

government
technology™

gt

OCTOBER/NOVEMBER 2018

Solutions for
state and local
government.

PLUS:

Lessons from Atlanta

*A post-mortem
on the city's massive
ransomware incident.*

*In the quest
to guard against
cyberthreats,
can we solve **the
people problem?***

THE WEAKEST LINK

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.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.



CONTENTS

Vol 31 | Issue 7

COVER STORY

16 / Cybersecurity's People Problem

Guarding against the latest cyberthreats requires an aggressive training program. But can the human element ever be completely overcome?

By Adam Stone

22 / Reckoning in Atlanta

The ransomware attack that wreaked havoc on the city may be a harbinger of more sophisticated attacks to come.

By Theo Douglas

28 / Arms Race

New technologies have emerged to help fortify cyberdefenses. Will they work for government?

By Tod Newcombe

The Texas State
Capitol building in
Austin.

DEPARTMENTS

36 / Setting the Cyber Scene (Infographic)

Data behind the state of cybersecurity.

40 / A Place for Cyber

Utah launches a multi-agency cyber-center — an idea whose time is overdue.

42 / Unrelenting Threats Inspire a New Model in Texas

A managed security services contract offers agencies prescreened cybersecurity tools.

COLUMNS

6 Point of View

Managing today's threats.

10 Data Points

The importance of website accessibility.

12 Four Questions

Garrett Dunwoody, Information Systems and Technology Manager, Midpeninsula Regional Open Space District, San Francisco Bay Area

46 Cybersecurity Strategies

Best practices for administrations in transition.

50 GovGirl on Social

The perils of hiding social media comments.

NEWS

8 govtech.com/extra

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

14 2018 Digital States Survey (Infographic)

Top-line takeaways from this year's digital benchmark of the states.

44 Spectrum

More research, more science, more technology.

47 Products

Samsung Portable SSD, ASUS ZenBook Pro 15, Pelican iPhone Cases

48 CIO Central

Career change across tech-driven roles in government.

IN OUR NEXT ISSUE:

2018 in the Rearview

The biggest news of the year in gov tech.

Now Hiring

We track the tech leaders who were on the move.

The Year in Data 2018 by the numbers.

FOLLOW
US ON



Publisher:

Alan Cox, alanc@erepublic.com

EDITORIAL

Editor:

Noelle Knell, nknell@govtech.com

Managing Editor:

Lauren Harrison, lharrison@govtech.com

Web Editor & Photographer

Eyragon Eidam, eeidam@govtech.com

Chief Copy Editor:

Miriam Jones, mjones@govtech.com

Copy Editor:

Kate Albrecht, kalbrecht@govtech.com

Senior Editor:

Tod Newcombe, tnewcombe@govtech.com

Associate Editor,

Ben Miller, bmiller@govtech.com

GT Data & Business:

Skip Descant, sdescant@govtech.com

Staff Writers:

Theo Douglas, tdouglas@govtech.com

Zack Quaintance, zquaintance@govtech.com

Adam Stone

Erik Hopkins, ehopkins@govtech.com

Contributing Writer:

Editorial Assistant:

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

Shelley Ballard, sballard@govtech.com

SALES DIRECTORS:

Melissa Sellers, msellers@govtech.com

Karen Hardison, khardison@govtech.com

Lara Roebelen, lroebelen@govtech.com

Carmen Besirevic, cbesirevic@govtech.com

Lynn Gallagher, lgallagher@govtech.com

Kelly Schieding, kschieding@govtech.com

ACCOUNT EXECUTIVES:

Rebecca Regrut, rregrut@govtech.com

Kathryn Nichols, knichols@govtech.com

Joelle Tell, jtell@govtech.com

Lisa Blackie, lblackie@govtech.com

Justin Windus, jwindus@govtech.com

BUS. DEV. MANAGER:

Nick Pedersen, npedersen@govtech.com

INSIDE SALES:

Katrina Wheeler, kwheeler@govtech.com

Paul Dangberg, pauld@govtech.com

Tracy Meisler, tmeisler@govtech.com

Dana Kansa, dkansa@govtech.com

SALES ADMINISTRATORS:

Jane Mandel, jmandel@govtech.com

Lien Largent, llargent@govtech.com

Laurie Roberts, lroberts@govtech.com

Alison Del Real, adelreal@govtech.com

Sharon Penny, spenny@govtech.com

Sr. Dir. of Sales Operations: Andrea Kleinhardt, akleinhardt@govtech.com

Chief Customer

Arlene Boeger, aboeger@govtech.com

Success Officer

Jeana Bigham, jbigham@govtech.com

Content Studio

Zach Presnall, zpresnall@govtech.com

Managing Editor:

Adam Fowler, afowler@govtech.com

Dir. of Web Marketing:

Ennie Yang, subscriptions@govtech.com

Web Advertising Mgr.:

Subscription Coord.:

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

Government Technology is published by e.Republic Inc. Copyright 2018 by e.Republic Inc. All rights reserved. *Government Technology* is a registered trademark of e.Republic Inc. Opinions expressed by writers are not necessarily those of the publisher or editors.

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

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

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

Printed in the USA.

WWW.GOVTECH.COM

IF YOUR CITY USES THESE



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

BUT DON'T WORRY. WE GOT YOUR BACK.



Managing Today's Threats

In the last several surveys of state, county and city tech leaders by the Center for Digital Government,* cybersecurity ranks No. 1 on the list of priorities. A growing number of localities have dedicated IT security staff, and an overwhelming majority say they'll need more cybertalent in the future.

It's hardly surprising. Our *Setting the Cyber Scene* infographic on p. 36 is filled with stats that justify the importance of adequate resources directed toward cybersecurity. For example, research firm Cybersecurity Ventures estimates that by 2021, damage from cybercrime will reach \$6 trillion.

To help get ahead of the threat, one strategy gaining traction in both the public and private sectors is a robust cybersecurity training program for staff. "Humans are still the No. 1 attack vector, the No. 1 target and they have to be the first line of defense," said Missouri's then-Chief Information Security Officer Michael Roling.

Training takes many forms — numerous vendors now offer a variety of options to fit the needs and the budget of government clients. And while most have made significant headway arming employees with cyberknowledge, some say that they've hit an awareness threshold they can't get past. Human nature, and the various stressors weighing on an employee on any given day, mean that even those who know better will sometimes click on

that link, open that attachment or offer up credentials on an insecure network. Our story *The Weakest Link* (p. 16) examines the benefits and limitations of cyber-training, and looks at what comprises an effective, comprehensive approach.

In *Arms Race* (p. 28), we look at the evolution of the technology driving cyberdefense and the market that has grown up around it. Like the tech industry in general, cybersecurity is evolving from manual and hardware-dominated to more automated and software-driven strategies. The steady migration toward the cloud over the past decade has helped many in government manage their security posture more easily, though these gains are tempered by environments that include aging legacy systems requiring manual updates — taxing a workforce that has far from recovered to pre-recession levels. Artificial intelligence is also playing a growing role in cybersecurity, yet it too has its limitations. Experts largely view AI as something that can enhance traditional threat analytics tools, rather than replace them.

Earlier this year, Atlanta suffered the most far-reaching ransomware attack to hit an American city, knocking both internal and citizen-facing systems offline for weeks. While the city reports that the recovery is largely complete, costs now dwarf the original bitcoin demand of \$51,000. For our story *Reckoning in Atlanta* (p. 22), we talk to city officials,

partners and outside experts who put the incident, and the evolution of the ransomware threat, in proper context.

Our hope in taking a deep dive into stories like this one about Atlanta is to help other jurisdictions find the lessons from the attack that can move them toward more secure, resilient IT infrastructure. Threats like ransomware are only growing in sophistication. Kevin Haley, Symantec's director of product management for security technology and response, said criminals trading in ransomware in 2018 are highly skilled.

"I think many of us just think that sort of thing is just not going to happen to us," Haley said. "You may be one of the lucky ones, but it's less and less likely that you're going to be one of the lucky ones every day."

Better not to bank on being lucky. 

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.

