government technology™ gt

Solutions for state and local government.

OCTOBER/NOVEMBER 2017

INSIDE:

Outsized Risk
Smaller governments face growing threats.

Secure Voting Revisited
Can blockchain finally enable online voting?

Cyber in the Lab
University researchers forecast what's next.

GROUND-BREAKING

NEW PARTNERS TEAM UP AS GEORGIA STAKES ITS CLAIM ON CYBERLEADERSHIP.

LEFT TO RIGHT: GEORGIA CHIEF INFORMATION OFFICER **CALVIN RHODES**, GBI DIRECTOR **VERNON KEENAN** AND AUGUSTA UNIVERSITY'S **MICHAEL SHAFFER** AT THE SITE OF THE GEORGIA CYBER INNOVATION AND TRAINING CENTER.

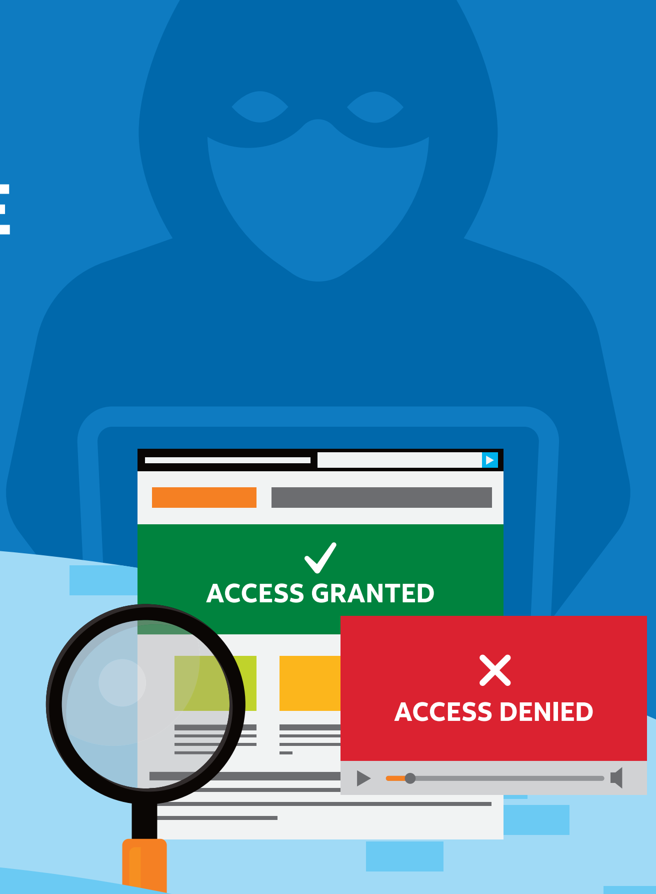
VOL 30 ISSUE 7 / A PUBLICATION OF e.REPUBLIC / **GOVTECH.COM**

PROTECTING THE PUBLIC SECTOR FROM RANSOMWARE

State and local government agencies are being held hostage by malicious adversaries and software designed to steal data.

How prepared is your organization to deal with a ransomware attack?

Take 3 minutes to learn more:
att.com/govsecurity



AT&T FIREWALLS

Fully managed security services to help prevent unauthorized access to your network

AT&T THREAT MANAGER

At-a-glance, situational threat awareness for multiple sites and "state of the org" view

AT&T CYBERSECURITY CONSULTING

Lifecycle approach to vulnerability, threat management and path to compliance

AT&T SECURE EMAIL GATEWAY

Best in class e-mail filtering and threat detection

All AT&T Cybersecurity solutions are powered by AT&T Threat Intellect.

AT&T

October/November 2017

CONTENTS

Vol 30 | Issue 7

COVER STORY

MICHAEL SCHWARZ

Government Technology (ISSN# 1043-9668) is published monthly except February, May, August, and November by e.Republic Inc, 100 Blue Ravine Rd, Folsom, CA 95630. Periodical Postage Paid at Folsom, CA and additional offices. POSTMASTER: Send address changes to: Government Technology, 100 Blue Ravine Rd, Folsom, CA 95630. Copyright 2017 by e.Republic Inc. All rights reserved. SUBSCRIPTIONS: Subscription inquiries should be directed to Government Technology, Attn: Circulation Director, 100 Blue Ravine Rd, Folsom, CA 95630, 916-932-1300.

SHUTTERSTOCK.COM

DEPARTMENTS

COLUMNS

NEWS

FOLLOW US ON

IN OUR NEXT ISSUE:

Looking Back at 2017
We revisit the biggest gov tech stories of the year.

Profiles in Smart
A look at some of the country's most connected communities.

Keeping Tabs
Who went where in the state and local IT universe this year.

WWW.GOVTECH.COM

government technology

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

EDITORIAL
GT Editor: **Noelle Knell,** nknell@govtech.com
Managing Editor: **Lauren Harrison,** lharrison@govtech.com
Web Editor & Photographer: **Jessica Mulholland,** jmulholland@govtech.com
Chief Copy Editor: **Miriam Jones,** mjones@govtech.com
Copy Editor: **Kate Albrecht,** kalbrecht@govtech.com
Senior Editor: **Tod Newcombe,** tnewcombe@govtech.com
Assistant News Editor: **Eyragon Eidam,** eeidam@govtech.com
Staff Writers: **Skip Descant,** sdescant@govtech.com
Theo Douglas, tdouglas@govtech.com
Ben Miller, bmiller@govtech.com
Zack Quaintance, zquaintance@govtech.com
Contributing Writers: **Julia McCandless, Ryan McCauley, Adam Stone**
Editorial Assistant: **Erik Hopkins,** ehopkins@govtech.com

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

PUBLISHING
SENIOR VP OF STRATEGIC ACCOUNTS:
Stacy Ward-Probst, sward@govtech.com
VPs OF STRATEGIC ACCOUNTS:
Kim Frame, kframe@govtech.com
Arlene Boeger, aboeger@govtech.com
Shelley Ballard, sballard@govtech.com
SALES DIRECTORS:
Melissa Sellers, msellers@govtech.com
Tracy Meisler, tmeisler@govtech.com
Karen Hardison, khardison@govtech.com
Lara Roebbelen, lroebbelen@govtech.com
Carmen Besirevic, cbesirevic@govtech.com
Lynn Gallagher, lgallagher@govtech.com
Kelly Schieding, kschieding@govtech.com
ACCOUNT EXECUTIVES:
Paul Dangberg, pauld@govtech.com
Rebecca Regrut, rregrut@govtech.com
Kathryn Nichols, knichols@govtech.com
Joelle Tell, jtell@govtech.com
BUS. DEV. MANAGER:
Maggie Ransier, mransier@govtech.com
Nick Pedersen, npedersen@govtech.com
INSIDE SALES:
Lisa Blackie, lblackie@govtech.com
Linda Clarke, lclarke@govtech.com
SR. SALES ADMINISTRATOR:
Kelly Kashuba, kkashuba@govtech.com
SALES ADMINISTRATORS:
Jane Mandel, jmandel@govtech.com
Danielle Murphy, dmurphy@govtech.com
Koy Saelee, ksaelee@govtech.com
Melesia Jimenez, mjimenez@govtech.com

Sr. Dir. of Sales Operations: **Andrea Kleinbardt,** akleinbardt@govtech.com
Content Studio 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.: **Eenie Yang,** subscriptions@govtech.com

CORPORATE
CEO: **Dennis McKenna,** dmckenna@govtech.com
President: **Cathilea Robinett,** crobinett@govtech.com
CAO: **Lisa Harney,** lharney@govtech.com
CFO: **Paul Harney,** pharney@govtech.com
Executive VP: **Alan Cox,** alanc@govtech.com
Chief Content Officer: **Paul Taylor,** ptaylor@govtech.com
Dep. Chief Content Ofc.: **Steve Towns,** stowns@govtech.com
VP Research: **Joe Morris,** jmorris@govtech.com

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

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

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

Printed in the USA.

e.Republic

BPA WORLDWIDE

By Noelle Knell / Editor

Pivoting Toward the Future

Anyone who's ever managed anyone or anything knows that things never roll along predictably. Declaring as a leader that you've got a complete handle on problem X, issue Y or project Z is dangerous talk indeed. There is always more to learn, and challenges will come your way that you can't totally anticipate.

As with technology as a whole, cybersecurity, an issue we come at from various angles in this edition of the magazine, is constantly changing. New threats, new tactics and new attackers require constant vigilance. Likewise, an effective strategy requires spending some time rising above today's challenges and planning for what's to come.

In Hawaii, Gov. David Ige is focused on building an innovation economy. He recognizes that while the state is in a good spot relative to unemployment (at nearly 3 percent, the third lowest rate in the country), growing the state's knowledge industries will best position Hawaii for job growth. One step on the path is an early college program that lets high school students earn enough credits through college-level courses to earn AA degrees at nearly the same time they finish high school. The first cohort of participants will graduate next May — they'll actually get their associates' degrees a couple weeks before high school graduation. Ige has some well-placed faith in the program, citing studies that show it's an effective way to point students who don't come from households with college graduates toward post-high school studies.

"It demonstrates to them in a very real way that they can take college-level courses and succeed," Ige said. "We are seeing a tremendous increase in the college-going rate for those who are first-time going-to-college family members." Further, as we've seen in several other states, Hawaii is eliminating the cost barrier to attending community college. In a partnership between the state and the University of Hawaii, they've pledged to make up the difference between the full cost of tuition and the amount the student is determined to be able to pay through the federal student aid program.

Another element in nurturing the innovation economy is applying resources to the development of entrepreneurship and innovation programs at the University of Hawaii. One component of their strategy is to relax some rules that have historically made it harder for leading research and development faculty to take their work to the commercial marketplace. "In all communities where you want an economic transformation, where you want to see innovation and technology take off, a thriving research-focused university is at the heart of each and every one of those transformations," he said.

And speaking of transformations, Ige argues that Hawaii is well-positioned to take advantage of the modern technological age, with its ubiquitous Internet and everything-as-a-service. "Before, in our history, our geographic isolation was a barrier," he said, clarifying that it hampered the state's abilities relative to economic development. But today, he makes a compelling case for an autonomous vehicle test bed in the state, as well as a testing site for UAVs — no border states to worry about, giving them more geographic freedom to fully explore the capabilities of these new technologies. Further, he recognizes the potential for drone and sensor technology to help combat invasive species and aid in conservation efforts.

"Encouraging companies and encouraging students to expand their scope of vision to really believe that Hawaii can be an innovator, can be a world leader, is important."

Now that's planning for what's next. gt

RAISE YOUR VOICE ✉

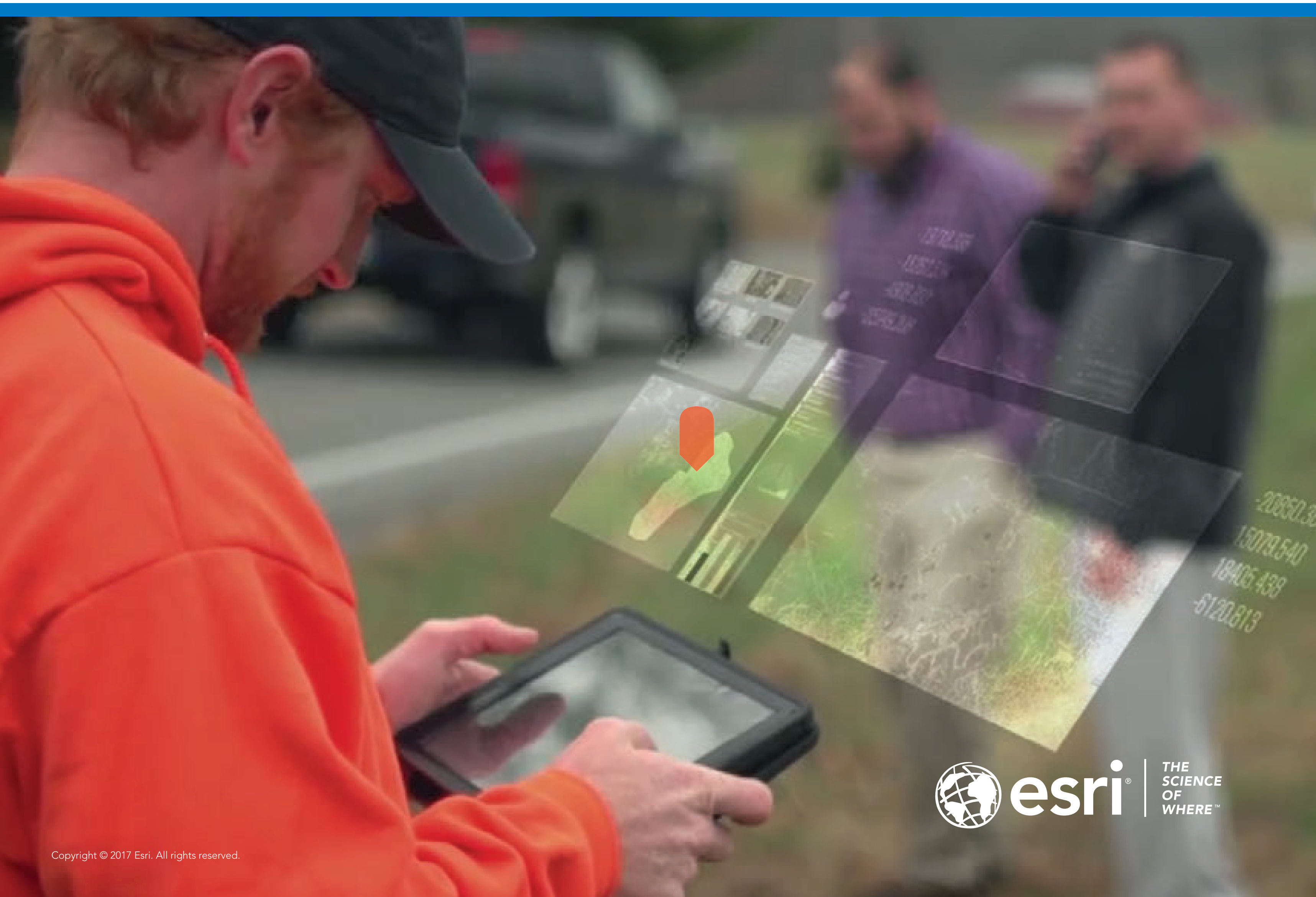
Your opinions matter to us. Send comments about this issue to the editors at **editorial@govtech.com**. Publication is solely at the discretion of the editors. *Government Technology* reserves the right to edit submissions for length.

Mobile Government Strategy: Take GIS to the Field and Back

Turn a routine data collection expedition into a data goldmine with GIS. From the very moment that your crew heads into the field, geo-powered data guides and simplifies their tasks. Data collection is exact and instantly useful back in the office. A perfect suite of apps, all working together to make your field operations smooth and efficient.

Next time, send your field crew out with ArcGIS, the mapping and analytics platform with a mobile strategy built in.

Learn more about building a government strategy with GIS at **go.esri.com/MobileTech17**.



esri® THE SCIENCE OF WHERE™

govtech.com/**extra:**

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

L.A. Strengthens Community Cybersecurity

In an average day, Los Angeles' municipal government analyzes more than **1 billion cybersecurity-related events**, automatically blocking about 4 million attacks on its own systems as a result. To share those effective measures with businesses throughout their community, the city has launched the Los Angeles Cyber Lab. The lab, the first of its kind in the nation, is a public-private partnership between the city and Cisco, with an advisory board including representatives from companies like Amazon and Motorola. "The reality is, bad guys have constantly been working together in the area of cybersecurity," said L.A. CIO Ted Ross, "and now, using our city government, we're having the good guys work together to help in the defenses."

Biz Beat

Civic activism has increased since Donald Trump's upset presidential win last November, prompting massive amounts of constituent feedback to legislative offices. The problem is that those offices often don't have great ways of dealing with that input. That's the issue a pair of brothers, both undergraduates at Stanford University, are seeking to solve with their startup **ePluribus, a civic engagement platform** meant to help constituents engage with elected officials more easily, and vice versa. Simply put, constituents could send messages categorized by issue to their representatives, who could then analyze that data to understand it more holistically. The company's crowdfunding campaign via Indiegogo began mid-September.

Pothole Prediction

Street conditions in **Kansas City, Mo.**, are bound to improve in coming years thanks to the development of "pothole prediction" technology. Currently in the pilot phase, the project uses existing traffic cameras to provide data related to traffic volume and other metrics, such as the age of the pavement, while also considering other factors like weather to anticipate when a section of road will fail. By doing routine preventive maintenance, the city will be able to stretch funds further and generate greater return on investment.

WHO SAYS?

> *"Whether the term is the right term, 'smart cities' is about doing things differently. It's about exponential versus linear. It's about evolution versus revolution."*

Govtech.com/quoteOctober17

MOST READ STORIES ONLINE:

Roads that Pay for Themselves: Startup Nears Two Smart Pavement Pilot Project Contracts
2,595 VIEWS

Rise of the Government Chatbot
2,375 VIEWS

Total Solar Eclipse 2017: How Data, Mapping Technologies Are Helping State, Local Oregon Agencies Prepare
2,059 VIEWS

10 Cities Taking a Nature-Driven Approach to Innovation
1,963 VIEWS

More States Explore Truck-Platooning Technology and Regulations
1,463 VIEWS

In Illinois, Cybersecurity Training for State Employees Now Required by Law
1,428 VIEWS

tech/**bytes**

44%

of the U.S. population was believed to be affected by the Equifax breach announced Sept. 7. While many government organizations use the company's data verification services, the impact on the public sector remains unclear.

