and best practices for cybersecurity. The NIST framework is helping jurisdictions assess their cyberstatus using a common frame of reference, and CIOs have told us that federal standards like FISMA and FedRAMP ease the vetting burden when considering the security of cloud technologies.

In addition, the Multi-State Information Sharing and Analysis Center has branches in every state, offering help to governments at all levels, while regional collaborative groups abound — an especially valuable resource to smaller governments that lack the resources to fully prepare for threats on their own. See *Who You Gonna Call?* on page 40 for a more complete list of ideas for cybersupport.

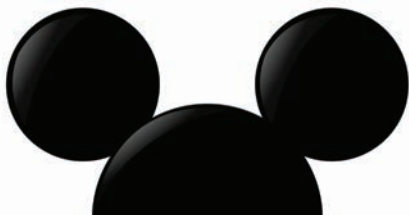
There's much more to cover than this column or this issue of the magazine could possibly address. But it's encouraging that we're all on the same page. 

RAISE YOUR VOICE

Your opinions matter to us. Send comments about this issue to the editors at editorial@govtech.com. Publication is solely at the discretion of the editors. *Government Technology* reserves the right to edit submissions for length.

Laying the Foundation

Kansas is joining the growing ranks of states employing a modular approach to developing Medicaid Management Information Systems (MMIS). In August it was announced that Hewlett Packard Enterprise will upgrade the Kansas Department of Health and Environment's MMIS and deploy the system in modules over the next three years. The \$215 million project, which began earlier this year, reflects the trend of states moving away from massive custom-developed systems that tend to run over budget and past deadlines. The upgrade will give the state a new foundation for Medicaid, said department Secretary Susan Mosier, and provide government leaders with information in near real time that allows for better decision-making.



Embrace Your Inner Mouse

Ottawa County, Mich.'s employees have been getting schooled on a type of training not typically found in government's halls. Over the course of more than two years, *The Disney Way* author Bill Capodagli worked with the county to guide employees through a multiday training based on Disney's customer service vision. Of the roughly 1,000 county employees, almost all have experienced the training, including the county's 28 IT staff members. "Part of it is to understand that IT is not a department that works behind closed doors," said David Hulst, the county's innovation and technology director. "We're accessible. It's all a part of building relationships between IT and other departments."



The decrease in the Bexar County, Texas, Jail's inmate population thanks to the addition of data analytics to the decision-making process.

WHO SAYS?

"We can see clearly now, thanks to Pokemon Go, what the rules of the road are. The challenge on the table right now is how simple and fast can you make [augmented reality] information appear."



govtech.com/quote-Oct16

MOST READ STORIES ONLINE:

Better Mapping Helps Federal, State, Local Governments Fight Zika
1,610 VIEWS

Cyberattack Compromises Unknown Number of Voter Records in Illinois
1,595 VIEWS

Millennials in Government — or Not?
1,574 VIEWS

4 Ways Self-Driving Trucks Could Improve Transportation
1,532 VIEWS

The Pokemon Go Effect: Why Augmented Reality Is Finally Taking Hold in Government
1,371 VIEWS

California Lt. Gov. Gavin Newsom Talks Transparency, Civic Tech, State IT Reforms
1,310 VIEWS

“The statement ‘Sometimes civic tech comes straight from the people,’ while accurate, should also stipulate that all civic tech should involve the people, and that goes beyond simply being the recipient of the technology, such as in the case of Code for America’s CalFresh Balance app. It doesn’t lessen the fact the Balance app provides an excellent public service. My point is we need to be sure we are not labeling everything government does with technology that benefits citizens to automatically attach the ‘civic tech’ label if we have not engaged citizens to exercise their rights, duties, privileges and obligations of citizenship to participate in that technology’s inception to its completion.

Dbevarly in response to *What Is Civic Tech?*

“The most important observation is the last one, that fiber isn’t necessarily the end game. In the overall scheme of things, consumers would rather have 50-Mbps mobile networks that reach everywhere than an arbitrarily fast wired network that only reaches their home and their office. Fiber is a necessary component of mobile networks, but it doesn’t need to go everywhere. The best networks are combinations of the best available tools.

RichardBennett in response to *Municipal Broadband? Federal Court Tells FCC ‘No’*

“I was interim city manager in California when we had a controversial development project. Despite having a ‘rumor page,’ which we called our ‘Frequently Asked Questions’ page, we still couldn’t overcome the misleading information of the plan’s opponents. It was easy for opponents to gain support for rumors like ‘the project will contaminate water,’ and we came off as defensive big government, even when we could point to studies showing that the water wouldn’t be contaminated. While we had some control over Facebook, rumors were rampant on sites like Nextdoor where our access was limited.

Kathy in response to *3 Major Concerns About Facebook Comments — and How to Address Them*



CITIZEN FEEDBACK

INSPECTION DATA

TRAFFIC DATA

CRIME DATA

PERMIT DATA



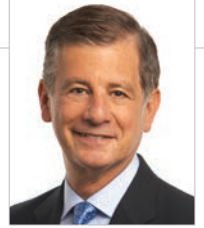
Turn Data into Action

Building a System of Insight

Who are the decision-makers in your organization? Field workers, analysts, data scientists, or government executives? All of the above? Smart communities move from siloed data to a hub of information to be shared with others—a system of insight. Esri's ArcGIS® platform provides the tools to quickly analyze information, communicate it to stakeholders, and move to effective action. As the expectation to make quicker decisions grows, empower your organization to build a complete data strategy.

To learn about what Esri can do for your community, visit esri.com/DataDrivenDecisions.





Civic Engagement

A five-point plan to cultivate citizen support.

A tech champion in a government entity needs to cultivate allies, especially when the innovation presents transformative opportunity. In my last column, I wrote about the importance of obtaining buy-in from departments when launching new tech initiatives — a key way to ensure initiatives fully take hold and revolutionize city hall. But another crucial stakeholder must be engaged as well: the public.

An intentional approach to cultivating citizen support would incorporate several threads. First and most obvious is the quality, quantify and usability of open data. Usable open data includes ease of use and high-quality visualization, which allow the casually interested resident to track his or her service request to see both the response time for that request as well as how the city is doing over time on various metrics.

The second element of citizen stakeholder management includes creating the conditions for advancing citizen collaboration, from crowdsourced traffic patterns to apps and algorithms built by civic tech community groups. Whether the city organizes big app contests with prizes or simply adopts the apps, utilizing residents as co-developers of knowledge and co-developers of apps will produce support as well as improve the quality of life.

Third, any effort to build community support for digital advancements must start with trust. When technology

is involved, the issue of trust must start by addressing privacy and security, or else the new initiatives will prematurely end. Residents want to know exactly what city hall is doing with personal data, how it is being handled and the lengths officials are going to in order to protect it.

As cities continue to pursue more expansive data projects that more directly affect citizens, such as the Internet of Things (IoT), the opportunities and risks related to data aggregation and mining will increase exponentially, as will the risk of having to cancel, delay or substantially modify a new project, all of which can be costly.

Seattle addressed many of these concerns with its citywide digital privacy initiative, launched in fall 2015. Led by CTO Michael Mattmiller, Seattle worked with citizens to develop a list of principles and an ethical framework to guide city departments on data usage and privacy matters. The policy requires departments to complete annual online privacy and security awareness classes to stay up-to-date on the latest practices. It will also provide them with a Privacy Impact Assessment protocol that requires departments collecting new types of data, embarking on new programs or introducing new technologies to go through a process to self-assess any privacy risk that innovation may entail.

By partnering with residents to develop these policies and continuing to actively inform citizens of how the city is using and protecting their data, Seattle can alleviate and pre-empt future

resident concerns about how data is handled in new innovative ventures.

Fourth, transparency around how a city plans to use the data will not only build support but also dampen anxieties. Chicago worked hard to ensure citizens' voices were heard in its Array of Things sensor project. The city partnered with the Smart Chicago Collaborative to inform residents about the project and garner feedback about proposed plans and policies. They held a series of neighborhood meetings where, beyond simply asking for feedback, city officials sought input and advice on sensor locations, privacy and security plans, and how residents want IoT and similar initiatives to be used to improve city life in the future. Chicago can now use the results of these meetings to better guide its Array of Things implementation, pre-emptively ease residents' worries and develop stronger IoT plans for the future.

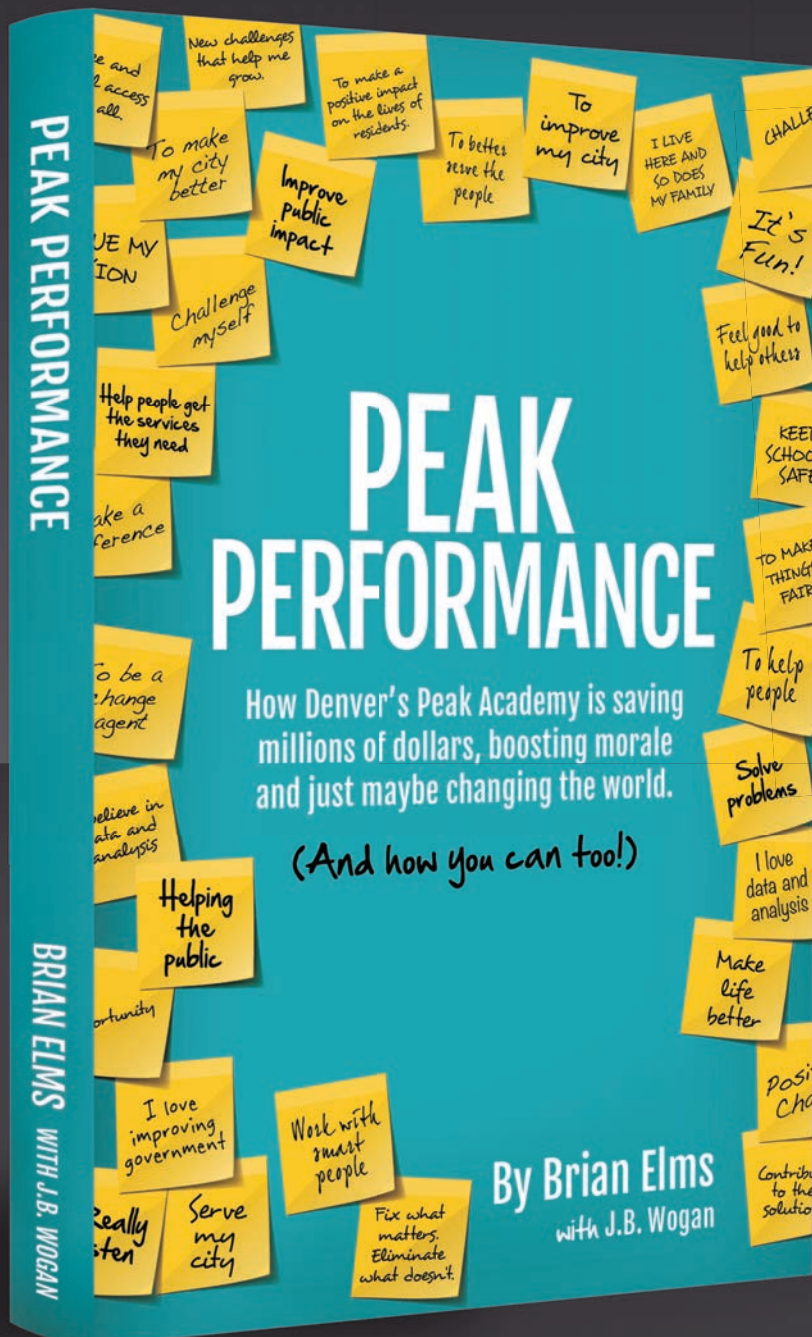
Fifth, any process of collaboration requires a city to find a way to curate and use the information it receives and to find ways to use social media and even SMS texting to improve the way it involves and responds to those who often are ignored.

Collaborating with citizens to gain buy-in on new initiatives can be a much larger task for a city than gaining internal support, but doing so is critical to ensure new technologies are being best leveraged to improve civic life. Including residents throughout all stages of a project can help cities prevent disputes, implement smarter policies and better solve pressing civic problems. **Bit**

Stephen Goldsmith is a professor at Harvard Kennedy School and director of the Innovations in Government Program and Data-Smart City Solutions. The former mayor of Indianapolis, his latest book is *The Responsive City: Engaging Communities through Data-Smart Governance*.

"This book is a must for anyone who believes government can make a difference in our lives. ... *Peak Performance* details how a courageous and visionary mayor and a highly dedicated workforce can give their citizens a more efficient and effective government ..."

Former Pennsylvania Gov. Edward G. Rendell,
author of *A Nation of Wusses: How America's Leaders
Lost the Guts to Make Us Great*



A quick, honest
& fun must-read
for anyone who
lives in a city
or works in an
organization!

Theresa Reno-Weber,
Chief of Performance & Technology,
Louisville, Ky.

Order today at
**[governing.com/
peakperformance](http://governing.com/peakperformance)**

Also available on amazon.com.
Bulk discounts available.





JONAH LIGHT PHOTOGRAPHY

Benny Chacko

CIO, Los Angeles County Probation Department

Understanding the more technical aspects of the job of a public-sector IT professional is just the beginning. Modern CIOs bring a very diverse set of backgrounds — educational and professional — to their positions, and the agencies they work for reap the benefits. CIO Benny Chacko, of the Los Angeles County Probation Department, supplemented his bachelor's degree in computer science with an MBA in finance to broaden his skill set, and had a number of private-sector jobs before joining the county workforce. We caught up with Chacko recently at the Los Angeles Digital Government Summit, where he talked about the importance of understanding your agency's unique business needs and thinking beyond technology.

By Noelle Knell, Editor

1 What are some of the unique challenges you face as the IT leader at the Probation Department?

The challenge that a CIO for Probation has is it's really a mix of services. We have a law enforcement aspect to it, we have a social service aspect to it and we also have a health service aspect to it. So it's getting someone who can bridge the gap in those three different domains and figure out a way to really drive strategy within the organization and push technology to enhance the business.


2 What are the most important skills a public-sector CIO needs beyond an understanding of technology?

It's really understanding business process, engaging with the executives, and at the same time coming back and translating strategy and vision from the executive team to the IT team to actually execute and drive projects forward to completion. So it's definitely people skills and communication skills, whether it's written or speaking skills. Those are absolutely critical, and then engaging not only with the executive team but also your own team ... looking for solutions based on problems that you observe, whether that's walking through a facility or observing someone do a certain business process. It's being able to bridge the gap and look for a solution that can help make their job easier.

3 What are some disruptive technologies that are impacting your work?

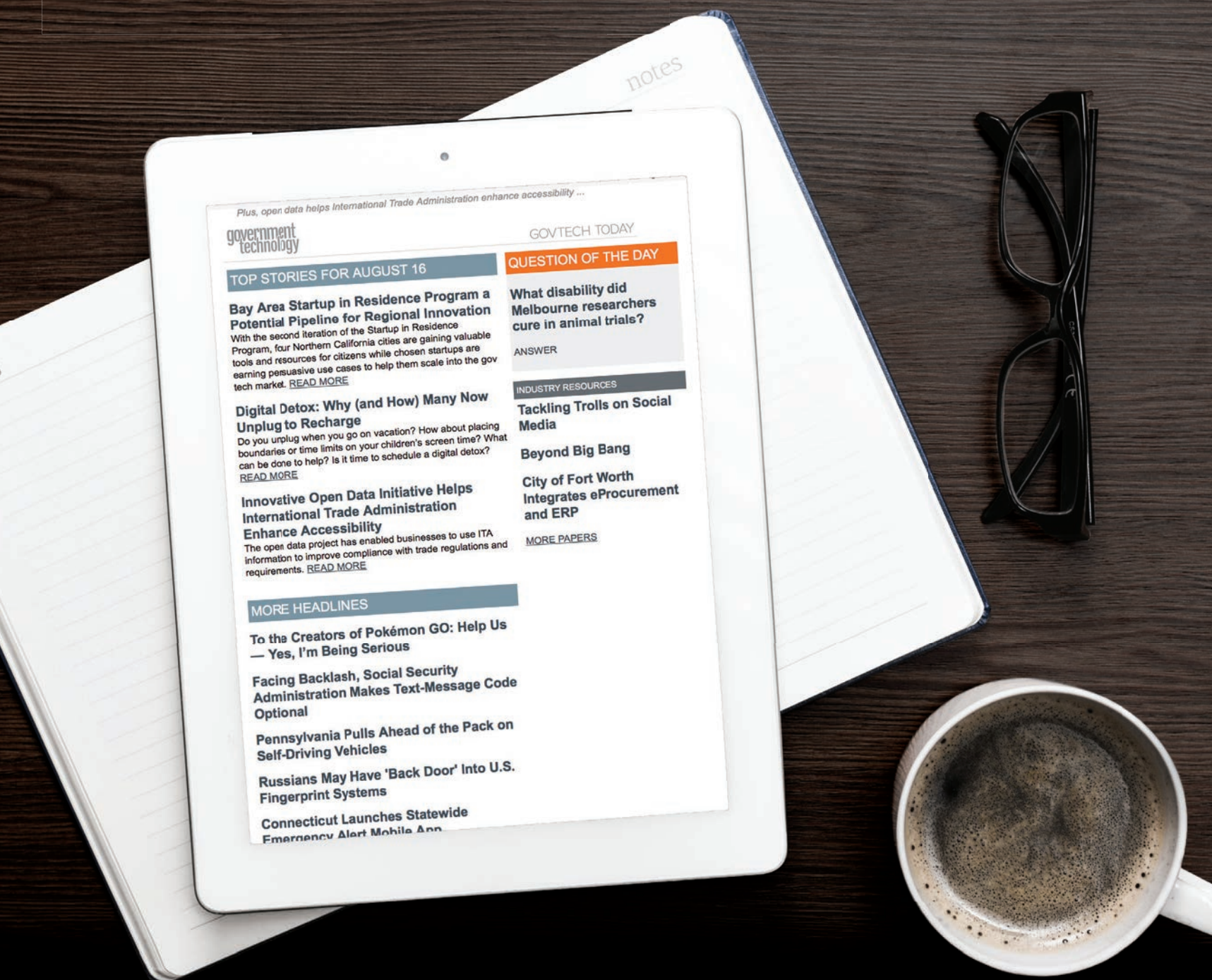
Data overall has been a challenge because we collect pieces of data in every form or fashion and it's spread out through the entire department. It's disruptive in the sense that we need to make something meaningful out of it. It's collecting data — whether it be video footage or actual text information within a database — and being able to quantify certain values of our service and provide metrics to our executives to make decisions. We're in the beginning phases of that.

4 Can you apply that data toward reducing recidivism?

Absolutely. Our goal in the organization is to reduce recidivism within our client population. We don't want repeat offenders. So we need to determine what services we're providing to that juvenile that are having the biggest impact so they don't come back through our system and they're able to sustain a life on their own without going through the system again. 

EVERYTHING YOU NEED TO KNOW TO START YOUR DAY.

government
technology



GovTech Today

Original and breaking technology
news for state and local
government readers.

Sign up today at
www.govtech.com/newsletters



Accelerate Efficiency: **THE THREE PILLARS OF** SECURITY RESPONSE



It's the stuff of sleepless nights:

The security team is hunched over a spreadsheet that lists security alerts and incidents from dozens of sources. The team is copying and pasting as fast as it can to consolidate incidents and notify the appropriate asset owners. There is no way to track what has been done, when and by whom, increasing the chance that alerts will slip through the cracks. Every moment of delay in threat detection and response increases the risk of breaches, data theft and downtime.

State and local governments can be inundated with alerts about security incidents and vulnerabilities, especially as they open their networks to provide new citizen services, modernize operations and collaborate across agencies. To accelerate resolution time and enhance decision-making, they need a clear, orderly incident response plan.

DESIRABLE TARGETS

State and local government websites and other internet-connected resources are prime targets for attack as they increasingly provide critical services and handle sensitive citizen information. These attacks are increasingly more sophisticated, persistent and stealthy, and motivated criminals are on the hunt for vulnerabilities and zero-day exploits that allow them to sabotage, steal, extort and defame.

From 2014 to 2015, the number of zero-day vulnerabilities increased by 125 percent.¹ Meanwhile, spear-phishing and other email exploits that plague state and local governments are rampant. A recent cross-industry study found that spear-phishing campaigns increased 55

percent between 2014 and 2015.² Part of the reason for the influx of threats is the simplicity in coordinating and launching attacks. Toolkits now allow even unskilled individuals to execute distributed denial-of-service attacks and other cyber crimes.

THE CAUSES AND COST OF POOR COORDINATION

Organizations have a limited window of time to patch serious vulnerabilities and act on high-priority incident alerts before damage is done, but poor coordination often delays response time and impairs decision-making. In many cases, alerts are overlooked, ignored or improperly categorized. Time spent on low-priority alerts translates to precious hours or days lost in resolving more critical threats. It also drains staffing budgets and opens the door to costly data losses.

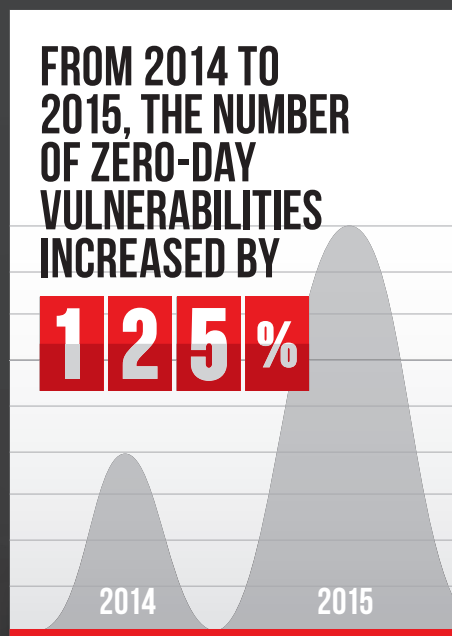
According to a Ponemon Institute study of data breaches, the average cost per lost or stolen record for public sector agencies is \$68.³ Multiplying that amount by the number of Social Security numbers, credit card accounts or medical records stored within an agency highlights the magnitude of potential risk and creates even more impetus for rapid resolution of incidents.

The following challenges contribute to poor coordination and prevent response teams from moving quickly.

- **Too much data with no context.** Agencies deal with an overwhelming number of tools generating thousands of unprioritized alerts without context; it's nearly impossible to process all of these alerts and know which ones need immediate attention. IT and security teams use different tools, further exacerbating the problem. In one study, respondents said the top incident response challenge was coordinating between security and IT teams.⁴
- **Poor visibility.** It's difficult to understand an agency's overall security posture when it is managed via multiple siloed products.
- **Lack of automation.** Security teams must rely on emails, phone calls and spreadsheets to document alerts and assign next steps. Manual processes waste time and introduce errors.
- **Inefficient use of talent.** Security analysts can be bogged down with administrative tasks such as copying and pasting incidents to consolidate them.
- **Approval delays.** Difficulties in identifying and tracking down decision-makers in the escalation process delays response time.
- **Unenforceable policies.** Although state and local governments may have

FROM 2014 TO
2015, THE NUMBER
OF ZERO-DAY
VULNERABILITIES
INCREASED BY

125%



a standardized security runbook, they don't always have a way to guarantee employees are following it. Lack of standardization leads to gaps in incident resolution.

- **No end-to-end tracking.** Organizations cannot easily follow through on incidents to ensure they are resolved and data collection for post-incident reviews can take hours.

SECURITY RESPONSE: MAINTAIN, UNIFY, AUTOMATE

1

MAINTAIN A DEFINITIVE, REAL-TIME VIEW OF YOUR SECURITY POSTURE

Accuracy is critical when prioritizing and responding to events. To get a clear view of your security posture, use a system with visibility across multiple products. Consider using a customizable dashboard that displays incidents and vulnerabilities, and correlates response data to quickly show whether assets are secure. To maintain security, be sure you can tailor the dashboard view in accordance with the role of the employee.

2

UNIFY SECURITY AND IT TOOLS — WITHOUT SACRIFICING CONTROL

Use a common platform. Doing so allows IT and security staff to access the same sets of data and thereby coordinate and unify their response. The platform should also allow the response team to:

- Control access to sensitive data via roles and access permissions
- Track each item to ensure the incident is remediated correctly
- Maintain mechanisms to send reminders, escalate items and hold staff accountable throughout the incident response life cycle

RESPONDING WITH AGILITY: THE THREE PILLARS OF SUCCESS

For a more agile and effective response, state and local governments must be able to visualize the security posture of their critical services and IT infrastructure, unify and streamline tools, and automate response. An integrated response platform provides a robust foundation for the three pillars of successful security response. With the right

platform, organizations can automatically import and prioritize security information and event management (SIEM) system alerts, respond to potential email phishing scams, address high-profile vulnerabilities and more.

3

AUTOMATE SECURITY RESPONSE

Automated, predefined incident response workflows ensure consistent remediation and support compliance with security policies and regulations. They also allow junior staff to track the workflows of routine incidents so senior analysts can focus on more complex issues. When automating security responses:

- Prioritize systems and resources based on their criticality to the organization
- Determine which systems are affected when an incident occurs
- Automate incident response/use predefined workflows based on the criticality of each resource
- Automate the approval process for patches and changes
- Automatically correlate threat intelligence data
- Document and time-stamp all activities and approvals to support auditing, process improvement and accountability

ENDNOTES

1. <https://www.symantec.com/security-center/threat-report>
2. <https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf>
3. <https://securityintelligence.com/cost-of-a-data-breach-2015/>
4. Enterprise Strategy Group. Status Quo Creates Security Risks: The State of Incident Response. February 2016

This piece was developed and written by the Center for Digital Government custom media division, with information and input from ServiceNow.

Produced by:

CENTER FOR
DIGITAL
GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. www.centerdigitalgov.com.