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



Simplifying Audits with Electronic Content Management

Preparing for a financial or program audit can be a monumental challenge if records aren't well maintained or if auditors can't access documents easily or securely. Several factors contribute to audit complications:

- Records and documents are often located in different applications for accounting, asset management and enterprise resource planning (ERP).
- Paper documents are difficult to locate because they can be misfiled, stored in multiple facilities and locations or become physically degraded or lost altogether.
- Relevant documents for a project, bond issue or other audit focus may be hard to locate because they weren't tagged for relevance or labeled consistently, if at all.

How Electronic Content Management Can Help

An electronic content management (ECM) system from Laserfiche stores all documents electronically and centrally. Audits become simpler because the system eliminates the need to maintain paper documents and delivers powerful capabilities for tagging, search and secure access.

For example, an auditor can directly access all documents related to a specific accounting journal entry through a single link. In a program audit, tags and metadata identify all related documentation, which can be accessed through an easily created auditor review folder. The Laserfiche system also maintains information privacy and security with configurable controls on what each auditor can access and do with retrieved documents.

Simpler Audits for Springfield

Springfield, Ore., integrated Laserfiche with its ERP system to streamline journal entries and audit activity. This integration offers several benefits to the city and its auditors, including:

- Quick and efficient access to all journal entry documents directly from the ERP system
- Journal entry documents can be accessed by multiple authorized users at the same time
- No misplaced or missing journal entry documents

Laserfiche®

Learn how your government or agency can streamline the audit process with Laserfiche content management solutions:
<https://www.laserfiche.com/solutions/accounting/>

Safety First

Data is central to making roads safer in Utah, thanks to a strong reliance on the state Department of Transportation on tools that gather and analyze what's actually happening when drivers get behind the wheel. A new median was installed across a 200-mile stretch of I-80 after DOT engineers looked at crash data from various sources to understand what factors were impacting traffic there. Data analysis tools like cloud-based Numetric that aggregate and organize high volumes of information are crucial to this work, and helped DOT spot parts of the highway where the existing median was insufficient. Along with Numetric, Utah DOT relies on the United States Road Assessment Program, offered by the Roadway Safety Foundation.

BIZ BEAT

To improve the traditionally complicated processes around local zoning codes, a California startup is offering a digital solution. So far 17 cities, including Los Angeles and Austin, Texas, have had their zoning codes digitized by idevelop.city, which creates interactive maps that users can customize to view certain kinds of zones. The company doesn't charge cities to use their software, but instead looks to them to

help make the product better and find out what it can do, and where. When, for example, a city leader uses idevelop.city's software to understand the potential impacts of a policy change, they not only get their answers more quickly than they would wading through traditional government processes, but are also offered other information they wouldn't get with those low-tech methods.

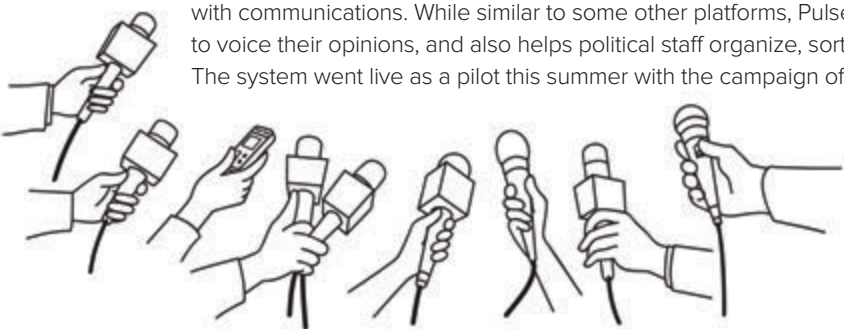
WHO SAYS?

"There is a need for data now like a person in the desert that needs water."

govtech.com/quoteOctober2018

Speaking Out

Interested in making it easier for citizens to impact how their government runs, four Stanford University undergrads built Pulse, a civic engagement platform designed to help constituents feel truly heard by their elected officials. After the 2016 presidential election spurred more people to get involved with the political process, lawmakers' inboxes and phone lines have been flooded with communications. While similar to some other platforms, Pulse both makes it easier for voters to voice their opinions, and also helps political staff organize, sort and understand those messages. The system went live as a pilot this summer with the campaign of U.S. Rep. Eric Swalwell, D-Calif.



MOST READ STORIES ONLINE:

5 Common Issues State Auditors See in Government IT Departments
7,597 VIEWS

Colorado Will Develop a Digital Highway Using Connected-Vehicle Technology
2,891 VIEWS

L.A. Metro Readies Launch of Multi-Purpose Mobility Payment Card
2,622 VIEWS

Traffic Data in Tampa Gets the AI Treatment
2,310 VIEWS

Chief Innovation Officers in State and Local Government (Interactive Map)
2,172 VIEWS

Ohio's Stu Davis Departs After Nearly 8 Years as CIO
2,066 VIEWS

31

The number of cities participating in the next Startup in Residence cohort.

20M

The number of data points available in Missouri's financial transparency portal, Show-Me Checkbook.

14

The number of jurisdictions (10 states plus four of the country's 10 most populous cities) that have websites that are "not secure" according to Google.

150

The number of traffic signals, out of a total of 248, in Gainesville, Fla., that are part of a connected network that can predict, among other things, how much time is left on a green light.

Equip^t to Innovate[®]

*Residents expect a lot of their city.
To perform under pressure, cities should be ...*

DYNAMICALLY PLANNED

BROADLY PARTNERED

RESIDENT-INVOLVED

RACE-INFORMED

SMARTLY RESOURCED

EMPLOYEE-ENGAGED

DATA-DRIVEN

HOW IS YOUR CITY DOING?

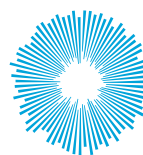
Equip^t to Innovate is a free, unique framework that nearly 100 cities are using to assess their capacity to meet today's challenges.

Join the movement by taking the survey at:

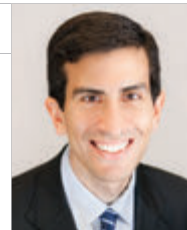
governing.com/equipt

A joint initiative of

GOVERNING



LIVING CITIES
INNOVATE • INVEST • LEAD



Accessibility First

Governments must make sure their websites are accessible to people of all abilities.

According to the U.S. Census Bureau, 56.7 million people — nearly one in five Americans — have a disability, such as vision loss, hearing loss or mobility impairments. People with disabilities face many challenges when websites are not accessible. For example, individuals who are blind may not be able to navigate a website using a screen reader if the website does not properly label graphics, and individuals who are deaf are not able to understand the narration in an online video if it is not properly captioned. When government agencies fail to make their websites accessible, people with disabilities are unable to get access to important government services and information. Unfortunately, according to a recent study by the Information Technology and Innovation Foundation (ITIF), many state government websites are not accessible.

The ITIF study reviewed 400 state government websites — eight sites from each of the 50 states. The websites were chosen to reflect some of the most popular online government services, such as finding election information, obtaining a driver's license and paying taxes. To test a site's accessibility, ITIF assessed its compliance with the Web Content

Accessibility Guidelines (WCAG) 2.0, a widely used set of accessibility guidelines for websites that is produced by the World Wide Web Consortium (W3C), an international standards organization for the Internet. WCAG 2.0 was created in 2008, so website operators have had almost a decade to adopt.

Overall, ITIF found that while 12 percent of state government websites received a perfect score, 41 percent failed the accessibility test, meaning that these sites had a substantial number of known problems that might prevent someone with a disability from using the site. Unfortunately, many of the states with the highest percentage of residents with disabilities performed poorly on the accessibility test. For example, West Virginia has the highest percentage of people with disabilities of any state yet ranked 46th for its average accessibility score. And none of the 10 states with the highest percentage of people with disabilities ranked in the top 10 in the accessibility rankings. States should require that all government websites adhere to the latest WCAG standard.

Accessibility testing is always tricky because automated tests can only tell part of the story. For example, an automated tool can verify that an image on a website is labeled, but it cannot verify that the label is correct or particularly helpful. Some of the states that performed the

best on accessibility engaged directly with people with disabilities to test and provide feedback on their websites. For example, Massachusetts partnered with the Perkins School for the Blind, the oldest such school in the United States, to test the accessibility of its websites. Similarly, Georgia partnered with an accessibility lab at Georgia Tech to review some of its sites. Given that every state has a local population of users with disabilities that can provide this type of feedback, more states should adopt this practice.