4.5 MILLION

The estimated number of self-driving cars that will be on U.S. roads by 2035.

$2.5M

The value of a contract with Michigan that government analytics firm Munetrix says Socrata underbid it on, after first agreeing to partner.

15K

The number of Boston residents city officials spoke with in crafting the Imagine Boston 2030 dashboard.

ADVERTISEMENT

Q&A
Building a Better IT Resiliency Strategy
Step One: Prepare

Doug Snyder, Information Availability Strategist, Veritas

Nationwide, resiliency has become an increased focus area for state and local governments. While the resiliency conversation initially focused on preparing for and responding to natural disasters, it has quickly morphed to preparing for and responding to a new set of evolving threats — including malicious cyber criminals. The blending of physical and virtual infrastructure and the increased reliance on IT systems for service delivery has made resiliency a critical topic for government technology leaders.

Government leaders must take three steps to build a resilient agency: prepare, respond and adapt. In this Q&A, we take a closer look at step one: prepare. Veritas Information Availability Strategist Doug Snyder discusses how the public sector can use software-defined storage to properly secure and manage data, and how the right partnership can help agencies modernize their approach to IT resiliency.

Q: What IT resiliency challenges do state and local agencies face?

Business continuity and IT resiliency have become mission critical as government agencies provide more services and conduct more transactions online.

The demand for the public sector to be highly available and highly performing has never been more intense, and now agencies are being asked to make that leap at the same time they're being told to look at cloud and other technologies. That adds to the complexity.

Q: How does Veritas help government agencies better prepare by properly securing and managing their data?

Most agencies take a multi-faceted approach. They start with simple data copy methods — can I just use my backup, for example, or can I set up some storage replication and worry about everything else later? That's not really a disaster recovery strategy.

We help clients focus on what we call "solutions for data orchestration." We put a wrapper around all the manual processes — failover, disaster recovery, application, storage replication — and make those processes as simple as pressing a button.

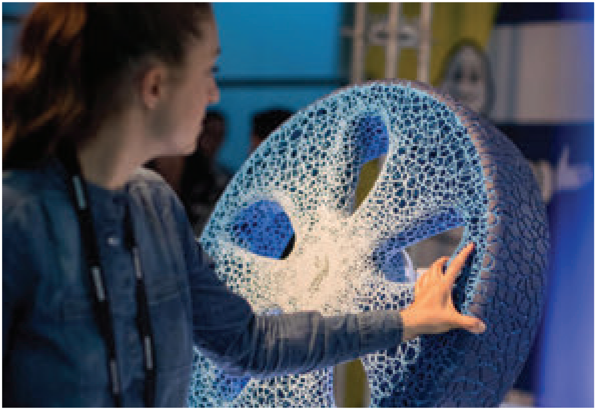
Q: What advice would you give agencies about how to achieve long-term IT resiliency?

The public sector is undergoing a significant IT transformation. Many agencies are just beginning to formulate strategies to manage this transition. To help them prepare and achieve IT resiliency, they need to be more process-driven. That could mean using regulatory frameworks like The Information Technology Infrastructure Library (ITIL) or ISO 9000 as a starting point. Working with the right partner and software-defined storage vendor also is critical to helping agencies properly secure and manage data.

Read about step two in building a better government resiliency strategy in the December issue of *Government Technology*.

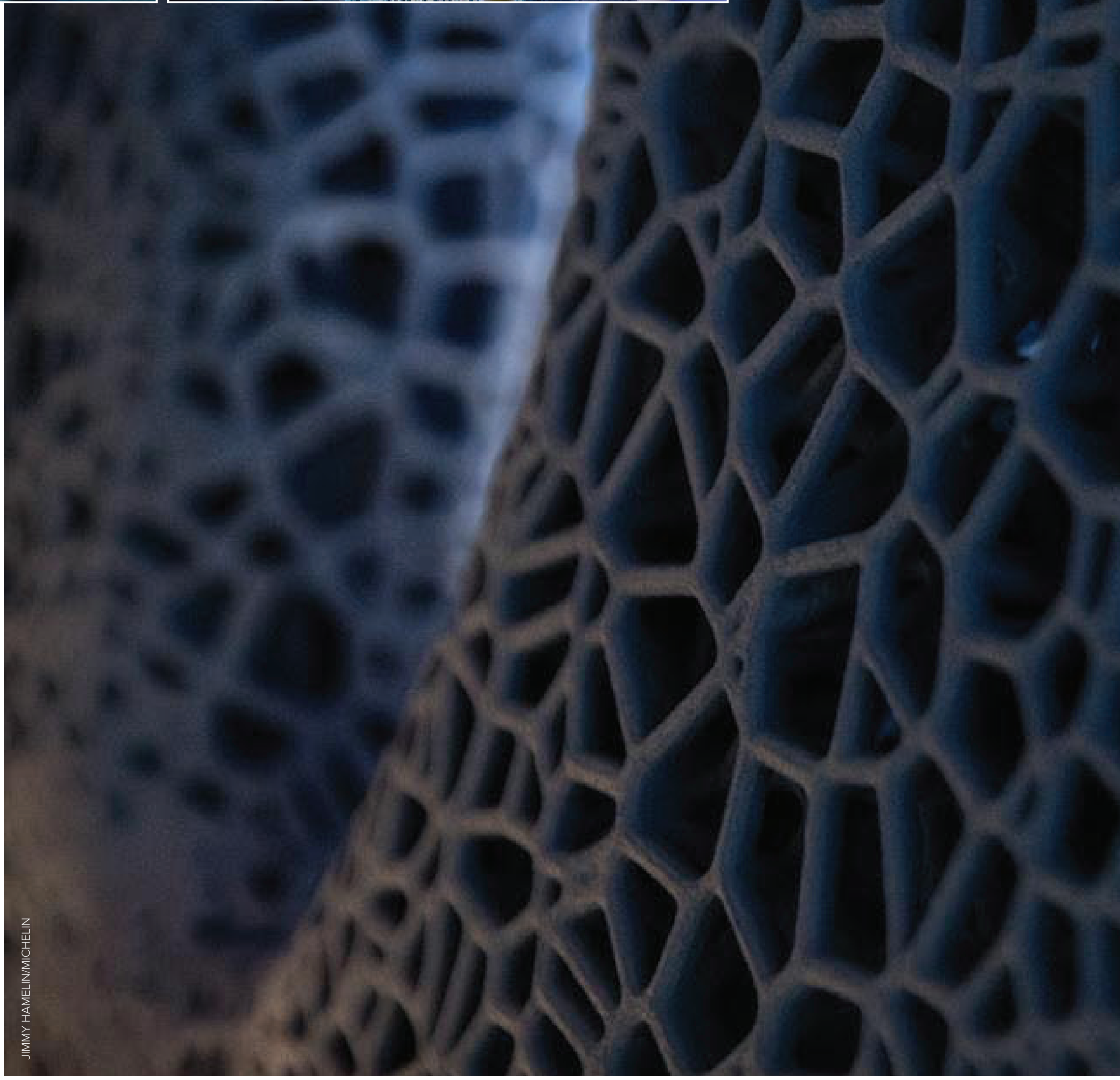
To learn more best practices about building government resiliency, download our handbook: **www.govtech.com/resiliencyhandbook**

VERITAS™ | carahsoft.

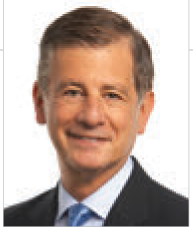


Rolling Forward

What if you never had to worry about putting air in your car tires again? That's one of the aims behind Michelin's concept for its Vision tire, a 3-D-printed organic, biodegradable, airless, connected wheel for vehicles. Introduced this summer, the product speaks to the future of mobility and is both sustainable and intelligent. In the spirit of reducing and reusing, Vision uses materials derived from natural products like wood chips, straw and sugar residue, as well as recyclables like aluminum cans. Inspired by natural life cycles, the solid woven blue material looks more like something you might find thriving on a coral reef rather than speeding down the highway. While Vision tires are not yet in production, Michelin anticipates that some of their features will trickle down to mass-market tires it releases in the future.



JIMMY HAMELIN/MICHELIN



Form Over Function?

Limiting resident paperwork could make for easier, more efficient service.

Few would consider forms a particularly exciting area of opportunity for government innovation. And yet, here's a solution that would probably spark the interest of anyone who's ever waited in line at the DMV: Let's get rid of them.

Recently, many governments have made efforts to redesign their forms in order to make them less time-consuming and confusing, and more likely to elicit honest responses from residents. Washington, D.C., for example, this summer hosted a "Form-a-Palooza," an event that invited residents to collaborate on projects like making limited-purpose driver's license forms easier for non-English speakers. New Mexico redesigned its unemployment insurance application process to include behavioral nudges that encourage residents to report their unemployment status and work search activities more honestly. And Indianapolis is broadly re-engineering its forms as part of a Web redesign.

However, perhaps these types of initiatives are asking the wrong question: Maybe we should not be asking how we can make forms better, easier, even more consolidated, but rather if we need forms at all.

Estonia — known as one of the most tech-savvy public administrations in the world — has moved toward a form-free system. The government operates under an "ask once, use twice" model, meaning that the government can only ask a resident for a particular piece of information once, but must use that information for at least two services. And almost every government service, ranging from filing taxes to voting, is available online. This means that if you input information for one service — for instance, submitting your address in order to apply for a license — applying for another requiring the same data — like registering to vote — is only a click away.

A number of American cities have taken steps in this direction, attempting to reuse resident data to limit the amount of required paperwork. For example, Los Angeles, Washington, D.C., and many others have allowed residents to complete their voter registration at the same time they renew their driver's license without filling out a separate form.

It seems, though, that governments could take these measures one step further. Cities, states and the federal government possess immense amounts of resident data; why should they not share this data across agencies and with each other in order to solve problems for citizens before they even ask? When low-income parents submit income, family size and other information to apply for reduced-fare transit, why should the state not automatically enroll them in earned-income tax credits? Of course, residents should maintain the ability to opt out of municipal services, but automatic enrollment could help those who do not know about such services or find the application process too complicated.

And as governments become increasingly connected with the private sector, opportunities to use existing resident data to offer services will become more and more ubiquitous. For example, under the current unemployment insurance process, recipients must document their work search activities on a weekly basis. However, if governments partnered with companies to access their human resources data, they could automatically verify work search activities and continue to provide insurance without time-consuming paperwork for claimants.

Reusing resident data where possible could greatly reduce the burdens of applying for many services and free up municipal workers to manage tasks more complicated than processing paperwork. This means shorter lines at the DMV and more residents receiving the benefits they need. That's something to get excited about. gt

Chris Bousquet, a research assistant/writer at the Ash Center for Democratic Governance and Innovation at the Harvard Kennedy School, co-authored this column.

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.*

A government technology Case Study | Laserfiche

ADVERTISEMENT

STREAMLINING THE RESPONSE TO PUBLIC RECORDS REQUESTS

HOW LA PLATA COUNTY USES PREBUILT PROCESS TEMPLATES TO AUTOMATE DOCUMENT GATHERING AND REQUEST MANAGEMENT

SNAPSHOT: **LA PLATA COUNTY**
LOCATION: **SOUTHWESTERN COLORADO**
POPULATION: **55,000**
FY 2017 BUDGET: **$77 MILLION**

All too often, fulfilling a public records request means carrying paper around from department to department because it's the fastest and easiest way to assemble all the right documents. And because one employee typically serves as the response coordinator, deadlines could be missed when that person takes time off.

This was the challenge for La Plata County, Colo., where state law requires a response to records requests within 72 business hours.

"The 72-hour response requirement is a tight timeline and requires everybody to be on top of things because the legal implications for not meeting the deadline are huge," says Sarah Jacobson, manager of the county's administration office.

Today, La Plata's response process is largely automated within its Laserfiche enterprise content management system. County staff used the Laserfiche Business Process Library, a feature in Laserfiche Forms, to find a prebuilt template that reflects a typical records request workflow and automates task routing, document forwarding and due date reminders.

Using Laserfiche to create online forms and automate workflows is a significant part of the county's initiative to mitigate declining tax revenues by reducing direct costs and working with leaner operations.

"Laserfiche helps us increase our capacity to get work done, even in times of tight budgets," says Mike Hawkins, enterprise content analyst. The improvements gained from process automation are instrumental to the county's goal of saving $1 million in hard and soft costs in FY 2017 and to its Innovate La Plata initiative, a program that empowers staff to think differently about their work in order to streamline processes, save money and improve their job satisfaction.

MEETING DEADLINES, REDUCING WORK

When a public records request is entered into La Plata's Laserfiche system, the automated workflow starts freeing up county employees' time by:

- Tracking the status of required actions for each department and automatically sending reminder emails about items due
- Supporting redaction and allowing drag-and-drop document submissions into the response file
- Avoiding the need to manually convert documents into a PDF format before responding back to the appropriate request
- Routing the response file to the county attorney's office for legal review
- Sending an email to the requester with cost information if the request will involve charges for staff time, then issuing an invoice when the response work is finished

When the documents are ready for release, Laserfiche posts them to the county's website for public access, with an automated email to notify the requester.

"Releasing the requested documents electronically through Laserfiche helps save taxpayer money because we don't have the expense of printing documents or copying them onto a CD," says Jacobson.

The automation helps La Plata County avoid delays in fulfilling requests because the overall process is less reliant on a single employee serving as the coordinator. Additionally, contributing documents to the response is now a significantly easier process for all staff involved.

"Working with the new process isn't complicated, so for most employees you will only need to offer training once," says Jacobson.

To adapt the Laserfiche process template to fit their needs, La Plata County employees only had to enter basic configuration information and slightly modify the tracking process for requests that involve multiple departments.

"We thought we would need to develop our own forms, but when we went into the Laserfiche Business Process Library, we saw a lot of templates that are pertinent to us," says Hawkins. "I think the world of the template library because of all the time and effort it would take us to develop the requirements and process for a workflow. With the Laserfiche templates, that work is already complete."

The Laserfiche system replaced a previous document management system that could not meet the county's requirements for automating processes. The county also evaluated a system designed specifically for handling public records requests, but found it too expensive and restrictive.

"We chose Laserfiche because of how robust it is, how seamlessly it works with other systems we use and how easily we can set up automatic document deletion," says Jacobson.

"Releasing the requested documents electronically through Laserfiche helps save taxpayer money because we don't have the expense of printing documents or copying them onto a CD."

— Sarah Jacobson, Manager, La Plata County Administration Office

EXTENDING FORMS-BASED AUTOMATION TO OTHER GOVERNMENT PROCESSES

La Plata now uses more than 80 forms to automate various county processes. Some forms cover specific functions within a single department, while others – such as forms for submitting budget information – are used by all departments.

Using the Laserfiche templates as a starting point, county departments develop their own forms based on guidance from the IT and administration teams on required standards, such as securing the form with user authentication.

Hawkins notes, "For IT, this approach avoids the time spent on defining requirements and getting the department's buy-in on something that IT has created."

Other departments that are automating processes include:

✓ **Assessor's Office.** Previously, when a property owner applied to split a land parcel, staff exchanged information by passing spreadsheets back and forth. The process required 17 steps and used seven software applications. By replacing those spreadsheets with a Laserfiche form, the process is now only six steps, uses two software applications, reduces paper use by 100 pages per day and saves an estimated 500 hours of staff time per year.

✓ **Finance Office.** Collecting budget information from 22 divisions is simpler with automated forms for requesting capital and technology items, as well as information about employee overtime and temporary positions. In the past, these requests were submitted as a printed document, and finance staff had to rekey the pertinent data into the finance system. Now, the Laserfiche workflow automatically compiles the forms each division submits, transfers data into the finance system and budget book, and performs calculations such as adding the cost of employer taxes for temporary positions.

✓ **Treasurer's Office.** The county treasurer uses Laserfiche forms to automate entries to the accounting journal system.

✓ **Human Resources.** County staff scan paper records related to worker's compensation claims and store them in Laserfiche where the metadata is integrated with the data file the county receives from its external claims management vendor. The HR department also uses a Laserfiche form to receive and track submissions for employee recognition.

✓ **Planning and Code Enforcement.** A work-in-process report form, maintained in Laserfiche, helps staff across multiple county departments track current project status.

✓ **Citizen Boards.** An online form offers local residents an easy way to apply for appointment to the county's various citizen boards and commissions. Other forms allow staff to maintain a database of candidates and track information and renewal dates for current board members.

MORE IMPROVEMENTS TO COME

La Plata County will continue to use Laserfiche templates to create more forms and automate more processes, generating additional cost savings and improving productivity. The county will also benefit from one aspect of process automation that can be overlooked, says Hawkins: "It helps our employees work more effectively by making their jobs easier and more fun."

Produced for: Laserfiche®

For more information, please visit:
www.laserfiche.com/slg

Shawn Riley

CIO, North Dakota

North Dakota Chief Information Officer Shawn Riley has about six months under his belt in this career turn toward government. Before coming to the state, Riley spent 13 years in IT leadership positions at the Mayo Clinic, where his responsibilities included oversight of the organization's security operations. With the support of Gov. Doug Burgum, Riley is making strides on plans to help state IT run as efficiently and securely as possible, including a unification plan that builds on past consolidation efforts, which will bring the state IT workforce from 400 to 700 by the end of next year. Also on his to-do list in the near term is a comprehensive citizen engagement strategy that effectively serves today's mobile-enabled citizenry.