For:

servicenow

ServiceNow is changing the way people work. With a service-orientation toward the activities, tasks and processes that make up day-to-day work life, we help the modern enterprise transform the delivery and management of services. ServiceNow provides service management for every department in the enterprise including IT, human resources, facilities, field service and more. www.servicenow.com/products/security-operations.html

States' Path to Digital

Every two years, the Center for Digital Government and *Government Technology* take a detailed look at the status of IT in states, issuing letter grades based on their internal processes and use of technology to connect with and provide services to citizens. Our 2016 Digital States Survey infographic details key trends and areas of focus across the U.S. as states strive to increase efficiency and meet the expectations of the public in the digital age. See our complete story and analysis at govtech.com/DigitalStates2016.

Digital States at a Glance

*Since the 2014 survey



17

trending up*



23

consistent*



10

trending down*

Dedicated Staff

Here's the percentage of respondents with employees devoted to these areas.



Cybersecurity



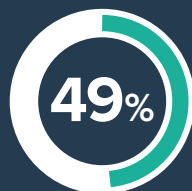
Data Analytics/
Business Intelligence



Performance
Metrics



Open Data



Innovation



Privacy

Head of the Class



Michigan

A

An Enterprise Fraud Detection system uses more than 20 data sources to identify attempts to defraud the unemployment and health and human services agencies.



Missouri

A

The Automated Criminal History System integrates with fingerprinting devices to provide instant information about an individual's background.



Ohio

A

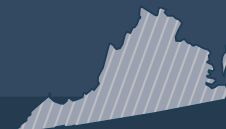
The state's cloud-first policy expedites project deployment timelines, while a mobile platform strategy ensures devices are considered from a project's outset.



Utah

A

By tracking traffic signal metrics, the Transportation Department has reduced the odds of getting stopped at a red light by 28 percent.



Virginia

A

A new case management system has processed more than 900,000 Medicaid applications since October 2014.

Current Workforce Gaps

Here are the areas where states most need to hire:



Cybersecurity



Business Intelligence and Data Analytics



Application Building, Integration and Modernization



Vendor-Managed IT Services



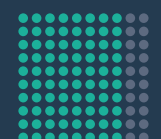
Shared IT Services

Top Tech Priorities

1. Cybersecurity
2. Shared or Collaborative Services
3. Cloud Computing
4. IT Staffing
5. Budget and Cost Control

Almost Ubiquitous

Most states are on board with:



The Curve

A's ●●●●●

A-'s ●●●●●

B+'s ●●●●●●●●●●

B's ●●●●●●●●●●●●●●

B-'s ●●●●●●●●●●

C+'s ●●●●●

C's ●●●●

C-'s ●

Still Catching On

Business Intelligence/Advanced Analytics
67%



Next-Generation LTE Networks
57%



Participatory Budgeting
30%



Software-Defined Data Centers
37%



CENTER FOR
DIGITAL
GOVERNMENT

DIGITAL STATES
PERFORMANCE INSTITUTE

government
technology

Accela

Deloitte.

DELL EMC

NiC
the people behind eGovernment

NUTANIX

shi

Symantec.

VERITAS

verizon

Using Cloud-Based Analytics to Reduce Cyber Risk



Tony Encinias, Vice President of Public Sector Strategy, ViON

State and local governments have more data at their disposal than ever before. Firewalls, intrusion detection systems and other tools constantly monitor the condition of government networks, and they can track millions of potentially suspicious incidents every day. Real-time monitoring is fundamental to modern information security in an era where threats grow more numerous and more sophisticated at an ever-increasing rate.

But monitoring is only effective if governments can get context for this data, analyze it and take action based on their findings. Cyber analytics is the next big opportunity and the next big

challenge for governments as they address the risk to valuable systems and information. Many government agencies lack the skills and financial resources to implement and operate cyber analytics on their own. Tony Encinias, Vice President of Public Sector Strategy at ViON and former CIO of Pennsylvania, provides insight into how cyber analytics delivered as a service can help agencies cost-effectively secure their networks.

Q: How are the security needs of government agencies evolving?

Encinias: Now that agencies have put cybersecurity tools in place, they can receive alerts and begin the remediation process. These tools are really the first steps to “triage” the network. Then “treatment” for breaches and compromises can be implemented. But they are struggling with the volume and velocity of data these systems generate. They don’t have the time or the resources to create context from the data to increase network security.

Q: How can cloud services help agencies use this data to strengthen cybersecurity?

Encinias: ViON’s cyber analytics platform takes security data from an agency’s network, ingests and analyzes it based on specific algorithms, and displays the information on a dashboard. The platform could be cloud based or on premises. Ascolta, a wholly owned subsidiary of ViON, delivers cyber analytics using the AWS GovCloud, which can give agencies real-time data analysis. While

internal data is a necessary condition for security, it is not sufficient to provide a complete picture, so the analytics platforms pull external data from black lists, the dark web and websites and maps it against what your network is telling you. This added capability can help your agency predict attacks or breaches. The service operates 24/7 every day, which is very difficult and expensive to do with in-house government staff.

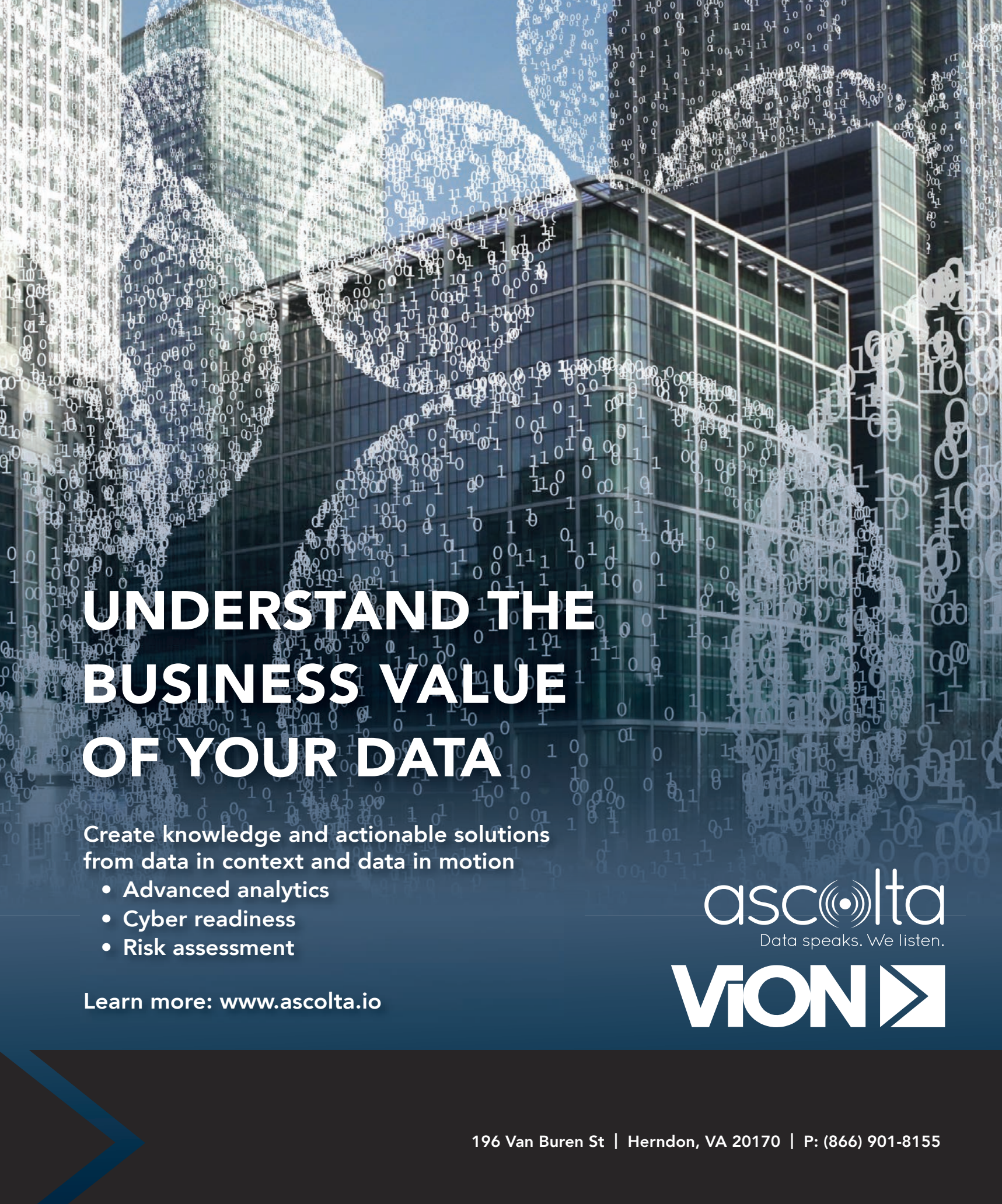
Q: How does a cloud-based analytics platform help preserve network performance?

Encinias: Network performance is a big issue as agencies add cybersecurity tools. On-premises tools often have a significant presence on the network — taking resources away from what that server was intended to do. State and local governments may not need or want another on-premises solution and many don’t have the budget or staff to support it. Because Ascolta’s cyber analytics platform is offered as a cloud-based service, there is zero footprint on the network.

Q: What best practices can you offer decision-makers regarding cybersecurity and cyber analytics?

Encinias: Before investing in analytics, agencies should:

- ▶ **Explore as-a-service solutions.** ViON and Ascolta’s cyber analytics platform is subscription based. If you want to have the services of a data scientist, security professional and analyst, you can do all of that through managed services as a single contract.
- ▶ **Review the cyber readiness of your cybersecurity.** To conduct cyber analytics you must have, at a minimum, a foundational defense-in-depth presence as outlined in the NIST Cybersecurity Framework. Once you have mechanisms in place like firewalls, malware detection and SIEM to generate, collect and manage that data, you can perform analytics to identify vulnerabilities.
- ▶ **Be vigilant 24/7.** What happens when an attack occurs at 3 a.m. on a Saturday? Without 24/7 monitoring, chances are you won’t know about the attack until Monday morning — and that’s too little too late. An alert sent to you via a mobile phone, tablet or text message allows you to see what’s going on from an analytics perspective, determine the potential impact of the issue and take proactive steps against it.



UNDERSTAND THE BUSINESS VALUE OF YOUR DATA

Create knowledge and actionable solutions
from data in context and data in motion

- Advanced analytics
- Cyber readiness
- Risk assessment

Learn more: www.ascolta.io

ascolta
Data speaks. We listen.

VION 



BY ADAM STONE | PHOTOS BY DONNELLY MARKS

Conne



Public safety now sits
alongside IT as formal structures
emerge to take on cyberthreats.

Massive ectedness

Even as Texas' chief information security officer (CISO), with the full weight of the state's IT apparatus at his disposal, Edward Block has a limited range of vision when it comes to cybersecurity.

"We don't see everything that is out there. We see a lot of stuff, and we tend to see things pretty early in their evolution. But we don't see everything. So collaboration is really critical," he said. To succeed in cyber, the state's 160 distinct agencies have to pool their resources. "The bad actors out there are happy to share information with each other all day long. If we don't do the same, we are letting them have a distinct advantage."

Given the unheralded complexity and severity of the threat, some say cyber is going to have to be a team effort. "There may be times when assets or authorities from one agency are needed to help another work its way through cyberproblems. And indicators of compromise in one system may indicate or presage indicators of compromise in other systems," said Martin Libicki, a RAND senior management scientist who works extensively on government issues.

This way of thinking increasingly typifies the government approach to cybersecurity — and necessarily so, said Steve Spano, president and chief operating officer of the Center for Internet Security, which operates the Multi-State Information Sharing and Analysis Center on behalf of the U.S. Department of Homeland Security.

"Any government agency can connect to 15 other government agencies," he said. "One system services health care, but health care ties to other state services. So once an adversary gets into one agency, it isn't hard to go from there to see what other agencies you can get into."

In response to this emerging landscape, government IT executives, emergency planners, security agencies and other key players across the nation are forming alliances. They're putting in place formal structures to ensure that when new cyberthreats emerge, all relevant players can be prepared to act.

Connected Networks

In Georgia an executive order in mid-2015 established the State Government Systems



Cybersecurity Review Board to be headed up by the state CIO, with members to include the adjutant general of Georgia and the leader of the Georgia National Guard, the commissioner of the Department of Administrative Services, and Jim Butterworth, director of the Georgia Emergency Management Agency/Homeland Security.

"With everything going more and more to the cloud, it is quickly becoming obvious that any network that is connected to other state networks could be vulnerable," Butterworth said. "That means we need to create the security across the entire infrastructure."

The group's first act was to request a self-assessment from agencies. Based on a December report, the state Legislature approved \$3 million over the next three years to fund a deeper study of Georgia's cybersituation. "That is going to get us out of the gate and get us some

good data that shows us exactly where we are," Butterworth said. "It is definitely a good push to get us started."

The effort is already having a direct practical impact. State agency IT leaders have been emboldened to get more aggressive on cyber, knowing they have a larger body backing them. Take the ransomware attacks, for instance. "Because of some of these conversations and because we have empowered these agency CIOs, they are beginning to back up systems more and more, so when these ransomware demands pop up — and they have been — we don't give in," said Butterworth. "We don't pay, and so far, we have been able to successfully stop those efforts."

The actual mechanics of collaboration are still a work in progress. Everyone says they want to work together; no one wants to be told what to do, and not



Mike Geraghty wants the New Jersey Cybersecurity and Communications Integration Cell to be a one-stop shop for the state's cyberefforts.

everyone likes to make it known when a problem has impacted their systems. These early days require finesse.

"We have to make it clear that we are not beating them over the head: 'We have the clout of the governor's office and we are throwing this in your face.' So we say up front that if an agency comes up red in some area, we aren't going to publish the name of that agency. This is not a punitive effort," said Butterworth. "Our philosophy is that a rising tide raises all ships. We are simply here to empower them in what they are already trying to do."

While the state CIO and security chiefs make an obvious fit on the board, some might wonder why Administrative Services is at the table. Simply put: These are the folks who ultimately purchase the systems. If there are going to be security concerns around IT purchases, best bring them in early. "They have the control to say yes to this system and

no to that system. If they are in the conversation, we can help them understand the needs for certain protections," Butterworth said.

Taking Center Stage

"The thing about cyber is, it is truly worldwide and it is instantaneous. So it requires massive connectedness to combat it."

That's Victor Chakravarty, an enterprise architect in the Maine Office of Information Technology. Like Georgia, Maine has in place a formal body designed to take cyber out of the IT closet and put it smack in the center of the room. The Maine State Information Protection Working Group is chaired by the state CIO and includes the Office of Information Technology, Maine Emergency Management Agency, Maine Information and Analysis Center (MIAC, or the fusion center), Maine National Guard, U.S. Department of Homeland Security, the University of Maine, and IT directors of the cities of Auburn and Bangor.

Different players bring different expertise. Some on the team look at cyber as a law enforcement or national security issue. Chakravarty just wants to be sure he can keep the lights on — like last year, when hacking group Vikingdom struck state and local agencies in 27 states with a denial-of-service attack. "My job is service restoration," he said. "The most important thing I care about is that the state of Maine services remain up and my customers' services are not affected. But when you look at the fusion center, they are focused on public safety, so they are more interested in the forensics and the prosecution."

Having that plurality of interests at the table works to everyone's benefit. "That is what makes it a rich, symbiotic relationship," said Chakravarty. "I personally do not have the wherewithal to do forensics and prosecution, but there are others who do. Because we meet and spend time together we have evolved these patterns of information sharing that play off of each other's skills, and that is something that can only come through a long partnership."

In practical terms, the relationship is very much about responding to immediate threats. "If new ransomware hits the state

of Maine, I consider it my sacred duty to inform the fusion center, and they then up-channel it to DHS and FBI," Chakravarty said. "If the university sees some variant in the malware, or if we see something in the state networks, we all consider it our immediate responsibility to share that. It is in my best interests to contribute to that sum total of community wisdom."

At the same time, the group takes a bigger-picture approach. Members share best practices among one another, and they are building cyber-recommendations to help guide the governor's office, the Cabinet and Legislature. "Part of our mission is to educate them," he said. "And we also would like to up the profile of cybersecurity, so that potentially they can help us overcome burdens we ourselves cannot overcome."

'Body Armor'

Mike Sena literally helped write the book on cybercollaboration. As executive director of the Northern California Regional Intelligence Center (NCRIC) he helped develop a toolkit on the topic, the *Bureau of Justice Assistance Guide: Cyber Integration for Fusion Centers from the U.S. Department of Justice*.

With Silicon Valley in the region, it is perhaps not surprising that the NCRIC fusion center has become a hub of cyberactivity. Partners in the effort range across the state and federal gamut: The highway patrol and state justice department stand shoulder to shoulder with representatives of DHS, DEA, FBI and local law enforcement.

The primary mission is defensive, with planners utilizing FireEye software to continuously monitor participating networks. "When one group is being attacked by an actor, and that attack fails, that actor is likely to go on to the next person. So the goal is to be able to collect and share that information in real time, to create the body armor as best we can for disparate networks," Sena said.

NCRIC does outreach too, engaging state agencies in cybertraining and readiness activities. Sena's team has gone spearfishing among critical infrastructure stakeholders, sending out bogus messages to ensnare sloppy users in a mock security breach,

and they usually get a bite. “The last time we did this, 7 percent of the folks clicked on the link,” he said. “My advice to the organization is you only need one person.”

Sena is angling to position the 80-person NCRIC as the go-to source for government IT when cybertrouble occurs. To that end, in addition to sending out a steady stream of warnings and updates, the center also has produced a mobile optimized application to help people report incidents and threats. It also mounts a 24/7 response team.

When an incident or threat is reported, “we have the ability to reach out to that agency, to reach out to law enforcement, to reach out to the IT folks. From there we can send a team out, to have a human body out there working with them,” said Sena. “We don’t have enough bodies to send someone every time, but if it is a priority issue we will have somebody on the ground.”

Why the pressing need for collaboration? Because, as Sena puts it, cyber is not like other threats.

“We come together on a unified message for physical threats. ‘If X happens you do Y.’ But when we get to cyber it isn’t the same,” he said. “With cyber, if A happens, you can either do B, F-I, M or 3. That’s not the best thing. We need to be able to say, ‘This is the way we handle cyberevents in America. This is the way we handle cyberinvestigations.’ We are not there yet.”

The Virtual Threat

Mike Geraghty joins with Sena and others in government in wanting to change that status quo. As director of the New Jersey Cybersecurity and Communications Integration Cell, he oversees a collaborative effort intended to forge a common front against the cyberfoe.

“No one agency has all the answers or is even capable of keeping up with information security on the necessary scale,” he said. “When you have a threat that is physical and local, you can protect against that. But this is a threat that is virtual, that can happen anywhere against anything, and the only way to protect against that is cooperatively.”

To get at it, the cell embraces a broad mandate. “We want to be the one-stop

shop for cybersecurity,” Geraghty said. “That may be information on current threats, it may be best practices to implement cybersecurity, or the current state of cyber. We are also doing a lot of analysis, looking to see what a viable threat is and making sure we can articulate the nature of that threat and why it is important.”

That’s a lot to bite off. Automation helps: A security information and event



“Any government agency can connect to 15 other government agencies. One system services health care, but health care ties to other state services. So once an adversary gets into one agency, it isn’t hard to go from there to see what other agencies you can get into.”

Steve Spano, president and chief operating officer, Center for Internet Security

management system deployed across state networks records up to 2 billion events a day. Operations and analysis teams track that feed; communications professionals get the word out to more than 1,500 members.

The cell gets regular alerts from outside sources like DHS and FBI. The art here lies in taking all that information and lining it up against what’s happening internally. “Others can receive the same sorts of external information from the same sources. Our secret sauce is in comparing that to what we see on our network,” he said. “We vet that information so that what we provide our members with what is most relevant. We strip out the noise. Otherwise you are just opening a fire hose.”

While agencies are generally cooperative, Geraghty admits encountering the occasional “reticence to disclose” — IT leaders shy about lifting the covers on their systems’ vulnerabilities. His promise: Tell us your troubles, and we’ll keep it anonymous. “Even if you don’t strip it out and sanitize it before you give it to us, we will do that on our end so that when we do make use of that

information, we will not disclose anything about you or your systems,” he said.

In the drive toward cybercollaboration, this appears to be the big looming hurdle: the need to drive cultural change in an IT environment that tends to play security issues close to the vest.

In Texas, agencies are required to report cyberincidents to CISO Block, “but they are really uncomfortable doing

so, because they don’t know where that information is going to go. Will it go to the people who manage their budget? Will it go to the Legislature? Will it end up in a report that is available to the public?”

Texas law says everything is public knowledge unless specifically exempted. Block will go to bat to shield agency IT leaders from the spotlight, but only to some extent. “If it is just something embarrassing, if it is just the news of a breach, that is not something I would try to protect” from disclosure, he said. “But how it happened? If showing that would put that system or another in jeopardy, that is something I would try to protect.”

Experts across government say IT leaders will need to find a way to walk this fine line. With collaboration virtually the inevitable next step in government cyber, they will have to construct not just the technical mechanisms to anonymize breach reports, but also the trust and relationships that will make it possible for all players to feel secure in putting their cards on the table. [bit](#)

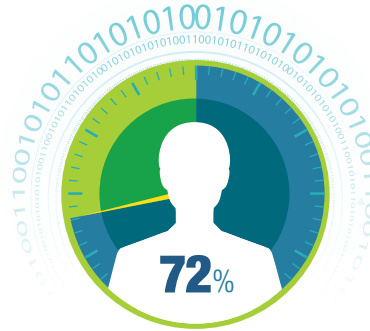


5 REASONS CYBERATTACKS POSE A REAL THREAT TO GOVERNMENT

1

THE RISK IS
CONSTANTLY
GROWING.

In a 2016 Governing Institute survey of 103 state elected and appointed officials,

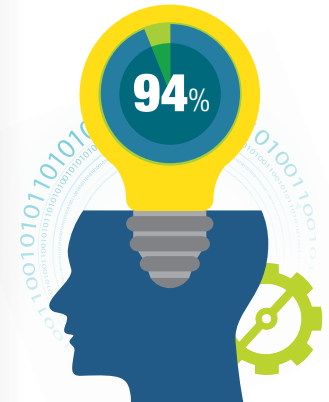


SAID THEIR STATE'S CURRENT
LEVEL OF CYBER RISK
IS **MODERATE TO HIGH.**

2

THE THREAT
IS CONTINUALLY
EVOLVING.

In the 2016
Governing Institute survey,

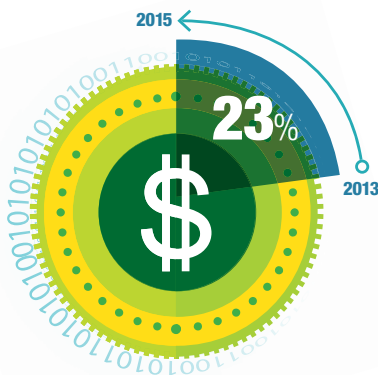


OF RESPONDENTS
AGREED HACKERS ARE
GETTING SMARTER.

3

BUDGETS & THE
ECONOMY TAKE
A BIG HIT.

The Ponemon Institute's 2015
Cost of Data Breach Study found the average
total cost of a data breach increased



FROM 2013 TO 2015 TO
\$3.79 MILLION.

4

HACKERS
WANT PUBLIC
SECTOR DATA.

Of all cyberattacks in 2015,

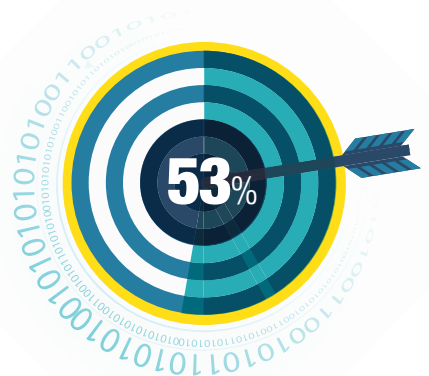


WERE AIMED AT **GOVERNMENT.**

5

THREATS ARE
INCREASINGLY
TARGETED.

A survey of 500 security leaders from
countries around the world found that



HAVE EXPERIENCED AN **INCREASE IN
CYBERATTACKS** AGAINST CRITICAL
INFRASTRUCTURE SINCE 2014.

For more information, download the "Guide to Cybersecurity
as Risk Management: The Role of Elected Officials" at:
www.governing.com/cybersecurity-guide

CGI

GOVERNING
INSTITUTE

A portrait of Lynne Pizzini, a woman with short brown hair and glasses, wearing a light blue patterned blazer over a black top. She is smiling slightly and looking towards the camera. The background is a blurred office setting with shelves and equipment.

Montana Chief
Information
Security Officer
Lynne Pizzini
also serves as
deputy CIO.

KELLY GORHAM



Cyber EXPOSURE

More governments are protecting their IT assets with cyberinsurance. Here's what you need to know when considering a policy.

By Robert Lemos

In 2014, a contractor for the government of Montana noticed signs of hacking on a server belonging to the state's Department of Public Health and Human Services.

The incident — which state officials do not classify as a “breach” as no data was thought to be lost — put millions of citizens' records at risk. While investigators found no signs that the data had been leaked, state officials triggered their 6-year-old cyberinsurance policy to help in notifying 1.2 million past and present Montana residents and providing a call center to answer questions, said Lynne Pizzini, chief information security officer (CISO) and deputy CIO of Montana.

“We have 1 million residents and we sent 1.2 million letters, so that kind of tells you that we were right at the edge — this is one of the largest incidents we will see,” she said, adding that the state's cyberinsurance policy was invaluable. “People ask if you need to pay for cyberinsurance, and I think you do, because we all know that it is not if, but when, you have a breach.”

The state has to date put no price tag on the incident, which is still being investigated, but it likely could have cost Montana millions of dollars. Yet, while the insurance coverage for monetary damage is important to protect taxpayers, a more significant value of cyberinsurance is that state


and local governments have a partner to work with during an incident, Pizzini said.