Just as some government agencies have begun to embrace a “mobile-first” strategy — where they design their websites for mobile devices, rather than designing for desktop and treating mobile as an afterthought — states should start adhering to an “accessibility first” strategy — where they design their websites to be accessible for people with disabilities from the outset, rather than treating accessibility as an add-on. The benefit of this approach is that websites designed for people with disabilities can be better for everyone — just like mobile-friendly sites work well for desktop users. For example, websites with proper contrast between text and background images are easier to read for everyone.

By embracing accessible design for websites, states can be more inclusive and ensure that e-government services are available to all. 

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.

DIGITAL GOVERNMENT SUMMITS

government
technology
events

*Spreading Best Practices
& Spurring Innovation*



SUMMIT LOCATIONS THIS YEAR:

Alabama
Arizona
Arkansas
California
Chicago (*new*)
Colorado
Connecticut
Florida
Georgia
Illinois
Indiana
Kentucky

Los Angeles
Louisiana (*new*)
Maine
Maryland
Massachusetts
Michigan
Minnesota
Mississippi
Missouri
Nevada
New Jersey
New York

New York City
North Carolina
Ohio
Oklahoma
Oregon
Pennsylvania
Tennessee
Texas
Utah
Virginia (COVITS)
Washington
Wisconsin

**ATTEND/
SPONSOR:**
govtech.com/events



Garrett Dunwoody

Information Systems and Technology Manager, Midpeninsula Regional Open Space District, San Francisco Bay Area

The issue of connectivity and access to broadband remains persistent through many swaths of rural America. Groups overseeing natural lands also encounter connectivity struggles as they navigate the day-to-day difficulties of managing open space. The Midpeninsula Regional Open Space District (MROSD) manages and protects 63,000 acres down the middle of the San Francisco Peninsula into San Mateo and Santa Clara counties in California. The district was formed in 1972 and is charged with building and managing a regional greenbelt in perpetuity. The area includes two dozen nature preserves and is operated by a staff of about 180.

Garrett Dunwoody, who has a background in public-sector data science, oversees the Information Systems and Technology Department at MROSD and has been leading efforts to improve connectivity among the organization's various offices.

1 How has MROSD been working to improve connectivity?

A lot of our field offices are in remote locations within our preserves. So we're in the process right now of working with Comcast Solutions to implement what we're calling a districtwide fiber-optic network. We're connecting all of our field offices with fiber-optic cabling.

This project is twofold. One is the capital project to actually run the fiber-optic cable to those various locations. And then the second part of the project is more services-based. What we're building is what Comcast calls Ethernet Network Service. We'll basically be connecting our field offices all within a virtual private network [VPN].

2 How will a strong fiber backbone (valued at about \$250,000) improve the workflow and operations for workers spread across MROSD's thousands of acres?

It will allow field staff to interface with the work-order system we're implementing, our enterprise GIS, because our field locations are "mesh networks," where somebody in a ranger truck, or somebody walking around in the courtyard with a tablet, will be connected to our network. They'll be able to download their work orders for the day and take them offline to go to the field to get their work done. Our experience for our field staff, rather than having them need a VPN into the file server or the finance system, will be all within our network. That's the big 800-pound gorilla that we've been trying to tackle.

3 When will the project be completed?

We're in contract right now. We've had the various site walk-throughs. The construction components are in permitting. I think based upon some preliminary new numbers, it will probably be close to March 2019. That's when the actual fiber line will be connected to our field offices.

4 Did MROSD look to other nature preserves or government agencies charged with managing natural lands as a template for how the Open Space District should structure connectivity?

We didn't necessarily look at a particular organization to see how they did a similar project. As a special district, I think we're different enough that a lot of the technical components are unique to us, meaning the location of our facilities, who might be our service providers, things like that. But we did do a pretty deep dive into the various solutions that were out there. [@t](#)

— Skip Descant, Staff Writer

MAXIMIZING YOUR RADIO FLEET

Government agencies can better manage complex radio provisioning and lower costs with device management services.

Managing a radio fleet is essential to enabling seamless mission-critical communications, but doing it on your own can be a costly and time-consuming effort.

When agencies try to go it alone they often waste valuable resources before they fully assess what a proactive approach to radio management can do for their operating expenditures.

Radios operating with out-of-date software and hardware are vulnerable to malfunction, poor performance, and security breaches. In mission-critical operations, a minor technology issue can quickly escalate during an incident or emergency, sometimes resulting in irreversible harm.

Whether it's software, training and support for managing radios in-house, or outsourcing your entire fleet management, Motorola Solutions offers expert services and training to help government agencies maximize performance, reduce complexity, and lower the total cost of ownership of their two-way radio fleet.

MANAGED & SUPPORT SERVICES KEEP RADIOS UP TO DATE

As radio programming and provisioning becomes more complex, it's important to have the right resources and tools to avoid downtime. Motorola offers three distinct packages that provide you with different entry points into radio management services. With budgets and resources stretched thin, you can choose the right level of support to bring you peace of mind when it comes to your mission-critical communication needs.

Essential Services delivers remote technical support during local business hours for radio software problems as well as a service center for hardware repair.

Advanced Services adds radio management software for batch programming multiple radios, as well as on-site training and secure storage for radio management data.

Premier Services transfer the risk and management of your radio fleet to Motorola Solutions. A dedicated team takes on accountability for all ongoing maintenance and repairs, including radio provisioning, programming, software support, hardware repair and annual preventive maintenance.

MAXIMIZING VALUE WITH RADIO MANAGEMENT

Motorola Solutions Managed & Support Services help agencies gain full value and better outcomes from their radio management investment, including:

- ✓ More reliable communications in the field
- ✓ Improved performance and longevity of your two-way radio investment
- ✓ Fewer programming errors
- ✓ Lower maintenance overhead with repeatable procedures
- ✓ Reduced security risk
- ✓ A platform for adding future support capabilities

Agencies of all sizes can benefit from a cost-effective, efficient and proactive approach to maintaining their two-way radios. With Motorola services, you'll get the most out of your APX radios and streamline programming and maintenance. When complexity is managed, agencies can focus on their missions to keep our nation's communities and citizens safe.

2018 Digital States Survey:

A Digital Benchmark for States

Every two years, the Center for Digital Government* and *Government Technology* conduct a comprehensive survey of the maturity of tech initiatives in all 50 states. Here are some top-line takeaways from this year's survey, revealing where states are on their journey to digital government. For our full story and details on each state, visit www.govtech.com/DigitalStates2018.

At First Glance (compared to the 2016 survey)

Improved
17 states



Holding Steady
27 states

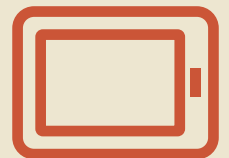


Declining
6 states



89%

of states use an on-premise, state-run cloud



30%

of states are working with startups to develop and deploy new tech

Following the Leaders

A- ✓✓✓✓✓✓✓✓ **8 States**

B+ ✓✓✓✓✓✓✓✓✓✓ **10 States**

B ✓✓✓✓✓✓✓✓✓✓✓✓ **17 States**

B- ✓✓✓✓ **4 States**

C+ ✓✓✓ **3 States**

C ✓✓✓ **3 States**

Tech Priorities



Cybersecurity



Shared Services



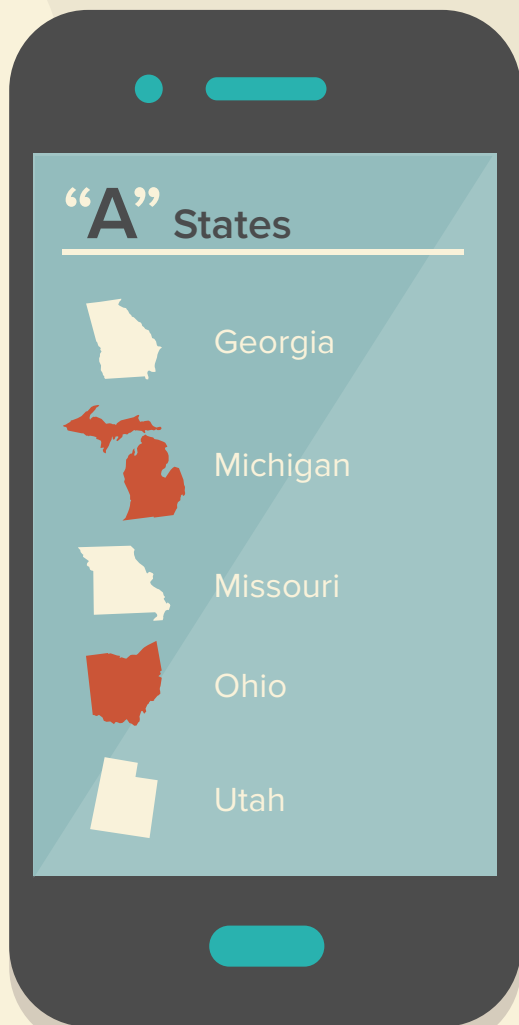
Cloud Computing



IT Staffing



Business Intelligence/Analytics



Citizen Engagement

TOP INITIATIVES:



Voice Assistants

States are increasingly making information available via voice-activated platforms:

Amazon Echo/Alexa:

17%

Google Home/Google Now:

13%

Microsoft Cortana:

4%

Siri:

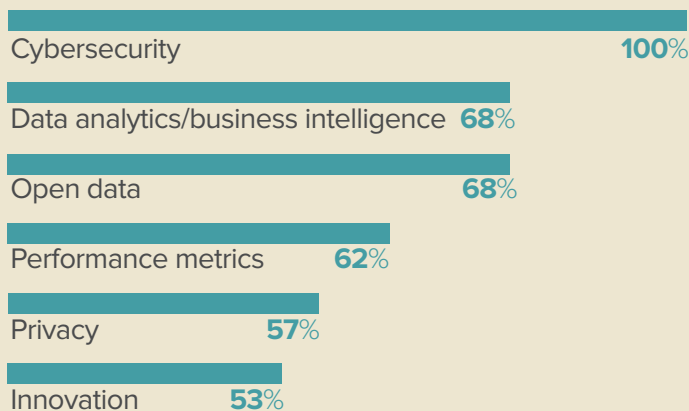
2%



15%
of states have developed augmented reality applications

Workforce

STATES THAT HAVE AT LEAST ONE FULL-TIME POSITION IN:



Cyber Initiatives



70% of respondents use security as a service today. Another 16% plan to within two years.



75% of respondents are spending 1-5% of their budget on cybersecurity.

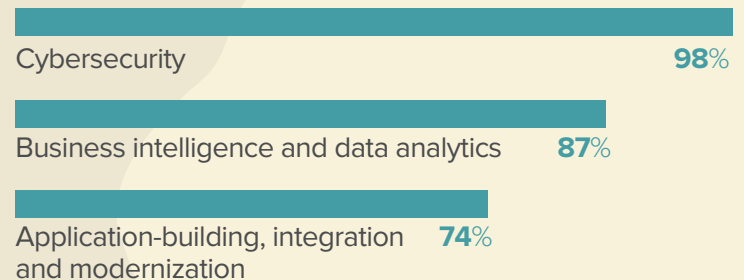


64% of respondents have implemented AI for cybersecurity (auto-threat detection).

Cyber Priorities

1. Security incident response
2. Enterprise security operations center/ransomware prevention and response
3. Cloud security
4. Cyberinsurance
5. Secure application development

BIGGEST WORKFORCE NEED GOING FORWARD:



CENTER FOR
DIGITAL
GOVERNMENT

government
technology

aws

nic
the people
behind
eGovernment

DELL EMC

NUTANIX

Deloitte.

shi

McAfee
Together is power.

verizon

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

THE WEAKEST LINK

Guarding against the latest cyberthreats requires an aggressive training program. But can the human element ever be completely overcome?

BY ADAM STONE



STEVE NICHOLS HAS SEEN

just how far training can go in safeguarding government from cyberattacks — and he's seen the limits of training, too.

"We run internal phishing campaigns against our employees. We have been doing that for over four years and it doesn't get any better than an 80 percent compliance rate," said Nichols, chief technology officer of Georgia. "In any given campaign, 20 percent of employees will click the bad link or do the wrong thing. I talk to my colleagues in other agencies, in other states, and no one gets into the single digits."

Statistics bear him out. While training, awareness and assessments all are a routine part of the cyberdefense strategy in government, workers still open malicious attachments and click on toxic links. Despite years of aggressive efforts, 35 percent of data breaches still are attributed to human error or negligence, the Federal Information Systems Security Educators' Association reports.

This is not to say that training is futile — not at all. Former Missouri Chief Information Security Officer (CISO) Michael Roling recently took a cybervulnerable local government entity into the state's cyberawareness program and saw stellar results. "That entity had a 20 percent higher victim rate than our worst state agency at the start," he said. "Now that

they are a part of our program, they are comparable to other state agencies."

Illinois CISO Chris Hill says he would like 70 to 80 percent of employees to report in when they see potential phishing, and he'd like a fail rate of not more than 5 percent on attack assessments. Training hasn't gotten him anywhere near those numbers, and so while Hill is passionate about training, he's also realistic about its limits. "Campaigns work. Awareness works. But training alone is not enough," he said.

Why not?

How come all the best training we've got does not seem sufficient? And if that's the case, what's next for government cyberstrategy? Here we'll consider the shortcomings of the current training paradigm, explore how awareness efforts could be improved upon, and finally look at some technological fixes that promise to fill the gap when training alone falls short.

'NOT VERY RELEVANT'

If training doesn't cut the mustard, some fault may lie with the trainers. Too often, the awareness effort is "very rote, with no worker involvement in its development," said Charlie Gerhards, executive director of the Government Technology Institute at Harrisburg (Pa.) University of Science and Technology. Often, training is "not very relevant to an employee's role."

The problem may also have to do with volume. An employee who gets five emails a day could easily stay compliant, "but we have created a virtual assembly line where workers spend all day clicking on links, reading and responding," Nichols said. "That's what they do all day long. Now if a bad thing just slips past the malware filters, it's asking them a lot to pick out that one thing among all those hundreds of emails."

Maybe we also need to ask ourselves who is running the cybertraining. Are the trainers skilled in the subtle arts of education and influence?

"Quite often the people in charge of human risk are really, really technical geeks. The depth of their expertise actually makes it hard for them to communicate what they know," said Lance Spitzner, director of SANS Security Awareness. "Security is easy for them, so they think it must be easy for everyone else, when in fact most people find it confusing, scary, intimidating."

Roling, meanwhile, says the shortcomings of training may track back to the executive suite, where IT leaders lay the plans for cyberawareness. They may be aiming for the wrong mark. "When I look at how we used to do it, we viewed it as just a compliance requirement — some external entity requires this awareness program," he said. "If you look at it like that, you will do the bare minimum,

**"CAMPAIGNS WORK. AWARENESS WORKS.
BUT TRAINING ALONE IS NOT ENOUGH."**

Illinois CISO Chris Hill



you won't refresh the content. Of course that method doesn't work well."

Given all these concerns, it seems reasonable to conclude that if training isn't getting IT all the way to the goal line, maybe the first thing to do is to rethink training. Could government be doing cyberawareness more effectively? Yes. Here's how.

DRILLING DOWN

Illinois CISO Hill is looking to improve cybertraining by making it more specific. Rather than heighten the general level of awareness, he wants to drill down, to develop materials that speak with a higher level of specificity.

"Right now, for instance, we are looking at programs that target law enforcement and fire officials, campaigns that speak more on their terms," he said. "Rather than say, 'A worker gets an email,' you say: 'I am a police officer and I am getting an email.' You want it to be down to that level of detail."

Tying cybertraining to specific roles and responsibilities is part and parcel with a larger effort to convince workers that their clicks have real, actual consequences. "We have to explain to them how important this is to them personally, to their specific piece of work," said Mark Testoni, president and CEO of SAP National Security Services. "It's not just about somebody getting into our system.

How does this affect your job, your pocketbook, your ability to succeed?"

Nichols meanwhile is pursuing a three-pronged course of attack to enhance the impact of training:

✗ BRING IT HOME: Cyber know-how helps people not just at work but in their personal lives as well. Nichols makes that a selling point. "People routinely come up and tell me that the training has made them better in their personal email use. If we can show them that this is making them better at home, then they appreciate that and they get more engaged in the training," he said.