1 **What are the biggest differences between health care and state government?** There's very little difference between health care and government. Physicians and the Legislature feel very similar in the way that they're able to change policy and change how the organization roams and moves. There are also a lot of similarities in that in government you have those stand-alone agencies out there all trying to serve their customer base, and in the health-care world, it's ophthalmology or nephrology, or pick your -ology. The biggest difference that I've seen is the way in which the finances work. But as you would imagine, health care is also very regulated, so their money model is coupled with many governmental aspects. They are both very complex, but it feels similar: a lot of people trying to do the right thing for the public, whether you call them citizens on the government side or patients on the health-care side.

2 **Where is the state now in terms of its cybersecurity position?** We have started a Zero Trust model in our data centers. We've been able to consolidate the state down to two main data centers (one primary and one redundant), so we have a very consolidated infrastructure compared to most other states. We've implemented Zero Trust, and to me, that is a best-in-class security model. We are well down that road. We also have a very significant focus on the client side, on the desktop-user type of environment in managing those systems, making sure that we have a comprehensive, across-the-state view of assets and asset management, and then what we can manage from a security perspective at a software level.

3 **What are your plans for a Unified Data Management Platform? Why was it needed?** We're putting together a way to restructure data to enable our agencies to communicate in vastly simplified ways and ways where we can do big data analysis in vastly easier and less expensive ways than we've ever been able to before. At the same time, we want to keep the classification in between the systems — whether it's protected health information, payment card information or Criminal Justice Information Services data, etc. — making sure we can keep that classification separate and still be able to do data research and mining and build applications across this large state entity. We want to position ourselves at a strategy level to do the [analytics] projects we don't even know exist yet. We want to be able to manage our data in a way that positions us to take on the next issue, whatever that may be, and vastly improve our time and response rates to the citizen using that technology as the baseline.

4 **How does the cloud play into your overall IT strategy?** We are moving to a cloud-first and a mobile-first strategy. It's not cloud-only and it's not mobile-only, but it is cloud-first. We're taking an "If not, why not?" approach to our new development and our new projects to ensure that we look at cloud as the initial capability and only go to on-prem if it's an absolute necessity.

— Noelle Knell, Editor

A GOVERNING INSTITUTE Case Study | Oracle

New York Uses Data to Transform Healthcare Delivery

An industrial-strength data warehouse provides the enriched data insights needed to improve Medicaid patient care.

There are six million eligible Medicaid recipients in the state of New York – the second most of any state. The program is costing the state $18.2 billion in FY 2017, or 19 percent of its $96 billion operating fund. That expense is expected to increase by another $1 billion in FY 2018. These numbers mean that if New York can make Medicaid more efficient by even a fraction of a percent, it will positively impact other programs the state supports – not to mention its bottom line.

Most states – including New York – have transitioned to a managed care model to gain more control over Medicaid-related expenses and provide better care to this often-underserved population. But this can be a difficult undertaking without a strong foundation of coordination among the variety of providers serving Medicaid recipients, and a holistic view of their care.

In 2014, New York began to implement Medicaid's Delivery System Reform Incentive Payment (DSRIP) program, a federally funded initiative that promotes community-level collaborations and focuses on system reforms. The goal of the program is to reduce avoidable hospital visits by 25 percent over 5 years.

To meet this goal, the state not only needed data, but also the ability to glean valuable patient insights from that data to help pinpoint risks and inform care decisions.

"DSRIP provides the runway and the funding for providers to come together, begin to work and act differently, and better coordinate and collaborate patient care – all with the intention to drive better outcomes," says Ken Romanski, executive vice president of CMA, the IT solutions and services company New York contracted with to design and operate a data warehouse to achieve its DSRIP goals.

Tackling Data Challenges at the Speed of Thought

Central to DSRIP's success is the collaboration and coordination of a tightly organized group of providers, or Performing Provider Systems (PPS). PPS units include primary care physicians, hospitals, laboratories, pharmacies, home care agencies and even durable medical equipment providers. Regardless of where a patient goes for help, "the essence of a PPS is to create the information and insights necessary so there is no wrong door," says Jeff Wendth, vice president of CMA Healthcare Solutions.

Essential to this objective is an industrial-strength data warehouse of patient encounters and payment claim information.

New York Medicaid has long operated a data warehouse, serving as the system of record for 20 years' worth of claims and encounter data. As experienced as the Medicaid program was in amassing databases of claims data, however, the existing data infrastructure wasn't set up to provide insight into care needs of Medicaid recipients and identify disease trends and cost – all of which are necessary to manage care successfully and meet the goals of DSRIP.

"DSRIP provided the motivation to tackle the challenge of manipulating and analyzing the data to be considerably more beneficial," says Bob Nevins, director of health and human services strategy for Oracle, a key supplier of data warehouse infrastructure products for New York Medicaid.

"The speed and rate at which we receive data, the number of disparate sources for the data and the scale of the data is all increasing pretty significantly."

– Brian Dougherty, Chief Technical Architect for CMA

To equip healthcare providers statewide with the detailed information they need to fully understand the medical problems of the patients they are contracted to manage, the data warehouse must handle prodigious amounts of information.

But th at's just the first step. The warehouse must also have a plan for how various data streams intersect and match them in intricate ways to yield insights and conclusions.

"The speed and rate at which we receive data, the number of disparate sources for the data and the scale of the data is all increasing pretty significantly," says Brian Dougherty, chief technical architect for CMA. "Now the big challenge for us is to handle those three dimensions and to do this at the speed of thought."

"Oracle provides a great set of technologies for dealing with the challenges that we have," adds Dougherty. "The database is very capable; it's been around for a long time – it's industrial-strength. It has features that allow us to scale and manipulate the data – especially on the back end – very, very well."

Next Up: Whole-Health Management

Using the data warehouse as a foundation, CMA worked with the state to build an intelligence platform to extract additional granularity from the data. It can now group together individual patient characteristics, test results, current conditions and other factors based on a variety of queries. The platform also supports executive dashboards, standard reporting, guided query and data mining capabilities for DSRIP metrics, which are used by administrators, payers and care providers.

The information has allowed the state to stratify its Medicaid population, and group individuals according to common health conditions such as diabetes or heart disease so PPS units can target the most seriously ill and costly patients. It also helps identify opportunities for improvement and guide action at the point of care with the clinical data that providers can immediately access.

That won't be enough, though, as the program evolves into more focused population health management, which reaches beyond the clinical environment to embrace social, economic and care-coordination factors.

"I know the state recognizes the need to move beyond the data it's working with today and expand it to clinical and social-determinant data sets to achieve a more holistic, 360-degree view of the individual," Romanski says. "In order to negotiate, contract and manage a value-based payment system, the whole ecosystem is going to need enhanced capabilities that the state is mindful of and looking to support."

This translates to looking for data never captured before and developing different collection architectures to plug into the multitude of analytical dimensions already in place, says Dougherty. Medicaid recipients who are homeless are one example of the need for a larger scope of data. For this population, traveling without transportation is a health-influencing factor, as is their lack of housing.

"Much of the population health expansion is still in the planning stage," says Daniel Hallenbeck, director of the Medicaid data warehouse for the New York Department of Health. "But the state recognizes the value of incorporating new data sets to create the whole view, including social determinants that might assist in producing more meaningful metrics for measuring outcomes. This is the future we are working toward."

ORACLE®

The Oracle Cloud delivers hundreds of SaaS applications and enterprise-class PaaS and IaaS services to customers in more than 195 countries and territories while processing 55 billion transactions a day. For more information about Oracle, please visit us at oracle.com.

CMA

CMA has provided information technology products and services since 1984, serving commercial, industrial, and public sector industries, with a primary emphasis on Health & Human Services. CMA has offices in New York, Ohio, Texas, Arizona, and Washington DC. CMA provides its customers the best in proven technology and experienced professionals. With more than 450 employees, CMA has conducted thousands of technology-oriented consulting engagements and developed hundreds of application system solutions for our customers. CMA is a New York State certified woman-owned business.

GOVERNMENT'S EMERGING SILO-BUSTING APPROACH TO CYBERSECURITY REACHES NEW HEIGHTS IN GEORGIA. BY ADAM STONE

UNCHAR

Government technology leaders have set their sights on forging dedicated cybersecurity facilities and initiatives. Maine's state CIO chairs the Information Protection Working Group. New Jersey has its Cybersecurity and Communications Integration Cell, while the Northern California Regional Intelligence Center continues to break new ground in cybercollaboration.

When leaders in Georgia opted to pursue their own cybercollaboration, they chose to paint with a bigger-than-usual brush. The $50 million Hull McKnight Cyber Innovation and Training Center now under development in Augusta is exceptionally ambitious. Named for local businessmen James M. Hull and William D. McKnight — credited with the original idea for the center — it brings together state government, academia, law enforcement and private-sector players in a bid to shore up the cyberworkforce and strengthen defenses.

"We have many different players focused on different pieces, and it seemed we could get a lot more done if we brought all those groups together," said Georgia CIO Calvin Rhodes, who is also executive director of the Georgia Technology Authority (GTA), the entity responsible for building the center.

Getting everyone together has been no small trick, with each constituency bringing its own needs and expectations, its own way of doing business. Concerns have ranged from the vital (securing a space for legal evidence) to the mundane (finding parking for everyone).

How to make these disparate pieces fit together? *GovTech* talked to key players from across the board to discover how they plan to get their needs met on the way to making this 167,000-square-foot center a reality by the scheduled July 2018 opening date.

MICHAEL A. SCHWARZ

RTED

GEORGIA CIO CALVIN RHODES (LEFT), GBI DIRECTOR VERNON KEENAN AND AUGUSTA UNIVERSITY'S MICHAEL SHAFFER WALK THE BUILDING SITE IN AUGUSTA IN LATE AUGUST.

GEORGIA CYBER INNOVATION & TRAINING CENTER

ACADEMIA

The center aims to train a future cyberworkforce, which makes Augusta University a key tenant. The university plans to house its School of Computer and Cyber Science at the center, and officials say they're eager to be part of the venture.

"To solve our issues around cyber, it is going to take academia, industry and government. Those three are going to have to work together to find solutions," said Michael Shaffer, the university's vice president for government relations and chief advocacy officer. "Our job is to interact with all the different players."

For the university, a successful collaboration hinges on the coordinated use of physical space. If the center is to serve as a training ground, its multiple tenants must choreograph an elaborate dance to ensure classroom facilities are available as needed.

"There is a level of complexity around scheduling. It's a Rubik's Cube. You can move two pieces, and when you do, you've just moved another piece somewhere else," Shaffer said.

The school's main campus is about 12 minutes away, so planners have to factor in travel time for students taking classes at the center. It helps that the Technical College System of Georgia will also be using the facility. "Educational space can possibly be a shared resource, because nobody uses a classroom every hour of the day," said Shaffer, "But then that involves yet another set of schedules."

The school also has to consider staffing, as an expansion into the training facility will put added demands on faculty. "One way of getting at that could be joint appointments," Shaffer said. Faculty could teach part-time and work part-time on the payroll of other center tenants. There might be some logistical advantages to this, as joint appointments could facilitate a freer flow of information and collaboration.

The school plans to hire at least six new faculty members to support this effort, and while demand for cyberexpertise is intense, Shaffer said the project's high profile is helping with recruiting. "With all the talk of this new building, there are a lot of people showing interest. They see an opportunity to be part of something unique. There is talent that is reaching out to us because they see something exciting happening," he said.

LAW ENFORCEMENT

For Vernon Keenan, director of the Georgia Bureau of Investigation (GBI), the new cybercenter represents a twofold opportunity. It will provide a space for law enforcement professionals to leverage GBI's existing expertise in digital forensics. It also will free up the agency's child-pornography experts to get back to doing what they do best.

KEEPING THE COMPLEX ENDEAVOR ON SCHEDULE FOR A JULY 2018 OPENING IS NO SMALL FEAT. A SERIES OF WORKING GROUPS ARE CHARGED WITH MAKING QUICK DECISIONS, AND THE FACT THAT THE GEORGIA TECHNOLOGY AUTHORITY IS AT THE HELM HELPS SLASH THE LENGTH OF TRADITIONAL PROCUREMENT CYCLES.

Georgia's digital law enforcement savvy is a direct result of their expertise investigating child porn cases: The experts in this unit are the ones who developed sophisticated techniques for ferreting out secrets from smartphones and computers. They've gotten so good at it that now investigators on a broad range of crimes come to them for help. If a cellphone is found at a murder scene, the child porn investigators typically are asked to pick it apart for evidence.

Keenan is eager to let them return to their main duties, and he says he can do that by basing a cybercrime unit at the new center. He expects 20 staffers to occupy 15,000 square feet in the building, including 12 permanent GBI personnel and a cadre of trainers devoted to helping local law enforcement get up to speed on cyber.

In making the transition, Keenan is most concerned about physical space, specifically the need for a secure environment. His people will be dealing with evidence in criminal cases, and that creates certain extraordinary requirements.

"When we extract data, we do it by court order, so we have to protect that information. There are a lot of privacy issues, a lot of chain-of-custody issues to maintain the evidence. There have to be inventories and audit trails," he said.

As a condition of entering into the center, GBI insisted on designing its own facilities. In addition to basic office space, GBI will have room for its investigative teams, along with a computer lab, secure servers and workspace for interns. The bureau will also have an expansive space for breaking down and investigating suspect devices. "We need to be able to line up all the computers that we are accessing, to hold all the instruments that we use to extract data," Keenan said.

At the same time, law enforcement officials want to be careful not to wall themselves off from their cybercolleagues: The whole point here is to foster collaboration. Given the security demands around their work, "the risk is that everything is so structured that there is no personal interaction with folks in the center," said Keenan. He's thus taking steps to ensure that there will be ample opportunity for interpersonal communication across teams. "Having that personal interaction is what breaks down barriers."

THE STATE CIO

The timeline on this beast is insanely aggressive — roughly 18 months — and Calvin Rhodes knows it only too well. In addition to massaging the various players, making sure their specific needs are met, he has been seeking creative ways to expedite what would ordinarily be a prolonged endeavor.

He has enlisted allies to help cut through bureaucratic red tape. It typically would take four months to get the land disturbance permits for a project of this scale. City officials stepped in and cut it to four weeks.

Rhodes and his team also accelerated the process by opting for a cookie-cutter architectural approach. They tapped the design firm Gensler, which has used a generic prototype to design similar facilities for at least seven other customers. That template helped give the design effort a running start. "On day one, they brought in a full set of plans for how the building is put together," said Rhodes. Customizing will be much quicker than creating from scratch.

It helps, too, that the project is operating under the auspices of the Georgia Technology Authority (GTA), which has greater flexibility than state agencies regarding procurement rules. As an authority, GTA can cut a typical 60- to 90-day RFP cycle down to 10 days and can pick a winning vendor almost instantly once proposals are in. "We would start in the morning and make our decision by close of business," Rhodes said. "If your company didn't have projects you could point to, you would get eliminated pretty quickly."

Finally, Rhodes has taken a divide-and-conquer approach to hastening the work, breaking down various aspects of the project among half a dozen working groups. There's a working group to address the needs of a future cyberacademy for state employees; a group to deal with private-sector and incubator issues; another for research and development; and another to ensure federal stakeholders have a voice.

Each working group has a specific agenda and a concrete timeline, and Rhodes pushes hard. "Some of these groups might

GEORGIA CYBER INNOVATION AND TRAINING CENTER

FACILITY SIZE:
167,000 square feet

COST: $50 million

GROUNDBREAKING:
June 19, 2017

EXPECTED COMPLETION: July 2018

PARTNERS:
Augusta Economic Development
Augusta University Cyber Institute
City of Augusta
Georgia Bureau of Investigation
Georgia Department of Education
Georgia National Guard
Georgia Technology Authority
National Security Agency
Private Sector Partners
Technical College System of Georgia
U.S. Army Cyber Command
U.S. Cyber School of Excellence
University System of Georgia

SOURCE: GEORGIA TECHNOLOGY AUTHORITY

take a year to make these decisions if they could, but we need them to do it in weeks and months," he said. "If you can't make a decision, we will make it for you."

Despite the tough talk, Rhodes has arguably bent over backward to accommodate the various needs of his future tenants. He's given law enforcement a free hand in designing its environment, and has tried to be flexible in assigning space in order to accommodate academia's scheduling needs.

Then there's the parking.

The city of Augusta will pay for construction of a five-story parking deck through a $12 million bond issue. Problem solved? Not quite. The university students, law enforcement officers and private-sector participants — all have different parking stickers and cards that work on their respective campuses. What system would the center use?

It may sound trivial, but these are just the kind of sticky details that can grind down a large-scale public project. So Rhodes convened a working group (of course), and it was determined that roughly half of the 250 to 300 cars expected at the center each day will have Augusta University parking credentials. The parking desk will therefore be outfitted with a system that syncs to those passes.

Even as he balances the needs of his diverse internal constituents, Rhodes has been looking outward. He says he doesn't want a facility where "everything is behind the fence," but rather a center that invites public participation.

"We want people to come in and see what is going on," he said. There will be an auditorium for public events, and connections to the local river walk to bring people to the campus. "We want people to get interested in the cybersecurity field. We want the community to feel welcome."