“The fact that insurance provides all those things that you need in the time of an incident, and they are automatically in place and you can utilize them, is huge,” she said. “We had forensics capability immediately, and we had counsel. They had a communications plan we could utilize and a call center — all of those things you need in the time of an incident.”

The insurance industry is looking at a tremendous demand for cyberinsurance. Increasing concerns about breaches and cyber-risks drove a 27 percent annual increase in the purchase of cyberinsurance policies, according to insurance broker Marsh. Across the industry, about a quarter of insurance brokers' clients have purchased some form of cyberinsurance, a significant proportion given that only 35 percent of clients have an information security program in place, according to the Council of Insurance Agents and Brokers.

More than 60 different insurers now have insurance products aimed at offsetting cyber-risk.

Yet government agencies have been among the slowest adopters. While 37 percent of financial services firms and 29 percent of retail companies had a cyberinsurance policy in 2013, only 19 percent of government agencies had insured them-



A 2014 hacking incident proved the value of cyberinsurance to decision-makers in Montana.

selves against breaches, according to a survey conducted by the Ponemon Institute. In 2015, only 20 percent of state CIOs had purchased cyberinsurance, according to a survey conducted by the National Association of State Chief Information Officers.

“If everyone in the private sector is buying cyberinsurance, why is the government not doing the same thing?” asked Jake Olcott, vice president of business development at BitSight Technologies, which rates the security of companies



Buying the Right Policy

Because there are no standard policies, getting cyberinsurance can be a lengthy process for any government agency. Here are some tips:

X Get enough coverage

The cost of breaches can be astronomical. Following its breach in 2013, retail giant Target has incurred more than \$291 million in costs associated with the compromise, only \$90 million of which was covered by insurance. Government agencies should

construct breach scenarios to estimate the insurance limits needed. The city of Phoenix, for example, bought \$10 million in insurance to cover potential losses.

X Beware of exceptions

When Georgia looked at initial policy proposals, there were too many exemptions. The biggest differentiator



KELLY GORHAM

for insurers, among other clients. “As far as I know, there is no governmentwide policy about insurance that government agencies are supposed to buy or take out. ... This is an area where the government is behind the private sector.”

Beyond compensation

While large government agencies can, and often do, self-insure, dealing with the monetary losses surrounding a breach is only part of the value of

cyberinsurance. Government networks are so varied, linking citizen data and operational infrastructure networks, that a breach could be very serious and responding to one can be complex.

To offset the risk, governments are increasingly looking at cyberinsurance. The state of Georgia, for example, is currently in the process of purchasing it.

“If you start contemplating a breach of tens of millions of dollars, that’s a big hit for even a state to take,” said Steve

Nichols, CTO of the Georgia Technology Authority, which manages information technology for the state.

San Diego has 1.4 million citizens and 24 different networks that connect city bureaus and departments, more than 400 applications, numerous smart devices, a fleet of police cars and point-of-sale systems. The sheer variety of systems means that a breach could cost anywhere from tens of thousands of dollars to, in an absolute worst case, a half billion dollars, said Gary Hayslip, deputy director of the Department of Information Technology and CISO of San Diego.

Having cyberinsurance means not only offsetting the monetary risk, but also better responding to the breach, he said.

“It is one of the things that you hope you never have to use, but in today’s environment and with the technologies that we are moving into — we are moving to the cloud and we have smart city initiatives — you need to have cyberinsurance as the security blanket behind the scene,” he said.

Hayslip and other state and municipal CIOs and CISOs agreed: While the coverage for damages is an important part of cyberinsurance, the most valuable aspect is the expertise that insurance companies and their partners can provide to agencies dealing with a breach.

for many insurers is what incidents and triggers they exempt from coverage. Some companies exempt breaches involving unencrypted data, while others require that USB drives must be barred from use.

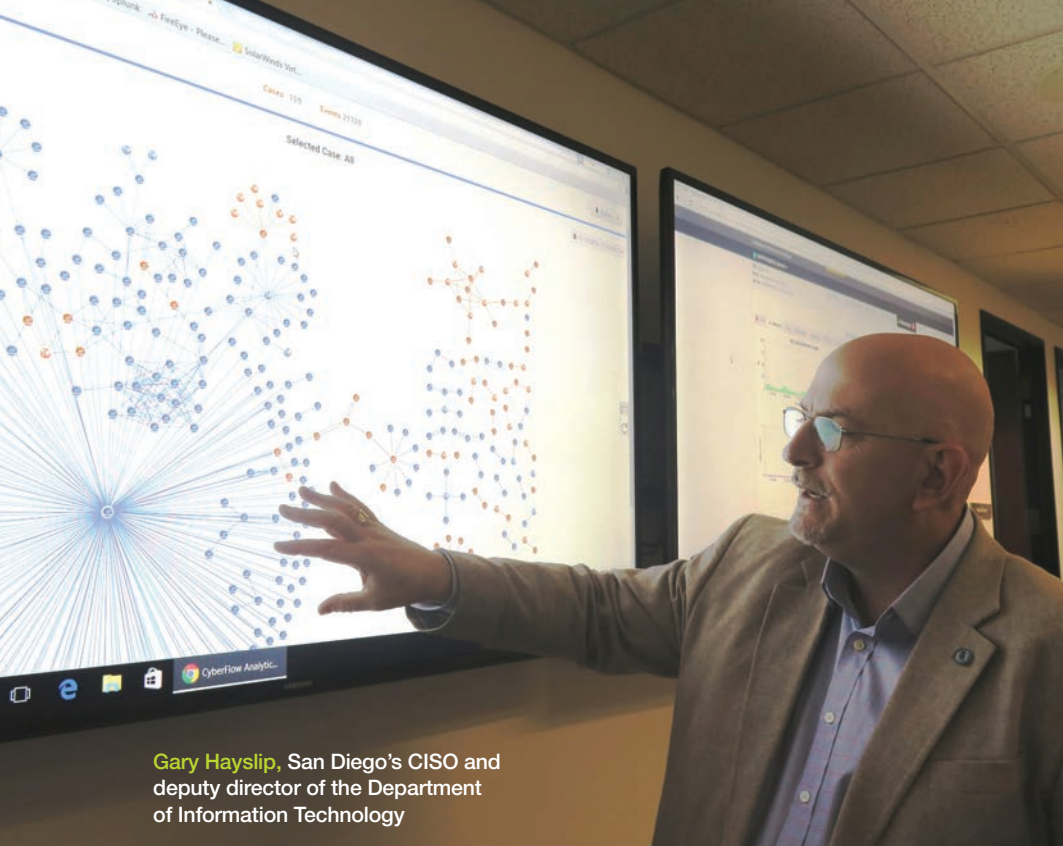
When the Georgia Technology Authority looked for a policy, it had to sift through them and decline those with too many exemptions, said CTO Steve Nichols. “In one case, they basically wanted to exempt lost laptops, and that does not help us at all,” he said.

X Test all scenarios

To check policies and prepare for possible breaches, government agencies should regularly run incident-response exercises. Such tabletop exercises are particularly important when evaluating insurance policies to make sure common incidents are covered, said Gary Hayslip, San Diego CISO.

“You do incident-response tabletop exercises where you go through

different types of scenarios: how bad could it actually get, how will you respond and what kind of damage you would take,” he said. “Then you start taking a look at what you can handle in house, what you have to outsource and what would be covered by an insurance policy. By doing that, you can figure out whether the insurance policy is worth the paper it’s written on.”



Gary Hayslip, San Diego's CISO and deputy director of the Department of Information Technology

No standard policy

As the ninth-largest U.S. state, Georgia has faced a long process to find an appropriate insurance policy. Because the state has so many different departments and bureaus — not to mention state universities and colleges — finding a solution to insure much of the infrastructure against breaches and cyber-risk has taken a long time.

“The underwriters have trouble getting their head around that there are different agencies, each with their own security processes,” said Nichols.

The complexity, uneven security controls, and the fact that agencies have access to comprehensive information on citizens often means that insurers are leery about underwriting policies for states, he said. In addition, added complexity means a higher premium rate: While an industry norm is a \$10,000 annual premium for \$1 million in coverage, Georgia has to deal with quotes much higher than that.

“The industry is realizing that these things can run way past the policy limit; that can happen very easily,” said Nichols. “So everyone is gun-shy about taking on a policy for a state. We were taken aback by the number of companies that don’t underwrite this domain.”

While government has many of the same threats as private-sector companies, the

infrastructure that states and municipalities manage can be more varied and more critical than the average company, said Denise Olson, chief financial officer of Phoenix.

“We, as a government agency, have to be more cautious,” she said. “We do have systems related to the water department and we have information on citizens. I think municipalities need to take additional means to protect our systems.”

Phoenix bought a policy for \$10 million with a \$500,000 deductible for a \$200,000 annual premium.

Complexity grows

Insurers continue to evolve and underwrite more complex policies. Many carriers have loss-control services that can be added onto a policy to give risk management advice, set up tabletop incident response exercises, and find other ways to help clients gauge and prepare for risks, said Jon Neiditz, partner in the Atlanta practice of law firm Kilpatrick Townsend.

“The most important thing for any entity is to understand the likely risk that it is scared about, and make sure that they are covered,” he said. “What are the biggest risks? Is it breach of unencrypted information, or is it not a confidentiality issue, but an integrity or availability issue?”

While offsetting the cost of a data breach is the most common coverage for cyberinsurance, policies may cover physical cyber-risks as well, such as the danger of attacks on utilities and medical facilities, according to John Farley, vice president of cyber-risk for insurance broker HUB International.

Property damage and injury from cyberattacks are covered by less than a handful of insurers, but more will venture into that area as the risks are better understood, he said. Yet it will take a while, because insurers have little data on regular breaches, nevermind more complex threats like cyberphysical attacks.

“The actuarial data is just not there yet,” Farley said.


Good security remains key

Finally, security and risk experts underscore that having cyberinsurance does not mean that companies and government agencies can neglect their information security program. Cyberinsurance needs to be part of a comprehensive information security program, not a way to absolve the IT department of responsibility.

As part of the insurance process, insurers will hammer the lesson home.

“Sometimes, organizations think that insurance can take the place of what you are doing, but that is not the case at all,” said Montana’s Pizzini. “You have to have a lot of things in place just to get the insurance. Just like to have insurance on your vehicle, you have to have a good driving record. You need to have good security processes in place to get cyberinsurance.”

In the end, cyberinsurance is about offsetting risk, but also about preparing for a breach. For government agencies, the ability to tap into a knowledgeable partner in a time of crisis is invaluable, said Pizzini.

“I do not have the resources to go out and get contracts in place with a forensics service, a call center and credit reporting, and maintain all those contracts,” she said. “They have all those contracts in place for you to utilize. I would say that is the greatest advantage.” 

INTERNET | VOICE | TELEVISION | NETWORK SERVICES | CLOUD




SAFEGUARD YOUR GOVERNMENT DATA WITH RELIABLE, SECURE CONNECTIVITY SOLUTIONS



Working in public service takes more than strong policies, staff and elected officials — it takes reliable connectivity to protect your mission-critical data. With Government Solutions from Time Warner Cable Business Class, you can rely on a credible and trusted connectivity partner to meet the unique needs of state and local governments.

**To learn more, visit or call us at
business.twc.com/government | 888.638.1791**

Not all products and services are available in all areas. Subject to change without notice. Some restrictions apply. All trademarks remain the property of their respective owners. Time Warner Cable Business Class is a trademark of Time Warner Inc., used under license. © 2016 Time Warner Cable Enterprises LLC. All rights reserved.

A portrait of Jacquie Irwin, a woman with shoulder-length blonde hair, smiling. She is wearing a bright yellow sleeveless top and a thin necklace with a small pendant. The background is a blurred indoor setting with large windows.

California
Assemblymember
Jacqui Irwin is
prepared to
ask the tough
questions when
it comes to
cybersecurity
in the state.

**LEGI
CYB**

IN MARCH 2016,

just a few weeks after a contentious legislative oversight hearing, Michele Robinson, California's chief information security officer (CISO), stepped down. The Feb. 24 hearing's focus was a 2015 audit that questioned the state government's cybersecurity preparedness.

One of the legislators holding the state's feet to the fire is Assemblymember Jacqui Irwin, D-Thousand Oaks, who chairs the Assembly Select Committee on Cybersecurity. Recalling that hearing, Irwin said legislators asked how much departments spend on cybersecurity and Robinson didn't have an answer. "That hearing did not go well for the Department of Technology. The state's approach was pretty decentralized and nobody was being held accountable for the decisions being made about how we manage the risk," she explained.

California has 160 departments required to do security assessments, Irwin added. "But when we looked more deeply into it, only 20 departments had actually done the security assessments. And the Department of Technology was not holding these departments accountable."

BY DAVID RATHS

Irwin authored a bill signed into law and now being implemented that requires the state to perform a minimum of 35 network security assessments per year on state agencies, departments and offices. The assessments are to be performed based upon a defined risk index that prioritizes the amount of valuable personal information, financial information or health records held by that entity.

Unfortunately legislators like Irwin, who take the time to study cybersecurity issues and ask tough questions of CIOs and CISOs, are still the exception rather than the rule. But that may be changing. High-profile government data breaches and recent ransomware incidents in health care have put the topic on the front burner in legislative committees.

"Five years ago cybersecurity was seen as an IT issue. But with threats so much in the news now, it is not something anyone can ignore anymore," said Agnes Kirk, CISO of Washington

SLATING ERSECURITY

State lawmakers begin to recognize their responsibilities with cyberthreats.

state. She has spent time working to raise awareness and education in the Legislature. In the 2013-15 budget cycle, the Legislature provided funding to increase the security posture of the state. "Since then I have reached out to legislators to create awareness opportunities, culminating in the governor's first cybersecurity and privacy summit," she added.

Privacy and security are the main IT issues that rise to the policy level, Kirk noted. People are trying to make appropriate laws, but it is such a complex issue and only one of the many that legislators need to address, so it is difficult to make good laws, she said. After the cybersecurity and privacy summit, she met with legislators, and in the most recent legislative session they created a state data privacy office and a cybersecurity jobs act. "They had a better understanding of the issues and they worked with us on those. It was an opportunity to collaborate on getting good policy into law."

One way Kirk reaches out is to hold tours of the Security Operations Center for legislators. "They can see in real time what is happening," she said. "They can see all these attacks coming in. I can talk more specifically about the types of attacks we are seeing right then, and what would happen if we weren't protecting our network the way we are. That gives them a real-life view."

Legislators who focus on cybersecurity tend to be people who have some technology or legal background. For instance, Irwin's training was in systems engineering, and she worked at the Johns Hopkins University Applied Physics Lab and Teledyne Technologies. "I think that gives me a little more comfort with the issue, because cybersecurity has

RECENTLY SIGNED LEGISLATION REQUIRES CALIFORNIA TO PERFORM A MINIMUM OF 35 NETWORK SECURITY ASSESSMENTS PER YEAR ON STATE AGENCIES, DEPARTMENTS AND OFFICES.

evolved very quickly," Irwin said.

Karen Jackson, secretary of technology for Virginia, headed up a state cybersecurity commission over the last two years and turned to the Legislature to pass seven bills related to cybersecurity and cybercrime. In the last session the Virginia legislature also invested more than \$20 million in cybersecurity for training, hiring and shared services for state agencies.

Jackson said that when it comes to cybercrime legislation, there are legisla-

tors who are prosecutors and defense attorneys who grasp the concepts quickly because they are in the legal system every day. "Cyber as a technology is a little more difficult," she admitted. "Unless you have somebody who spends a lot of time in the environment, it is difficult to keep up with. We don't have one constant cyberchampion in either party who is always the go-to person. It is more spread out based on committee."

BREACHES GRAB LAWMAKERS' ATTENTION

One thing that tends to get legislators' attention is a high-profile data breach. "My philosophy is, never waste a data breach, and hopefully, it is not one of ours," said Kirk. "You always want to take advantage of somebody else's breach to educate. It does bring home the fact that you either invest in front of the problem or you are investing by trying to clean up at the back end of the problem. It is a tough job to find out where that balance is. It is important to me that we don't spend our tax dollars cleaning up something that could have been avoided."

In fact, it often takes a data breach for lawmakers to pass significant legislation around cybersecurity, said Doug Robinson, NASCIO's executive director. For instance, after a high-profile breach

NCSL TASK FORCE ALLOWS LEGISLATORS TO SHARE BEST PRACTICES

Besides leading the charge on cybersecurity in the California Legislature, Rep. Irwin is co-chairing a cybersecurity task force recently created by the National Conference of State Legislatures (NCSL). "We just had a conference call on the new federal data-sharing legislation," she said. "My hope is to produce a working product that would be a list of recommendations or best practices for states. We all know the important thing is to get the word out and tell legislators about their responsibility for oversight. It can't just be the executive branch that is worried about this, so we want to come up with a list of questions legislators should be asking."

Jeff McLeod, director of the Homeland Security and Public Safety Division of the National Governors Association Center for Best Practices, said there is a crucial role for legislators to play in terms of investing in workforce training and oversight. "The biggest thing is at the policy level, making sure the state is organized effectively in terms of governance, and making sure the state is taking a risk management approach and using resources where they can have the biggest impact in addressing or reducing the threat."

Susan Parnas Frederick, NCSL's senior federal affairs counsel, said her organization had been tracking cybersecurity activity at the state level for several years, and it seemed like a good time to form a formal body to create a work product to inform legislators who may sit on technology and appropriations committees. "This task force gives those people with expertise an opportunity to work with colleagues in other parts of the country to share information on what they have done in their state," she said. The task force, which also includes Rhode Island's state Sen. Louis DiPalma and state Rep. Stephen Ucci as members, has a two-year time limit, but Frederick said it could be extended. "What we found was that as soon as it was announced to the membership, we got lots of requests to join. There is a lot of interest out there."

A portrait of Agnes Kirk, Chief Information Security Officer of Washington State. She is a woman with short, wavy brown hair, smiling at the camera. She is wearing a bright blue blazer over a black top, a gold necklace with a tassel, and small gold hoop earrings. The background is a blurred outdoor setting with a concrete wall and some foliage.

“FIVE YEARS AGO CYBERSECURITY WAS SEEN AS AN IT ISSUE. BUT WITH THREATS SO MUCH IN THE NEWS NOW, IT IS NOT SOMETHING ANYONE CAN IGNORE ANYMORE.”

AGNES KIRK, CHIEF INFORMATION SECURITY OFFICER, WASHINGTON STATE

DAVID KIDD

in 2012, the South Carolina Legislature passed a bill that made the CISO and chief privacy officer positions a legislative requirement. The number of conversations between state CIOs and legislators is increasing, said Robinson, “but there is so much more for CIOs to do in terms of communicating to stakeholders, including legislators. Too much of that is ad hoc and not formalized.” NASCIO’s research notes an increase in the level of communication on cybersecurity with policymakers, but also that less than half of states are engaged in the conversation.

CIOs and CISOs need to communicate with legislators in terms of business risk to state government, Robinson stressed. Unfortunately in many states, it is seen as being all about technology, so legislators defer to the CIO. “When I talk to legislators I try to characterize this as just another business risk that the state has to address. The digital world is now part of the fabric of government, and risks are associated with that. It is not a project or an initiative. It is not going to end. They have to become comfortable with that, and it is very new to them.”

Francesca Spidaleri, a senior fellow for cyberleadership at the Pell Center for International Relations and Public Policy, a think tank at Salve Regina University in Newport, R.I., authored a 2015 report called *State of the States on Cybersecurity*, which found that most states lack strong cybersecurity measures, leaving themselves largely unprepared to respond to cyberthreats. (Her report identified eight states with strong approaches to cybersecurity, including Virginia.) “Few states are considering the exposure and costs of less resilient critical services,

data breaches, theft of intellectual property and sensitive information, and the impact of e-fraud and e-crime, all of which lead to a weaker economy and unstable national security,” her report noted.

“Most legislators are poorly educated on these issues and very few have taken the time to understand how this helps a state economically or from a security standpoint,” she said. “We see the same issues in state legislatures that we see in the U.S. Congress. Although it is a bipartisan issue, the reason so many cybersecurity bills are stalling in Congress comes down to those who have taken the time to educate themselves and those who haven’t.”

Legislators want to promote digital connectivity and extend broadband capability to remote areas of their state, Spidalieri noted. “What they don’t understand is that cybersecurity is the other side of the same coin. If you encourage people to connect more of their sensitive information to services and you don’t protect it, you are actually making your state more vulnerable.”

In her own state of Rhode Island, Spidalieri noticed that the data breach laws had not been updated since 2005, and she reached out to two legislators she knew had an interest in the topic, state Sen. Louis DiPalma, D-District 12, and state Rep. Stephen Ucci, D-42nd District. Both had an interest in cybersecurity because of their day jobs: DiPalma works as a technical director at Raytheon, and Ucci is an attorney who works on privacy issues.

Spidalieri brought them together with executives from law enforcement, the health-care and financial sectors, and other stakeholders. “Together, in a few weeks of hard work, we came up with a new draft of the legislation that was not only updating the old law, but offering a clear course of action for businesses and agencies that might get breached.”

Ucci said it was tough to get consensus on the bill. “I have been in the Legislature for 12 years, and there is a difference of opinion on everything, but with this particular piece of legislation, every piece of the bill was a bone of contention,” he said. “There were some folks who thought every single possible breach should immediately be reported to the police, whereas others said you should have a very high



CONNECTICUT
REP. CAROLINE
SIMMONS

“NONE OF US IS AN EXPERT ON THE TECHNOLOGY, BUT I THINK ALL OF US RECOGNIZE THE INCREASING THREAT WE ARE FACING.”

threshold. We had businesspeople who saw it as a burden on them. It was a tug of war around what you disclose, how you disclose it, and to whom and in what form.”

The bill passed because they brought the stakeholders together with the legislators upfront to address issues and reach compromise, Spidalieri said. “That same year 31 states proposed updates to the data breach notification law, and only two passed.”

LEGISLATORS BALK AT FISCAL COST

Although she is new to the Legislature in Connecticut, Rep. Caroline Simmons, D-Stamford, took the lead in co-introducing cybersecurity legislation. “I have some experience working at the federal level on this issue at the Department of Homeland Security,” she said. “That is what first got me interested in it and I think that having strong cybersecurity laws at the state level is critical to our national security fabric, and this is one of

the most dangerous and difficult national security threats we face. States have an increasing role to play, given the sophistication and evolving nature of the threat.”

With two colleagues, Simmons introduced a bill that became law, directing the creation of a state cybersecurity task force co-chaired by the Department of Administrative Services and the Department of Emergency Services and Public Protection to conduct an in-depth study and assessment to identify the main cybersecurity issues facing Connecticut and to develop specific actions the state can take to improve its defenses and better protect state infrastructure, utilities, businesses and the public from cyberattacks.

The administration’s department heads were supportive about the creation of the task force, she said, but the legislation couldn’t call for a big investment. “There is a difficult fiscal environment here in Connecticut because we were facing a deficit going into the 2015 session,” she said. “The only difficulty I faced was that it couldn’t have a large fiscal note on the bill, so we decided to start with an assessment.”

Simmons said she believes other legislators are grasping the importance of cybersecurity, because of high-profile incidents, particularly the Anthem breach, which happened in Connecticut while they were debating this legislation. “None of us is an expert on the technology, but I think all of us recognize the increasing threat we are facing.” **BT**

draths@mac.com

IF YOUR CITY USES THESE



YOU'RE REQUIRED TO KEEP RECORDS
FOR UP TO 10 YEARS.

BUT DON'T WORRY. WE GOT YOUR BACK.



SCALING DOWN SECURITY

A SMALLER STAFF AND
A SMALLER BUDGET DON'T
LESSEN THE CYBERSECURITY
BURDEN. HERE'S HOW
CYBERLEADERS AT THE
LOCAL LEVEL ARE APPROACHING
TODAY'S THREATS.

BY LISA KOPOCHINSKI



Steve Monaghan,
CIO, Nevada
County, Calif.

Nobody lives the refrain “do more with less” more faithfully than local government. In the area of cybersecurity, CIOs and chief information security officers (CISOs) in cities and counties across the country are faced with the daunting task of finding new and unique ways to protect themselves against evolving threats and keep hackers at bay.

Steve Monaghan, CIO of Nevada County, Calif., cites the biggest cybersecurity issue his agency faces as keeping up with the pace of change and learning what they don’t know.

“Counties have a very broad breadth of technology with multiple interconnections to the state, feds, schools, cities, courts, consortiums, CBOs [community based organizations], and SaaS [cloud] providers,” he explained. “Counties are also in a constant state of motion with changes continuously occurring with new programs, services, locations and collaborations. These all drive a constantly changing technical environment.”

Add to this a fluid environment of regulations and an increase in new state laws focused on technology.

“Prudent cybersecurity is built on a solid foundation of knowing your environment,” Monaghan said. “The pace of change is greater than our shop’s ability to keep up with the demand for change, let alone to know everything we really need to know to effectively secure all the changes.”

Michael Finch, CIO of Lane County, Ore., said one big challenge is educating key partners in a variety of different lines of business about the security implications of their decisions.

“They must be educated enough about technology to understand the risks they accept when they make a business decision that involves technology or funding for it,” he said.

Some of the precautions taken by the Lane County Information Services Department are providing core workstation, network and server security infrastructure that includes antivirus protection, Internet proxy services and encryption. These services are managed by the Security and Audit Division, which was re-established in 2015 after being cut in 2012 for budgetary reasons. The division, which is working on implementing a centralized security model, is now focused on secure access principles, incident response and business continuity, among other things. It’s a tall order for a group of four full-time employees and less than 5 percent of the county’s IT budget.

Monaghan said that this year, Nevada County is pushing to modernize its IT security infrastructure. And the proof is in the budget. The county CEO and Board of Supervisors have earmarked \$250,000 for the effort. The sum represents about a 5 percent increase to the annual IT budget, which is used for infrastructure upgrades.

Job No. 1 is to build a countywide culture of cybersecurity/IT risk awareness and sensitivity.