✗ KEEP IT TIMELY: When cyberstories hit the news, Nichols builds training modules around the most recent threats. "You've got to make it relevant. When we see something happening and people are reporting it, we want to tell employees about that. Then if they experience that thing — well, we nailed it," he said.

✗ OFFER VARIETY: He introduces new training and testing materials frequently. "It's a novelty thing, to get the employees to pay attention. After a year or two, they get stuck in a rut in the training paradigm, so we look for something with a different look or feel," he said.

This imperative to keep training fresh and new resonated with Roling. He'd been using the training firm Security Mentor to deliver interactive cyberawareness, but recently switched to Habitu8, largely in order to give employees a new take.

"I have nothing bad to say about their program, they did a good job for us, but I want to provide a fresh experience for our end users. I feel it's important to keep the content fresh and its delivery fresh, or else you get that glassy-eyed look from people," he said.

The previous vendor offered quizzes and problems to solve, an approach that Roling found effective. He'd roll out monthly iterations and employees would engage readily. The new supplier takes a different approach. "They create short videos using

35%

OF DATA BREACHES ARE DUE TO HUMAN ERROR OR NEGLIGENCE

Source: Federal Information Systems Security Educators' Association

professional actors and actresses that are hilarious and engaging in a very different way. They're about people having fun while learning at the same time, and we are hoping that will bring our awareness program to a different level," he said.

Experts in the field put a lot of weight on this notion of entertainment: They encourage government IT leaders to think hard about the form of training, and whether it is geared for maximum impact.

Where past presentations may have been somewhat static, today's best offerings "leverage a short, 'bite-sized' security lesson in the form of cartoons or short funny sketches or parodies. These tend to have much better acceptance from a broad employee base," said Gerald Beuchelt, CISO at LogMeIn.

PHISHING TRIP

A routine part of most government agency cyberefforts these days is the phishing expedition: sending employees fake emails loaded with traps to see who takes the bait. In considering potential improvements to training, it's worth taking a deeper look specifically at how the phishing expedition ought to be handled.

"If we send 5,000 messages, do we know that all 5,000 were received? Do we have good logs in place? Do we track them all the way through?" Hill said. "Proactive phishing is a good way to see if your training is working, but you have to really push the reporting piece, and then you have to follow through. Once we do get a report, do we have the correct procedures in place to respond to that?"

Many organizations fall short on follow-through. If training is less than

fully effective, some say, it may be because the IT team isn't sufficiently aggressive in how it closes the loop when employees fall for a trap in testing.

Some suggest radical surgery.

At the cyber trade association (ISC)², Director of Cybersecurity Advocacy for North America John McCumber talks about the Passover Principle. "Slaughter the lamb and spread the blood on the doorposts and the lintels," he said.

McCumber proposes publicly broadcasting the names of those who fail the phishing test, letting everyone know it was Bob or Sally who allowed the faux invaders to breach the walls. For IT chiefs who balk, he proposes the Pontius Pilate corollary: Wash your hands of the deed. "You have to have human resource management step into the breach, so that it is not a security problem, it's not a CISO problem," he said. "You want this to be the shared responsibility of organization leadership."

Many will cringe at the proposed public shaming.

"If you get it wrong, you should get feedback: Why did you click on this? What could you do differently next time? You use it to get people thinking about things," said Jason O'Neill, head of global training services at consulting firm Kepner-

Tregoe. "One-on-one personal feedback is key. If you want them to really think about this, you can't just send an email."

Positive reinforcement could also help. Rather than call out those who miss a cue, "you create an award or a commendation or a scoreboard to track who is the best at reporting these kinds of things," he said. "You create an environment where people are recognized and rewarded for doing the right thing."

TECH FIXES

Better training could raise the cyberbar, as would improved efforts around phishing follow-up. Ultimately, though, people are fallible and all the training in the world won't fix cyber. Enhanced efforts on the back end — new technologies and cyber-practices — will need to close the gap.

"Most organizations are still struggling with the basics," Spitzner said. "We need to patch. We need to manage access. This is well-known, there are entire frameworks like the Center for Internet Security's Top 20 Critical Security Controls. How many devices do we have? What software do we have? Who is using it?"

For resource-strapped government tech leaders, automating where possible can


help to move the needle. Even as we wait for machine learning and artificial intelligence to save the world, there's a lot IT can do to build up security routines. "It might just be a warning, a little trigger that says: 'Hey, do you really want to click on that?'" A reminder like that could definitely be helpful, once people have had the training," O'Neill said.

In Illinois, Hill has pursued a couple of structural changes that he said will help to offset the human propensity to goof. All email that comes from outside of government gets flagged "EXTERNAL" in the subject line, as a quick and easy way to put recipients on their guard. The system also strips embedded links from emails: You can still copy and paste a link, but it's harder to get to, and there's a built-in moment for reflection. "That's a simple trick, but it can dramatically reduce clicking," he said.

In Georgia, Nichols is looking at emerging techniques like two-factor authentication to better safeguard systems, but he said it can be a struggle to balance security against usability. He said AI could help in the long term, potentially building up user profiles that can be leveraged to automatically flag suspicious activity.

"We can know every single thing that your computer is going to do, that your phone is going to do. We can watch where you go and what you follow," he said. "What is the typical day in the life of this individual? What do they open? Where do they visit? There are all sorts of algorithms to leverage against that."

Such efforts could help reduce the impact of human error. Until this comes to fruition, though, government IT leaders say they will continue to look to workers as the foot soldiers in the cyberwars, and they'll continue to lean on training and awareness as the most potent weapons in the fight.

"Until computers can think like a human and identify human-based threats, technology will not be able to put a complete stop to these attacks," Roling said. "Humans are still the No. 1 attack vector, the No. 1 target, and they have to be the first line of defense." 

TRAIN TO WIN Looking to take cybertraining up a notch? The Center for Internet Security recommends getting out of the classroom and creating a hands-on experience around cyberawareness.



PHISHING CAMPAIGNS:

An internal "red team" launches a bogus attack, training employees to spot and report suspicious emails.



DESKTOP/TABLETOP EXERCISES:

Make cyber tangible by putting employees through the paces, showing them how to handle incidents such as a DDoS attack or website defacement.



USB DROPS:

These exercises give employees firsthand experience in handling a mysteriously found USB device.



INTERNET OF THINGS TIP CARD

The Internet of Things refers to any object or device that sends and/or receives data automatically via the Internet. This rapidly-expanding set of “things” includes tags [also known as labels or chips that automatically track objects], sensors, and devices that interact with people and share information machine to machine.

WHY SHOULD WE CARE?

- Cars, appliances, wearables, lighting, healthcare, and home security all contain sensing devices that can talk to another machine and trigger other actions. Examples include: devices that direct your car to an open spot in a parking lot; mechanisms that control energy use in your home; and other tools that track your eating, sleeping, and exercise habits.
- This technology provides a level of convenience to our lives, but it requires that we share more information than ever. The security of this information, and the security of these devices, is not always guaranteed.
- Though many security and resilience risks are not new, the scale of interconnectedness created by the Internet of Things increases the consequences of known risks and creates new ones.

SIMPLE TIPS

Without a doubt, the Internet of Things makes our lives easier and has many benefits; but we can only reap these benefits if our Internet-enabled devices are secure and trusted. Here are some tips to increase the security of your Internet-enabled devices:

1. **Keep a clean machine.** Like your smartphone or PC, keep any device that connects to the Internet free from viruses and malware. Update the software regularly on the device itself as well as the apps you use to control the device.
2. **Think twice about your device.** Have a solid understanding of how a device works, the nature of its connection to the Internet, and the type of information it stores and transmits.
3. **Secure your network.** Properly secure the wireless network you use to connect Internet-enabled devices.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit www.dhs.gov/stopthinkconnect.