THE PRIVATE SECTOR

The long-range vision calls for the center to include a vigorous private-sector presence. Tech entrepreneurs are a driving force on the cyberscene, and private companies say they're eager to pool resources and swap notes with law enforcement and the research community.

Getting private-sector tenants on board is complex. As Rhodes points out, there are laws that govern how the state leases space to private firms, and at what rate. "If I have to give away a few months of free lease to help a company offset costs, we just have to be very careful about how we do that," he said.

As vice president of security solutions for Check Point Software, which has a sizable Georgia presence, Avi Rembaum said his firm is interested in the collaborative opportunities presented by the center, but like all other stakeholders, he too has his needs. He wonders how the organizational ground rules will evolve.

"You need everyone jointly contributing, not in an ad hoc way but as a regular way of operating," he said. "There will have to be a shift in mindset, where everyone understands that this is a shared responsibility and that each individual entity is better off by participating in this ecosystem."

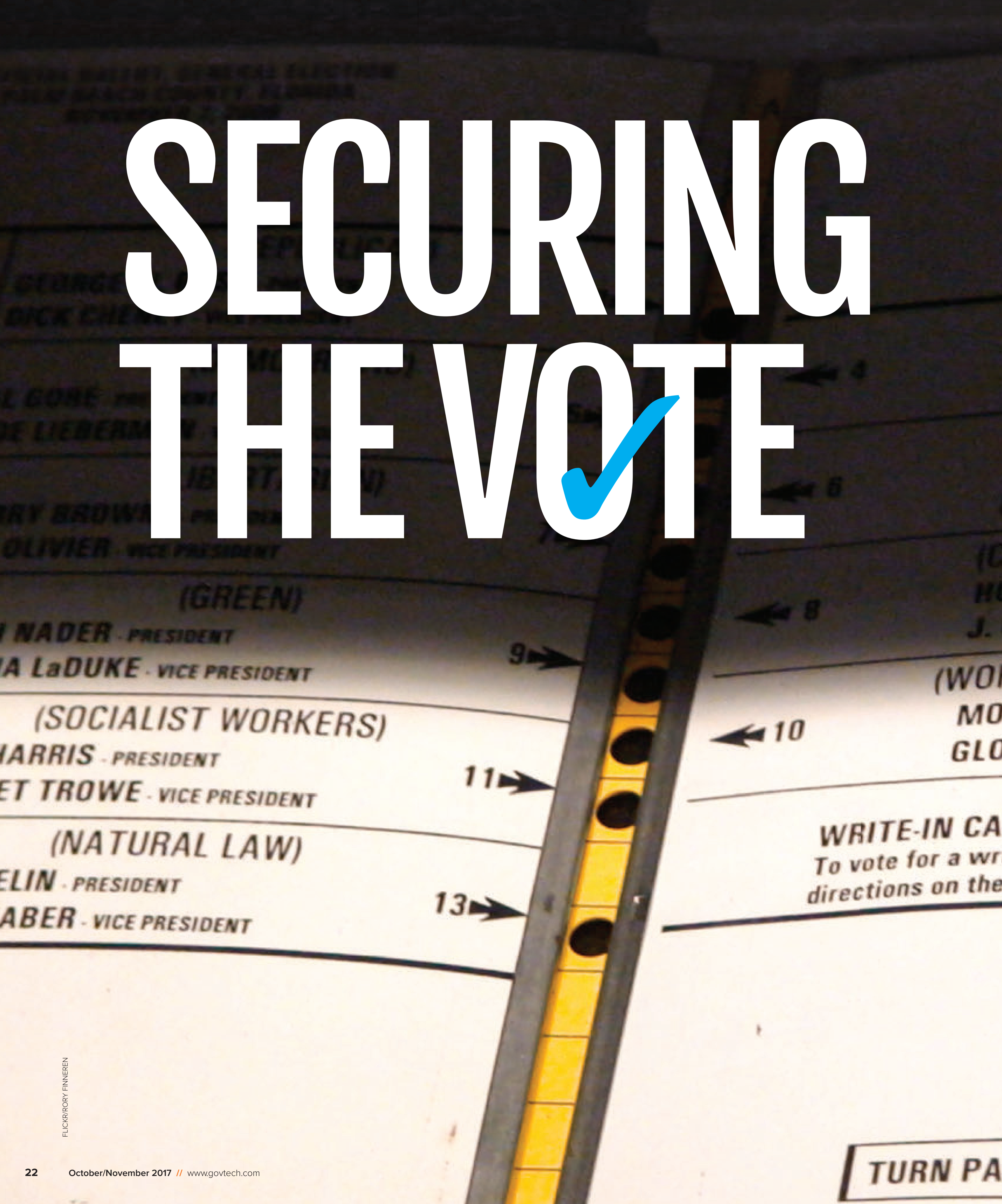
Reassuring potential private-sector partners will be a crucial part of the long-term success of the center, but it's just one step. In addition to executing on the various components described above, planners also must forge a working relationship with the U.S. military. The U.S. Army Cyber Command is expected to take up residence at nearby Fort Gordon in 2018 and is expected to be a key contributor to the state's emerging cyberecosystem.

That means Rhodes needs military certification for security-cleared personnel to work in certain spaces. The Defense Department isn't used to doing that at a venue with multiple non-military users, and it's required some heavy lifting.

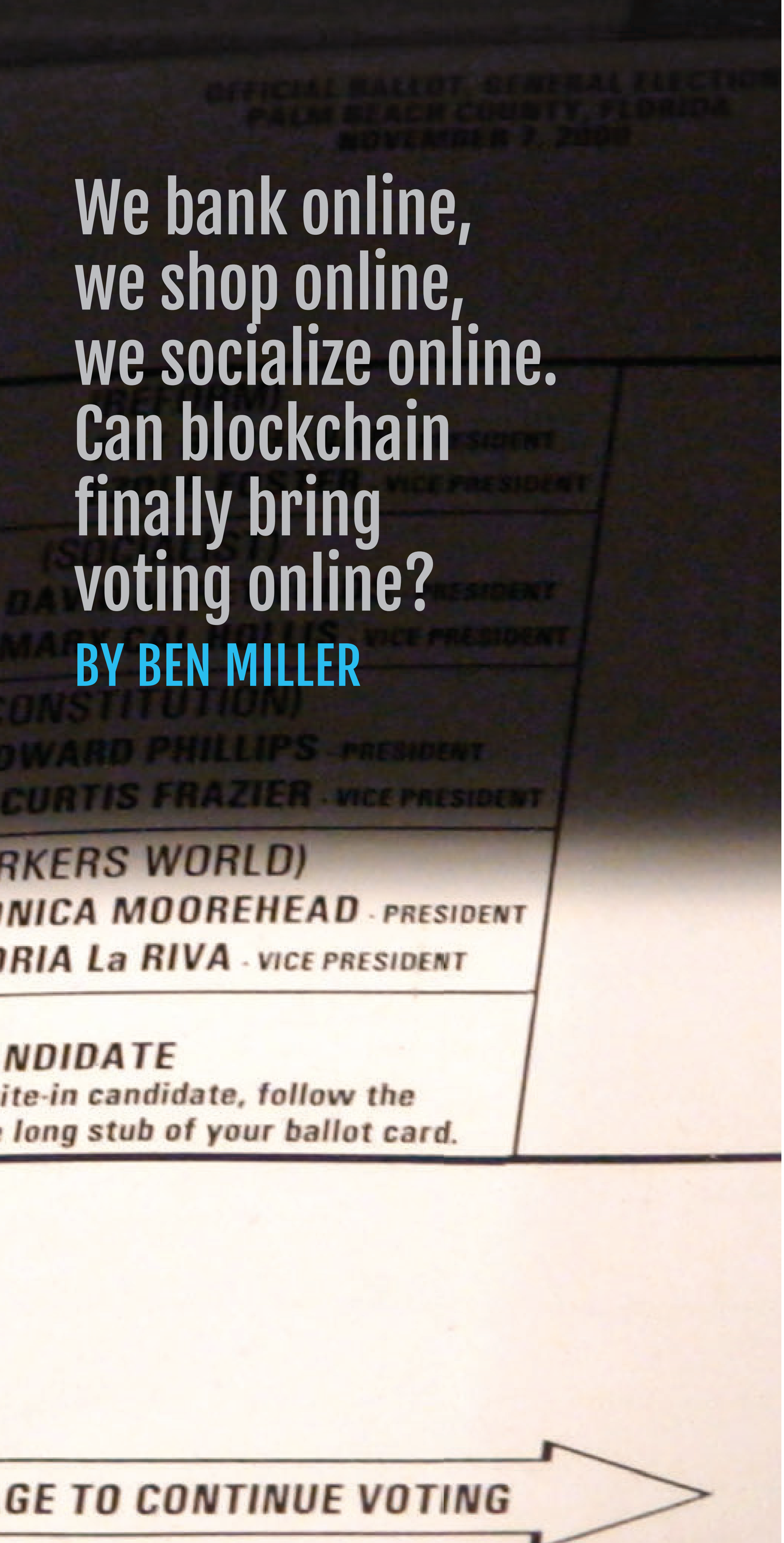
"There is no defined process for this. It is uncharted," Rhodes said. The same could be said for the entire Innovation and Training Center. Georgia is literally breaking new ground here, as it seeks to build a cyberworkforce, bolster law enforcement and foster private-sector ingenuity ... with ample parking for all.

adam.stone@newsroom42.com

SECURING THE VOTE



FLICKR/RORY FINNEREN


OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000
VICE PRESIDENT
VICE PRESIDENT
ONSTITUTION)
WARD PHILLIPS - PRESIDENT
CURTIS FRAZIER - VICE PRESIDENT
RKERS WORLD)
NICA MOOREHEAD - PRESIDENT
RIA La RIVA - VICE PRESIDENT
NDIDATE
ite-in candidate, follow the
long stub of your ballot card.
GE TO CONTINUE VOTING

We bank online, we shop online, we socialize online. Can blockchain finally bring voting online?

BY BEN MILLER

Should somebody develop a means of conducting elections online that the nation finds acceptably secure and private, it could very well transform democracy for the better. It is the hope of those people working on such efforts — and no stretch of the imagination to those who aren't — that online voting would mean more participation from a more representative portion of the people, faster results and even unchallengeable records of the outcome.

If only.

The minor mountain standing in the way of this vision is, to simplify the issue, cybersecurity. The public is treated regularly to stories of vaunted, savvy organizations brought low at the hands of faceless hackers. The victims: Target, Sony, Equifax, LinkedIn, the U.S. Department of Defense, the U.S. Office of Personnel Management. When hackers hit Dyn, the service that helps browsers find websites, the East Coast effectively lost large pieces of the Internet.

And then there was the hacking of the Democratic National Committee during the 2016 presidential campaign, followed by election system breaches in multiple states. The resulting political chaos has led some, such as U.S. Rep. Hank Johnson, D-Ga., to propose disconnecting voting machines from the Internet entirely.

"My recommendation," said Ron Rivest, a computer science professor at the Massachusetts Institute of Technology for more than four decades, "is to have all voting be done on paper."

Why? Because paper inherently solves all the most pressing concerns about elections: It is secure from hackers because one cannot digitally alter it, it is auditable because it is physical, and voters can check it for accuracy because they can experience it with their own senses.

And yet it was paper ballots, playfully dubbed "butterfly ballots," and their hanging chads, that caused such confusion and anger in the wake of the 2000 election.

There are workarounds. Optical scan machines employ technology to more quickly process paper ballots, improved design can make ballots less confusing, there are even systems in place to add some measure of voter verification by comparing handwritten signatures.

These all help. But they're not in the same league as online voting.

The specter of all the terrible possibilities of a cyberattack halting, changing or simply undermining a U.S. election have not stopped the country's technology-minded from trying. Recently a new(ish) technology has sparked some hope.

Of all things, it comes from digital coins.

VOTES ON THE CHAIN

Hash chains are not a new concept in cryptography. They are, essentially, a long chain of data connected by values called hashes that prove the connection of each part to the next. By stringing all these pieces together and representing them in small values, then, one can represent a large amount of information without doing much. Josh Benaloh, a senior cryptographer for Microsoft Research and director of the International Association for Cryptologic Research, gives the rough analogy of taking a picture of a person, then taking another picture of that person holding the first picture, and so on. Loss of resolution aside, each picture would contain all the images from the previous pictures.

It's only recently that people have found a way to extend the idea to commonplace applications. That happened with the advent of bitcoin, a digital "cryptocurrency" that has attained real-world value and become a popular exchange medium for ransomware attacks. The bitcoin community operates using a specific type of hash chain called a blockchain. It works by asking a group of users to solve complex problems as a sort of proof that bitcoin transactions took place, in exchange for a reward.

"Academics who have been looking at this for years, when they saw bitcoin, they said, 'This can't work, this has too many problems,'" Benaloh said. "It surprised everybody that this seems to work and to hold."

But the blockchain concept is by no means limited to money. It's simply a public ledger, a bulletin board meant to ensure accuracy based on the fact that everyone can see it — and what's been done to it — at all times. It could be used to keep property records, or to provide an audit trail for how a product got from factory to buyer.

Or perhaps it could be used to prove the veracity and accuracy of digital votes in an election.

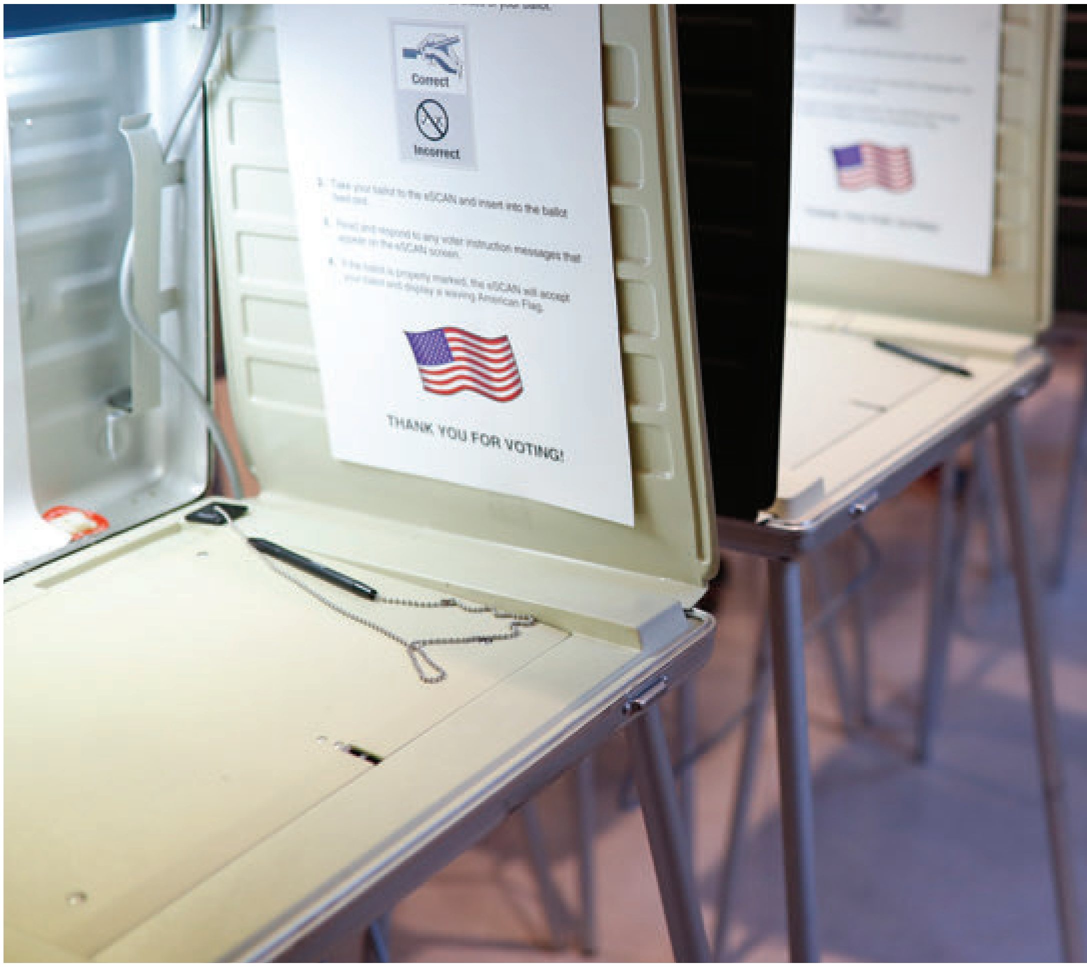
It is a potential solution to the problem of cybersecurity in online elections because the foundation of blockchain is the audit trail: If anybody tampered with votes, it would be easy to see and prove.

And in fact, blockchain elections have already been run in the U.S. — just not in the big leagues. Voatz, a Massachusetts-based startup that has struck up a partnership with one of the few companies in the country that actually builds voting systems, has used a blockchain paradigm to run elections for colleges, school boards, unions and other nonprofit and quasi-governmental groups. Perhaps its most high-profile endeavor was authenticating delegate badges at the 2016 Massachusetts Democratic Convention.

The Voatz idea is to put a spin on bitcoin's approach to blockchain. The company thinks government could limit the blockchain miners — or validating peers, the term Voatz CEO Nimit Sawhney prefers — to a handful of trusted, verified partners. They wouldn't make money from their work the way bitcoin miners do.

"Your incentive to participate is essentially to help democracy and ensure we have better elections," Sawhney said.