“We are too small to codify this into every policy and procedure, so we need every county employee — from line staff in the customer departments to every IT employee — to be cybersecurity sensitive,” Monaghan said. “That way, as they take on new projects and implement changes, they are thinking about cybersecurity and IT risk impacts. We are working cybersecurity and IT risk management into our processes such as change management, project charters and contracting. However, it all has to first have a solid cultural foundation across the countywide organization.”

Adding to the challenge faced by local cybersecurity teams is having to achieve compliance with the many regulatory requirements imposed by higher governments. Federal rules include CJIS, which governs criminal justice information systems, and the Health Insurance

THE CYBERSECURITY LANDSCAPE: THEN AND NOW

What a difference five years makes.

When asked how cybersecurity issues have changed for their departments between 2011 and 2016, these CIOs offered their take.

“Lane County has recognized two important things. First, the business must drive the acceptance of risk/benefit when it comes to technology and how it’s used. Second, our users are our greatest asset — and our greatest threat. The difference between 2011 and today is a far more mature governance model, as well as a focus on training and awareness for all our users and customers.”

Michael Finch, CIO, Information Services Department, Lane County, Ore.

“The cloud has had the biggest impact. Data can live anywhere now, and trying to keep a handle on where data is living, and how employees across the enterprise are storing and moving data, is much more fluid and complex. Add in data classifications and the regulations around breach notifications, and an organization has more exposure now, and the costs of a data breach are much greater.”

Steve Monaghan, CIO, Information and General Services Agency, Nevada County, Calif.


Portability and Accountability Act. Accepting citizen payment for taxes, permits and other services administered by local government also necessitates compliance with Payment Card Industry standards. Adhering to regulations like these (or noncompliance with them), of course, is costly.

“Additionally local governments face the threat of cyberactivism/hacktivists that may occur due to an unexpected local controversial event unfolding,” said Finch. “While this exists at many levels, resources at the local level are far less than at other levels. Additionally, governments must serve a wide array of businesses — from building roads to running

jails to providing health care. This creates an extremely diverse set of technologies and requirements that most businesses don’t have to deal with.”

Finch also added that the issues his department faces are very similar to those faced by the state of Oregon, although compatibility between systems can be a challenge.

“That being said, we are also users of many of their systems, so it’s important that services we are required to use that are provided by the state run on the latest operating systems and browsers,” he said. “Funding is also one of the biggest differences. Counties are very limited on what



Michael Finch, CIO, Information Services Department, Lane County, Ore.



they can tax or derive revenue from, where the state has far more options.”

Riverside County, Calif., CIO Steve Reneker said his department invests about 3 percent of its IT budget on security, such as staff, tools and services. The main cybersecurity issues unique to local government, from his perspective, are impacts to emergency services and targets as a result of providing public safety services (officers, jails, public records).

“Local counties keep records of residents on welfare, unemployment, [who] owns property, [have] committed a crime, medical records, who is in jail, who is in the hospital, criminal history,

foster care, child support, food stamps — [all of] which drive cyber-risks.”

With this in mind, Reneker’s department has tightened email security using Symantec Brightmail, and a sophisticated five-person cybersecurity team focuses on additional security tools and remediation. Their task lacks a clear end game. Reneker said new strategies are needed to adapt to the ever-changing cyberlandscape and suggested the need for 24/7 monitoring and notification systems.

“We also need more employee training to protect them at work and home,” he stressed. “We need to invest in dedicated staff and tools to proactively block and eradicate malware active in place or attacking systems. We need to create a security operation center to actively monitor threats and show your customers that you take these issues seriously and that you have programs in place to help protect threats from impacting day-to-day operations. Annual audits and penetration tests [are also needed] to learn best industry practices and to ensure your environment is secure.”

For Monaghan, Nevada County has a wide breadth of technology, spanning 25-plus business lines. “We have very specialized and critical technology that needs to operate flawlessly 24/7/365, such as 911 dispatch, mobile officer data systems, jail control systems, suicide hotlines and wastewater treatment plants,” he said.

Jelani Newton, director of survey research for the International City/County Management Association, echoed a common concern among public-sector IT professionals at all levels: Local governments are having difficulty offering cybersecurity professionals salaries that are competitive with the private sector. The organization is currently studying the issue in conjunction with the University of Maryland, Baltimore County.

Newton said cybersecurity is becoming increasingly important as more local governments seek to use technology to improve service delivery and operating efficiency.

“As jurisdictions increasingly rely on social media, cloud-based solutions, smart

city platforms and other new technology solutions, new cybersecurity challenges need to be considered,” she explained. “Every discussion about enhancements in information and communication technology should include consideration of the potential cybersecurity threats, and plans to address or avoid them.”

So, in today’s ever-threatening cyberworld, what is a local government IT department to do?


Kevin Haley, director of product management for Symantec security response, said there are two cybersecurity issues he thinks will have the greatest impact on agencies in the coming year.

“First, agencies must protect their records from targeted attacks, both from insiders and hackers outside the agency. Second, agencies must protect critical files and data from crypto-ransomware attacks, which according to Symantec’s 2016 *Internet Security Threat Report*, grew by 35 percent in 2015, and are now more focused on enterprises rather than individuals.”

In order to combat these threats, Haley said agencies are going to have to step up to implement best practices to keep their data safe.

“It is also important that they understand where their critical data is, and back it up,” he said. “Finally, if an agency has never tested its backup strategy and processes, now is the time to do it, before an attack takes place.”

Finch made a good point when he said that security and — in particular — breaches, need to be treated more like a public health outbreak instead of a blame game.

“Currently whenever a large breach occurs, it’s often a game of victimizing the victim and firing people instead of going after the bad guys who broke the law and stole data,” he said. “This does not foster a collaborative approach between all organizations in going after the law breakers. Instead, attacks should be treated more like an outbreak in health, where people are free to share information without fear of retribution to ensure an informed, collaborative approach to ending the problem. This must change before any organization can hope to overcome this threat permanently.” 

lisakop@sbcglobal.net

Who You Gonna Call?

Have a pressing cybersecurity question or unsure what to do after a breach has been detected? Numerous organizations and resources have become available to government through the years to address these pressing issues. Here's a look at some of the key resources available to state and local agencies.



InfraGard

A partnership between the FBI and the private sector,

InfraGard is dedicated to information sharing and relationship building across organizations including with state and local law enforcement agencies. While it also has a physical security focus, the program started with a cybersecurity case in 1996. Its 85 chapters hold meetings and training sessions around topics that benefit members and develop special interest groups to address topics like cybersecurity in-depth.



National Guard

The National Guard is installing cyberprotection

teams throughout the U.S., with plans to have them in 23 states by the end of fiscal 2019. Collectively the deployments are geared toward a federal effort to protect against mounting cyberthreats. The teams will run simulations and share contacts, information and resources with local organizations to help thwart and prevent attacks.



Internet Crime Complaint Center

The center has been receiving complaints from the public since 2000 about cybercrime issues like hacking and fraud. Analysts review and research the complaints, and work with the appropriate government or law enforcement agency as necessary. The center does not investigate complaints, but is a helpful resource for citizens who don't know how to respond to a potential online crime.



National Governors Association

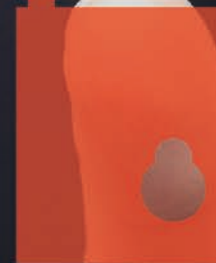
The association's Resource

Center for State Cybersecurity aims to provide governors with resources and tools for implementing effective policies and practices on the topic. Launched in 2012, the initiative's primary goal is for states to develop strategies for strengthening cybersecurity practices as they relate to IT networks, health care, education, public safety, energy, transportation, critical infrastructure, economic development and the workforce.



Multi-State Information Sharing and Analysis Center (MS-ISAC)

As part of the Center for Internet Security, the MS-ISAC offers free managed security and advanced monitoring services to state, local, tribal and territorial governments. As of 2011, the center was working with all 50 states and was home to a first-of-its-kind facility that's staffed 24/7 to guard against electronic attacks on government systems and information.





National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity

Acting as a how-to guide for the critical infrastructure community, version 1.0 of the framework was released in 2014 in compliance with President Obama's February 2013 order directing its development. The framework is a living document of best practices that users can reference to establish a risk-based approach to improve cybersecurity. It provides a series of actions to anticipate and respond to attacks on systems. If the majority of organizations adopt the framework's principles, they'll be speaking the same language and have an easier time contracting with one another and protecting against cyberthreats.



United States Computer Emergency Readiness Team (US-CERT)

As part of the U.S. Department of Homeland Security, US-CERT runs a 24-hour operation to provide intrusion detection and prevention for federal agencies; analyzes data about and responds to emerging threats; and distributes actionable information to all levels of government, the private sector and international organizations. When the Conficker worm was infecting millions of computers in 2009, US-CERT developed a tool that state and local governments could download to detect and remove the worm from their systems. [get](#)

Cheat Sheet

Here's a quick rundown of the terms you're likely to hear in cybersecurity conversations.



CJIS

The FBI's Criminal Justice Information Services security policy provides guidance on the lifecycle — creation, viewing, storage, etc. — of law enforcement data.



DoS and DDoS

A denial-of-service (DoS) attack makes websites and other online resources unavailable to users, and a distributed denial-of-service (DDoS) attack makes services unavailable through a flood of access attempts from many IP addresses.



FedRAMP

The Federal Risk and Authorization Management Program is a cloud-specific standard created to streamline security auditing across multiple federal agencies.



FISMA

The Federal Information Security Management Act outlines a framework for protecting government information and assets from natural or man-made threats, and requires agency leaders to conduct annual reviews of information security programs.



PCI

The Payment Card Industry Data Security Standard outlines encryption rules for credit card payments.



PII

Personally identifiable information is one of the targets of many data breaches and its use can lead to identify theft.

Erasing Human Error

Can security awareness
training change behavior
and reduce risk?

BY TOD NEWCOMBE



LEA DEESING, CHIEF
INNOVATION OFFICER,
RIVERSIDE, CALIF.

In 2014, a Durham, N.H., police officer opened what she thought was a digital fax attached to an email about an investigation she was working on. Earlier this year, an employee at the Lansing Board of Water and Light in Michigan opened what seemed to be a legitimate email attachment. In both cases, the government employees were victims of a type of phishing attack known as ransomware, which encrypted the victims' computer files and sent them a digital ransom note, demanding money to decrypt them. Both agencies were able to resolve the issue without paying any ransom, but not before dealing with a costly cleanup.

State and local governments continue to be victims of data breaches and cyberattacks, with unauthorized access to files and data as the most persistent problem, according to IBM's 2016 Cyber Security

"THE EFFECTIVENESS OF EMPLOYEE AWARENESS TRAINING IS SO HIGH THAT IT WOULD BE ONE OF THE LAST THINGS TO GO IF WE HAD TO CUT."

Intelligence Index. And the attacks are becoming more frequent. In 2015, government joined the ranks of four other industries — health care, manufacturing, financial services and transportation — as the most frequently attacked sector in the world, according to the report.

Despite investments in intrusion detection software, firewalls and a host of other cybersecurity tools, attacks, breaches and extortions continue to plague states and localities. A chief reason why security fails is the human factor, say experts. "Over 95 percent of all incidents investigated recognize 'human error' as a contributing factor," according to a 2014 analysis of cyberattacks from IBM's worldwide security services operations. "The most commonly recorded forms of human error include system misconfiguration, poor patch management, use of default user names and passwords or easy-to-guess passwords, lost laptops or mobile devices, and disclosure of regulated information via use of an incorrect email address."

Thanks to personal information available on the Internet and via social media, hackers and data thieves have become extremely sophisticated at sending what look like emails from colleagues or businesses with the goal of gaining victims' trust and having them open an attachment or click on a link that installs malicious software on a government agency's server. The technique is called social engineering, and over the past three years, most major cyberattacks on U.S. corporations have included it, according to *The Washington Post*.

CIOs and CISOs in both the public and private sectors realize that human error is perhaps the biggest weakness in any information security program. Not surprisingly, a fast-growing business has sprung up to deal with changing human behavior. Called security awareness training, the aim is to condition employees not to click or open anything that looks remotely suspicious.

Michael Roling, CISO of Missouri, reported that every tax season, the state's email system sees a spike in W-2 phishing campaigns. "They go through the roof," he said. Data thieves, hoping to gain a crucial bit of personal information that can be used to file fraudulent tax returns, try to trick employees into sharing information. "Sometimes the only thing that is suspicious might be a misspelled name," said Roling.

Since 2009, Missouri has used awareness programs to train employees what



MICHAEL ROLING,
CISO, MISSOURI



VENNARD WRIGHT,
CIO, PRINCE GEORGE'S
COUNTY, MD.

DAVID KIDD

to look for in a suspicious email, how to work with two-factor authentication or how to create strong passwords. The initial programs weren't that effective, according to Roling, but recently the state switched to its latest training program, an online service from Security Mentor. Roling described it as more educational than past efforts, as well as interactive and consumable.

Security Mentor is one of a burgeoning number of firms that specialize in awareness training. It's a business worth \$1 billion a year and growing 13 percent annually, according to Gartner, the technology research firm. Other firms in the market include the SANS Institute, MediaPro, Wombat Security, Digital Defense and BeOne Development, to name just a few.

Missouri's program is delivered online monthly and is taken by 40,000 end users in 14 state agencies. Each lesson lasts 10 to 15 minutes and covers a specific security issue. In addition to explaining about phishing, authentication and passwords, the program also teaches employees about physical security, data loss prevention, what's acceptable to send over the state network and even how to keep data secure while traveling. "The program also includes games and puzzles to keep it interactive," Roling said.

"AWARENESS TRAINING IS ONE OF THE MOST IMPORTANT COMPONENTS OF OUR SECURITY POSTURE. ALL THE SECURITY TOOLS OUT THERE WILL NEVER BE AS SHARP AS THE HUMAN MIND."

The awareness program costs the state \$4.68 per user, per year, but it's well worth the investment, according to Roling. "The effectiveness of employee awareness training is so high that it would be one of the last things to go if we had to cut," he said. "Not only does it raise awareness, it keeps the security culture alive that we struggled to get going five years ago. Even cabinet-level officers have to take the training."

Unlike security training, which focuses on teaching employees and testing their knowledge on a set of rules, awareness

training focuses on changing human behavior and making security part of the workplace culture. "It's all about changing behavior as it is about actual security training," said Lea Deesing, chief innovation officer of Riverside, Calif. "Awareness is key because it's the users who can put the integrity of our network at risk."

Riverside used to perform awareness training as a classroom exercise, but this year the city began using an online program from the SANS Institute called Securing the Human. The training is now mandatory; if employees don't take and complete the one- to two-hour course within the designated time frame, they are locked out of the city's network. The training is modular and can be tailored to the type of data the employee works with, such as legal documents or Health Insurance Portability and Accountability Act forms, for example. Deesing described the training as interactive, and should an employee fail the short test at the end of the course, he or she must take it over again.

Another program is Managed Online Awareness Training from Awareity, which is used by Loudoun County, Va. Wendy Wickens, the county's IT director, said all employees must take the training once a year; the session lasts 30 to 90 minutes and is also interactive, with videos, test questions and a review of the county's security policies. The program costs \$39,000.

Along with awareness training, the county has ratcheted up security by turning off employee access to personal email on the county's network. "That has drastically reduced the instances of ransomware, which has become rampant," said Wickens. However, the county offers public Wi-Fi (separate from the county network) to employees who have a personal device and want to access personal email when they're not working. "Since we instituted that policy, we haven't seen any instance of ransomware [on the county network], which is significant," she said.

Not all state or local governments are investing in cloud-based awareness training programs from third parties. In Prince George's County, Md., the 6,500 government employees receive their awareness education through a

Exposed: THE STUPID THINGS WORKERS DO



13%

let their colleagues use a device that can access their employer's network; **9 percent allow their partners to access such a device.**

20%

of employees share their work email password; **12 percent share passwords** to other work applications. Nearly half of all employees are unaware of any company policy around password sharing.

One in five

employees **do not have any security software** on their mobile work devices, beyond what ships with the operating system.

SOURCE: INFORMATIONWEEK; RESEARCH CONDUCTED BY ARLINGTON RESEARCH IN 2016 ON BEHALF OF ONELOGIN

custom learning management solution that has been crafted by the county, according to CIO Vennard Wright. The training takes place annually and is both online and offline for certain workers who don't have access to a computer.

Wright also has seen a big drop in employee-triggered malware attacks since the county made the awareness training mandatory, and bars employees from the county network who haven't taken the training or failed to pass the course. "The first year we made it mandatory, there was a lot of pushback, but now the training is accepted," he said.

Not all security awareness programs are foolproof when it comes to changing behavior in the workplace. The programs can fail to perform as expected for a variety of reasons. Ira Winkler, president and co-founder of Secure Mentem, a consulting firm that focuses on security awareness, said problems can start with the basic objective. "There's a difference between awareness and training, and most people are providing training, not awareness," he said. "Training is putting a fixed body of knowledge on employees and testing them. Awareness is about changing behavior. But most people don't know that. Showing employees a video is not going to work as far as changing behavior."

Online awareness programs need to be part of a broader, more holistic approach toward security, according to Winkler. Making awareness ubiquitous requires a broad array of tactics, including pervasive messaging to workers through posters, newsletters, message boards, events and contests. "It's up to CISOs to create a security culture, an environment where people do the right thing," he said.

Awareness experts criticize the approach where security awareness training takes place once a year, with a short quiz at the end. "That's compliance and checking a box, not true awareness," said Winkler.


In Missouri, making security awareness part of the employee culture includes the use of gamification techniques to maintain interest. Roling said his department will also periodically test employees by sending out fake phishing attacks, usually tied to a theme around a current event. Employees who fail to identify the fake phishing email and click on the link will find themselves at a website

"AWARENESS IS KEY BECAUSE IT'S THE USERS WHO CAN PUT THE INTEGRITY OF OUR NETWORK AT RISK."

that explains what has happened and what they should have been looking for.

Roling keeps track of which agency makes the lowest number of mistakes and which makes the highest. The rankings are posted, and agencies that struggle are encouraged to improve and increase their awareness ranking. It's part of a broader set of metrics Roling keeps on how employees fare with awareness training, and it's considered an effective way to measure what's working and what isn't.

By mixing gamification, a little competition and metrics with the overall awareness program, Roling said that state employees see the monthly exercises as less of a burden and understand that it is a regular component of work. "Awareness training is one of the most important components of our security posture," he said. "All the security tools out there will never be as sharp as the human mind."

It's a point that more government CISOs agree with and has made them realize just how critical security awareness has become. In Riverside, security awareness has broadened into a larger education program for city workers, according to Deesing. "We are educating our people about how to handle different types of data and whether or not they should even be storing different types of data. We are also scanning our data to ensure there aren't any human errors that could put the city at risk." 

tnewcombe@govtech.com

THE CENTER FOR DIGITAL EDUCATION'S

converge

re:thinkedu

Q2 2016

Inside:

Can analytics
get an A grade?

The yellow
school bus
goes wireless.

How good is
virtual reality?

Richard Culatta's

Rhode Island's
chief innovation
officer wants to
bring new ideas
to education.

CRUSADE

To download a free copy, visit:
www.centerdigitaled.com/magazines



Predicting the Future

Data can help governments solve specific problems and prepare for major events.

Wayne Gretzky once said, “A good hockey player plays where the puck is. A great hockey player plays where the puck is going to be.” But how can government leaders move from good to great with technology and security? Where will the “puck” be for your business area?

As we address these questions, there are new industry tools to consider and new ways to predict the future more accurately using available data.

Just as many people have moved from relying on traditional radio traffic reports describing road congestion to real-time warnings and alternative routing from smartphone apps, there are now thousands of new tech tools that incorporate real-time data to improve productivity and effectiveness. The opportunities to use big data analytics to solve specific problems are expanding rapidly in virtually every area of life.

For example: How does Chicago know which trash bins need to be emptied today? How can law enforcement use

advanced analytics to predict, anticipate and prevent crime?

The answer is that an algorithm is mining big data or using new data that’s available via sensors as part of the Internet of Things.

So where can you start to better predict the future in your enterprise?

First, examine your current program and

specific project assumptions. Do this by picking a government business area and assessing where you are regarding innovation compared to industry norms and best practices. Ask: What data are we collecting? How is the data shared? What are the privacy implications? Look at the data management guidance provided by the National Association of State Chief Information Officers (NASCIO).


Second, ask, “What if?” Imagine an alternative future in your particular area of interest. Start by examining technology trends. Utilize prediction reports from Gartner, Forrester and others that have crunched the data and checked the forecast percentages. Analyze and learn from the free end-of-the-year summaries as well as New Year predictions from media sources and vendors. We are seeing more technology and security predictions in every area of life, and you can benefit from this analytical trend. Look at award-winning projects and best practices from NASCIO and the National Association of Counties to inspire your teams.

And third, build project road maps that use this updated or real-time data. Re-examine tactical and strategic plans based on this new data-centric world. *Forbes* magazine reported that “fast data” and “actionable data” will replace big data, so companies should focus more on asking the right questions and making use of the data they have. Also look outside your organization to gain access to specific data needed to improve your customer’s experience. This is an ongoing process.

One way to make your vision a reality is to build scenario-based alternative futures for the service being provided. For example, your team can explore what can be done given various situations or assumptions in the year 2020. Answer set questions for each alternative path.

This approach is similar to the way that first responders and others in government prepare for emergency management scenarios such as fires, floods, tornadoes or even cyberattacks. Tabletop exercises can help you ask the right questions about what data is needed by various functions, who will communicate with whom and which metrics are important.

Some skeptics may ask, “But how can my government prepare for major unpredictable events like the United Kingdom leaving the European Union?” My answer is that even major events are not unpredictable. There will certainly be times when circumstances on the ground bring surprises, but we can have scenarios to plan for a wide variety of potential outcomes in any area — including defending against cyberattacks, business disruptions or technology breakthroughs.

Like Gretzky, we can be at the right place at the right time by knowing the data. 



Daniel J. Lohrmann is the chief security officer and chief strategist at Security Mentor. He is an internationally recognized cybersecurity leader, technologist and author. From 2002 to 2014, Lohrmann led Michigan’s award-winning technology and cybersecurity programs, serving as CSO, CTO and CISO.

Modern Government Powered Through Cloud

Join this briefing
to learn what
Oracle Cloud can
do for you.

Upcoming Locations:

Atlanta / Nov. 2

Nashville / Nov. 3

San Francisco / Dec. TBD



REGISTER NOW

800-820-5592 Reference the event date and location
www.oracle.com/events

ORACLE®

CLOUD

Work Together ▶

InFocus Corp. announced its 70-inch Mondopad Ultra touchscreen collaboration system, an all-in-one video-conferencing, interactive whiteboarding, presentation and data-sharing display for teams. Mondopad allows team members in multiple locations to see and hear one another while brainstorming on a shared whiteboard, and to collaboratively edit documents and draw directly onscreen. Documents can be saved to the system, stored to the network or emailed to anyone directly from the device. The 4K high-definition screen resolution provides four times the detail of a 1080p HD display. The Mondopad features a sixth-generation Intel Core i7-6700T processor and Q170 chipset, 8 GB memory, and a 256 GB solid state hard drive. www.infocus.com



Print Pro ▼

Xerox introduced the WorkCentre 3345 Multifunction Printer (MFP), which operates at up to 42 pages per minute and 1200 x 1200 dots per inch. Users can scan to email or print, from the cloud or USB memory drive right at the MFP. The printer carries Apple AirPrint, Google Cloud Print, and the Xerox Print Service Plug-in for Android and Mopria, a set of standards that enable printing from a mobile device to printers from different manufacturers or brands. The 3345 features a monthly duty cycle of up to 80,000 prints. www.xerox.com



Storage Sense ▲

Spectra Logic expanded its BlackPearl P Series of storage, which more than triples the throughput and number of tape drives managed compared to the standard BlackPearl S Series. The P Series can store more than 1 billion objects, transfer up to 3,000 MBps sustained to disk or tape, and manage 20 or more linear tape-open (LTO)-7 tape drives, paving the way for future generations of LTO and TS tape drives. The P Series offers a 10-serial-attached-SCSI solid state drive with 960 GB SSD cache. www.spectrallogic.com



For more product news, log on to explore *Government Technology's* Product Source. govtech.com/products

ARE YOU

DOB: 06-09-85
P: 614
555
7242

SSN: 123-45-6789
SEX: F
G.S.H.: 45-6789

I'M HOMEALONE
RIGHT NOW

YOUR USERNAME
YOUR PASSWORD

YOUR NAME1234@EMAIL.COM

ID: 120345678

2345 ANYPLACE

ANYTOWN
AVE, NY 12345

EX: 6-13
CC#: 47167167
A2031071

YOURSELF?

PROTECT YOUR IDENTITY BY PRACTICING SAFE HABITS ONLINE.

STOP other people from accessing your information by using strong passwords. **THINK** before you download apps you aren't familiar with. **CONNECT** with friends safely online by checking your privacy settings regularly.

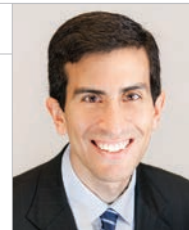
Visit www.dhs.gov/stopthinkconnect for more information on how to get involved with the Stop.Think.Connect. Campaign.



Homeland
Security



STOP | THINK | CONNECT



Smarter Together

If only one U.S. city wins the smart city race, the whole nation loses.

Many governments around the world are working diligently to build smart cities — those that use sensors, data and analytics to tackle important urban issues such as how to better manage sanitation systems, improve transportation networks and deliver government services more efficiently. For example, cities can install sensors in water mains to detect leaks or conduct computer-based analysis on real-time video feeds to combat crime. Unfortunately the United States has woefully underinvested in smart city efforts compared to other leading countries. To address this shortcoming, federal, state and local governments should come together to create a new stream of funding for U.S. cities to increase investment in the digital infrastructure they need to ensure they are modern, sustainable and competitive.