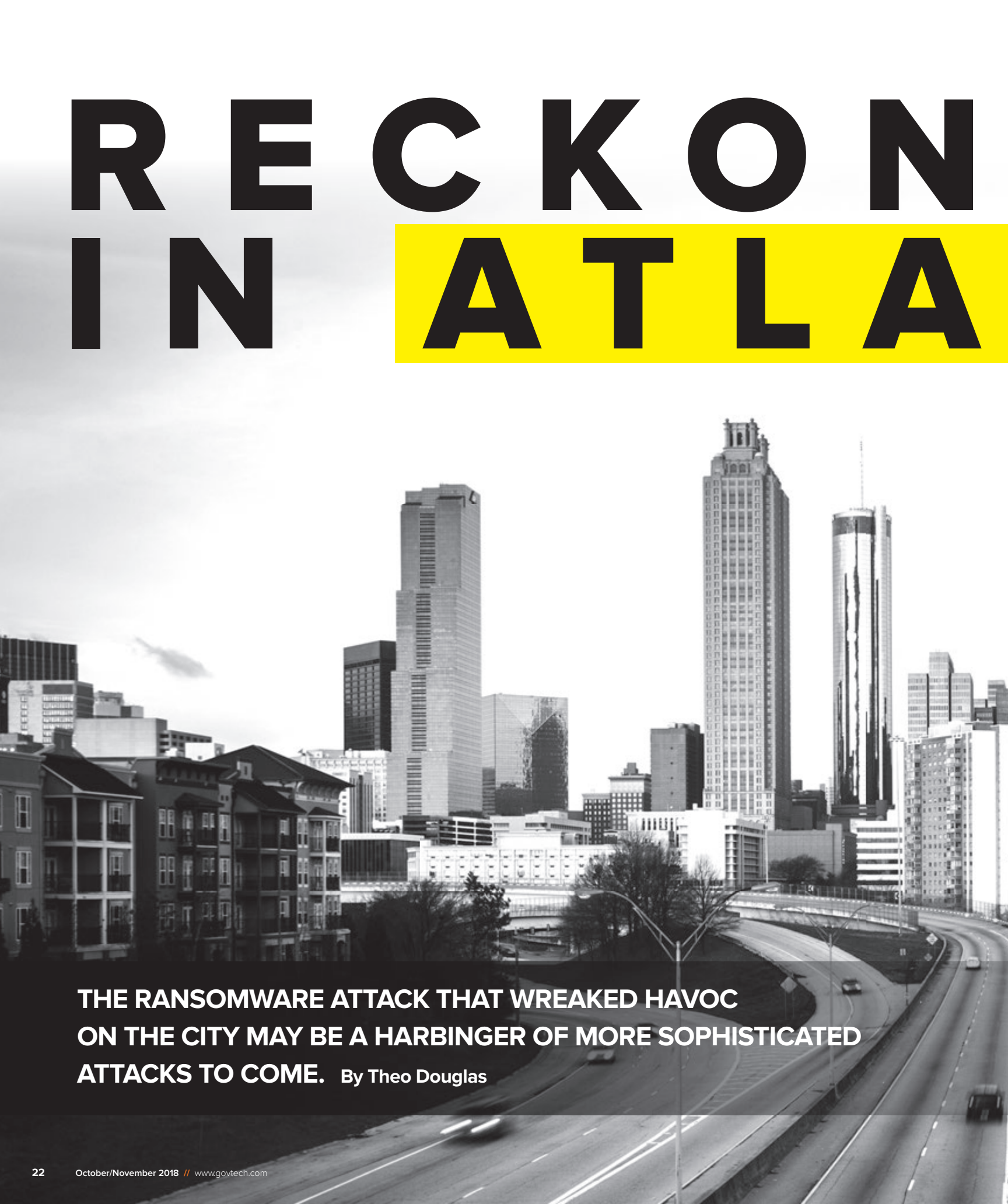
Homeland
Security

www.dhs.gov/stopthinkconnect



STOP | THINK | CONNECT™

RECKON IN ATLA



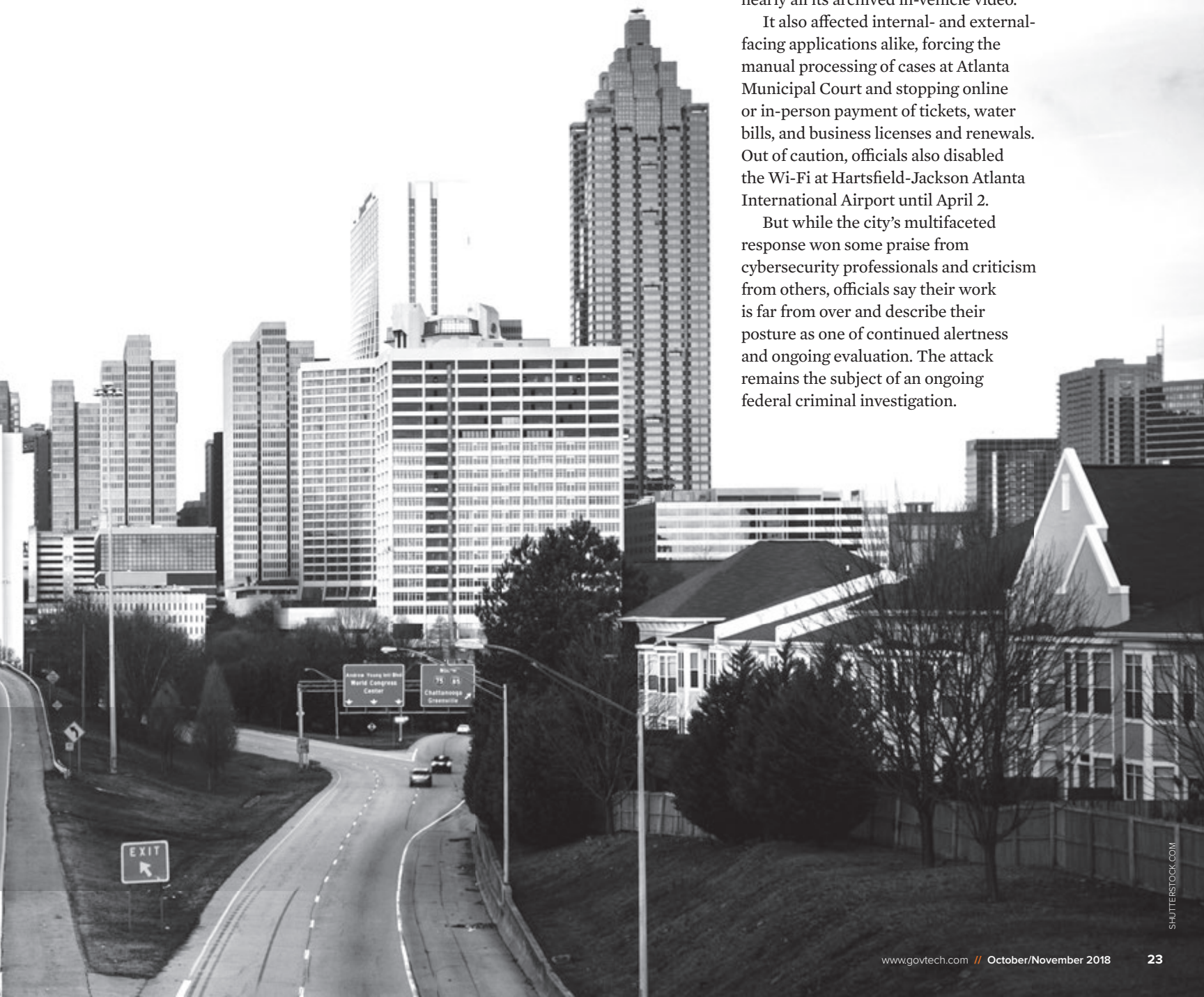
**THE RANSOMWARE ATTACK THAT WREAKED HAVOC
ON THE CITY MAY BE A HARBINGER OF MORE SOPHISTICATED
ATTACKS TO COME. By Theo Douglas**

ING NTA

In the early morning of March 22, a large ransomware cyberattack dealt a widespread blow to the city of Atlanta, the state capital and home to the nation's busiest airport. The breach shuttered many devices at City Hall for about five days in an extensive infection. Elsewhere across the enterprise, it significantly impacted law enforcement — temporarily returning police to writing incident reports by hand and costing the department access to nearly all its archived in-vehicle video.

It also affected internal- and external-facing applications alike, forcing the manual processing of cases at Atlanta Municipal Court and stopping online or in-person payment of tickets, water bills, and business licenses and renewals. Out of caution, officials also disabled the Wi-Fi at Hartsfield-Jackson Atlanta International Airport until April 2.