The system can also work with paper ballots. Sawhney said his company has written a standard for incorporating those ballots into the blockchain, and in those situations, Voatz would augment the existing systems rather than replace them.



Voatz isn't the only company working on this. There's Follow My Vote, a Virginia-based company with its own blockchain-based platform. Then there's Blockchain Technologies Corp. in New York, and E-Vox in Kiev, Ukraine.

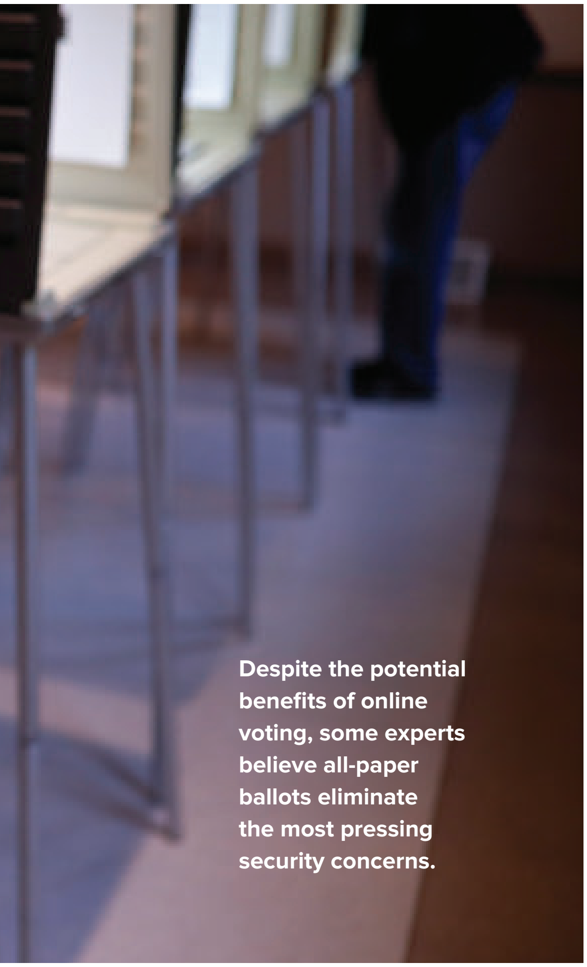
The Estonian government is considering blockchain voting. The Republican Party used it in Utah in 2016 for its primary voting. There are governments eyeing blockchain all around the world.

But for all this enthusiasm, it's hard not to notice the lack of love coming from researchers and academics.

COLD SHOULDERS

Benaloh is pretty clear when he talks about whether blockchain is a good way to hold online elections.

"Blockchains just don't help," he said. "They create ambiguity and uncertainty, they move the power around and they're much more complicated than they need to be."



Despite the potential benefits of online voting, some experts believe all-paper ballots eliminate the most pressing security concerns.

APIMAGES.COM

It's fine for other applications, he said, but when it comes to elections, the stakes tend to be higher. American democracy, and the government built upon it, rests on the assumption that election results can be trusted. Anything that undermines that confidence undermines faith in the government.

Benaloh sees many problems with blockchain. One of them is that the system trusts miners not to ignore votes, and to record them accurately, but he doesn't see a way to actually force them to do so.

"You're not necessarily trusting the blockchain miners to be honest about what they put. They might put something in the blockchain, like a transaction, that didn't really happen," Benaloh said. "So it's not a matter of honesty, it's a matter of agreeing on what's in the blockchain. Not whether what's in the blockchain is true."

And in fact, he can imagine some easy scenarios in which the miners could either be influenced or even have a direct interest in influencing the outcome of the election.

"Suppose the transactions are votes, and I am the leader of a movement to oppose a heavy tax on blockchain miners," he said. "If I'm going to vote in that referendum, then I have to convince some blockchain miner to pick up my vote and put it into the chain. In that case they may know who I am and they may say 'No, I don't want to do this,' and I may be disenfranchised."

Another criticism: There are ways for miners to increase their own influence. Because validating the blocks relies on computing power, if one miner is able to achieve computing power greater than half of the group of miners as a whole, they in effect win the ability to create the majority of the blockchain.

"If you have a majority of blockchain mining power, the most CPU cycles or whatever, you can take the blockchain basically in any direction you want," Benaloh said.

Sawhney says Voatz employs safeguards against these possibilities and that there are measures to find out when a vote is being ignored. As for deliberate misrecording of votes, he said that too would be apparent to all validating peers, and that anybody caught unfairly manipulating the tally would be kicked out of the pool of validators.

One of Rivest's concerns is the simple problem of individual confidence. A person who writes their choice down on a piece of paper can simply refer to the paper if they want to check their vote. A person who votes by a screen can see what their vote was, but they can't see what information that screen actually transmitted to the election authority, or whether that information was tampered with at any step in the process.

Or, for that matter, whether anybody was able to look at their vote.

"It could be that the program on your computer is secretly shipping your information off to a government agency and telling them how you voted," Rivest said.

> "I think we owe it to the taxpayers of the state, if we can make [voting] cheaper then that's money saved for everything else."

Sawhney also believes he's found an answer here. Voatz is specifically made for smartphones and tablets that have security features built in. They can write their programs in such a way as to take advantage of existing tampering-detection features in those devices in order to shut down systems that attackers are trying to work with. Further, mobile devices can offer biometric and pseudobiometric tools like fingerprint checking and facial recognition to ensure that the person using the device is not attempting to vote for somebody else.

Ron Rivest of MIT says in-person voting solves the problem of individual confidence. A person who writes their choice down can refer to the paper and check their vote, a luxury screens don't afford.

APIMAGES.COM

"If you give your phone to somebody else they cannot impersonate you," Sawhney said.

THE UTAH EXPERIMENT

When the Utah branch of the Republican Party decided to use blockchain as a means of allowing online voting in its caucuses in March 2016, virtually all of those problems surfaced.

Just not in a very dramatic way.

The Utah GOP used Smartmatic for the experiment, and ran a somewhat limited version of the concept: It was only used for the vote on presidential candidates, and users had to apply before the caucus date to use the online system. First the party verified their GOP membership and state voter identification, and then they issued those users an encrypted ID number to vote with. Local newspapers reported at least 30,000 successfully applied to use the system, but party spokespeople did not have readily available information about how many people wound up voting online.

The move to try out blockchain, made with very little fanfare on the part of the state party organization, met with instant skepticism from technologists in the press who warned that use of blockchain in voting could cause security issues. On caucus day, the *Salt Lake Tribune* and *Deseret News* both reported that some users couldn't figure out the system and many more had confused the rules about when they needed to sign up or how to cast their vote. Some felt hesitant to use a system where they couldn't see where their vote went the same way they could when they physically inserted it into a ballot box.

Peter Simonsen, who was working on a gubernatorial campaign at the time and has since become the assistant director of the Utah GOP, said those concerns were overblown.

"The upset people are the most vocal," Simonsen said. "When somebody's happy with something, they rarely tell you."

If some people were confused by the rules or had trouble using the system, he said, then the issues are nothing new to voting.

"The same thing can happen at a polling place," he said. "A big stack of paper, and you show them your driver's license and for some reason it's not on the paper — what do you do? It's the same problem."

Following the caucus, the party identified no security concerns with the online system, nor any issues with voting accuracy. Nobody has come forward to challenge the results, he said.

"This was the first time [we] did something like this, and I think they did remarkably well," he said.

Since the experiment, Simonsen said more companies have been approaching the party with different solutions. He's enthusiastic about finding solutions more tailored to multiple races and issues. And for the 2018 election season, he said, the party wants to approach the state about considering online voting in a wider context. He thinks it could save time, as well as money spent on voting equipment.

"I think we owe it to the taxpayers of the state, if we can make it cheaper then that's money saved for everything else," said Simonsen.

ANOTHER SOLUTION, ANOTHER PROBLEM

Rivest and Benaloh both talk about another online voting solution with much more enthusiasm. And much in the spirit of academia, the technology's name is pragmatic rather than sleek and buzzworthy: end-to-end verifiable Internet voting (E2E-VIV).

It's not too far off from blockchain in spirit, but it relies on a centralized approach instead of a decentralized one. Votes are sent from remote electronic devices to the election authority, most likely the secretary of state for the state the person is voting in, and posted online in an encrypted format. The person voting can use her decryption key to check that her vote was recorded accurately.

But there are no validating peers, no chain of blocks stretching back to the first vote.

"It's much cleaner, it's much easier, and it's also much more accountable," Benaloh said.

Even so, both Benaloh and Rivest think E2E-VIV isn't ready yet either.

The first reason? Cybersecurity.

Actually, one of the biggest concerns about E2E-VIV is one that would also apply to blockchain, or any other online voting system: denial of service attacks. These types of attacks use Internet traffic as a weapon, overloading systems with so much activity that they simply move too slowly to perform their intended functions. It's the same kind of attack that took down Dyn.

Imagine, for example, a presidential election in California. The state is notoriously Democratic, but that's largely a product of the state's urban areas — there are people in rural areas just as conservative as anywhere in the country. So if hackers were to perform a denial of service attack in just one area, like San Francisco or Los Angeles, they could be sure they were blocking mostly Democratic votes.

"Suddenly you've taken California and turned it into a red state, just by limiting the vote in a few parts of the state," Benaloh said. "And we don't really know any way of addressing that."

Or, one could target the more conservative areas of Texas to turn it blue. Or one could nudge Florida a certain way. Or Ohio, or Pennsylvania, or Michigan.

Nevertheless, that's the horse Benaloh is betting on. Meanwhile, say Rivest and others, there's always paper.

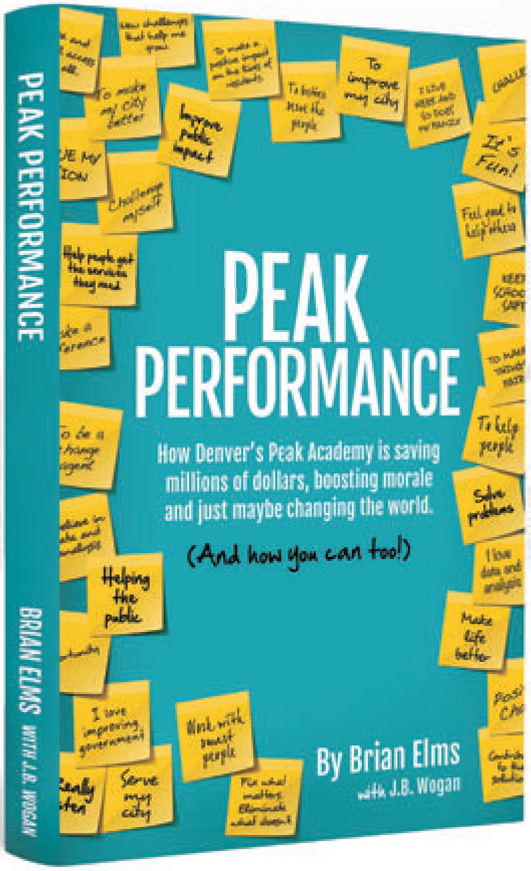
Sawhney takes a different stance. To him, it's unreasonable to think that the country can continue to leave voting machines disconnected.

In other words, he's ready to move forward.

"You have to build resilient systems that can connect to the Internet and survive in the face of these threats," he said.

First, there's a minor mountain in the way.

bmiller@govtech, twitter@BenArnoldMiller


PEAK PERFORMANCE
PEAK PERFORMANCE
How Denver's Peak Academy is saving millions of dollars, boosting morale and just maybe changing the world.
(And how you can too!)
By Brian Elms with J.B. Wogan
BRIAN ELMS WITH J.B. WOGAN

TEST-TUBE SECURITY

CAN UNIVERSITY RESEARCH LABORATORIES UN

2016 was a banner year for cybersecurity events: the hacking of the presidential election by Russia; the theft of NSA cybertools; the revelation of Yahoo's data breach with 1 billion accounts exposed between 2012 and 2014. This year is proving to be just as active, and that means cybercrime is becoming increasingly costly for industry and government.

The financial loss from cybercrime in the U.S. exceeded $1.3 billion in 2016, a rise of 24 percent, according to a report issued by the FBI's Internet Crime Complaint Center. Worldwide spending on security-related hardware, software and services reached $73.7 billion, according to IDC, an IT research firm. That number is expected to hit $90 billion in 2018.

While private companies race to keep up with the latest cybercrime tactics, the nation's universities are also doing their part, conducting research into the vulnerabilities that exist in current computers and systems. More importantly, they're looking at ways to engineer the next generation of technology so that it's easier to defend against attacks.

More than 80 universities around the country have cybersecurity degree programs, but a handful are conducting advanced research in the topic. Schools like Carnegie Mellon, Johns Hopkins, Indiana,

SHUTTERSTOCK.COM

LOCK THE SECRET TO BETTER CYBERSECURITY?

BY EYRAGON EIDAM

Syracuse, Nebraska-Omaha and Florida State are among a cadre of top-tier universities that are attracting some of the best minds to delve into cybersecurity research.

To find out what is going on in the field of cybersecurity research and where it is headed, *Government Technology* spoke with three renowned professors who are experts in the field of cybersecurity: Deepak Khazanchi, associate dean of Academic Affairs for the University of Nebraska at Omaha; Professor Shiu-Kai Chin of Syracuse University; and Professor Xiuwen Liu of Florida State University.

Khazanchi is the associate dean of Academic Affairs for the University of Nebraska at Omaha (UNO), a university that prides itself on its steadily growing cybersecurity program, technical prowess and applied research, not to mention being a National Security Agency Center of Excellence in both cyberoffense and cyberdefense.

For Khazanchi, there is no easy answer to what might come next with cyberthreats, only looming challenges presented in several different places. The massive web of connected devices known as the Internet of Things (IoT) is a major issue. It shouldn't come as any surprise that IoT is under anyone's microscope; but it's the scale and complexity of IoT that concerns Khazanchi.

The sheer number of devices that make up the IoT are a cause for alarm, according to Khazanchi. Of particular concern are the devices and structures never meant to be connected, like older infrastructure, dams and power plants.

"Those act as a challenge for security in the future," he explained. "There is so much computing that is being embedded into our infrastructure and into our

“THE INTERNET OF THINGS IS REALLY A GLOBAL AND CONTROL AND COMMUNICATIONS SYSTEM ANY SECURITY CONCEPT OF OPERATIONS.”

Researchers at New York’s Syracuse University are looking at the Internet of Things and “assurance by design,” making sure security is built into systems from the start.

SHUTTERSTOCK.COM

lives, but the problem is that as everything gets more and more connected in terms of devices and people, security becomes even a bigger problem.”

The value placed on the data these devices put out is unquestionably enormous, especially where it comes to monitoring bridges or dams, where inspections might not be possible due to funding or staffing limitations. UNO is looking at how to secure the nation’s aging, and now connected, infrastructure, which was never designed to be connected to the Internet in the first place.

Keeping the bad guys out of critical networks is an obvious part of this discussion, but Khazanchi said the challenge is making sure hardware and software are engineered with security in mind. The old ways of building an application or entire system only to tack on security later allows for vulnerabilities from the start and is not sustainable.

Deepak Khazanchi, associate dean of Academic Affairs at the University of Nebraska at Omaha

UNO is focusing on how to build security assurance into hardware and software. Khazanchi has no delusions about the scope of this task, but he considers it critical. For this reason, the university is looking at developing some interesting new tools.

One area cyber-researchers are focusing on is the procurement and automation of software security compliance, or what the university calls “assurance-based software engineering.” The idea is simple: Design a system that not only knows the regulations, but also holds new software accountable before ever being implemented.

Researchers are also looking at where compliance automation can be applied to open source software code, explained Khazanchi. Open source libraries, many of which have NIST-recognized vulnerabilities, are a popular source for bits of code that ultimately make their way into the value chains of larger, more critical code.

By creating “systematic mechanisms” that coders can use during the software development process, university officials believe the security of open source code could be greatly improved. “Not all vulnerabilities are killers, but at least you know where they are,” said Khazanchi.

At New York’s Syracuse University, Professor Shiu-Kai Chin and his colleagues are also thinking about the implications and ramifications of IoT. He describes IoT security like blocks of Swiss cheese, with plenty of holes.

“The Internet of Things is really a global command and control and communications system without any security concept of operations. So, that’s the problem,” he said.

While there are obvious vulnerabilities in the system, Chin takes a somewhat optimistic view of the situation and explains that lining up all of the holes in IoT for some massive attack is not impossible, but highly unusual.

“The fear is that somebody could manipulate all of the blocks of cheese for a straight shot to the heart of society and that’s very difficult,” he said. “To get everything to line up at a particular place and time under a particular set of circumstances under somebody’s control — we can’t completely rule it out, but that’s like the government conspiracy: It requires

COMMAND WITHOUT

a high degree of capability that is really quite unusual and unpredictable."

As for the general state of cybersecurity, Chin described IT's current cyberweaknesses like the shanty towns that preceded the big cities in New York, Hong Kong and San Francisco. There were no building standards or safety codes, and eventually a fire, earthquake or hurricane hit, forcing people to do things a different way.

Chin — whose area of expertise is mission assurance — agrees that cybersecurity needs to be included in the design process, as well as part of the organizational culture.

"I hate blaming users for problems they didn't create because we did not design these particular systems with authentication and authorization in mind from the very start. Users are unprotected and they have to think at this level. That really can't be the ultimate state of affairs," he said.