The U.S. government has committed approximately \$160 million over the next five years to support smart city initiatives. This is a pittance compared to some of the investments other countries are

making to develop smart cities. For example, in India, Prime Minister Narendra Modi announced a \$74 billion initiative last year to launch 100 smart cities in the country by 2020. And in Singapore, Prime Minister Lee Hsien Loong launched the Smart Nation initiative, which has led

to nearly \$7.5 billion in technology investments over the past three years.

One of the single largest investments in smart cities in the United States occurred this past June when U.S. Department of Transportation (USDOT) Secretary Anthony Foxx announced that Columbus, Ohio, had won the Smart City Challenge — a \$50 million federal prize awarded for a single city to address important issues such as safety, mobility and climate change through better use of data and technology. This


The U.S. government has committed approximately \$160 million over the next five years to support smart city initiatives.

is an important milestone because most smart city projects in the United States, like Chicago's efforts to build the Array of Things — a network of sensors that collects “real-time data on the city's environment, infrastructure and activity for research and public use” — have mostly been small-scale projects focused on a particular application or problem rather than the broad integration of sensors, data and analytics across virtually all public services.

The most impressive aspect of the Smart City Challenge is that so many cities responded to the call. From Anchorage to

Atlanta and Albuquerque to Albany, the USDOT received a total of 78 applications representing 85 cities in 36 states. Many of these proposals identified important challenges facing municipalities and proposed novel solutions that leveraged technology to improve the community. For example, Boston outlined its plan to integrate additional sensors, data and analytics with other government systems to combat injuries and fatalities among pedestrians and bicyclists, address disparities in its transportation system, and more.

Unfortunately the Smart City Challenge only funded one city's proposal, even though many more were also deserving. This is an inadequate approach for funding critical digital infrastructure. Just as it would not make sense to only fund bridges and highways in one city in the United States, it makes no sense to limit investment in the sensors, systems and networks needed to build smart cities to a single location. Instead, policymakers at the city, state and federal levels should be working together to fund promising proposals and develop strong partnerships with the private sector. This could take the form of new grants or repurposing existing funding for physical infrastructure to include digital initiatives.

While there is enormous potential to leverage data-driven innovation to improve the quality of life in urban environments, the United States will need to take action soon if it does not want to fall too far behind in the race to build smart cities. 

Daniel Castro is the vice president of the Information Technology and Innovation Foundation (ITIF) and director of the Center for Data Innovation. Before joining ITIF, he worked at the Government Accountability Office where he audited IT security and management controls.

PULLING DATA TOGETHER

MAKING DATA INTEROPERABLE ISN'T EASY, BUT TAKING THE RIGHT FIRST STEPS CAN HELP STATES THROUGH THE PROCESS.

INTEROPERABILITY: HARD WORK, BUT WORTH THE EFFORT

The holy grail of the big data era is an integrated data architecture that allows government enterprises to integrate siloed data to help make better decisions for themselves and their citizens.

For health and human services agencies in particular, interoperable data is the foundation for several important initiatives, including integrated eligibility programs. It also provides caseworkers with a better view into how well those programs are providing assistance.

In addition, state leaders can more easily apply analytics to integrated data to see which programs are succeeding and where money could be better spent. For example, if data showed a large number of babies with low birth weight in a particular region within a state, decision-makers could target that area for additional outreach by maternal health services. Better prenatal services could, in turn, improve birth outcomes and reduce Medicaid spending in the future.

In both the private and public sectors, it's been a heavy lift to pull together a fully integrated data architecture. A recent study found that although it is a priority for corporations, 79 percent of private organizations have not yet integrated their data sources.¹

State governments are making some progress: As of early 2015, 19 states had interoperable data platforms that they used to develop integrated eligibility programs and 12 indicated they

had plans to phase in a number of assistance programs in the next few years.²

WHY DATA INTEROPERABILITY SHOULD BE TOP OF MIND

The timing is right for states looking to make their data interoperable. The extension of the enhanced 90/10 federal funding match for Medicaid system modernization, along with the current waiver of OMB A-87 cost allocation rules, help states integrate Medicaid data with insurance exchanges. These federal rules also help with integration of data from other human services programs such as the Supplemental Nutrition Assistance Program (SNAP, formerly known as the Food Stamp Program), Temporary Assistance for Needy Families (TANF) and the Special Supplemental Nutrition Program for Women, Infants and Children (WIC). Funding might also be used to integrate corrections or education department data, so long as the data sharing can be shown to add value to the Medicaid program.

The Centers for Medicare & Medicaid Services (CMS) isn't alone in offering incentives. The Administration for Children and Families and the Food and Nutrition Service, among others, are also working toward interoperability and offering assistance for federal and state data exchange projects.

However, even with additional funding, states face many challenges. Along with technological change, this effort requires a culture shift that can be difficult for agencies to implement. But the payoff is worth the effort. For those states that have not yet started down the

road toward data interoperability, here are four guidelines for laying the groundwork:

4 STEPS TOWARD MAKING DATA INTEROPERABLE

STEP 1: INVENTORY ASSETS

Before starting a data initiative, a state or locality needs to inventory its data to determine where the information resides, and who has access to and control of it. Many states and localities struggle with this step. Most agency programs operate in silos, and each is likely to have distinct data security and access policies. In addition, the owners of the data can be wary of giving up control of their information.

When integrating HHS programs and data sources, it is advisable to implement an organizational change management (OCM) strategy to educate staff on the value of creating the inventory and to ensure that all stakeholders are aware of their responsibilities and understand the need to participate. Employees should be assured that creating a data inventory can help identify opportunities for process and data quality improvement, which will in turn benefit their individual program areas. Understanding the inherent value in this process helps uncover hidden gaps and inconsistencies while building trust among groups around security, processes, ownership and disposal of data.

STEP 2: THINK SMALL

While the overall goal is to one day integrate data from multiple agencies, it helps to start with one small, manageable project. Find a program and gain experience by integrating its data sets. This helps employees gain confidence and builds support for larger efforts.

For example, two of Michigan's early interoperable projects were vital statistics and immunization records, both of which can feed into a larger system. Similarly, Illinois started with WIC and family case management data and then integrated vital statistics and immunization records with Medicaid data. Since many of the same recipients spanned multiple programs, there was a solid business case to use the integrated data for program analysis.

Medicaid data is at the heart of any effort. Once a state makes its Medicaid databases interoperable, integrating with other programs becomes easier.

STEP 3: ENGAGE LEADERSHIP

As a data interoperability effort moves forward, it's important to find executive sponsorship within the agency — someone who can both influence people within the agency and go to the legislature for guidance or funding when the program grows beyond the department's span of control. Agency or departmental leaders often spearhead integration efforts within their own departments, and then seek broader support based on their success.

As the program expands into multiple agencies, it becomes more important to have the support of the governor and the legislature. Laws and rules will need to be updated, changed or written. Leadership for that should come from the top.

STEP 4: ADDRESS PRIVACY HURDLES

Those in charge of data tend to point to the Health Insurance Portability and Accountability Act (HIPAA) and other privacy laws and say, "My data is protected; I can't share it."

These fears and concerns need to be addressed and discussed. In general, staff members need to be reassured that the new system will take into consideration HIPAA and other data protection rules and still allow for sharing.

States that have moved ahead with interoperable data have found workable solutions to the legal issues raised by privacy laws. For instance, California's Healthcare Eligibility, Enrollment and Retention System (CalHEERS) is an integrated system that determines eligibility and helps with enrollment in insurance exchange health plans and Medi-Cal (the state's Medicaid program). It has legal documents in place that spell out who can use the data and for what reasons. HIPAA guidelines are followed in the sharing of data for specific purposes.³

CONCLUSION

Integrating data is hard work, but the payoff is worth it. For instance, after making its health and human services data interoperable, Utah went on to develop a data warehouse that collects, compiles and standardizes information from different state and federal data sources (such as quarterly wage, unemployment insurance and Social Security). The integrated data gives decision-makers a holistic view of all citizens and enables them to suggest appropriate services accordingly.

This piece was developed and written by the Government Technology custom media division, with information and input from Optum.

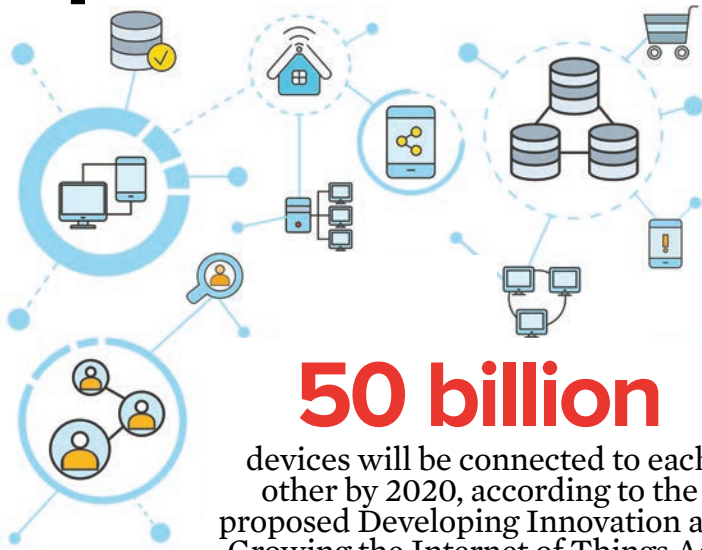
Endnotes

1. <http://ebooks.cappgemini-consulting.com/cracking-the-data-conundrum/>
2. <http://kff.org/report-section/modern-era-medicare-eligibility-and-enrollment-systems/>
3. <http://www.calpirg.org/reports/caf/calheers-protecting-consumer-data-developing-and-implementing-strong-physical-technical>

BY: **government
technology**

FOR:  **OPTUM®**

FOR MORE INFORMATION,
go to optum.com/government
or call 866-223-4603.



50 billion devices will be connected to each other by 2020, according to the proposed Developing Innovation and Growing the Internet of Things Act, which could give the IoT a boost in the form of federal assistance.

SOURCE: FUTURESTRUCTURE

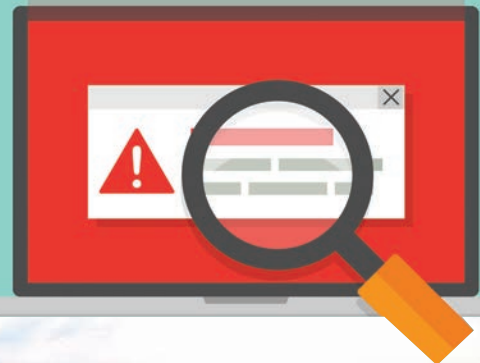
PARTNERING FOR ENERGY:

Nest, the maker of smart thermostats, is partnering with a California utility in an effort to get 50,000 participants in an energy conservation program. Following a massive natural gas leak in 2015 that has restricted supply, the company wants to encourage enough Southern California Edison customers to participate by next summer to reduce energy demand by 50 megawatts, or the amount produced by a small natural gas plant. Demand-response programs automatically curb energy use during times of peak use to help avoid blackouts. SOURCE: BLOOMBERG



90% The number of people who ignore security warning messages on their computers or mobile devices.

Researchers from Brigham Young University in collaboration with Google Chrome engineers found that messages that appear while users are focused on a task like typing or watching a video are usually disregarded. Timing security warnings to pop up after users watch a video, while they're waiting for a page to load or after interacting with a website can enhance their security behaviors. SOURCE: PHYS.ORG



Ready, Set, Sun

A solar-powered car built by students at the University of Michigan won the American Solar Challenge, an eight-day race that began July 30. Powered by a 65-square-foot solar array, the university's car, called Arium, stores energy in a lithium-ion battery pack and can reach speeds of up to 80 mph (although the race limits the vehicles to 65 mph). Twenty-four teams of college students participated in the biennial competition in which Arium beat the pack by 11 hours, finishing the trek from Ohio to South Dakota in 48 hours, 26 minutes and 46 seconds. SOURCE: NEW ATLAS



Send Spectrum ideas to Managing Editor Elaine Pittman, epittman@govtech.com, [twitter@elainerpittman](https://twitter.com/elainerpittman)



Make it a Team Effort

How to get all staff members involved in your agency's social media efforts.

Most of your agency's employees are not directly involved in managing social media or even contributing content. That's not necessarily a bad thing (managing 1,000-plus contributors is tricky), but you should consider the benefits of getting all staff members involved with your agency's social media presence.

Why bother? It's really hard to present a united front when most of your staff members are unaware of your agency's social media strategy. Department representatives might not even know what profiles your agency maintains on various platforms. They might also be unaware that they can contribute content (can they?) and the process they can use to do so.

There are likely a large number of staff members who work for your agency, but don't work with programs that traditionally have public-facing social media content because they are an internal-facing division, such as auditors or fleet maintenance. But there are still opportunities to get them involved with your agency's social media

presence. This leads me to my first recommendation, which speaks to how you develop the social media strategy in the first place.

Get departments involved in social media goal-setting.

A good social media strategy starts off by identifying goals. Involving other

departments at this stage ensures that the high-level goals of your organization as well as departments are considered and incorporated from the beginning.

Social media strategies should be unique to each organization — what works for one city or county does not necessarily work for another. A comprehensive social media strategy is guided by a number of variables, ranging from the high-level mission of the agency, to the strategic goals for key departments, to the city's communication goals. Setting social media goals that complement the government's

the community about alternative mobility options. Be creative and get agency staff involved in social media goal-setting.


Empower staff members to monitor social media. A best practice I like to teach is empowering agency staff to monitor social media for citizen activity related to the programs and projects that directly relate to their role. Several free online tools can easily allow staff to monitor keywords and hashtags while also keeping track of conversations and posts related to a specific subject matter. Free

Here's a pro tip: Many department goals can be found in annual budget documents. While some of them will be very project specific, the higher-level goals may be a perfect fit to incorporate into your social media strategy.

guiding principles will help ensure a consistent and meaningful message.

Here's a pro tip: Many department goals can be found in annual budget documents. While some of them will be very project specific, the higher-level goals may be a perfect fit to incorporate into your social media strategy. Better yet, talk to department representatives and ask them what the long- and short-term goals are. For example, if the public works division has a priority over the next couple of years to conduct major traffic flow infrastructure improvements, that can evolve perfectly into a new social media goal: educating

tools available today include setting up Google alerts or using Twitter advanced search and social mention services.

Ensure the availability of ongoing social media training. Offer regular social media training agencywide for all staff, leadership and elected officials — not just for social media content authors. Consistent training helps employees and electeds stay up-to-date about the policy, rules and legal aspects of posting on social media, as well as stay informed as to why certain social media platforms were selected for an agency presence. 

Kristy is known as "GovGirl" in the government technology industry. A former city government Web manager with a passion for social media, technology and the lighter side of government life, Kristy is the CEO of Government Social Media.



MANAGED SERVICES.

A POWERFUL IT SOLUTION FOR GOVERNMENT AGENCIES.

Secure your network. Protect your data. And rest assured your IT infrastructure is cared for by a leader in the business. We'll work with your IT team to handle the day to day network tasks, so they can focus on the big picture. From reliable bandwidth to accountability and cost efficiencies, nobody knows networks, and your network needs, like we do.

1-877-900-0246

brighthouse.com/enterprise

BRIGHT HOUSE NETWORKS
enterprise solutions



WE'RE WIRED DIFFERENTLY



MANAGED SECURITY | MANAGED NETWORK | MANAGED WIFI

©2016 Bright House Networks. Some restrictions apply. Serviceable areas only.
Service provided at the discretion of Bright House Networks.

WORK SITTING or STANDING

VARIDESK® sits on top of your existing desk and lets you switch easily between sitting and standing whenever you like – and it only takes 3 seconds! It ships fully assembled and sets up in minutes with no tools required. Order online or call 877-629-1462.

FREE SHIPPING
TO LOWER 48 STATES



Pricing and product availability are subjected to change. Taxes will be added for delivery into California, Texas, and Nevada. For patent and trademark information, visit VARIDESK.com/patents. ©2016 VARIDESK®. All Rights Reserved.

VARIDESK®.com
WORK ELEVATED™

Special Report 2016

A Research Report from the
Governing Institute and
Center for Digital Government

HHS

IN TRANSITION

What's Happening.
Who's Doing It.
Why You Care.



American Public Human Services Association



INFLUENCE BUILD CONNECT

Association of Administrators of the Interstate Compact on the Placement of Children

Establishing Uniform Legal and Administrative Procedures Governing the Interstate Placement of Children

IT Solutions Management for Human Services

Sharing Innovative Solutions, Connecting IT Professionals, Collaborating with Private Sector Partners

National Association for Program Information and Performance Measurement

Enhancing the Integrity and Outcomes of Human Service Programs

National Association of State TANF Administrators

Providing Expert Support and Consultation on TANF and Human Service Program Issues

AAHSA

AAICPC

AASD

ISM

NAPCWA

NAPIPM

NASCCA

NASTA

NSDTA

American Association of Health and Human Services Attorneys

Attorneys Sharing Knowledge and Promoting Innovation

American Association of SNAP Directors

Strengthening Long Term Family Health and Well-Being

National Association of Public Child Welfare Administrators

Developing Public Child Welfare Agencies to Improve Performance and Consumer Outcomes

National Association of State Child Care Administrators

Focusing on the State, Affordable, High-quality Care of Children

National Staff Development and Training Association

Sharing Ideas and Resources on Organizational Development, Staff Development and Training

Creating Strategic Directions in the Transformation of Health and Human Services

www.APHSA.org



INTRODUCTION

04 INTO THE GREAT UNKNOWN

06 SOCIAL ISSUES DEMANDING YOUR ATTENTION

The Opioid Epidemic 06

America Ages 07

Complexities of Mental Illness 08

12 HOW YOU'RE DRIVING DOWN COSTS — AND IMPROVING LIVES

Focusing on Outcomes 12

Getting Smarter with Data 13

Changing Tactics 16



CONTENTS



HOW YOU'LL SHARE DATA SAFELY 28

Simplifying the Regulatory Maze 30

Going Mobile, Securely 32

23



HOW YOU'LL MODERNIZE HHS SYSTEMS 20

Why You'll Build Differently 21

The Challenges You'll Face 26

CONCLUSION

A TRANSFORMATION IN PROGRESS 34

© 2016 eREPUBLIC. ALL RIGHTS RESERVED
100 BLUE RAVINE ROAD, FOLSOM, CA 95630
916.932.1300 PHONE | 916.932.1470 FAX

MULTIPLE FORCES ARE PUSHING HHS PROGRAMS TOWARD AN INTEGRATED AND DATA-DRIVEN FUTURE, THE ULTIMATE FORM WHICH REMAINS TO BE SEEN.

THE WAY OUR NATION DESIGNS AND RUNS HEALTH AND HUMAN SERVICES (HHS) PROGRAMS

is in the midst of unprecedented change. Spiraling demands, evolving policies and new technologies are pushing the HHS field into uncharted waters.

For agencies in this space, the future looks like this: There will be growing pressure to inter-connect separate benefits programs into something that works better and more cohesively for citizens.

INTO THE GREAT UNKNOWN

There will be a push to understand how factors such as where citizens live impacts their health and well-being. And there will be an expectation that agencies analyze data to measure the effectiveness of the programs they run.

Behind the scenes this will drive big changes in the technology systems that support HHS programs. Individual systems will need to integrate more tightly than ever before; they'll need to share and consume data in innovative ways; and they'll need to offer new levels of mobility and other user-friendly features. Sophisticated data analytics and visualization tools will take on more prominence, too, as agencies seek to turn mountains of information into actionable insights.

Even the way HHS systems are deployed is undergoing a seismic shift. In an effort to reduce the cost and risk that are inherent in the modernization of large computer systems, the federal government is incenting an approach known as modular development. The approach envisions breaking big complex systems into smaller logical components. In theory, this makes modernization easier since systems can be deployed one piece at a time. But it also demands that agencies develop new skills around how to plan for these upgrades and fit the pieces together.

As if that weren't enough, the looming presidential election injects

still more uncertainty into the mix. Experts say growing integration of HHS programs and greater use of data-driven decision-making are here to stay, regardless of the election's outcome. But a new administration certainly will bring its own nuances and priorities.

"I think there are a number of factors that have come together that are triggering changes across the entire sector — both in health programs and in human services," says Tracy Wareing Evans, executive director of the American Public Human Services Association (APHSA).¹

"Funding available through the Affordable Care Act is helping to modernize technology on the health side and maximize the opportunity to bring integration and interoperability to human services systems," she adds. "Beyond the technology, there's also a compelling need for more evidence-based work, both from a fiscal standpoint and to simply do what's right for families that are served by these systems. We need to know what works and what doesn't."

Feeling the Strain

Our annual health and human services survey — conducted in partnership with APHSA — reflects the pressures HHS agencies are feeling. Respondents ranked better data sharing among agencies as their top priority, followed by closer integration of services and technology systems, and adoption of analytics tools. They also told us they're busier than ever. Seventy-five percent of respondents said demand for HHS services has increased over the past year, with 20 percent estimating workloads grew anywhere from 25 to 50 percent.

Although 70 percent said their agencies are moving in the right direction, respondents were less confident in their ability to use data to drive better results.

That pessimism may stem from a couple of factors: First, HHS is still rife with clunky old computer systems that neither integrate nor share data

easily. And second, privacy and security concerns — real or imagined — tend to be a drag on innovation in this area. Almost all survey respondents told us they have technology that needs to be replaced, with 25 percent saying anywhere from a quarter to half of all their systems require modernization. Sixty percent also said increased data sharing brings with it greater security and privacy challenges.

Seizing the Opportunity

Still, we think all of this means HHS agencies are on the cusp of great opportunity — but one that can't be realized without a massive culture shift and a great deal of hard work.

Policy innovations are driving HHS programs toward a more holistic view of citizens and more comprehensive program offerings. Funding streams are evolving as well, allowing dollars to be spent more flexibly on integrated approaches and better data tools. As our research shows, agencies are beginning to adapt their thinking, but will need to react with even more agility and innovation to make the leap.

Luckily, technology has evolved to the point where systems more easily support the development of tightly interconnected platforms that serve multiple HHS functions. And growing acceptance of off-the-shelf software packages and cloud-based services mean agencies no longer need custom developed software — or to even own software at all. However, agencies will need to think differently to exploit these changes.

Pushed by new policies and powered by modern technology, HHS is in the midst of dramatic change, the ultimate form of which remains somewhat uncertain. This report maps the forces that are driving this transformation, both to build understanding of the current environment and to push toward a markedly different — and more effective — approach to serving the people and communities that rely on these services.



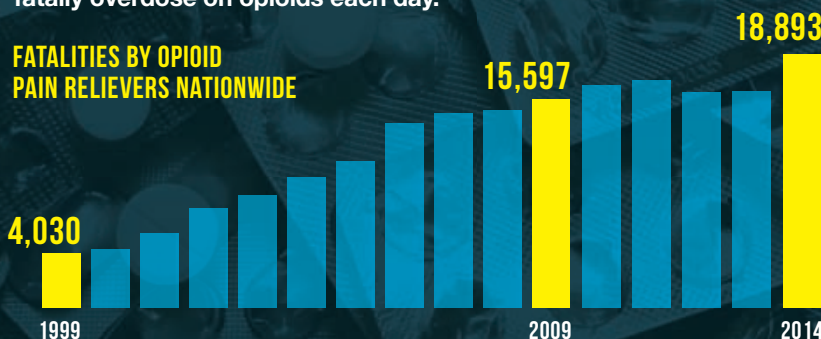
A LOOK AT THE SOCIAL ISSUES DEMANDING YOUR ATTENTION

The shifting HHS landscape is being driven by several social issues: The U.S. population is aging, the opioid epidemic is spreading at an alarming rate and mental health issues are becoming more complex. All of these issues are causing HHS agencies to take notice and take action. As a result, governments across the country are refocusing their efforts on coordinating care and finding innovative solutions.

THE OPIOID EPIDEMIC

What once may have been a silent epidemic is now impossible to ignore. Killing more people than automobile accidents, opioids are the leading cause of accidental death in the U.S. According to the Centers for Disease Control and Prevention (CDC), fatalities from opioids more than quadrupled between 1999 and 2014, crossing all socioeconomic groups in urban, suburban and rural areas. It is estimated now that 78 Americans fatally overdose on opioids each day.

FATALITIES BY OPIOID PAIN RELIEVERS NATIONWIDE



Source: Centers for Disease Control and Prevention, 2015

What You're Doing:

GETTING THE WORD OUT

Earlier this year, [Virginia](#) unveiled its “Sink or Swim” campaign with a website (www.drugfreeva.org) and app. The website creates a one-stop shop for addiction resources — users can enter their ZIP code to find nearby treatment centers and support groups.



AN AGING AMERICA

The graying of the baby-boomer generation — combined with longer lifespans — means that individuals aged 65 and older will comprise about **22 PERCENT OF THE U.S. POPULATION BY 2030**. According to the U.S. Census Bureau, the 65-and-over population is projected to double over the next three decades to about 88 million by 2050. Since the majority of older Americans express a desire to age at home, these changes will drive spending on long-term care and technologies to allow them to live independently.

DESIGNING SENIOR-FRIENDLY COMMUNITIES

To prepare for its aging baby-boomer population (by 2030, the over-65 population is projected to double), Arlington County, Va., is making senior-friendly improvements. The county offers a door-to-door transportation service for individuals with disabilities and passed a zoning ordinance that allows some homeowners to build “granny flats.”³

What You’re Doing:

DELAYING NURSING HOME PLACEMENT

To lower Medicaid expenses, many states are trying to delay or prevent unnecessary nursing home placements, which account for some of the highest Medicaid costs for long-term care. For example, in Nebraska, the average cost of nursing home care is \$75,000 per person. Conversely, home and community-based services (HCBS) cost significantly less — home care is roughly half the cost of a nursing facility and community-based care is roughly one-quarter of the cost. By taking advantage of federal funding and partnering with organizations such as Area Agencies on Aging, governments can offer HCBS to their communities and lower the Medicaid burden.²

TAPPING TECHNOLOGY

States can educate their communities about available technologies to help seniors maintain their independence. For example, pill dispensers can send voice or text messages to seniors when it’s time to take their medication and include alerts when pills are missed. Shoes with GPS trackers can provide real-time location mapping. If a senior leaves the pre-determined zone, the caregiver receives an alert.