But while the city's multifaceted response won some praise from cybersecurity professionals and criticism from others, officials say their work is far from over and describe their posture as one of continued alertness and ongoing evaluation. The attack remains the subject of an ongoing federal criminal investigation.



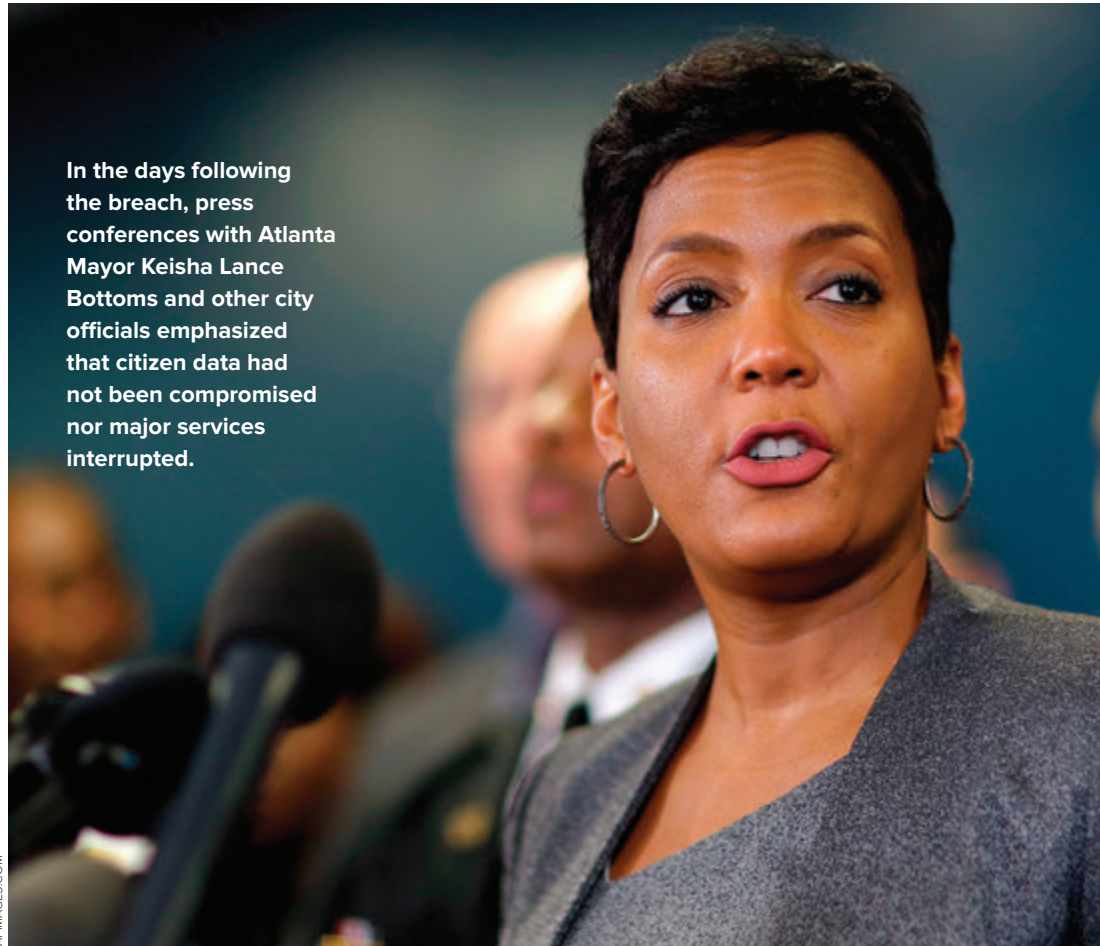
In May, the city restored its online water bill payment system, and the court's online bill payment option and docket boards returned in June. Any additional systems not yet restored, according to then-Interim CIO Daphne Rackley, are minor, lower-impact systems and are being closely scrutinized for their enterprise-level usability.

Historically, the attack on Atlanta is considered the largest, most expensive cyberdisruption in city government to date. A troubling new trend may be part of the reason why the attack was so pervasive. Ransomware attacks have become more sophisticated, according to Kevin Haley, Symantec's director of product management for security technology and response. Bad actors who entered the arena when the crime rose in popularity about two years ago have since left it to criminals who are really good at what they do, he said.

"I think many of us think that sort of thing is just not going to happen to us. You may be one of the lucky ones, but it's less and less likely that you're going to be one of the lucky ones every day," said

In the days following the breach, press conferences with Atlanta Mayor Keisha Lance Bottoms and other city officials emphasized that citizen data had not been compromised nor major services interrupted.

AP IMAGES.COM



“ I THINK MANY OF US THINK THAT SORT OF THING IS JUST NOT GOING TO HAPPEN TO US. YOU MAY BE ONE OF THE LUCKY ONES, BUT IT’S LESS AND LESS LIKELY THAT YOU’RE GOING TO BE ONE OF THE LUCKY ONES EVERY DAY.

Haley. Lower-level, lower-cost attackers are still out there, but the duration of service impacts in Atlanta and the potential cost of the city's response to the breach confirm a significant event occurred.

Brian Calkin, vice president of operations at the Multi-State Information Sharing and Analysis Center (MS-ISAC), supports the sophistication theory. Attackers are well aware they can increase ransom demands proportionately relative to the amount of data they encrypt, he said.

Marc Spitler, senior manager at Verizon Security Research and co-author of its most recent *2018 Data Breach*

Investigations Report, also sees a disturbing trend toward more professional attacks aimed at government and other institutions. "The breadth of the attack certainly shows that this was not your everyday, fire-and-forget, see-if-someone-takes-the-bait-style of attack," he said.

Despite the breach, Atlanta's 911 system and its emergency response were unaffected; and major utilities including water and sewer services continued unabated, said Roy Hadley, attorney at Adams and Reese LLP in Atlanta and legal counsel for cybersecurity controls to the city. This was possible because Atlanta retained

the manual processes and institutional knowledge it needed to revert to traditional methods of service provision; and had plans in place to keep doing business while the incident unfolded, said Hadley and other city officials.

As the city responded to the breach, business continuity and operational impact assessment were going on simultaneously, said Ria Aiken, Atlanta's director of the Office of Emergency Preparedness.

"A lot of municipalities and private-sector counterparts get so caught up in the response effort that they don't recognize that as part of that response, you should



immediately be thinking about how you are going to continue operations,” she added.

City officials quickly reached out to the FBI, the Department of Homeland Security and the Secret Service and experts in the private sector, including Secureworks, as well as incident response teams from Microsoft and Cisco. They also worked with staff from Atlanta Information Management (AIM) to identify the threat and its magnitude, and to protect the perimeter of the technology footprint.

To keep residents and the media informed about the problem, the city utilized social media, adding a page to its website with information and news about the response and embedding video of two press conferences with Mayor Keisha Lance Bottoms. In the days immediately after the breach, C-level executives including Rackley and Chief Operating Officer Richard Cox joined Bottoms at

press conferences that were livestreamed. Bottoms emphasized the uninterrupted availability of major public services and said residents’ information was not believed to have been compromised.

Calkin said MS-ISAC, part of the not-for-profit Center for Internet Security, offered to assist the city but got no response because they were busy, he assumed. “It sounds like they did everything that they could, leveraged all the resources both from the federal side and the private sector,” he said.

“To be able to pull that off successfully and then end up with a mitigated incident at the end, I think, speaks a lot to their strategy on how they’re coordinating all of this. And how well it’s going,” said Calkin, who characterized the breach as “significant.”

City officials have said little about the type of attack leveled against the city, its origin and whether they met attackers’ demands. But earlier this year, Kennesaw State University Professor Andrew Green, who lectures on information security and assurance, reviewed screengrabs of information from an Atlanta NBC affiliate and said it’s likely the attack was based on a virus from the Samas or SAMSAM family, which typically encrypts information or portions of a disk. The bad actor or actors in this breach reportedly demanded payment of around \$50,000 in bitcoin.