Chin said cyberthreats are continually evolving with the technology, but are especially troubling when it comes to the increased focus on capturing what are called "root credentials" — basically, an organization's master key. Whether obtained through social engineering methods, like phishing, or direct hacks, once those credentials are in the open, it becomes harder to contain the attacks.

"Once you have lost the guarantee of integrity, your entire organization is at risk," he explained. "What that really means is people at the very top, if they get phished or harpooned or spearphished, however you want to say it, then an organization is in deep trouble."

Syracuse is also researching "assurance by design" and how to make sure security is built into systems from the start. "There is no single tool that will make things go away, it's a culture and a willingness to not only do the right thing, but the enforcement to see that the right things are done and an understanding of the standards as well as the technology, the education and training to do it," said Chin.

Xiuwen Liu, professor of computer science, Florida State University

Despite these harsh realities, state and local governments have options. Chin recommends organizations think long and hard about their mission, how they complete it and what the acceptable losses are. With those questions answered, he said, they can move forward in protecting the priorities and focus on accountability throughout the entire organization.

Florida State University is also looking at the relationship between the Internet of Things and cybersecurity — especially where it relates to critical infrastructure like the country's increasingly connected power grid. While FSU Professor Xiuwen Liu acknowledged the danger of unsecured, connected devices, he takes a more measured perspective on the situation.

"I think sometimes people spin the story too far," he cautioned. "For example, when you have a bridge, and it isn't connected to anything, then the structural elements of the bridge are safe; whether it is connected or not is not going to affect the safety of the bridge. In order to affect the safety of the bridge, physics has to be involved."

Where the power grid is concerned, FSU researchers with the Center for Advanced Power Systems study and test the power grid and equipment through simulations. When researchers conduct probes and analysis, they are better able to predict threats and defend the critical infrastructure.

Despite his focus on cybersecurity, Liu doesn't believe in easy fixes, or even permanent fixes, for that matter. In no uncertain terms, Liu said that some things just cannot be done. "No matter what you do, cybersecurity in some sense has its own intrinsic limitations. In theory, you just simply cannot design a system that is secure," he said. "Systems can be designed to prevent known threats and different kinds of threats, but you can never write a program saying this program can prevent all threats."

There are options for making the Internet and all things connected more secure, but it would come at the cost of openness. For example, the Internet might become more secure if the government were to step in and take control, but he countered, "people do not want that."

Given all the promising research taking place at major universities around the country, the sobering reality is that there likely never will be an end-all solution to the cybersecurity problem. While government could one day see artificial intelligence defend its networks and critical infrastructure, technology is not there yet. The evolution of new technology will continue to allow unintended access into guarded systems, and the best government can do is develop a culture of vigilance and awareness.

"Cybersecurity is an important area, but some of the problems are technical and some of the problems are in awareness," said Liu. "I think many times, people who may not have the technical background ... they may not realize they are connected to the world and others may have access. That kind of awareness is probably a bigger problem in terms of securing the Internet."

A government technology Case Study | AT&T

So Many Threats, So Little Time

Despite a small budget and staff, the Brevard County Tax Collector protects an enormous amount of financial data with the help of AT&T security services.

Brevard County, Fla., stretches approximately 72 miles along the state's eastern coast, from Titusville in the north to Melbourne and Palm Bay in the south. The size of the county means government offices within it serve many customers and manage a large number of transactions.

Despite the county's size, the Brevard County Tax Collector's office relies on just four IT personnel to see to it that citizen tax data is protected. The office is responsible not only for the network within its headquarters, but also for networks in six satellite offices located throughout the county.

Over the last few years, Rhonda Thomas, Chief Information Officer for the Brevard County Tax Collector, has grown increasingly concerned about cybersecurity.

"As a government tax agency, we tend to be a target for cybersecurity threats," says Thomas. "We have a fiduciary responsibility to the public, so we need to make sure we are protecting our data."

Thomas wanted to improve her office's ability to monitor its networks and manage cybersecurity risks. But without the ability to grow its IT headcount, the county needed help.

"When you have a small staff, you have to find technologies and services that can augment what you're able to do," says Thomas. "We didn't have a group of 10 network analysts and programmers to develop a solution in house."

Brevard County has been engaged with AT&T for a long time, so it was natural for the Tax Collector's office to turn to AT&T for assistance. After examining the office's needs and requirements, AT&T implemented its Vulnerability Scanning Service, Security on-Demand and Threat Manager – Log Analysis.

A 24-hour security guard

Managed security services from AT&T greatly reduced the amount of time and effort Brevard County Tax Collectors' IT staff spend on protection and monitoring. Today, as the office collects data logs, they are automatically run through AT&T security analyzers, which highlight any suspicious activity. Anything abnormal is isolated and vetted by AT&T's Threat Manager – Log Analysis to determine whether it warrants a closer look.

Thomas says going through all that data internally would take her staff weeks.

"We'd need many more people than we currently employ just to be able to keep up with looking at network logs, firewalls, routers, servers, etc.," says Thomas. "And by the time we could even collect all of that data, it would be too late. AT&T helps compile all of it and informs us of anything suspicious. We are able to draw on their existing knowledge and analytical skills. Ultimately, it gives me access to a whole slew of IT security people that help me do my job."

Meanwhile, AT&T's Vulnerability Scanning Service helps the county conduct vulnerability assessment and management.

"Nearly everything we use today has an internet connection, whether it's a printer, a fax machine or scanners," says Thomas. "Now every time we put something on the network we can determine if that product is secure enough. If it's not, we are alerted and receive suggestions on actions we can take to better protect ourselves."

For example, if a piece of software needs an update or printer software contains a security vulnerability, the system identifies those issues and provides Brevard County Tax Collector IT personnel details on how to correct it, including vendor information and, in some cases, a phone number to call.

The network visibility AT&T's solution provides has proven invaluable to the Brevard County Tax Collector. For example, if someone attaches a new product to the network, Thomas and her staff are alerted. They can then track where the new product came from and determine whether it's legitimate or not.

The AT&T security system also gets more intelligent as the county uses it.

"The more data AT&T collects, the more they're able to determine what's normal for us," says Thomas. "The abnormal stuff is highlighted more quickly because AT&T builds a track record of our network behavior."

Making the most of limited resources

Collaborating on security with AT&T also enables the Brevard County Tax Collector's office to make the most of its limited resources.

"The ability to monitor and respond to security threats 24x7x365 is a complex and time-consuming task that a lot of customers cannot provide themselves," says AT&T Strategic Account Lead Thomas Gill. "This was about figuring out how to offer the best value to the Tax Collector for the limited budget and staff they have."

For Thomas, AT&T's security solution was a more viable proposition than hiring new IT security personnel.

"Hiring a good security analyst today is a very expensive proposition, especially for a small agency," says Thomas. "IT security people are in huge demand right now, so they are difficult to find. Then, you have to deal with training and turnover. When you start adding that all in, the product basically ends up paying for itself."

With AT&T's managed security solution, Thomas now has the strength of an entire analytical staff behind her. The county also meets with a dedicated AT&T security analyst monthly to review any needs, changes or important considerations.

"He lets us know how we're doing and discusses anything they see that we need to address," says Thomas. "They help pinpoint where we need to focus our attention so I can better utilize my own resources."

Ultimately, the AT&T solution provides security services that are managed around the clock, allowing Brevard County Tax Collector IT staff to focus on other critical operational duties.

AT&T's security solutions will also enable Brevard County to better prepare as the security landscape evolves. As new cybersecurity threats emerge, the county is alerted and can take proactive steps.

"It's a big help to have somebody in your corner that's able to provide that type of critical information," says Thomas.

> "AT&T helps compile all of [the information we need] and informs us of anything suspicious. We are able to draw on their existing knowledge and analytical skills. Ultimately, it gives me access to a whole slew of IT security people that help me do my job."
>
> – Rhonda Thomas, CIO, Brevard County Tax Collector

Steve Sedore, executive director of operations, Allegan County, Mich.

Small Towns, Big Risks

Small to mid-sized local governments struggle with cybersecurity. Here's how some are confronting the threat.

On Feb. 25, 2016, a civilian employee in the Sarasota, Fla., Police Department clicked on an attachment to an email. Instead of opening a document, the worker inadvertently launched a ransomware attack that encrypted 160,000 city files and triggered an extortion that demanded up to $33 million in the virtual currency known as bitcoin to unlock them.

The situation was so dire that the city's IT department literally had to unplug the city's computer system and then spent the following night getting rid of the malware and restoring its systems. City IT Director Herminio Rodriguez later told city investigators, "In 25 years, that was the worst disaster I've ever encountered. It was an end-of-life event from the IT perspective."

Sarasota, population 56,000, and its IT department weathered the attack. But smaller governments haven't been so lucky. In Cockrell Hill, Texas, a small city of 4,200, a ransomware attack back in December 2016 encrypted all the files in the police department. When the department refused to pay the $4,000 ransom demand, the department's records, dating back to 2009, were lost.

Ransomware is just one type of attack on local governments. Other incidents involve breaches to gather information, such as personally identifiable information and credit card numbers, which can be used to commit fraud, for example. Whether the attacks are intrusions or breaches, their number and sophistication are increasing.

Nearly 40 percent of local government CIOs report experiencing more attacks during the last 12 months, according to a 2016 survey by the International City/County Management Association (ICMA). And the frequency is increasing too, with 26 percent of CIOs reporting an attack, incident or breach attempt occurring hourly, while another 18 percent report a cyberattempt at least daily.

That's bad news for local governments, which have fewer resources than many larger jurisdictions to fight back. But it's especially bad for small to mid-sized cities, counties and towns, which may have only one full-time person devoted to IT — including cybersecurity — if they are lucky.

By Tod Newcombe

JAMIE BROKUS FOX

Local governments are attractive targets for cybercriminals for the valuable data they store, and the fact that many are connected to state systems and big networks, where the quantity and quality of data is likely to be greater. And in a few cases with small jurisdictions, local governments are attractive targets because some are willing to pay the extortion fee to regain access to their records.

Lou Romero, e-gov cyber liability and risk practice lead at Pivot Point Security, surveyed nearly 200 municipalities in New Jersey, and what he found out was both sobering and worrisome. "Take passwords. I found that 78 percent of municipalities don't have an adequate password management policy," he said. "That means the majority of the passwords never expire and they typically use six characters."

Romero ticked off other troublesome statistics: 97 percent of the municipalities he surveyed don't have a well-documented disaster recovery plan; 46 percent store their backup files and records onsite rather than offsite or in the cloud; and 90 percent of local governments don't bother to encrypt sensitive emails. These kinds of basic cyberhygiene mistakes indicate a lack of preparedness, especially among smaller local governments.

Local governments, in general, tend not to outsource cybersecurity operations — 61.8 percent keep it in house, according to ICMA. But as local governments get smaller in size, the inclination is to outsource all IT operations, including cybersecurity, according to Romero. A 2015 survey of 200 small local governments in Washington state by the nonprofit Municipal Research and Services Center found that a majority of respondents didn't have any staff members dedicated to IT or cybersecurity. While most did use some kind of anti-virus protection and email security, only about 25 percent of the local governments surveyed reported updating their security policies on an annual basis.

The lack of good policies and practices can be traced to some fundamental

Paying the Price

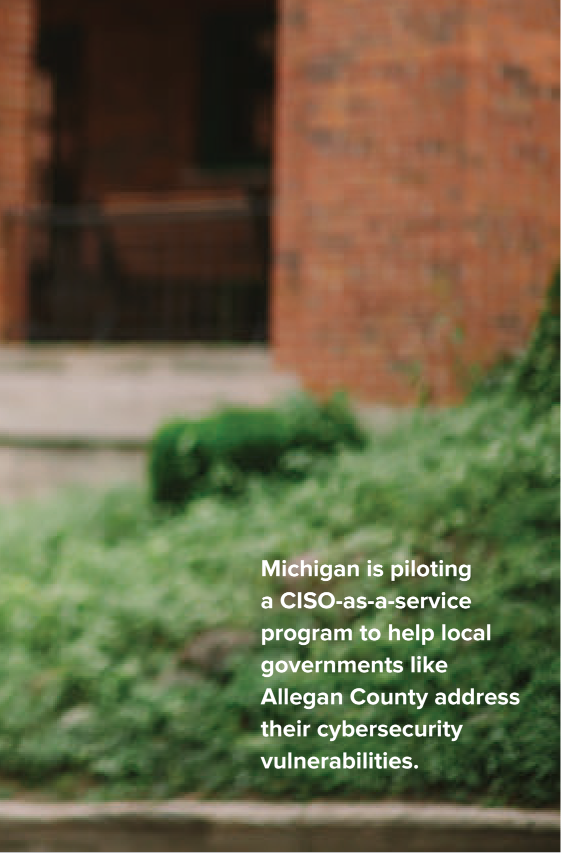
IN JANUARY 2017, Licking County, Ohio, was hit with a massive ransomware attack, affecting more than half of the county's servers and locking up and encrypting data. Even the phone system was crippled, impacting the county's 911 system. The hackers demanded 28 bitcoins, or the equivalent of $30,000, in order for the county to access its information and resume operations. By the time county tech workers discovered the malware, they had a choice: Pay the ransom or use backups to recover the data and work through every system and delete the malicious code. They opted for the latter, and while most county operations were slowed for nearly two weeks, after the initial recovery, most vital systems were back online.

Licking County, Ohio

"We thought we were pretty good," said Licking County Commissioner Tim Bubb. "We found out we weren't as good as we thought."

Bubb hopes that others can learn from their experience, and a neighboring county is taking that message to heart, working to protect itself from potential ransomware attacks. On July 18, Franklin County, Ohio, approved the purchase of a $140,000 cyberinsurance policy that included extortion-specific protections. "It just makes sense in this day and age to expend the funds to make sure we have protections in place," explained Franklin County Administrator Ken Wilson. "We want to be able to be in a situation where we aren't reactive … but proactively protecting ourselves."

The rise of ransomware, a type of malicious software that invades computer networks and encrypts data until a ransom is paid, has been exponential. The bugs often take advantage of older operating systems with security vulnerabilities. "Every government level is going to be a target because they have



Michigan is piloting a CISO-as-a-service program to help local governments like Allegan County address their cybersecurity vulnerabilities.

JAMIE BROKUS FOX

problems that plague government at every level. "We just don't have the resources to do this kind of thing," said Steve Sedore, executive director of operations in Allegan County, Mich. Those missing resources include: lack of funds; insufficient cybersecurity staff; inability to pay competitive salaries for security talent; lack of training; and lack of end-user accountability and awareness.

The less rigorous a local government's cybersecurity practice is, the more challenging it becomes to reduce risk. And that's a problem that has caught the attention of the cyberinsurance industry. While the market for cyberinsurance has matured in recent years, municipalities will pay a hefty premium for a policy if their cyberhygiene isn't up to snuff. Some experts argue that the money on insurance might go to better use providing more robust protection.

Lack of good cyberdefenses, policies and practices raises an even more troubling issue for any local government that uses the bond market to pay for capital projects, such as new sewers, schools and roads. A cyberattack could end up lowering a government's credit rating. While no government yet has been downgraded because of a cyberattack, S&P analyst Geoff Buswick told *Governing** magazine in June that the risk is real, "particularly for smaller governments with less financial flexibility." According to Buswick, cyberattacks can cost a lot, including taxpayer trust. That, in turn, can hinder a government's ability to raise taxes.

For small local governments, getting a handle on cybersecurity issues starts with information. Knowing what your vulnerabilities are allows a local government to direct its limited resources toward the weakest link in the chain and beef up security. For example, many municipalities that operate with just a handful of employees often outsource their payroll services, credit card processing and other basic administrative functions. Yet few small-sized municipalities conduct the due diligence on the robustness of the security of these third-party providers or try to find out if the contracts include contingencies if the provider suffers a data breach. One answer is to conduct such due diligence or hire a firm to carry out a third-party risk assessment.

Another valuable source of information that local governments often lack is data on the effectiveness of their security controls. The solution is to conduct an audit that includes penetration testing of cyberdefenses. But that can be very expensive. For help, local governments have turned to state governments, and some have responded. Washington state earlier this year began offering free cybersecurity audits to more than a dozen municipalities. The state pays for the tests through an initiative approved by voters in 2014 that has allowed the state auditor to appropriate approximately $20 million for various performance audits, including cybersecurity.

Michigan is another state that is making a concerted effort to ease the burden of cybersecurity on its more than 1,300 local

tons and tons of data," said Erin Ayers, editor for Advisen Ltd., an insurance company. Ransomware is "prevalent enough of a threat that most sophisticated cyberbuyers are not buying coverage if it does not have some kind of recovery for ransomware."

Cyberinsurance policies increasingly include ransomware protections that can be used to help recover losses that otherwise result in business disruptions or actual ransom paid. Ransomware insurance usually takes the form of a "separate extortion endorsement that is added to a policy if you want coverage for ransomware," explained a representative from the National Association of Insurance Commissioners (NAIC).

One issue for the widespread adoption of ransomware extortion riders is the lack of standardization in cyberpolicies. Because the industry is still in its relative infancy, there are a number of criteria buyers need to abide by in order to ensure their policy covers cyberattacks. For any public agency looking to purchase cyberinsurance, NAIC recommends doing your research beforehand, understanding what you're getting and asking lots of questions.