SHARING DATA

Washington is one of the few states that gives public agencies — including law enforcement, corrections, social services, labor and industries, and more — access to its prescription monitoring system. This allows the Department of Labor and Industries, for example, to closely monitor workers who were already chronic opioid users before filing an injury claim, and to flag doctors who may be prescribing too many drugs or potentially dangerous combinations of drugs.⁴

PUTTING TECHNOLOGY TO WORK

Every state except Missouri now has a prescription monitoring database. Last year, **Ohio** became the first state to link its prescription monitoring database with the electronic medical records already maintained by doctors and pharmacists.

LIMITING PRESCRIPTIONS

This March, **Massachusetts** began limiting initial opioid prescriptions to a seven-day supply, except those for chronic or cancer-related pain or palliative care. To prevent addicts from doctor shopping, practitioners must check the state’s prescription monitoring database before prescribing certain drugs. In July, governors of 45 states signed on to “A Compact to Fight Opioid Addiction” based on the Massachusetts law.⁵

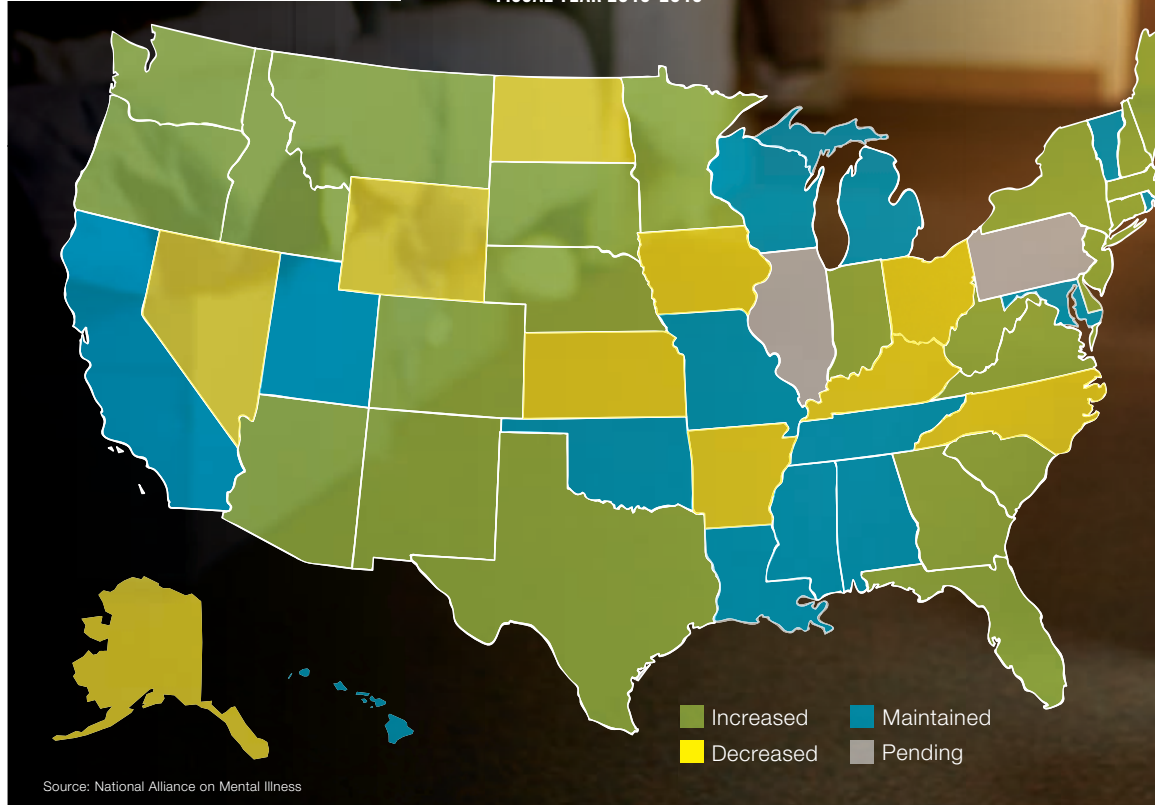
FINDING BETTER TREATMENT

The Centers for Medicare and Medicaid Services (CMS) advocates for medication-assisted treatment (MAT), which is treatment that uses medication as well as counseling and other support. After using MAT for opioid-addicted Medicaid patients, **California** cut its medical costs by one-third over three years, including hospital, emergency room and outpatient clinic expenditures.⁶

THE COMPLEXITY OF MENTAL HEALTH ISSUES

States and localities are struggling with how to address mental health issues. According to the National Alliance on Mental Illness (NAMI), 1 in 5 adults will experience a mental illness in a given year and nearly 10 million Americans live with a serious mental illness such as schizophrenia or bipolar disorder.⁷ However, only 24 states increased mental health funding from 2015 to 2016, while 11 states and the District of Columbia cut their budgets. Mental illnesses are also taxing America's correction systems. According to a 2012 Treatment Advocacy Center report, U.S. prisons and jails housed over 356,000 inmates with severe mental illness — 10 times the number of mentally ill patients in state psychiatric hospitals in the same year.⁸ **Incarcerating individuals with mental illnesses is not only expensive, it produces poor outcomes.**

STATE MENTAL HEALTH CARE BUDGETS
FISCAL YEAR 2015-2016



What You're Doing:

TAKING ADVANTAGE OF FEDERAL HELP

In March 2016, the Obama Administration released its final rules for Medicaid's mental health coverage, which aim to strengthen the 2008 Mental Health Parity and Addiction Equity Act that requires health insurers to offer the same level of benefits for mental health as they do for physical health. To help states comply, the federal government offered \$94 million in new funding for community health centers and \$1.4 million for education projects in rural areas focused on health and safety.⁹

OFFICERS IN
MIAMI-DADE
COUNTY
RESPONDED
TO OVER
10,000
mental
health calls
IN 2013 — AND
ONLY MADE
9 arrests.

DECRIMINALIZING MENTAL ILLNESS

Miami-Dade County in Florida has a mental illness rate that is approximately three times higher than the national average. To address this, the county offers a continuum of services to combat the criminalization of mental health problems. Led by Judge Steve Leifman, the county launched a post-arrest diversion program that offers individuals the option to undergo treatment instead of receiving a jail sentence. Approximately 80 percent of the individuals who are eligible to participate in the program enroll, and recidivism rates are just 20 percent. The county also trains all of its police departments in the Crisis Intervention Team (CIT) program, which teaches them to distinguish between different types of mental illness and respond accordingly. In 2013, officers responded to over 10,000 mental health calls, but only made 9 arrests, which allowed the county to close 1 of its 5 corrections facilities.¹⁰

USING TECHNOLOGY AS A SOLUTION

Telemedicine can be a game changer for rural states such as Alaska, which has the nation's second-highest suicide rate. It can be extremely difficult to find adequate mental health care in remote areas — one study found for every 10 miles you move from a city, it becomes 3 percent more difficult to find a behavioral health worker. The use of telemedicine, however, breaks down these barriers and easily connects patients to mental health facilities despite distance. Experts do caution that telemedicine should be implemented in conjunction with initiatives to attract more mental health workers to rural areas until high-speed internet access is pervasive.¹¹



A Powerful Tool to Pinpoint and Prevent Prescription Drug Abuse

Opioid Abuse: An Escalating Problem

In 2014, nearly 19,000 people died from prescription opioid-related causes – a 16 percent increase from 2013.¹

Killing more people than automobile accidents, approximately 78 Americans are fatally overdosing on opioids each and every day, according to the CDC.

One of the most devastating aspects of opioids is their ability to cut across all socioeconomic classes and demographics. “This is not a problem that is only impacting people who have gone astray and break the law,” says Dr. Este Geraghty, chief medical officer and health solutions director at Esri. “This is a problem that affects a lot of people and it could be your neighbor, your mother — people you might not have initially expected.”

Across the country, state and local government leaders are grappling with how to get ahead of the problem, including limiting painkiller prescriptions and launching prescription drug monitoring programs. In July, President Obama signed the Comprehensive Addiction and Recovery Act of 2016 (CARA), which increases the availability of naloxone, strengthens monitoring and expands educational efforts.

But funding is an issue. While Obama had asked Congress for \$1 billion for CARA, the Act included a fraction of that at \$181 million. Advocates say funding to address prevention and early treatment of opioid abuse is critical.

“We know that public health is traditionally under-funded and resources are always limited,” says Geraghty. “And so you need to use resources in the best way possible. You need to get to smaller, neighborhood-level analysis so you are targeting your interventions where they are needed the most.”

Raising Awareness and Targeting Resources

Geraghty points to the power of mapping to help leaders make strategic decisions regarding plans for prevention and intervention. Perhaps most importantly, visualization tools allow governments to raise awareness and make the epidemic real to their communities.

“Simple resource maps can be just the start in helping others understand addiction and find help,” says Jeremiah Lindemann, a solution engineer at Esri who lost his brother, J.T., to a prescription drug overdose and who has since become an activist for increasing awareness and using maps to help solve the problem.

“Visualizing trends provides a deeper understanding of the factors that may contribute to opioid use in a given area and the resources available to prevent and treat addiction,” says Lindemann.

Sometimes, simply putting a face to the problem makes the biggest impact in rallying a community to battle prescription drug abuse.

“Simple resource maps can be just the start in helping others understand addiction and find help.”

— Jeremiah Lindemann, Solution Engineer, Esri

1. <http://www.forbes.com/sites/cjarlotta/2016/07/23/obama-signs-opioid-legislation-despite-funding-concerns/#577fe58134e6>



How Maps Make a Difference

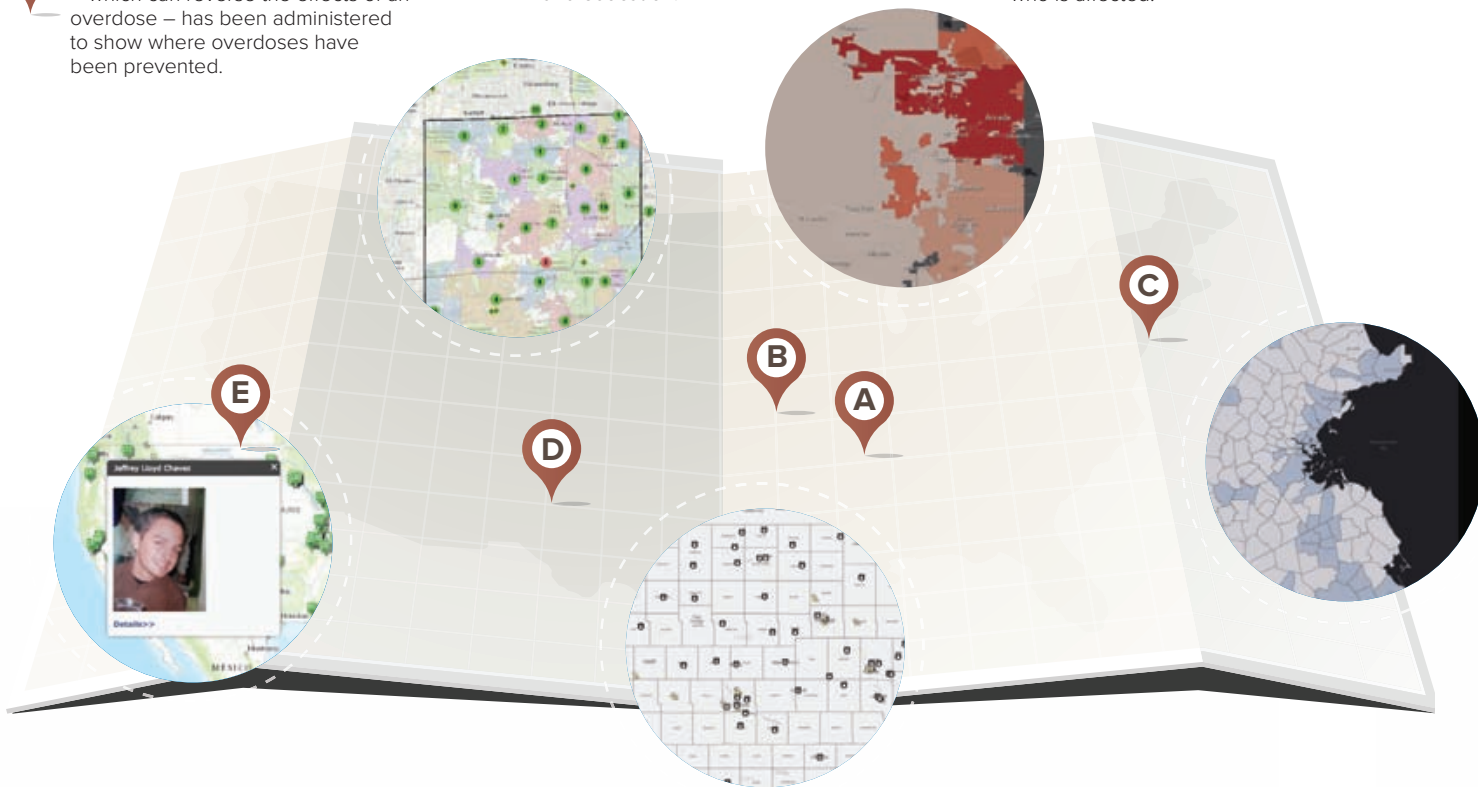
A DuPage, Ill., maps out where Narcan – which can reverse the effects of an overdose – has been administered to show where overdoses have been prevented.

B Iowa maps out the location of drug drop boxes so residents can safely dispose of prescriptions and prevent them from getting into drinking water or the hands of others.

D Jefferson County, Colo., uses a visualization map to show where prescription drug and heroin deaths have occurred to help raise awareness and stop the epidemic.

C Massachusetts performs spatial examinations of the opioid addiction within the state to determine where to target interventions and education.

E Celebrating Lost Loved Ones is a national map that aims to personalize the problem and break down perceptions of who is affected.



For more information, visit go.esri.com/Opioid.



HOW YOU'RE DRIVING DOWN COSTS — AND IMPROVING LIVES

TRANSITIONING TO OUTCOME-BASED PAYMENTS

Medicaid has traditionally reimbursed providers based only on the services delivered, but that is changing. Increasingly, states are incenting health care providers to meet performance measures. This practice, known as **paying for performance**, focuses on producing better health outcomes for citizens, or put another way, on quality rather than quantity of services rendered. In fiscal year 2014-2015, 34 states implemented quality improvement initiatives such as adding or enhancing pay-for-performance arrangements to their managed care contracts.¹²

What You're Doing:

LINKING PAYMENTS TO HEALTH OUTCOMES

New York

In the wake of the recession, New York State's Medicaid program was unsustainable, with significant cost increases as state revenues were declining. A Medicaid Redesign Team helped get costs under control, and now the state is using outcome-based payments to lock in those improvements.

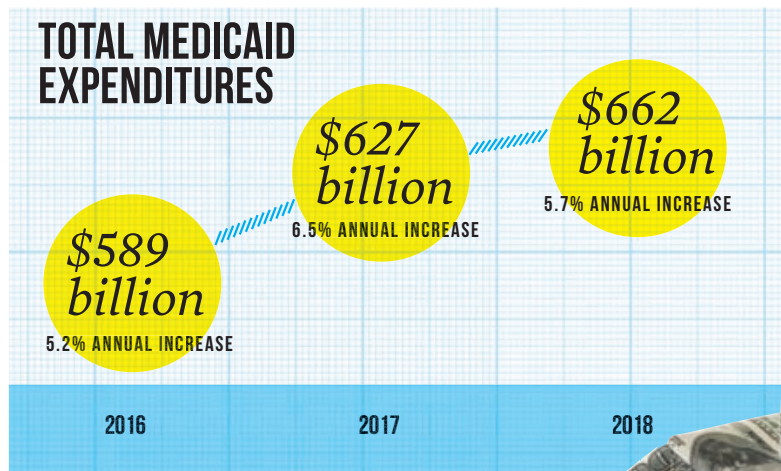
Funded with a \$7.3 billion grant from CMS, the Delivery System Reform Incentive Payment Program (DSRIP) provides incentives for hospitals and safety net providers to collaborate and form networks that promote integrated and holistic care. Approximately 90,000 providers — including hospitals, practitioners, clinics and behavioral health organizations — are split into



25 networks that have committed to reforms that link payments to the health outcomes of network members. By the end of 2019, 80 percent of provider payments will be value based.

Combining outcome-based payments and a shared-savings model for providers creates incentives for efficient, patient-centered care, says New York State Medicaid Director Jason Helgeson. He uses the example of children suffering from asthma: "If

Health and human services — and particularly health care — eat up a large portion of state and local budgets. The cost of Medicaid, which largely serves low-income individuals, is shared between states and the federal government and accounts for the biggest portion of those expenses. More than one-quarter of all state expenditures and over 15 percent of state-funded expenditures are Medicaid related — and those costs are rising (see table to the right). This section shows how governments are decreasing costs in their Medicaid and other HHS programs.



Source: Centers for Medicare and Medicaid Services

GETTING SMARTER WITH DATA

One thing government HHS programs are not lacking is data. The challenge has always been in accessing, sharing and analyzing data to produce better outcomes. Once data is tapped, however, the results can be transformative. A lack of funding for systems investment has largely left HHS behind the curve when it comes to the use of sophisticated analytics, but that is beginning to change. CMS launched the Medicaid Innovation Accelerator Program (IAP) in July 2014 with the goal of improving health and health care for Medicaid beneficiaries by supporting states' efforts to accelerate new payment and service delivery reforms, including the use of analytics.¹⁴

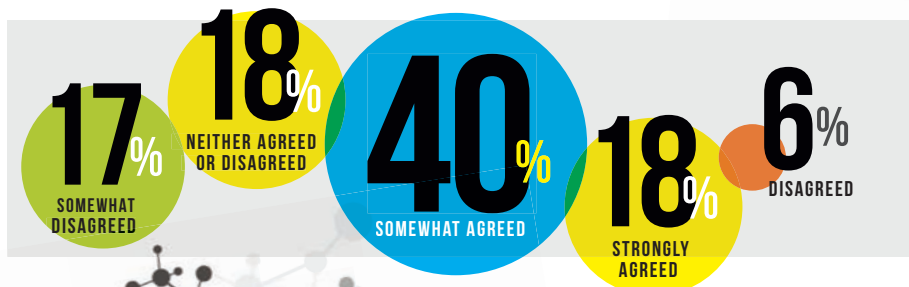
Jason Helgeson,
New York State
Medicaid Director

35 percent of the cost of treating them is the result of preventable complications that cost \$100 million per year, and we cut those complications by half, the provider networks share the savings. It's a win-win for patients and providers."

The initial results are encouraging. New York's Medicaid expenditures are no longer the highest in the country, and the state's average cost per beneficiary is declining.¹³

What You Told Us:

We asked respondents to the CDG/Governing Institute 2016 HHS survey if their agency consistently embraces data in new and innovative ways to improve program outcomes.



What You're Doing:

MAKING BETTER DECISIONS

Colorado

Data analytics has been integral to Colorado's Medicaid reform initiative, the Accountable Care Collaborative, which uses coordinated care efforts to produce better outcomes for beneficiaries, improve population health and reduce costs. The foundation of the initiative is a statewide data and analytics contractor (SDAC) that centralizes and tracks Medicaid eligibility and claims data. An online portal allows primary care providers, regional collaborative organizations and Medicaid officials to access actionable data on utilization and spending to identify areas of high need and improve care management. In fiscal year 2013, the Accountable Care Collaborative saw a 15 percent reduction in hospital admissions and a 25 percent reduction in high-cost imaging, contributing to \$44 million in savings.¹⁵

TARGETING INTERVENTIONS

Los Angeles County

In a pilot conducted from 2012 to 2014, the L.A. County Department of Children and Family Services screened youth to assess their risk of committing a crime and entering the juvenile justice system. Using an actuarial tool and predictive analytics, the department identified children as high risk by assessing them based on factors associated with criminal behaviors. Caseworkers then connected these children with drug treatment, additional schooling, therapy and other services intended to address the problem. Another group of high-risk children being monitored by the department did not receive intervention services.

An evaluation by the National Council on Crime and Delinquency found that after 6 months, the children who received services had no arrests, whereas 9 percent of the control group did. For the county, the pilot is a significant step toward keeping children out of the justice system.¹⁶

COMBATING FRAUD

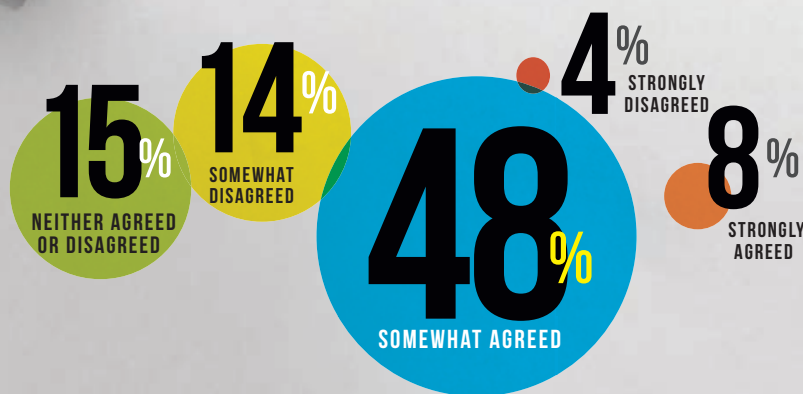
Florida

Florida's Department of Economic Opportunity (DEO) used a \$1.7 million grant to develop its Fraud Initiative Rules and Rating Engine (FIRRE) to help root out fraudulent unemployment insurance claims. The system can almost instantaneously process unstructured data and identify relationships that trigger early detection of fraud. So far it has helped the state stop 110,000 fraudulent claims and prevent wrongful payouts totaling \$460 million.

"Businesses pay taxes to fund Florida's unemployment program," says DEO Executive Director Cissy Proctor. "By limiting the amount of fraudulent benefits paid out, we're able to reduce how much businesses have to pay in taxes." Proctor says FIRRE could be modified to detect fraudulent applications in other benefits programs such as SNAP and TANF.¹⁷

What You Told Us:

We asked our survey respondents if their agencies had effective ways of monitoring and abating fraud with their current systems.



9.8%

The percent the federal government conservatively estimates is the annual improper payment rate for the Medicaid program.¹⁸

WHY EASY ACCESS TO DATA VISUALIZATION & SELF-SERVICE ANALYTICS IS CRUCIAL IN HHS

HHS LEADERS KNOW DATA & ANALYTICS ARE IMPORTANT

82%

say analytics are critical to lowering costs and improving health outcomes

77%

say analytics help identify fraud

VISUALIZATION HELPS WITH DECISION-MAKING

83%

say the ability to visualize data in new ways would add value to the organization

BUT DEPARTMENTS LACK THE RIGHT TOOLS TO GAIN INSIGHTS

74%

still use spreadsheets to display data

33%

rely on IT or other departments to create reports, which can be a slow process

47%

say current reporting practices do not meet their needs¹

WE LIVE IN A DATA-DRIVEN WORLD,

and health and human services (HHS) is no different. HHS agencies are more dependent on data now than ever before. Due to the Affordable Care Act (ACA) and Medicaid expansion, the number of people served by HHS is growing every day.

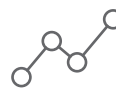
Lack of access to accurate and comprehensive data can leave vulnerable populations unserved, result in duplicative services, waste funding on fraudulent claims and decrease agency efficiency. This drain on state and local government budgets is exacerbating an already unstable financial environment. Agencies need a highly available, easy-to-use solution to glean insights — that's where Tableau comes in.

Tableau offers on-site and cloud-based solutions to help agencies visualize data — leading to faster, well-informed decisions. The ability to visualize data — and prepare and share timely reports — helps improve health care outcomes while eliminating waste and fraud.

Tableau can help agencies:



Put big data to work. By optimizing resources and identifying the most effective health care programs, HHS leaders can make more informed decisions that have a direct impact on individual outcomes.



Increase accountability and transparency. HHS leaders can analyze data to spot trends and outliers, ultimately reducing fraud, waste and abuse, and improving transparency.



Utilize advanced analytics. Everyday HHS decision-makers shouldn't have to be statisticians. Visualization can help all stakeholders understand and gain insights from data.



Have access to tools where and when they need them. Data and visualization tools can be available via desktops, servers, cloud, web or mobile devices.



To learn more, visit: www.tableau.com/hhs

¹In June 2015, the Governing Institute and the Center for Digital Government conducted a nationwide survey of 285 state and local government leaders about the status of health and human services in their jurisdictions, the challenges they face and how they are working to overcome them.

CHANGING TACTICS

Agencies across the U.S. are taking a new approach to serve some of the nation's most vulnerable populations. Instead of relying on historical data and previous experiences to draw insights, they are turning to factors such as geography, income and behavioral responses to identify health disparities and solutions.

What You're Doing:

LOOKING AT SOCIAL DETERMINANTS OF HEALTH

While habits such as diet and exercise certainly play into a person's health, there are also a range of social, economic and environmental factors that can impact a person's well-being. Social determinants of health are the conditions in which individuals are born, grow, live, work and age, such as their physical environment, employment and social networks. Analyzing social determinants of health can help government officials determine when and where to target interventions for the greatest impact.

Used wisely, the combination of data, technology and social factors can also drive a transformation within health and human services from a system based on outputs to one that is flexible, patient-centered and responsive to each individual's needs.

What You Told Us:

54%
OF RESPONDENTS TO THE CDG/GOVERNING INSTITUTE HHS SURVEY SAID THEY HAVE OR PLAN TO INTEGRATE SOCIAL DETERMINANTS OF HEALTH INTO SERVICE DELIVERY.



“We’re not just here to identify how our community is ailing. We need to develop solutions.”