While updating its cyberinsurance policy, the Indianapolis Airport Authority recently included protections against ransomware attacks. Senior Director of Information Technology Reid Goldsmith said the move was spurred by a ransomware incident in nearby Madison County, Ind., in late 2016. The county eventually paid more than $200,000 for data recovery services and offsite backups. Goldsmith took a lesson from that, and ensured that ransomware "was top of mind when we were discussing a cyberliability policy."

But no cyberstrategy, even one that includes robust protections backed up by cyberinsance, is foolproof. "It's like you live in a house with 1,000 doors," Bubb said. "If one is left cracked open, that's enough for a break-in."

— RYAN McCAULEY

governments. For three years, the state has had a squad of volunteers, known as the Michigan Cyber Civilian Corps, or MiC3, standing by, ready to provide technical assistance if the state gets hit with a crippling cyberattack.

But MiC3 has yet to be deployed. This year, state officials are pushing the state Legislature to pass a bill that would broaden the scope of MiC3 so it could help local governments, as well as nonprofits and businesses.

More proactively, the state has also launched a pilot program with five local governments to test whether a chief information security officer (CISO) can operate as a shared service. The idea is to have a certified, trained cyberprofessional who could help local governments that lack such expertise, according to Allegan County, Mich.'s Sedore.

"The proliferation of attacks has reached a height that you can no longer sit and wait. You have to proactively put measures in place to reduce the risk level."

The program starts with an audit using an assessment tool that identifies what critical controls Allegan should have in place. Eventually the pilot will identify what proper procedures and policies should be in place to mitigate potential cyberissues.

"The state has agreed to be the parent to this program, and through their funding, they have hired a CISO to provide a shared service role," said Sedore. "The objective is to find out how we can tap into the CISO-as-a-service to address specific cyberconcerns."

After 18 months, if the pilot generates evidence that the shared service approach is beneficial for local governments, then Sedore thinks the effort could become a full-fledged program. That, of course, would require a sustainable funding mechanism, as well as a sustainable business plan, according to Sedore. "It's been a great program so far and we have all progressed in a very short period of time," he said.

Sedore cited lack of cybersecurity knowledge as a big challenge for his small IT staff. General county employees also lack a good awareness about cybersecurity risks. Another challenge is auditing and logging of incidents. Again, better information can generate better defenses. But without that data it's hard to be proactive. "The proliferation of attacks has reached a height that you can no longer sit and wait," he said. "You have to proactively put measures in place to reduce the risk level. Having a CISO-as-a-service is one of the key measures that can make a difference for a small local government."

For some smaller local governments, the importance of good cybersecurity crystallizes when a breach occurs, systems are impacted, files aren't available and the network is shut down. Several years ago, a cyberattack hit the city of Sugar Land, Texas (population 87,000), forcing city officials to confront an issue that had received little attention in the past.

The result: The city now has its first CISO. Anthony Leatherwood's title is officially manager of IT operations, "but my background is cybersecurity," he said.

The attack was a wake-up call to city officials. "It really impacted the network," explained Leatherwood. "After that, one of the initiatives was to better secure the city, so I came in, started locking things down, putting controls into place."

Leatherwood said the most frequent type of cyberincident involves phishing, including ransomware attacks. Viruses are another concern and hard to control in today's world of Web services. "Everyone wants to deploy their own types of applications, which means trying to get a security architecture review [of the software] before it is deployed," he said. "That's a challenge for local governments."

Leatherwood also cited the open government trend as another example of how access to information has changed as demand for transparency has increased, yet it has also made it easier for the "bad guys" to access information that can be exploited. "If you scan any website, you can pick up on how to reach the city officials and workers. That's information that any private-sector firm would guard from exposure. But we have all these distribution lists out there," he said.

To cope with the ever-growing challenges, Leatherwood operates much like any CISO working for a large government organization. He runs awareness training to keep city staff alert to the latest in phishing exploits and to reduce mistakes; he has built up a layered defense, involving several different vendors; and he is partnering with the Department of Homeland Security to start a project that will give the city's supervisory control and data acquisition (SCADA) systems better defense. "It may mean going with a system that may cost a little bit more money, but it will mean better security," he said.

Despite having been a victim of a cyberattack, Leatherwood said it is still a challenge to keep cybersecurity front and center as a priority. "Senior officials are aware [of the problem], but they are not aware enough. The awareness level has risen, but not to the point where it is part of every decision."

Leatherwood is not alone on this issue. Only 20 percent of local government CIOs believe their top appointed managers are exceptionally aware of cybersecurity risks, according to ICMA.

"We need to stay on top of this," said Leatherwood. "You have to keep it at the forefront of everybody's mind. Security is no different than cops and guns. If you want to consider your city safe, it can't just be about cops, guns and bullets. It's got to be cybersecurity as well."

**Governing* is part of e.Republic, *Government Technology's* parent company.

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™

Beyond the Cyberheadlines

We break down the biggest cyberevents from the past year.

By Zack Quaintance

When Stanton Gatewood, Georgia's chief information security officer (CISO), started out in cybersecurity more than 30 years ago, co-workers thought of him and his peers as "the paranoid ones," constantly warning about the risks of cyberattacks and system breaches.

This perception has changed a great deal. Cybersecurity events are ubiquitous in today's news, and breaches are wide-ranging, affecting customer data at Target, the municipal website in Flint, Mich., and the servers of the Democratic National Committee during the presidential election. Cyberdefenders like Gatewood have gone from "the paranoid ones" to vital lines of defense, heavily relied on by private companies, nonprofit groups and, increasingly, governments.

"You can't open the paper, you can't go online, you can't watch TV without hearing that some sort of cyberevent has taken place," Gatewood said.

Georgia is currently investing heavily in defense, building a cyber and innovation training center (See *Uncharted,* page 16) aimed at enhancing its workforce, bolstering training and bringing representatives from all levels of government to practice on a cyber-range, where they can test defense skills and abilities.

And Georgia is not alone. Technologists in jurisdictions across the country say recent global cyberattacks are catalysts for policymakers and other officials to devote funds and resources to defense.

"I hate to gain on the pain of my peers," said Mike Dent, CISO of Fairfax County, Va., in the Washington, D.C., metro area, "but the more people understand the threat, the more leadership will invest in it."

Dent, whose jurisdiction has been lauded for cybersecurity work, emphasizes this is a complex and evolving battle, one requiring institutional awareness, vast collaboration, funding and changes in the way technology is manufactured.

So far, most state and local governments have avoided being victimized by large-scale hacks, but most face ransomware and phishing attempts on a near-daily basis. This is unlikely to stop, with experts saying instead that they expect threats to increase.

"Anytime you have a lot of data at rest, even if that data's not immediately valuable at its face, that data is at risk," said Timothy Blute, program director with the Homeland Security and Public Safety Division of the National Governors Association. "If you've got a lot of data, you've got a target on your back."

Here's a look at some of the biggest cyberevents of the past couple years, and their impacts on state and local government:*

WannaCry

WannaCry is the most infamous example of a worldwide ransomware attack. By targeting systems that ran Microsoft Windows, WannaCry encrypted data and demanded bitcoin cryptocurrency for its release. Launched on May 12, 2017, it infected more than 300,000 computers in roughly 150 countries but was quickly stemmed by a cybersecurity professional in England who found a kill switch. Another factor was that Microsoft had discovered the vulnerability months earlier, subsequently releasing patches. Users who had installed updates were not at risk.

Types of Data Breached:

Any within Microsoft Windows.

Method:

Ransomware.

Direct Impact to State and Local Governments:

Many officials say WannaCry served as an excellent catalyst for working to guard against future large-scale ransomware events. Notable international victims included the United Kingdom's National Health Service, as well as other health-care providers.

What They Say:

"In an organization that may not have backups pre-ransomware, once something like this happens, they always seem to find the money in the budget afterward to go that route."

Brian Calkin, Vice President of Operations, The Center for Internet Security.

Petya/NotPetya

Petya exploits similar vulnerabilities in Microsoft Windows as WannaCry, also demanding a ransom in bitcoins. Petya, however, has greater longevity. After officials thought they'd patched it, a variation dubbed NotPetya began posing a threat. Another difference is intent. WannaCry aspired to sheer financial gain, restoring encrypted data if demands were met. Petya seeks money while also sowing disruption through wide-scale system wipes, regardless of whether demands are met.

Types of Data Breached:

Any within Microsoft Windows.

Method:

Wiper disguised as ransomware.

Direct Impact to State and Local Governments:

Although no major breaches have been reported domestically, Petya/NotPetya is ongoing. Widely believed to have originated in Ukraine through an update to an accounting program used by that country's government, it has affected many systems there, most notably radiation monitoring at the Chernobyl Nuclear Power Plant.

What They Say:

"I know state agencies are watching ransomware events because these techniques have a tendency to come back to life. We saw that with NotPetya."
Timothy Blute, Program Director, National Governors Association Center for Best Practices' Homeland Security & Public Safety Division.

Dallas Emergency Sirens Hack

One Saturday in April, all 156 emergency sirens throughout Dallas sounded more than a dozen times. Officials first attributed the incident to malfunction, later saying it resulted from a hack, albeit a unique one without computers. Unknown culprits likely activated the sirens by replicating a tonal code with a radio. Rocky Vaz, Dallas' director for emergency management, said catching the culprits was nigh-impossible, while Mayor Mike Rawlings vowed to find and prosecute those responsible. No arrests have been made, and the city is working to safeguard the system from another hack.

Types of Data Breached:

None.

Method:

Replicating a tonal code with a radio.

Direct Impact to State and Local Governments:

Officials in jurisdictions across the country say they paid attention to this incident. Dallas, for its part, is working with the Federal Emergency Management Agency on an evolved alert system to send messages to cellphones.

Russia and the 2016 Presidential Election

The U.S. intelligence community has concluded with confidence that Russian agents hacked the Democratic National Committee's servers during the 2016 Presidential Election, also breaching Clinton campaign chairman John Podesta's email account. Russian officials have denied involvement, and President Donald Trump has oscillated between downplaying the significance of the hack and blaming it on his predecessor, President Barack Obama. In the eyes of many, questions remain.

Types of Data Breached:

Democratic National Committee servers and Clinton campaign chairman John Podesta's email account.

Method:

Private email and server hacks.

Direct Impact to State and Local Governments:

Politics aside, local officials who administer elections are faced with questions about the integrity of U.S. election systems.

Local Hacktivism

The past few years have seen a new trend in cyberattacks: news breaks — a water crisis, the passage of a bathroom bill related to transgender people, a police shooting — a government website is hacked and an activist group takes credit. Known as hacktivism, government technologists say it has become their greatest exterior cybersecurity concern, as well it should be. To date, hacktivists have frozen government services, defaced websites and released sensitive data online.

Types of Data Breached:

Varied, including emails between officials, website content and citizen data.

Method:

Various, including email phishing, denial-of-service and doxing, or compiling and posting personal information about government officials online.

*At press time, news was breaking on the Equifax data breach, estimated to affect the personal information of 143 million Americans. While many government agencies use the service for identity verification, direct impacts on government remain unknown.

SHUTTERSTOCK.COM

Serving a Purpose

States look to veterans to help fill the cybersecurity staffing gap.

By Julia McCandless / Contributing Writer

As technology continues to speed ahead, many state and local governments are challenged with an impending shortage of IT talent to fill key positions in areas like cybersecurity. At the same time, CIOs at all levels of state and local government name cybersecurity as their No. 1 priority. To address this challenge, a growing number of states are taking a new approach: investing in veterans returning from active duty to take part in specialized cybersecurity training and fill the growing staffing gap.

Growing Demand

Cybersecurity repeatedly stands out as a top priority for state and local IT leaders, yet in a nationwide survey by the Center for Digital Government,* 93 percent of states reported cybersecurity as a current workforce gap. Numbers are similarly high for cities and counties.

Many states have partnered with local colleges and universities to offer cybertraining or internship programs as a way to attract and filter employees to public-sector roles. Case in point: In Maine, interns take on key IT projects, like writing code and conducting industry research on cutting-edge business solutions. According to state CIO Jim Smith, about 70 percent of interns go on to become full-time employees with the state.

Investing in Veterans

A growing number of states are starting to tap a new talent pool to fill staffing needs related to cyber. It's an approach that makes a lot of sense: A wealth of cybertalent exists among military veterans returning from active duty.

Virginia is looking to veterans to fill its approximately 36,000 open cybersecurity positions. The Cyber Vets Virginia initiative is open to service members transitioning from the military, as well as their spouses and National Guard members, and offers free cybertraining for about 200 participants in the state. Through the program, veterans can train with top corporations like Amazon Web Services, Cisco, Yyotta and Fortinet.

The state also offers apprenticeships and sponsors the Virginia Cybersecurity Public Service Scholarship Program, which awards cybereducation funds to students committed to working in a state agency or institution. Virginia is also among select states partnering with the SANS Institute to offer a free online aptitude course called CyberStart to help drive students to cyberpositions.

Karen Jackson, Virginia's secretary of technology, notes that reaching out to veterans is just one piece of the staffing puzzle. "We have to continue to be creative and create more opportunities to get people into the cyberpipeline. People coming out of the military generally have some kind of IT experience," she said. "Now we want to take a continuum — put in place programs that cast the net even wider to those who don't already have an IT background."

In Washington state, officials are also looking at veterans as ideal candidates for cyberjobs. The state has partnered with the University of Washington to offer scholarships to veterans seeking cybersecurity degrees, and the Washington International Trade Association offers opportunities for veterans to retrain themselves for cyberwork in the public or private sector. The state also partners with local colleges on online certification programs that could help jumpstart a veteran's retraining for a position in the cybersecurity field.

"Our veterans make great employees because they understand discipline and technology they’ve learned in the military,” said Washington Chief Information Security Officer Agnes Kirk. She also pointed out that many veterans find the transition to the public sector easier than to the private sector because of the work-life balance offered. “The private sector has a bit of a reputation for chewing through their IT people,” she said. “It’s a different mindset. It’s hard to learn a new business that way.”

Colorado recently launched a Veterans Transition Program, a paid internship for veterans with backgrounds in cybersecurity or threat intelligence seeking training for the next phase of their career. The state has partnered with the Colorado Department of Labor and Employment and veterans organizations to fill 10 internship positions. The program is designed to help veterans with military experience make a smooth transition to a cybersecurity career.

As chief information security officer at the Colorado Governor’s Office of Information Technology, Deborah Blyth points out that while it’s hard to compete against the private sector’s high salaries, public service is often a good match for veterans. “They are great candidates to come to state governments. These are individuals who like to be in positions where they feel like they’re making an impact and don’t want to move around. They are coming out of the military with skills and knowledge that translate to my environment, but their resume doesn’t draw that line of distinction,” she said. “I think they’re a perfect fit, and I can train them in the pieces that are unique to my environment.”

> “Our veterans make great employees because they understand discipline and technology they’ve learned in the military.

Looking Ahead

While the trend of investing in veterans to fill cyberpositions is growing, many agree that it’s just one element of the solution to the larger challenge of nurturing cybersecurity talent in the numbers that the field needs. “The entire bubble keeps getting bigger. There are supposed to be about 1.6 million open cyberjobs by 2020,” said Jackson. “The problem is that the need is growing much faster than we can impact the supply.”

While pointing veterans toward cyber doesn’t solve the whole problem, it’s an effective way to make a dent. “There’s no one solution to fix a problem,” said Kirk. “Retraining our veterans is a super-important aspect. It could make a significant difference. We owe our veterans the opportunity to have great paying jobs and take advantage of things they’ve learned, and these are great programs. It’s a win-win.” gt

julia@aftonink.com

*The Center for Digital Government is part of e.Republic, *Government Technology’s* parent company.

government technology
GOVTECH TODAY
TOP STORIES
Rise of the chatbot
Increasingly diverse group of public agencies are deploying automated chat platforms to assist users online. READ MORE
Rural Broadband: Taking a Broad-Scope Look at State Legislation
Broadband Internet access has been a focal point for legislators across the U.S. In 2017 sessions alone, many states have taken their own shot at crafting pro-access legislation. READ MORE
Report: Funding, Focus Are Issues as Agencies Eye Internet of Things
A new survey from Northeastern University-Silicon Valley highlights issues public agencies may face as they contemplate Internet of Things initiatives. READ MORE
10 Cities Taking a Nature-Driven Approach to Innovation
READ MORE
MORE HEADLINES
Did Maine Mistakenly Defund its Office of Geographic Information Systems?
Pilot Project in Montgomery County, Ohio, Brings Cognitive Computing into Juvenile Court Cases
Eye on Cybersecurity: 6 Priorities for Investment and

cio central

Read full reports and breaking news about career changes across tech-driven roles in government at **govtech.com/people.**

Los Angeles County Picks Bill Kehoe to Lead IT

After serving as King County, Wash., CIO for seven years, **Bill Kehoe** will move down the coast to serve in the same capacity for Los Angeles County. He replaces Richard Sanchez, who retired from the position in 2016, ending a 40-year career in public service. Kehoe is poised to be more than capable in his new role given his success in King County, which took first place in the Center for Digital Government's* 2017 Digital Counties Survey.

NEW CIO NAMED BY MICHIGAN

On Aug. 30, Michigan Gov. Rick Snyder appointed **David DeVries** as state CIO, after DeVries most recently held that position in the U.S. Office of Personnel Management. DeVries' new role also includes directing Michigan's Department of Technology, Management and Budget. He replaces former Michigan CIO David Behen, who stepped down in June for a private-sector position.

"David's efforts to modernize aging IT infrastructure and improve cybersecurity at the federal level highlight his wealth of skills and experience that make him an excellent fit for this role," Snyder said in a press release.

Inaugural Government Experience Awards Look Beyond the Website

For the last 20 years, the Center for Digital Government celebrated the successes of governments big and small through the annual Best of the Web and Digital Government Achievement awards. But the time has come to pivot to a new way of looking at good government. This year, the Government Experience Awards take over, putting customer experience center stage in a new program honoring governments with the broadest possible definition of what it means to be digital. Utah, Oakland County, Mich., and Denver took first place in their respective categories for their outstanding connections with constituents across digital platforms. For our full awards coverage, visit govtech.com/GovExAwards2017.

DAVID KIDD

Illinois Loses Hardik Bhatt to Amazon

After more than two-and-a-half years serving as CIO for the state of Illinois, **Hardik Bhatt** is leaving for a role with Internet titan Amazon. His new job will be as part of a public-sector-facing team focused largely on the Internet of Things (IoT) as it relates to transportation and smart cities. Appointed by Gov. Bruce Rauner in March 2015, Bhatt led the Illinois Department of Innovation and Technology in an aggressive transformation program.

Though he will miss the work he does for Illinois, Bhatt's role at Amazon will afford him the opportunity to continue serving governments and their citizens. "I am going back into the private sector, but will continue working with the public sector," he said. "That has always been my passion." State Chief Information Security Officer Kirk Lonbom will step in as acting CIO until a permanent replacement is named.

DAVID KIDD

Colorado's Digital Transformation Officer Goes Local

As of early October, Colorado's first digital transformation officer (DTO), Brandon Williams, will assume new duties as the operations and process improvement manager for the Eagle County, Colo., Department of Public Health. He has served as DTO since November 2016, and before that he spent four years leading the state's Google Services team. Though he said he has enjoyed his time with the state, he looks forward to being directly involved with the community at the local level.

CIO Maricopa County, Ariz., Heads to Private Sector After nearly five years with Maricopa County, CIO David Stevens announced his last day of work would be Oct. 2 after accepting a position as executive vice president of corporate relations at IT services firm Valor Global. Stevens had served in county government since 2001 in positions including CIO of the county's judicial branch and deputy county CIO before ascending to CIO in Oct. 2012. As of press time, the county had not yet named a replacement.

Chicago Looks to Fill New Digital Experience and Design Director Position

Roughly four weeks after Chicago's mayor officially tapped Danielle DuMerer to lead its Department of Innovation and Technology, the city announced it is looking to fill a new position within its executive ranks: a digital experience and design director. Whoever is picked for the role will be tasked with boosting digital engagement and access across the city's online assets.

O'NEIL ARNOLD

LOUISVILLE CIO DEPARTS

Just before Labor Day, Louisville, Ky., CIO Jason Ballard stepped down from his post after three years in the position. Louisville has been increasingly lauded for its tech efforts, most recently winning a Government Experience Award from the Center for Digital Government* for its "If This Then That" tool. Ballard will be replaced on an interim basis by the city's innovation chief, Grace Simrall, pictured at left.

Cook County's Inaugural CISO Takes Same Post at Morningstar

Ricardo Lafosse, who joined Cook County, Ill., in May 2013 as its first chief information security officer, is leaving to join investment research and management company Morningstar Inc. as its CISO. After nearly four-and-a-half years in his position, Lafosse said working for the county has been a tremendous opportunity to build a program from scratch for a large organization — coordinating large cybersecurity initiatives quickly and building stakeholder relationships.

HONORS GO TO CALIFORNIA'S BEST

At the 2017 California Technology Forum in Sacramento, 18 individuals and agencies across the state were recognized with a Best of California award for a common trait: Each provided return on investment to both citizens and their governments. Winners included Los Angeles County for Best Application Serving an Agency's Business Needs; Stockton police Capt. Antonio Sajor for Demonstrated Excellence in Project Management; and the California Department of Public Health for Best Application Serving the Public.

*The Center for Digital Government is part of e.Republic, *Government Technology's* parent company.

By Dan Lohrmann

Fighting the Talent War

How to get and keep top cybersecurity staff in government.

History teaches us that great leaders build great teams. Surveys confirm and reconfirm that attracting and retaining talent is key to achieving organizational objectives and building a culture that makes a positive difference.

But attracting or retaining professionals with any credible cybersecurity experience into government positions has never been harder than it is right now. Constraints such as compensation packages make it hard to compete in our new "talent war."

Further complicating this problem are government employees eligible for retirement. A public-sector "brain drain" is still predicted when staff with more than 30 years' experience decide to retire.

Sadly things will likely get worse. One study by Frost & Sullivan forecasts a cybersecurity industry worker shortage of 1.8 million workers by 2022. Meanwhile, in mid-August 2017, four more top cybersecurity officials announced that they are leaving federal government.

In response to this competition for talent, a variety of government staff retention programs are commonplace. Offering telework, more vacation and flexible hours, and emphasizing very competitive health insurance plans are a few ways to keep staff from jumping ship. Defined benefit retirement plans are still available in some state and local governments, but these incentives are going away.

And while pay scales for technology and cybersecurity professionals are being raised in some public-sector organizations, it's hard to see how governments can compete with private-sector pay — especially if stock options and bonuses are included.

So what can be done? Here are three strategies to consider:

1. Grow your own team. Just like in professional baseball, you can build a "farm team" of young cyberprofessionals, students, interns and recent college graduates with technology knowledge and passion, but less experience. There are ways to attract young talent into government roles, since research has shown that public service and making a difference in society are a higher priority than pay for millennials.

There is a strong case to be made for starting one's career in government IT, since public-sector positions often offer a wider breadth of opportunities and challenges than initial private-sector roles.

TIP: Make a concerted effort to recruit and engage young people starting in high school and early college. Get involved with cybercompetitions to find the right students.

2. Retrain staff from other parts of government. Offer cross-training and technology transfer programs from the business side of government. Since cybersecurity roles often pay more, agency staff from other parts of the tech organization and/or business areas are often keen to make the jump to security roles. These pros know how government runs, so they bring added value to the security team.

TIP: Consider programs like Hiring Our Heroes to bring military veterans into the workforce. These veterans often bring hands-on experience from the front lines of cyberbattles around the world. (See *Serving a Purpose,* p. 44).

3. Ensure vendor management excellence. Enlarge your vision and make sure the best private-sector cyberpros keep working on your contracts.

Most governments rely on vendor staff to meet cybersecurity needs. Whether you use a staff augmentation approach, outsource certain functions or both, government leaders must ensure that contracts are well written and professionally managed after signing. Successful security leaders ensure that their private-sector partners don't rotate out the best contract staff after an initial period or lower the quality of their work using bait-and-switch techniques.

TIP: Attract and maintain the best contract oversight staff who understand procurement and keep the top vendor talent working on your projects. Also, include these contract professionals in team-building events.

Our future promises autonomous vehicles, robots and more, which means millions of Americans will need to be retrained to use new technology. Artificial intelligence may help someday, but these innovative paradigm shifts should challenge gov tech managers to rethink their recruitment practices now. Security may be the most noticeable part of government's staff retention challenges, but other areas like database administrators and programmers with secure-coding skills are also difficult to keep.

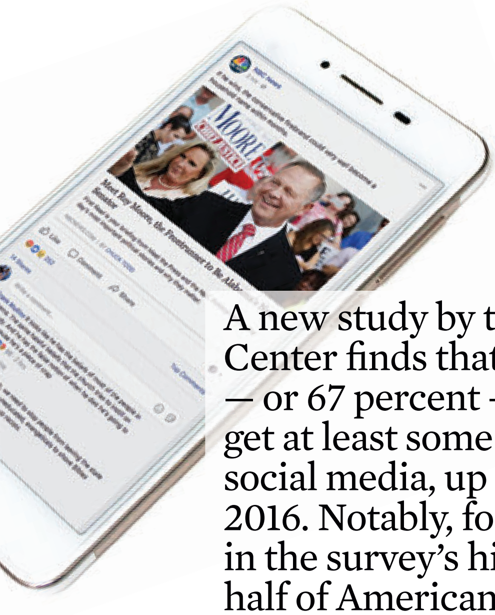
Finally, could a tech bubble burst change the hiring landscape? Government jobs have offered stability during hard times, and no doubt, this will happen again at some point.

My advice: Be ready whenever cybertalent becomes available. gt

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.

spectrum

More research, more science, more technology.



67%

A new study by the Pew Research Center finds that about two-thirds — or 67 percent — of U.S. adults get at least some of their news via social media, up 5 percent from 2016. Notably, for the first time in the survey's history, more than half of Americans over the age of 50 report getting news from social media. And while Twitter, Snapchat and YouTube increased their traffic from news-gatherers, Facebook remains the primary social platform Americans turn to: 45 percent of U.S. adults report they get news from the site.

SOURCE: TECHCRUNCH

PIN Protection

When we carry our smartphones with us everywhere, all that stands between our secret stats and the outside world is a short series of digits. So what happens if that stranger standing in the coffee line behind you as you unlock your phone sees your PIN? A team of researchers at New York University is developing a solution: IllusionPIN. The idea is that the configuration of numbers you see changes based on how far you're standing from the screen. The intended user, the closest to the screen, sees one configuration and enters the correct PIN. Someone standing 3 feet away will see a different configuration and therefore won't know the right code. And since the "correct" screen changes with each use, a nefarious lurker can't simply memorize one combination of positions.

SOURCE: NEWATLAS.COM

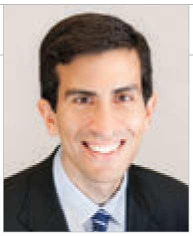
$305 MILLION:

The price farm equipment giant John Deere paid to acquire artificial intelligence (AI) startup Blue River Technology. The 60-person company based in Silicon Valley uses AI to identify and spray herbicide on weeds. John Deere says the tech will allow its tractors to understand individual plants in crops like lettuce and corn. Blue River's other farm tools include a device that trims lettuce and software for drones to analyze crops. SOURCE: QUARTZ

Send Spectrum ideas to Managing Editor Lauren Harrison, lharrison@govtech.com

SHUTTERSTOCK.COM

By Daniel Castro



Leaders of the Pack

Which states are winning the data science race?

States have long competed for jobs and investment, and this dynamic is now playing out in the race to be the state with the most data scientists — the highly sought-after professionals who combine the technical knowledge needed to wrangle large data sets, the analytical expertise necessary to make sense of all that information and the social skills needed to communicate these insights to their colleagues. The appeal is obvious. Not only do data scientists command top salaries — Glassdoor reports that the national average salary for the position is $113,000 — but states with high numbers of data scientists employed in local industries are also well-positioned to be more competitive in these sectors.

Data scientists are solving a hard problem: How can organizations convert the rapidly growing deluge of data into insights that will make them more successful? But recruiting data scientists is a challenge for most firms — McKinsey estimates that by next year, the United States will face a shortage of 140,000 to 190,000 data scientists. Moreover, this problem gets even worse further up the org chart: The U.S. needs nearly 1.5 million data-literate managers who can make use of the insights produced by the data scientists.

Unlike some professions where the distribution of jobs is spread fairly evenly across the United States — for example, the concentration of elementary school teachers does not change much from California to New York — the distribution of data scientists varies considerably. While no source gives a definitive answer, a variety of information gives us clues about current trends.

First, we can look at the number of people working in closely related professions, such as computer scientists and statisticians, as a share of total workers. According to the Center for Data Innovation, Maryland, Virginia and Delaware top the list for employing workers in statistics and database management, and Washington, Massachusetts and Virginia lead in software service jobs, such as computer programming and software development. North Dakota, Wyoming and South Dakota, along with Mississippi, Idaho and Wyoming, rank last in these two areas, respectively.

Second, we can see which states have the most job listings for data scientists as a share of total job listings. On this metric, Washington is the clear front-runner, with Maryland, Massachusetts and Virginia as its closest peers. At the back of the pack, Louisiana, Montana and Mississippi have the lowest share of data science job listings.

Third, we can determine which states have the most active data science community by measuring participation in data science events. The top three states for this metric are New York, California and Massachusetts — all states with large metropolitan tech hubs. They have thriving data science communities where knowledge-sharing, network-building and collaboration are common. But data scientists in Mississippi, South Dakota or Wyoming are likely pretty lonely, as none of these states has an active data science community.

The biggest question for most state policymakers is how to change the status quo. One important factor is the pipeline for data scientists. At the high school level, the best metric for whether schools are preparing students for careers in data science is the percent of students taking computer science and statistics advanced placement (AP) tests and these students' test scores. Massachusetts leads the nation with the highest ratio of students taking the computer science or statistics AP tests compared to other tests. However, while its students perform well, it is not the highest ranked. This distinction goes to Utah and Illinois, which tie for the top position, though both states have a lower ratio of students taking these tests. This suggests that these states need to find a way to scale their programs to more students. Finally, some states, such as Mississippi, Louisiana and New Mexico, have few students taking these tests, and those who do perform relatively poorly, on average.

As states vie to be the front-runner in data science, regardless of position, every state should recognize the importance of data science jobs and grow their data science talent if they want to be competitive in the data economy. gt

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.

product news

By Miriam Jones | Chief Copy Editor

Send product review ideas to mjones@govtech.com, twitter@mjonesgovtech

Flip Out

The Lenovo Yoga 920 convertible tablet/laptop contains up to an 8th-Generation Intel Core i7 processor, Windows 10 OS and an almost-bezel-less 4K IPS touchscreen in a 13.9-inch frame. Weighing 3.02 pounds, the four-mode convertible flexes 360 degrees from a laptop into a tablet. The computer offers an optional Lenovo Active Pen 2 for Windows Ink that has 4,096 levels of pen sensitivity for drawing and making notes with no discernible lag. Using Cortana, the tablet recognizes voice commands in standby mode and from up to four meters away so users can add items to a list, check traffic, send short emails, track packages and more. Cortana even uses artificial intelligence to learn from its owners, so the Yoga 920 grows smarter over time.

www.lenovo.com

Carry On

The Samsonite Xenon 3.0 15-inch laptop shuttle bag features padded vinyl-wrap textured handles and a padded drop-in single-zip laptop compartment that will fit up to a 15.6-inch notebook. The front pocket features organizers and a tricot-lined tablet pocket. The Xenon weighs 1.5 pounds, and has micro-forged matte gunmetal logo and zipper pulls. The bag consists of 1680 Denier ballistic poly construction, a durable nylon material originally specified by the federal government for military use.

www.samsonite.com

Print Genius

The Hewlett-Packard LaserJet 600 Enterprise Flow MFP is designed to print sharp, consistent documents — plus scan, copy, fax and improve workflow. The LaserJet 600 offers a maximum input capacity of 3,250 sheets, and scans up to 75 pages per minute and up to 180 images per minute. The MFP offers Ethernet, wireless and mobile printing options. It can also scan to Microsoft Office 365 and SharePoint, email, USB and network folders. The printer provides OCR, HP EveryPage, a pull-out keyboard and auto orientation/crop/tone. It also has an 8-inch pivoting touchscreen control panel. **www.hp.com**

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

By Kristy Dalton

Problem-Solving Prowess

Social media coordinators can use their skills to help solve government's non-social issues.

Social media can be used in sophisticated ways to support your agency's mission and get real results. But are leadership and departments that have problems to solve taking advantage of it?

We must condition our staff to consider social media as a valuable resource that can help work toward solutions to government problems.

Most public-sector agencies aren't in the mindset of turning to their "social media person" to see if there's a potential social technique, campaign or platform that could help with their objectives. They see social media as the icing on the cake that the communications people take care of.

Let's walk through a few scenarios where social media experts may be able to help.

I recently spoke with a group of government CIOs working through a big problem: how to attract and retain IT staff, especially millennials. All too often, job announcements for IT positions go unanswered.

While this issue isn't directly related to social media, the social media coordinator at their agencies can probably help. They may recommend launching a social recruitment campaign, or they may follow in the footsteps of many agencies and help produce a video campaign highlighting what it's like to work there. These days, you can't rely on simply posting job announcements on your agency's website.

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.

Law enforcement can help solve crimes in the community by using social media to crowdsource surveillance footage. That's what the Orem Police Department in Utah does with their #TattletaleTuesday posts on Facebook, which alert followers to footage of recent unsolved crimes and have resulted in a decent success rate in catching criminals. By approaching crime through a social lens, the department is engaging the community and improving public safety.

But what about the underlying problem of general distrust of government? Trust in government officials is at an all-time low globally, and it takes a toll on public entities that run citizen services. Take a look at the Edelman Trust Barometer, an annual international survey that shows government officials are seen as some of the least credible people. This suggests that there is tremendous value in humanizing government.

Your social media coordinator can use techniques to relate to citizens on social media, helping to build trust. One popular technique for humanizing government is to show citizens what it's like behind the scenes. People love getting an inside look at things they don't see every day. Many agencies have also made a concerted effort to talk in a conversational way, show humor and be "real" on social media. These tactics have paid off in spades by increasing their following, reach and notoriety both online and offline.

While all departments may not be expected to look through a social media lens to find solutions for big challenges, they can benefit from turning to their social media coordinator to tap into their expertise. Unless your department is working on a very specific, internal-facing issue, there is likely something that can be done on social media to contribute to a solution. It might not be your only approach, but it's a great tool in your toolbox. gt

SHUTTERSTOCK.COM

Instagram
LinkedIn
facebook
Pinterest
YouTube
flickr
flickr