Dr. Betina Jean-Louis,
Harlem Children's Zone
Director of Evaluation

EMCF.ORG

The Harlem Children's Zone (HCZ)

represents an ambitious place-based effort to support children from birth through adulthood. The program serves 13,000 children in and around a 97-block area of central Harlem that suffers from high rates of chronic diseases, infant mortality, poverty and unemployment.

It provides a range of family and social services, including training and education for expectant parents, full-day pre-kindergarten, after-school and weekend programs, nutritional education and access to healthy meals for students.

One major problem HCZ identified within its community was asthma.

Nationally, approximately 8 percent of children suffer from asthma. HCZ officials were stunned to find that about 30 percent of children in the area they cover suffered from the condition — it was the top cause of children missing school and visiting the emergency room. To solve the problem, HCZ partnered with Harlem Hospital and Columbia University to visit homes and identify asthma triggers, educate families and provide access to preventive

medication. “We’re not just here to identify how our community is ailing,” says HCZ Director of Evaluation Dr. Betina Jean-Louis. “We need to develop solutions.”

HCZ tracks metrics across its initiatives. By asking the same questions as the CDC, HCZ leaders were able to match data and determine that their asthma efforts reduced the number of missed school days, emergency room visits and overnight hospital stays.¹⁹

Convergence is IMPROVING HHS Outcomes

Health and human services is at an inflection point. Changing demographics, emerging technology and ever-growing fiscal pressures are combining to transform the nation's priorities:

- Medicaid expansion under the Affordable Care Act (ACA) is bringing in new populations, **leading to a spike in spending**. The rate of increase in total Medicaid spending from 2014 to 2015 was nearly double the previous year's increase (7.8 percent vs. 3.94 percent).
- The population is graying. **Individuals aged 65 and up will comprise about 20 percent of the U.S. population by 2030**, and the 65-and-over population is projected to double to about 72 million over the next 25 years.
- Advances in analytics and other technologies are **leading to more preventive and outcome-based care approaches**.

This convergence of economic, technological and social changes is allowing for more coordinated and data-driven service delivery that can significantly improve citizen services and ensure better outcomes. HHS agencies can take advantage of this unique environment with the following steps.

3 Steps to Convergence

Step 1: Empower leaders to focus on outcomes.

Engage leadership at the top and ensure high-level decision-makers provide support for staff to leverage analytics and data-driven decision-making to improve outcomes.

Step 2: Eliminate silos. Remove barriers to access and break down silos. For statewide initiatives, all impacted state and local agencies should have the opportunity to provide input and collaborate during the planning phase.

Step 3: Overcome legal challenges. Legal hurdles can weaken a transformative effort. For example, one state looking to transform human services delivery had several antiquated and inconsistent laws that made service delivery divisive and inefficient. To resolve this issue, the state created a protocol that stipulated agencies could work together and share financial resources, data and staff with simple, not legalistic, agreements between them.

Your Qualified Convergence Solutions Provider

A leader in helping states on the convergence path, Accenture develops strategies and solutions for coordinated, collaborative and cost-effective service delivery to improve health, social and financial outcomes. Accenture can help your agency:

- Make transaction-based processes adaptive, efficient and productive, reducing costs and improving quality fast
- Grant citizens easy access to insight-driven services customized to who they are and what they need
- Deliver outcomes that matter to people's lives, and positively impact your mission and business outcomes

APPLYING BEHAVIORAL SCIENCE

Behavioral science — the study of activities and interactions among humans, including the analysis of relationships through aspects such as biology, geography, law and political science — is becoming increasingly popular as a solution to challenges in HHS. In 2015, President Obama ignited a newfound interest in the science with an executive order encouraging agencies to use behavioral science insights to streamline welfare programs, help citizens find better jobs, improve health care outcomes and increase educational opportunities.

Says APHSA's Wareing Evans: "People are using things like rapid-cycle evaluation and applying behavioral economics and other sciences to understand questions such as: How do you actually best engage with children and families? What works and what doesn't?"



Oklahoma

Thirty-nine thousand Oklahoma households receive government assistance for child care, however, only about one-third of families renew their benefits on time. Delayed renewal applications result in interrupted payments to families and redundant work for caseworkers, who must re-interview parents and re-verify income information.

With funding from the U.S. Administration for Children and Families (ACF), the Oklahoma Department of Human Services (DHS) partnered with a social policy research organization to resolve this issue through the use of behavioral science. DHS ran an experiment where providers who cared for children participating in the government subsidy program were sent a list of color-coded participants nearing their renewal deadline. Green, orange and red were used to indicate how far families were from missing their renewal deadline. Providers

were instructed to notify their clients about the upcoming deadline and offer assistance in collecting the necessary documents. This intervention resulted in a 3 percent increase of on-time renewals, when compared to a control group that did not receive the intervention. While the bump may seem small, statewide it's equal to 1,000 families per year.²⁰



Indiana

Approximately one-third of families in Indiana receive childcare subsidies. However, despite a statewide ranking system to help families find high-quality care, 35 percent still pick providers who have not received the state's seal of approval. Through an ACF grant, the Indiana Office of Early Childhood and Out-of-School Learning partnered with the same policy research organization Oklahoma used to improve participation in high-quality care through behavioral science.

The 12,600 families on the childcare voucher waiting list were split into two groups — the control

group and the treatment group. Parents in the control group received a standard letter and brochure about choosing a quality care provider, which the state had already been distributing. The treatment group received a special mailing and a follow-up phone call. The special mailing identified that the majority of parents use their voucher to pay for childcare providers who participate in the state's review program, and included a map of the highest-rated providers near the family's residence. The result was a 2.1 percentage point increase in the use of high-quality providers.²¹

HHS AND THE MOVE TO AN INTEGRATED ENTERPRISE

Nearly 40 percent of HHS decision-makers said they need to modernize over half of their agency's IT systems, according to the 2016 CDG/Governing Institute survey. These outdated, siloed systems are a classic example of the traditional agency-centric approach to HHS, which makes it costly and time consuming to obtain an integrated view of constituents.

To enhance the access, outcomes, accountability and quality of HHS programs and services, a new approach is

needed – one that is more person, family and population centric and takes into account social determinants, such as education and economic security, to obtain a more holistic view of a person, family or population.

Just over half of the survey respondents reported their agencies have or plan to integrate social determinants of health into service delivery to obtain this more person-centered approach, but how can they ensure they manage the transition to a more integrated enterprise successfully?

TO ACHIEVE END-TO-END INTEGRATION, HHS AGENCIES CAN USE THE FOLLOWING ROADMAP:

DEFINE THE HHS ENTERPRISE ARCHITECTURE.

This includes determining what outcomes you're trying to achieve (the business architecture) and the information needed to anticipate, support and validate key decisions. It also includes deciding how you will facilitate the secure exchange of that information (information architecture) and the technology investments needed (the technology & solution architectures).

IDENTIFY AND INTEGRATE FUNDING OPPORTUNITIES.

States can take advantage of several federal funding streams and opportunities such as CMS' 90/10 funding for MMIS modernization and the State Medicaid Health Information Technology Plan and the OMB Circular A-87 Cost Allocation Waiver to integrate HHS programs on one rules engine platform.

ESTABLISH STRONG GOVERNANCE.

Executive leadership, such as the HHS commissioner, Medicaid director and/or governor's office, should spearhead the effort. Stakeholders from across the full continuum of HHS program areas need to define and agree on the business imperatives and performance indicators.

LOOK TO AGNOSTIC, MODULAR TECHNOLOGY.

Agnostic solutions leveraging third-party, commercial-off-the-shelf (COTS) components for gateways, master data management, rules engines, service bus information exchange capabilities and analytic capabilities allow you to build a common integrated enterprise platform. These agnostic solutions can be leveraged across multiple programs – build it once and use it many times.

CREATE A CULTURE OF INFORMATION SHARING.

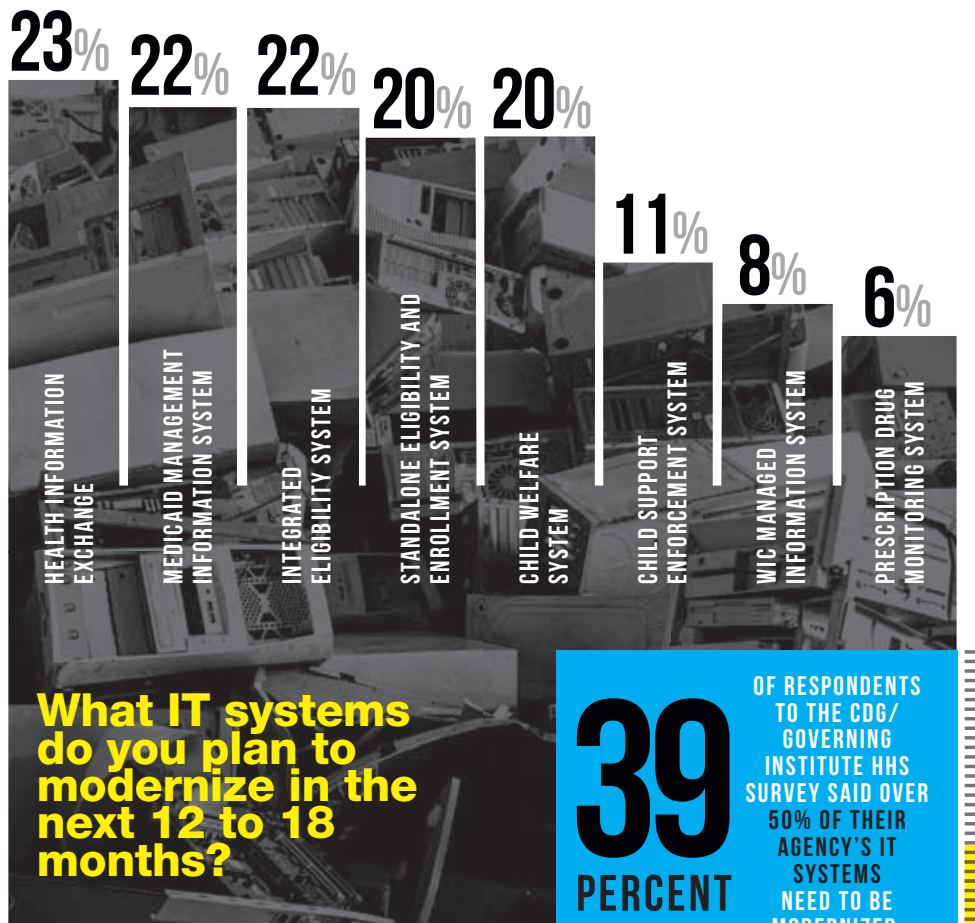
Start with the low-hanging fruit of aggregate and de-identified data to build more robust performance and trend analyses that demonstrate the benefits of data sharing. Think about how you can effectively share data without compromising privacy, and what the program advantages are for sharing that information.

HOW YOU'LL MODERNIZE HHS SYSTEMS

According to the Government Accountability Office (GAO), the federal government spends \$80 billion a year on IT, much of which goes toward maintaining legacy IT systems. Decades-old hardware is a major problem for state and local governments as well. HHS decision-makers in our 2016 HHS survey said outdated IT systems and their corresponding issues were one of their most critical challenges — exacerbated by the fact that 75 percent of them reported that demand for their services has increased.

But there is some good news. The federal government, recognizing this urgent need for system modernization, continues to provide enhanced funding and more flexibility around how federal dollars can be used on systems that support multiple programs. It's also adjusting rules to promote modular deployments and cloud-based approaches.

What You Told Us:





WHY YOU'LL BUILD DIFFERENTLY

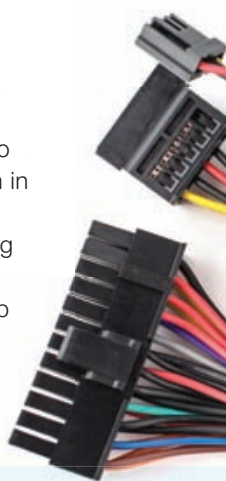
The systems used to support evolving HHS programs will look much different than the technology they replace. Legacy HHS systems typically were custom-developed to serve a single program, and they neither share data nor adapt to new processes easily. The next generation of systems will be faster to deploy, more interconnected and easier to update. Here's why.

MODERNIZATION IS MORE FLEXIBLE

Since 2011, CMS has provided enhanced funding to states for building and maintaining Medicaid eligibility and enrollment systems. The agency will pay 90 percent of states' costs for designing and developing new systems (commonly known as 90/10 funding) as well as 75 percent of the ongoing maintenance and operation expenses. The federal government also relaxed its cost allocation rules contained in OMB Circular A-87 to promote integration between health and human services systems. Previously, the OMB required specific cost allocations for state programs that shared IT systems, which aligned with the proportion of their use of these

systems. The current A-87 waiver lets states bypass the normal cost allocation methodologies. Instead, they can charge the initial build to Medicaid — paid for with 90/10 funding — and pay for the additional cost under the A-87 exception that's required to make the system reusable for other programs.

Together, these changes give states an opportunity to not only modernize aging HHS systems, but build them in a more integrated way. The opportunity may not last forever, though. While CMS has extended 90/10 funding indefinitely, the A-87 cost allocation exception only will be in place until 2018, meaning states that want to reap significant cost savings from implementing shared IT systems have less than two years to do so.



What You're Doing:

Integrating HHS Programs and Systems

Washington State used a portion of its \$65 million grant from the CMS State Innovation Model Initiative — which has awarded nearly \$300 million to 25 states to design or test innovative models of service delivery and health care payment — to integrate physical and behavioral health services for its Medicaid population. This particular change effort is significant, impacting how services are administered, financed and delivered for Medicaid beneficiaries, according to Dorothy Frost Teeter, director of Washington's Health Care Authority. It also requires

deep engagement with members of the community who haven't always been at the table for health transformation efforts. Washington's approach relies on multi-sector collaborative organizations called Accountable Communities of Health for this new form of engagement.²²

Ohio also is testing value-based payment models that rely on provider-specific performance reports to expand access to comprehensive primary care and reduce the incentive to overuse unnecessary services within high-cost episodes of care. Ohio has also taken advantage of enhanced federal funding to build an enterprise eligibility system for most

income-tested programs, including Medicaid, SNAP and TANF.

"One of the things we tried to do differently was focus on infrastructure changes that result in broad impacts across multiple programs," says Greg Moody, director of Ohio's Office of Health Transformation. "Broad reforms — like expanding Medicaid coverage and creating online tools to make it easier for citizens to access benefits — increase the state's capacity to deal with specific challenges, like reducing diabetes or infant mortality. Almost all of the reforms we've done are like that. They're systemic and structural."²³

BIG BANG IS OUT; MODULAR IS IN

Large, complex IT projects have a history of missed deadlines, blown budgets and poor results. Therefore, the federal government is encouraging state HHS agencies to take a modular approach where large systems are divided into smaller pieces that can be deployed one at a time.

In the Medicaid space, CMS finalized rules in late 2015 that support the modular deployment of Medicaid Management Information Systems (MMISs). These systems, which pay claims and collect data for Medicaid services, are among the largest IT investments for states with price tags ranging from \$50 to \$150 million.²⁴

Critically, the new CMS rules include changes to the MMIS certification process to accommodate the modular deployment model. State MMIS deployments must be certified by CMS before they can begin receiving enhanced federal matching funds for operation and maintenance. MMIS projects typically have been certified once the entire system is complete, but the new rules allow certification of each module as it's finished, giving states faster access to enhanced funding levels.

"What modular certification means is that states can accumulate quick wins," says Jessica Kahn, director of the Medicaid data and systems group at CMS. "They can get the enhanced match for the operation of those pieces as they stand them up, as opposed to a five-year build where you have to wait until everything is done."²⁵

Child welfare systems are undergoing a somewhat similar shift. In 2015, ACF issued a Comprehensive Child Welfare Information System (CCWIS) Notice of Proposed Rulemaking (NPRM), which provides funding for states to update or implement new case management systems that are more modular and interoperable.

What You're Doing:

Taking a New Approach to Child Welfare Systems

California's Department of Social Services (DSS), which runs one of the largest child welfare agencies in the country, has launched a project to establish what it calls "an innovative statewide 21st-century information technology application" that improves its child welfare operations. It intends to take a modular approach to procurement and work with multiple vendors. One of the state's overarching goals is to create an underlying technology platform that DSS and its other HHS departments can reuse, while continuously improving services for its end users.²⁶

Other states, such as Pennsylvania, already have moved in this direction. While updating its existing legacy systems, Pennsylvania's Department of Human Services took the opportunity to layer on additional technology — a business rules engine — to improve data collection and automation. It shifted from a process where mainframe changes were hard-coded and took months to perform to one that was more agile and could process more than 2.6 million records in just 43 minutes. This led to improved compliance and transparency, a reduction in manual processing and better citizen services — including faster eligibility determination and more self-screening processes.²⁷

Building Enterprise Platforms to Support Modularity

The impact of enhanced federal funding and greater flexibility can be seen in Hawaii where the state's Department of Human Services (DHS) deployed an enterprise platform several years ago to support multiple functions. Pankaj Bhanot, deputy director of the department, sums up the approach as "buy once, use many times."

Hawaii funded the \$144 million project using the 90/10 federal match. Now the state intends to plug a growing number of modular systems into the platform to support SNAP, TANF and other programs. In addition, the department built a Medicaid application on the platform, laying the groundwork for more integrated services.

Bhanot says many of these programs have operated in silos from a technology standpoint. However, the enterprise system will allow them to function with more interoperability because the components are agnostic. "They are reusable, interoperable, extensible, scalable and easily supportable," Bhanot says.

DHS, which is focused on serving families and children concurrently, also plans to integrate data and analytics into the platform to improve service delivery and outcomes. "We want to be the agency of one, where we will be able to take care of the needs of our clients through the same system and the same processes that we will use across the board," he says.²⁸

PENNSYLVANIA'S
DEPARTMENT OF
HUMAN SERVICES
SHIFTED FROM A
PROCESS WHERE
MAINFRAME CHANGES
WERE HARD-CODED
AND TOOK MONTHS
TO PERFORM TO ONE
THAT WAS MORE
AGILE AND COULD
PROCESS MORE THAN
2.6 MILLION RECORDS
IN JUST

43
MINUTES.



“What modular certification means is that states can accumulate quick wins.”

Jessica Kahn,
CMS Medicaid
Data and Systems
Group Director

WITH CMS
SIGNALING THAT
**CLOUD-BASED
SERVICES**
CAN BE USED TO MEET
MMIS REQUIREMENTS,
A NUMBER OF STATES
ARE INVESTIGATING
THE APPROACH.

SHUTTERSTOCK.COM

from commercial insurers. “We think there are a lot of transferable technologies,” she says. “There are things we see in other industries that are moving at light speed. We would love to benefit from that.”

In another move to attract new providers for MMIS, CMS is developing a process for pre-certifying MMIS modules. The approach potentially gives states access to a suite of plug-and-play modules that are pre-tested to meet CMS requirements. That stamp of approval could be important for vendors new to the Medicaid market.

“[States] would feel more comfortable knowing that a particular set of software they might choose has already gone through a level of scrutiny to make sure it works,” Kahn says. “On the vendor side, it’s hard to get your foot in the door when people have never heard of you. Pre-certification, in a way, will give you some free marketing.”

INNOVATION IS IN DEMAND

The federal government is trying to spark innovation within Medicaid IT. Included in the new CMS rules around MMIS modularity, for instance, is clarification that the agency encourages the use of off-the-shelf software and cloud-based services. This is a sea change for a sector that’s been dominated by custom-developed software and

systems. Besides potentially lowering the cost of MMIS replacement, this shift is being driven by a desire to pull innovative ideas from other sectors into the MMIS space.

For instance, Kahn says there’s potential to adopt best practices for information security from commercial health care providers or the banking industry, as well as claims processing innovations

What You’re Doing:

Moving MMIS to the Cloud

With CMS signaling that cloud-based services can be used to meet MMIS requirements, a number of states are investigating the approach. Wyoming may be the first to make the shift.

The state is launching procurements for services-based MMIS modules that include core benefits management; business intelligence; and fraud, waste and abuse detection. A systems integrator was hired to combine multiple services modules, share technical expertise and oversee contractor performance, and the state is using multiple vendors to avoid over-reliance on one company. Leaders there are deploying a state-owned data warehouse and leveraging what’s already in the market rather than building something similar from the ground up, which can be costly and time consuming.

Wyoming also is working closely with CMS to ensure its technology investments meet the agency’s standards. The state’s Medicaid population is small — only 90,000 enrollees and 3 million claims processed annually — but its approach could serve as a model for other states.²⁹

5 WAYS HHS AGENCIES CAN MODERNIZE FOR GREATEST ROI



In a recent Governing Institute survey of 320 health and human services (HHS) decision-makers, nearly

1/3

of respondents said **OUTDATED IT SYSTEMS IS ONE OF THE MOST CRITICAL CHALLENGES** their agencies will face over the next year.

According to Software AG, there are **five ways HHS agencies can modernize** for relatively quick return on investment:

TAP REUSABLE SERVICES.

Existing mainframe and other legacy systems contain valuable information and data that can be harnessed. Smart approaches to digital business transformation can help organizations convert existing business, presentation and data logic as reusable services.

BUILD AND MANAGE SELF-SERVICE APPS.

72% of respondents in the Governing Institute survey said **DEMAND FOR HHS SERVICES HAS INCREASED IN THE LAST 12 MONTHS.**

Providing self-service options for citizens can help meet this demand. HHS agencies can also benefit by letting third parties securely access government data via application programming interfaces (APIs). Private citizens or developers might then use the data to create beneficial mobile apps.

SHARE INFORMATION.

63% of HHS decision-makers in the Governing Institute survey said **INCREASED DATA SHARING AMONG AGENCIES WOULD IMPROVE SERVICE DELIVERY.**

HHS agencies can also share data to gain a more holistic view of a citizen's health and detect fraud. For example, Pennsylvania's Department of Labor & Industry – which also oversees unemployment payments – leveraged the state's database of incarcerated residents to find out which prisoners were collecting unemployment, which helped uncover millions of dollars in related fraud.

TAKE ADVANTAGE OF STREAMING ANALYTICS.

Monitoring data in real time, rather than looking for trends after the fact, allows HHS agencies to take a more preventative approach to citizens' care. For example, leveraging streaming analytics helps agencies determine health trends within their communities so they can provide more targeted services and education.

ADD STORAGE.

Modernizing systems can help agencies take advantage of big data and analytics. By also adding "big memory," they can ensure the new functionality doesn't slow backend system performance and delay citizen services.

software AG

For more information, visit <http://government.softwareag.com/>

THE ELECTION'S IMPACT

With a new president entering the White House in January, there's no certainty that the current funding landscape will remain the same. Still, experts and industry observers say the U.S. Department of Human Services' move to focus on technology as an innovation driver is the best strategy it has had in the last 20 to 30 years.

APHSA's Wareing Evans expects current trends around program integration, the use of data analytics for validating program performance and greater focus on social determinants of health to remain in place regardless of who is president next year.

"This notion that we really need to understand what works and hold ourselves accountable for ensuring that government dollars are going to programs that are effective — I don't see that as particular to one administration or one party," she says. "We have a lot more information knowledge and capacity to do that kind of thing now, and I don't think that's going away."

But states also must be prepared for changes in policy details and emphasis as a new administration implements its HHS philosophy. Perhaps the best advice comes from Washington State's Dorothy Teeter who says states need to deeply understand their own requirements and take a long-term view.

"What's most important for states, first and foremost, is to identify a five-year technology and infrastructure data and analytics plan," she says. "What are their business intelligence needs? What does this imply for the infrastructure that they need and where they stand now? Asking these questions gives them both a very clear business case and a technical solution that matches up going forward."

Teeter adds: "The work of building out this infrastructure is legacy work. Whatever we build has to last well beyond those five years, but you have to build it in a way that you can continue to enhance it and not have to throw it all away and start over again."

THE CHALLENGES YOU'LL FACE



✓ **Modularity is still emerging**

Because the concept is new, there's no standard way to break MMIS into modules. Different states are taking different approaches. Arkansas, for example, broke its system development into three parts, using three different vendors. At the same time, CMS is still working out the details of modular certification. The agency is putting the finishing touches on formal guidance for how the certification process will operate. However, CMS already has released a good deal of information on how states should plan for and implement modular MMISs, including an enterprise certification toolkit published in April 2016.

✓ **Planning and procurement are even more important**

States will need to fully define their Medicaid ecosystem before they begin procuring MMIS modules. That will require rigorous internal review to clearly understand their business needs and the technology solutions that can address them. Agencies should consider a draft RFP that includes an extensive inventory of their available data and resources — and require input from key stakeholders — before they solicit vendors. Bottom line: Although deployment can be done module-by-module, planning cannot. Developing a clear idea of what your Medicaid enterprise will look like — both now and in the future — will be a critical first step.

✓ **Interoperability is critical**

As states implement modular MMISs, all of the pieces will need to fit together seamlessly. Service-

oriented architecture (SOA) will be the glue that holds modular MMISs together. SOA is the foundation for the Medicaid Information Technology Architecture, which CMS developed to serve as a pathway for implementing interoperability and service orientation across the Medicaid enterprise. SOA skills will be at a premium as modularity moves forward.

✓ **Agency culture must adapt**

Modularity and broader integration of programs across the HHS enterprise are big changes for agencies accustomed to traditional development techniques and siloed program models. Government leaders shouldn't underestimate the amount of change management needed to evolve HHS organizations toward these new models. Agency workforces will need to share more data, change their business processes and create new ones for shared services.

✓ **Stronger governance will be needed**

Rigorous IT governance processes will need to be in place, especially as more pieces are introduced into the system. This process should define responsibilities for tasks and data, policies for making changes to systems and compliance standards across the enterprise. Putting these measures into place will help ensure state agencies don't create more challenges for themselves as they move toward modularity.

SOCIAL SERVICES, STREAMLINED

INTEGRATED ELIGIBILITY
PROVIDES CITIZENS THE
CUSTOMER EXPERIENCE
THEY DESERVE.

HHS AGENCIES

are continually pressed to modernize their systems in a way that promotes efficiency, cost effectiveness and customer service.

Optum™ Integrated Eligibility solution helps agencies meet the challenge by automating the administration of social programs, which adds client convenience and frees caseworkers to handle other important duties. Optum's integrated eligibility services can allow HHS agencies to:

Streamline operations — A modular integrated platform allows HHS agencies to determine client eligibility for Medicaid, SNAP, TANF, CHIP and other benefits programs based on a single client application. Client updates and changes can be applied across all programs automatically, saving time and reducing human error.

Centralize case management — Caseworkers across all services can see a consistent, holistic view of each client to instantly understand which programs each participant qualifies for or is enrolled in.

Know the “truth” — Master data management allows agencies to reconcile complex client identities – many of them with similar names – across multiple systems and databases. It can serve as a single point of truth spanning all HHS programs.

Gain deeper insight — Cross-program analytics assist administrators in identifying potential fraud, waste and abuse; forecasting caseloads versus actual participation; and understanding eligibility compared with enrollment. Analytics help agencies make smarter decisions to improve services and drive customer satisfaction.

A LEADER IN LARGE SYSTEMS INTEGRATION FOR HHS

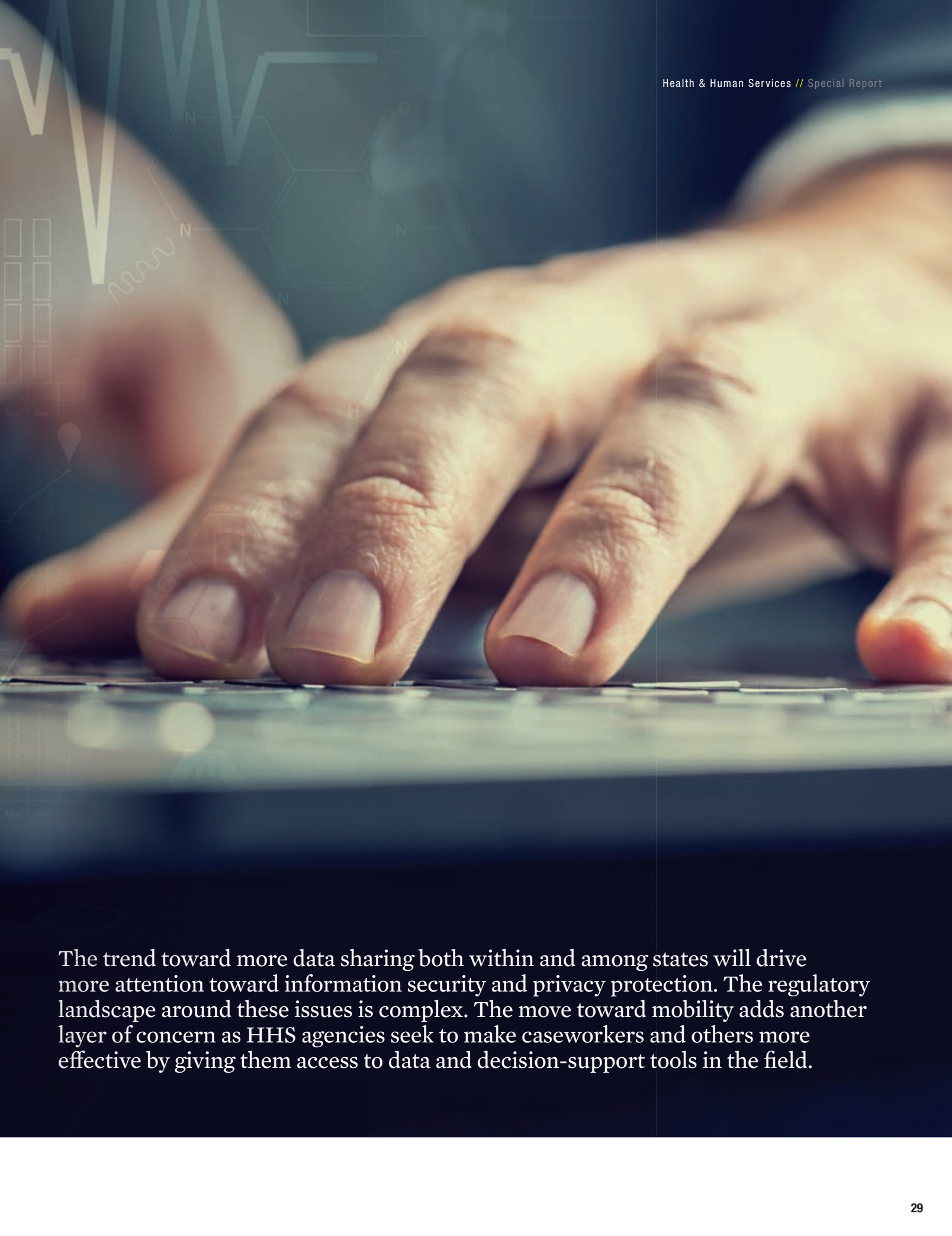
Optum is a health services and innovation company focused on making the health system work better for everyone. In addition to providing world-class analytics and systems integration, Optum offers program and policy consulting, and technology development, implementation, maintenance, operation and security — as well as hosting on the Optum cloud. It serves a majority of the nation's Medicaid agencies, and integrates data sources across many public HHS programs.

To learn more about Optum's integrated eligibility services, visit www.optum.com/solutions/government, or contact Optum at innovate@optum.com or 1-800-765-6092.



OPTUM®

HOW YOU'LL SHARE DATA SAFELY



The trend toward more data sharing both within and among states will drive more attention toward information security and privacy protection. The regulatory landscape around these issues is complex. The move toward mobility adds another layer of concern as HHS agencies seek to make caseworkers and others more effective by giving them access to data and decision-support tools in the field.



SIMPLIFYING THE REGULATORY MAZE

HHS agencies must balance the need for greater data sharing with their fundamental responsibility to protect sensitive citizen information. The regulatory environment often doesn't make this easy. State officials say a patchwork of federal laws meant to protect confidential data can hinder sharing. "Federal law has all these requirements that are siloed because they run their own programs their own way," says Hawaii's Bhanot. "Food and Nutrition Service (FNS), the ACF for TANF and Child Welfare Services, and Medicaid all have their own rules."

HIPAA adds another layer of complexity. The law is often misinterpreted to be more restrictive than it is, which prevents states from sharing data with each other — or even

within their own agencies. And HIPAA is impacting more agencies as HHS programs become more integrated and health data flows into social services programs that typically haven't dealt with HIPAA-protected information.

In addition, some states have their own privacy laws that may be broader or more narrow than HIPAA. For

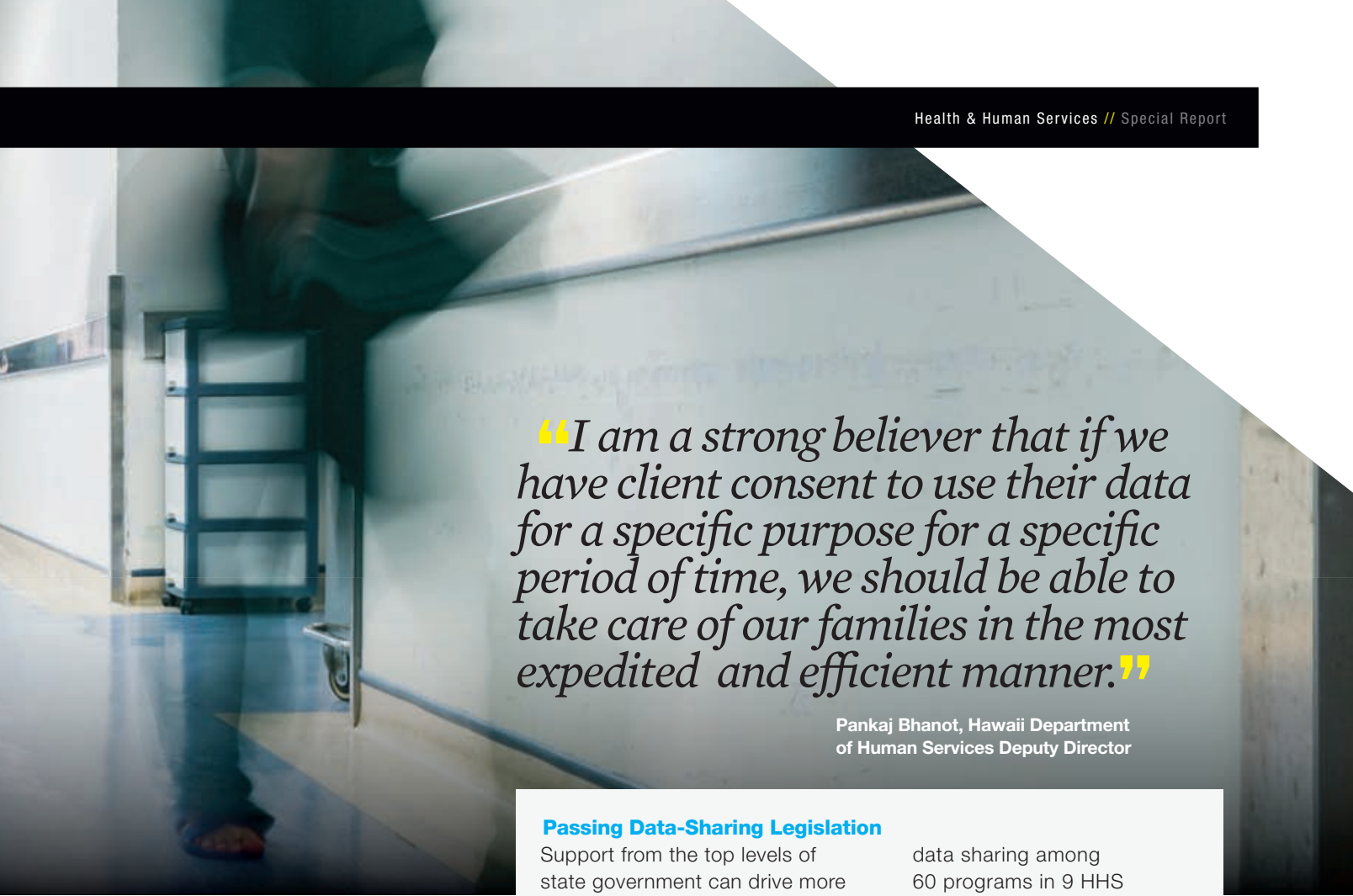
instance, the Texas Medical Records Privacy Act is broader than HIPAA and requires covered entities — health care providers, insurers, claims processors and others — to obtain patient consent for most types of information sharing.

However, states are finding ways to clarify privacy and data protection rules to facilitate safe information sharing.

What You're Doing:

Reconciling State Laws with HIPAA

Ohio has made state law consistent with the HIPAA privacy rule. Ohio's Moody says the state had multiple, separate privacy laws. "It created a non-standard environment where people could then say, 'We can't share because of the privacy considerations,'" he explains. In response, Ohio clarified its health-related privacy laws and adopted HIPAA as the state standard. "That single action eliminated many of those barriers to data sharing," Moody says.



“I am a strong believer that if we have client consent to use their data for a specific purpose for a specific period of time, we should be able to take care of our families in the most expedited and efficient manner.”

Pankaj Bhanot, Hawaii Department
of Human Services Deputy Director

Getting Smarter About Consent

Getting information to the right people at the right time is fundamental to improving care. Experts say consent is the key to giving HHS programs the information they need to take a holistic view of individuals and families. “I am a strong believer that if we have client consent to use their data for a specific purpose for a specific period of time, we should be able to take care of our families in the most expedited and efficient manner,” Hawaii’s Bhanot says.

States should consider including a consent registry in any enterprise or integrated eligibility platform they build. But consent should be for a clearly defined period and purpose. For example, agencies could ask for a 12-month period of consent to share protected health information to support population health or pay-for-performance efforts.

Passing Data-Sharing Legislation

Support from the top levels of state government can drive more data sharing, too. In Washington State, the legislature passed a law that required all health plans in the state to contribute claims data with pricing information to a claims database. The move will enable more price transparency for consumers, help them make more informed health care decisions and could improve the state’s value-based payment efforts, Washington’s Teeter says.

Illinois recently launched a wide-ranging project that involved

data sharing among 60 programs in 9 HHS agencies. However, existing state regulations required identity information be stripped from the data, making the process more cumbersome and the data less useful. In response, Illinois passed a new state law that established a framework for the development of open data platforms and an architecture for regulatory compliance.³⁰

SHUTTERSTOCK.COM

Taking Advantage of Co-Location

Ohio is considering, as an extension of value-based payment reforms, providing additional financial support for primary care practices that work with schools to give children better access to care and improve academic performance. Co-locating primary care and schools has the potential to make life easier for parents and also presents data-sharing opportunities. For example, having parents sign a consent form at the beginning of the school year could allow the clinical care site and the school to share information that may lead to more effective intervention.

Florida has given its more than

2,300

foster care caseworkers smartphones and laptops with built-in cameras to capture images with time and location information that they can upload to the state's online database.

MOBILIZING SECURELY

Mobile technology is a key tool for making field staff more effective. It's also becoming the favored communication channel for clients of HHS programs. But security and privacy will be more complex as mobility is widely deployed.

What You're Doing:

Equipping Caseworkers with Mobile Devices

In health and human services, we're already seeing how agencies are leveraging this technology. New York's Office of Children and Family Services allows caseworkers and staff to use laptops and other mobile technology to access information and assist clients when conducting their field work.³¹ Florida has given its more than 2,300 foster care caseworkers smartphones and laptops with built-in cameras to capture images with time and location information they can upload to the state's online database, along with the caseworker's notes from site visits and interviews. The new approach has led to a 30 percent increase in home visits, better reporting on child welfare cases and more compliance in Miami-Dade County.³²

MORE THAN

165
K

MOBILE HEALTH APPS ARE AVAILABLE FOR DOWNLOAD IN THE ITUNES AND ANDROID STORES. ONE STUDY ESTIMATED THAT 500 MILLION PEOPLE WILL HAVE USED THESE APPS BY 2015.

THERE ARE SEVERAL RESOURCES

available for help agencies implement secure mobility. For instance, the Healthcare Information and Management Systems Society offers a mobile security toolkit at HIMSS.org. And the HHS provides extensive information on mobile privacy and security at HealthIT.gov. Both HealthIT.gov and the HIMSS Mobile Security Toolkit provide a helpful checklist that agencies should keep in mind when they deploy mobile technology. Key steps include:

- * DETERMINE HOW YOUR ORGANIZATION WILL USE MOBILE DEVICES, WHETHER IT BE TO ACCESS, RECEIVE, TRANSMIT OR STORE HEALTH INFORMATION.
- * ASSESS THE THREAT AND VULNERABILITIES THAT MOBILE DEVICES PRESENT TO YOUR ORGANIZATION AND ITS DATA.
- * REQUIRE PASSWORDS, PASSCODES, PIN NUMBERS OR OTHER FORMS OF AUTHENTICATION.
- * MAKE SURE MOBILE DEVICES LOCK AFTER A SPECIFIED PERIOD OF INACTIVITY.
- * ENSURE MOBILE DEVICES EITHER HAVE BUILT-IN ENCRYPTION OR THAT ENCRYPTION CAPABILITIES CAN BE INSTALLED ON THE DEVICE.
- * DISABLE OR DON'T INSTALL FILE-SHARING APPLICATIONS.
- * INSTALL SECURITY SOFTWARE AND FIREWALLS ON ALL DEVICES AND TASK YOUR IT DEPARTMENT WITH ENSURING THIS SOFTWARE IS REGULARLY UPDATED.
- * TRAIN EMPLOYEES, VIA REQUIRED SELF-DIRECTED LEARNING MODULES OR IN-PERSON SESSIONS, ON HOW TO PROTECT PRIVACY AND DATA SECURITY.
- * DEVELOP A LEGAL USER AGREEMENT FOR EMPLOYEES WHO INTEND TO USE THEIR PERSONAL DEVICES FOR WORK-RELATED TASKS.

A SMARTER WAY TO SERVE

Mediware SaaS solutions allow HHS agencies to cost effectively monitor and provide high-quality, person-centered care.

Individuals with physical and developmental disabilities

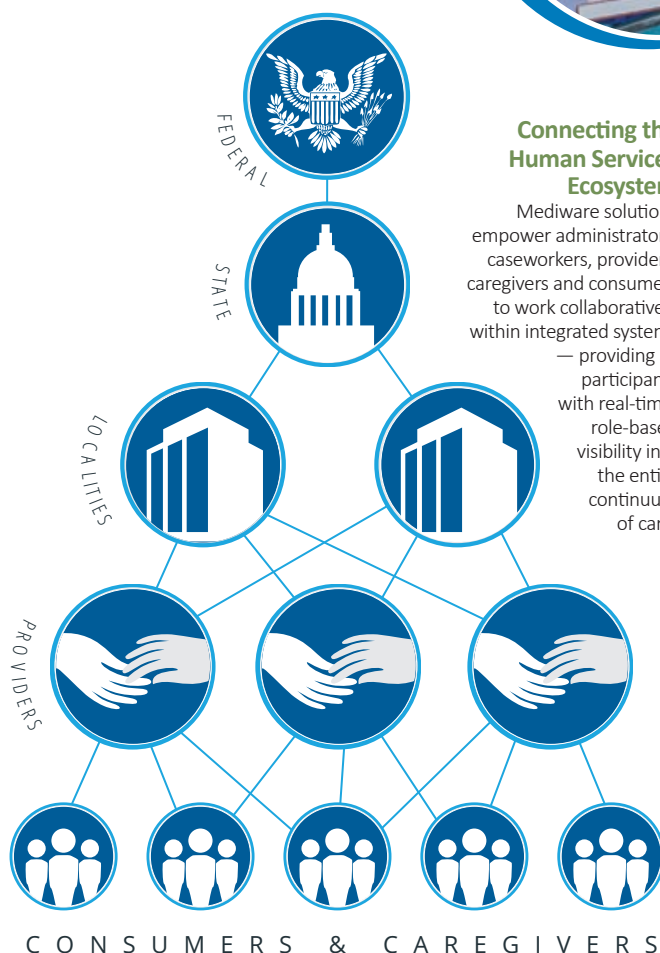
, substance abuse issues, and/or mental illnesses will all require an increasing number of public health and human services as they age. Services to people with these special needs and older Americans are often delivered at home or within community settings. To meet this increasing demand for services, agencies must continue to stretch budgets further through IT modernization projects that drive business efficiencies and mobile solutions that support field-based caseworkers.

Mediware, an industry leader for more than 20 years, helps HHS agencies and managed care organizations work smarter with proven cloud-based software-as-a-service (SaaS) solutions that benefit caseworkers and administrators:

- **Connect payers, providers, caregivers and consumers** within a fully integrated system, and provide a global client record that follows each user through the continuum of care
- **Conduct remote client assessments** to reduce duplicate entry and human error, while freeing caseworkers to work with more consumers
- **Manage person-centered services** to adults, seniors, clients with disabilities and others at home and within community settings to maximize resources and improve outcomes
 - **Analyze consumer and program data** to provide insights into overall program effectiveness via powerful dashboards, and guide future service improvements and program development

Today, more than 1,000 HHS organizations across 40 states rely on Mediware solutions to better coordinate and manage delivery across the spectrum of care.

Mediware modules support programs in aging, intellectual and developmental disabilities, behavioral



Connecting the Human Services Ecosystem

Mediware solutions empower administrators, caseworkers, providers, caregivers and consumers to work collaboratively within integrated systems — providing all participants with real-time, role-based visibility into the entire continuum of care.

health, adult protective services, homelessness and more. Mediware's SaaS options provide access anywhere, anytime via the web or mobile devices, reducing IT infrastructure costs and implementation times — and its highly configurable options let agencies apply changes across many systems as their requirements evolve.

A TRANSFORMATION IN PROGRESS

HHS POLICIES AND SYSTEMS MAY BE IN A STATE OF TRANSITION, but we can see which way they are headed. Individual programs — and the technology behind them — are becoming more integrated as policymakers seek to treat individuals and families more holistically.

At the same time, the field is becoming more science- and evidence-based. Advances in neuroscience are reshaping how programs interact with clients, and better data analytics tools are giving policymakers quick feedback on the effectiveness of their efforts. In some cases, HHS programs are taking a cue from national retailers, adopting techniques developed to entice shoppers and using them to nudge citizens toward healthier choices.

“We’re talking with leaders around the country who are seriously exploring how behavioral economics can play a part in our work,” says APHSA’s Wareing Evans.

As the policy landscape evolves, technology has never been better positioned to support it. Platform-based and modular systems are

giving agencies a new option for modernization — one that reduces the risk of cost overruns and deployment delays while enhancing the flow of data among related programs.

But the technology transformation won’t stop there. Influential federal agencies like CMS are supporting greater use of standard off-the-shelf software and cloud-based services instead of traditional custom-developed systems. The goal is to help agencies reduce their focus on technology development and have the flexibility to iterate with their technology as the policies and business needs evolve.

“Looking at quality and access; that’s where we want states to be,” says CMS’ Kahn.

The push toward standardized solutions also includes efforts to deepen the pool of vendors selling to the HHS market, particularly by attracting innovative new firms into the sector. In the Medicaid space, CMS is establishing a certification process that will let vendors offer pre-tested solutions to meet the agency’s functionality requirements. It’s also trying to make the market less intimidating to newcomers.

“[New companies] have to be willing to work with government and that doesn’t always send warm

and fuzzy feelings to everyone,” says Kahn. “We need to listen to them. What are the challenges? What would make it a more hospitable business model? We need to work with the states to balance the risk.”

None of this, of course, will be easy. It will demand massive changes in how HHS agencies work internally, how they interact with other departments and programs, and how they plan and deploy critical technology systems.

“Part of the reality right now is that folks are discovering how much it takes to move the culture in these big institutional areas,” says Wareing Evans. “Even with all that’s going on with technology, how do you make it happen from a service delivery perspective? We’ve operated in these silos for so long — you cannot underestimate the scope of cultural shift required to shift long-standing approaches.”

Yet you can see the future taking shape. New York State is using outcome-based payments to incentivize hospitals and safety net providers to collaborate and provide more integrated and holistic care. Colorado is giving primary care providers, regional collaboratives and Medicaid officials online access to sophisticated data to help them identify areas of high need and improve care management. Hawaii is building a modular technology platform that will seamlessly connect multiple HHS programs and allow them to interact in new ways. And Wisconsin is pioneering the use of innovative cloud-based services to run its Medicaid program.

These are just some of the ways agencies are shifting toward a new HHS model — one that’s more integrated, data driven, modern and effective. The transformation isn’t complete, but it’s getting closer every day.

Helping HHS Agencies **Make a Bigger Impact** with Vulnerable Populations

Modernizing decades-old IT systems can pose serious risks for public agencies, but also provides them with opportunities to improve their operations and service to their constituents. Health and human services (HHS) agencies increasingly realize they must make the transition to succeed in today's environment.

Microsoft can help lower the risk with flexible, easily configured software-as-a-service solutions that have key compliance, regulatory and security requirements built in. These solutions can shrink development time and capital costs, delivering quick victories to HHS agencies.

At the same time, Microsoft health analytics solutions combine diverse data types in ways never before possible, creating actionable intelligence. Together, these solutions can help HHS agencies enhance services for the most vulnerable populations and improve service delivery and outcomes.

Following are two program areas where Microsoft solutions make an impact:



CHILD WELFARE – A child-centric view helps agencies coordinate an integrated response. Caseworkers can automatically create and route abuse and neglect cases to supervisors, and send alerts in high-risk cases. Online maps and other resources enable supervisors to assign investigators based on experience, skills and proximity. Mobile functions may allow employees to access case materials from a laptop and easily dictate notes via a cell phone. These efficiencies can enable them to spend more time with individual at-risk children and families.



WOMEN, INFANTS AND CHILDREN (WIC) – Robust reporting and data-centric insights help officials better measure health outcomes as well as prevent fraud, waste and abuse. Caseworkers can gain mobility and scheduling efficiencies, which allows them to focus more on one-to-one services and nutrition education for clients.



Microsoft

To find out how Microsoft solutions can help HHS local, state and federal agencies reduce IT risk and improve outcomes, visit www.microsoft.com/government.





THE GOVERNING INSTITUTE advances better government by focusing on improved outcomes through research, decision support and executive education to help public-sector leaders govern more effectively. With an emphasis on state and local government performance, innovation, leadership and citizen engagement, the Institute oversees Governing's research efforts, the *Governing* Public Official of the Year Program, and a wide range of events to further advance the goals of good governance.
www.governing.com/gov-institute

Both are divisions of e.Republic.



THE CENTER FOR DIGITAL GOVERNMENT is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.
www.centerdigitalgov.com

FOR A LIST OF ENDNOTES

download the special report at
www.governing.com/papers



IBM **Watson Health™**

Transforming how health and human service organizations can fund, regulate, deliver and measure programs

IBM Watson Health is pioneering the use of cognitive technologies that understand, reason and learn; technologies that can help Health and Human Services organizations unlock the potential of data and analytics to improve service delivery.

Check us out online at:

<http://ibm.co/socialprograms>

to learn how Watson Health solutions are working to help Health and Human Services organizations enhance, scale and accelerate human expertise to transform their programs.



Sponsors





Transformation Without the Trauma

Complex modernization programs require leadership across many stakeholders, experience in navigating requirements and expert integration of data across multi-vendor ecosystems.

CGI's **ModernSI** approach provides for not only effective program management and governance of health and human services IT projects, but the critical work of data integration in an era of modular and agile deployments.

With deep expertise in both HHS programs and technology, agencies trust CGI to deliver modern, best-fit integrated systems — and so much more.

cgi.com/hhs

CGI

Experience the commitment®