Green criticized the city for withholding details about the attack. “I find it disappointing that the city has chosen to stay mostly closed-mouthed about the incident,” he said in an email. But Hadley pointed out that the criminal investigation led by the FBI is still ongoing, which “limits what we can say in terms of the vectors and the actual variant of the malware and stuff like that.” Atlanta City Council President Felicia Moore confirmed that the City Council hasn’t received “the extreme details” either, but acknowledged the sensitivity of the situation.

“The day-to-day operations is the responsibility of the executive branch and to the extent that it had sensitive security information, I think you have to accept that you don’t want to push for something that could jeopardize what they’re doing,” Moore said.

RANSOMWARE COSTS ON THE RISE

Symantec’s 2018 *Internet Security Threat Report* pointed out that ransomware infections have steadily increased year-over-year since 2013, reaching a record high of 1,271 detections per day in 2016. However, in 2017 the number of new types of ransomware actually dropped, indicating a lack of new attack groups, according to the report.

While the number of attacks may be fluctuating, ransomware is no longer considered just another tool for cybercriminals. According to Symantec, ransomware is morphing into a highly sophisticated weapon of choice. For example, attack groups, including nation-states, are using ransomware to raise revenue, such as badly needed foreign currency reserves. Ransomware has also been used as a decoy to steal data or to sow confusion and to delay an effective response, which was the case when hackers used it to disrupt the electrical grid in Ukraine.

However, ransomware attacks continue to be costly. In 2017, costs from ransomware attacks reached \$5 billion, 15 times the amount in 2015, according to CSO Online; damages from ransomware in 2019 are expected to hit \$11.5 billion, according to Cybersecurity Ventures.

The cost of the city's response to the cyberattack is also unclear, Aiken said, in part because while the city has cyber-insurance, the reimbursement process is ongoing. Citing a confidential, seven-page document it obtained in collaboration with a television news station, the *Atlanta Journal-Constitution* reported in August the city's cost could top \$17 million, a figure Moore also mentioned. "The last I heard, we were around \$17 million, and it may be more. It's not a static, one-time thing. It's gone toward the emergency shoring-up, emergency procuring, for people, the company we hired," Moore said.

The city council president's characterization of Atlanta's response — as an ongoing, evolving matter — reflects the city's actual strategy following the breach and for the foreseeable future, officials said.

"We really want to look holistically at our applications and really rationalize applications," Rackley said, noting that when the cyberattack happened, Atlanta had plans in place to migrate some applications, and had already moved its email systems and main enterprise resource planning system to the cloud.

According to Hadley, not all services will be 100 percent until that evaluation is complete. "As the threat continues to evolve, the city's posture, architecture and holistic view will continue to evolve," he said. "We're restoring stuff but we're also taking the opportunity to revalidate things and say 'OK, is there a better way, a safer way, a more secure way in order to continue to provide these functions to the citizens of Atlanta?'"

When it comes to best practices to avoid a debilitating cyberattack, outright prevention should be a goal, said Verizon's Spitler. IT officials must know their network architecture, invest in email infrastructure, and remain vigilant at all levels, scrutinizing emails and their attachments and looking for browser vulnerabilities. Multi-factor authentication is immensely valuable and segmentation is crucial, he added.



Finally, state and local governments should have security zones segmented well within their own network to hinder bad actors from moving laterally should they open one device by brute force.

"If you cannot get on one system, then you cannot use that system to get on another one," said Haley, the Symantec executive, who also urged agencies to have a plan to do backups, to back up data regularly and make it secure; and to be prepared to quickly take infected machines off the network should an incident or breach occur. He recommended agencies consult guidelines from the National Institute of Standards and Technology.

Calkin said governments should do regular user training and awareness, which are "often overlooked," despite the fact that many compromises the organization has seen come from people "receiving phishing emails and clicking on links or opening malicious attachments."


Atlanta officials highlighted the importance of protecting government data and information, and of bringing discipline to an agency's approach to cybersecurity. According to Rackley, the city's approach to cybersecurity rests on three pillars: governance with compliance, vulnerability management and overall threat management. In addition to limiting the financial impact of an incident or breach, a cyberinsurance policy can serve as a road map and help an agency develop

the sustained drive it needs to further its cybersecurity goals, Hadley said.

"Part of the takeaway would be yes, get insurance. But use that insurance and the process of getting it to take a more critical look at what you're doing as a municipality. Because it can help you figure out where you need to go, from a planning standpoint, from a resource standpoint," Hadley said.

He also stressed the value in connecting with potential partners in the public and private sectors before an incident or breach occurs; and of identifying available resources before they may be critically needed.

But equally valuable is the idea of taking a step back from the smaller day-to-day tasks of enterprise-level IT management and cybersecurity to see the larger view. Getting the big picture, they noted, can better inform C-level executives on the individual surfaces in their enterprise; identify existing IT investments and any roadblocks such as siloing; and help reduce unnecessary applications.

"Our ultimate goal continues to [be to] evaluate the overall architecture, infrastructure, and evaluate our understanding of what the interdependencies are between systems and minimize the vulnerability of bringing particular applications online," Aiken said. "Quite honestly, this will never stop. Because this is truly our core of our governance." 

tdouglas@govtech.com



Congratulations

to the 2018 Special Districts Technology Innovation Award Winners!

MIDWEST REGION

LEADERSHIP CATEGORY

Wesley Goodwin

IT Manager, Applications,
Greater Cleveland Regional
Transit Authority, Ohio

OPERATIONS CATEGORY

Wet Weather Map

Great Lakes Water Authority, Michigan

CITIZENS CATEGORY

Website Redesign

Chicago Park District, Illinois

SOUTHEAST REGION

LEADERSHIP CATEGORY

Edward L. Johnson

Chief Executive Officer,
Central Florida Regional
Transportation Authority

OPERATIONS CATEGORY

Remote Monitoring of Plant Operations

Key Largo Wastewater Treatment District, Florida

CITIZENS CATEGORY

Landlord Program Enhancements

Atlanta Housing Authority, Georgia

To learn more about the winners' initiatives and the Special Districts Program, visit:

www.govtech.com/districts

AN AT&T
PROGRAM



government
technology

ARMS

New technologies have emerged to help fortify cyberdefenses. Will they work for government?

BY TOD NEWCOMBE

IRAN, desperate to boost revenue following the return of sanctions imposed by the United States, has encouraged its hackers to pursue ransomware attacks on individuals and organizations, according to a report in the *Wall Street Journal*. “Cryptomining and theft is an opportunity to get cash for cash-strapped countries,” Keith Alexander, former director of the National Security Agency and U.S. Cyber Command, told the *Journal* in August.

Back in the United States, the number of state and local governments and agencies that have suffered ransomware attacks has continued to grow. During the month of July alone, *Government Technology* reported hacks in Riverside, Ohio, the state of Alaska and Washington, D.C. Earlier in the year, Atlanta suffered one of the worst ransomware attacks ever recorded against a government (see p. 22).

These anecdotes provide a glimpse of what has become a tech problem that has grown so significant that it nearly overwhelms discussion of all other topics in the gov tech space. The explosion in cyberthreats and data breaches has

RACE



fueled the growth of cyberdefense products and services. In 2004, the military and civilian cybersecurity market was a modest \$3.5 billion, according to Cybersecurity Ventures, a research firm. Last year, organizations spent \$120 billion on tools and products, and the market is expected to grow by an annual rate of 12 to 15 percent for the next three years.

The cybersecurity market is also becoming more complex as it responds to the increasing number and type of attacks and threats. CB Insights, a market research firm, categorizes cybersecurity into 11 different markets, ranging from mobile and cloud security to threat intelligence, behavioral detection and even quantum encryption (see sidebar).

Despite the fast-growing number and range of products and services, a few key trends are emerging when it comes to security and risk management. First, executives, both in the public and the private sectors, are finally aware that cybersecurity has a significant impact on the ability to achieve business goals and to protect an organization's reputation, according to a recent report by Gartner, the technology research firm. Legal and regulatory mandates to protect data are impacting business plans and have increased the emphasis on data liabilities.



Georgia Chief Information Security Officer Stan Gatewood has made threat analytics a key component of the state's cybersecurity strategy.

carry out what was a laborious maintenance task, resulting in gaps of coverage that hackers could easily exploit. "But the cloud allows vendors to deliver security products that are more agile and easier to maintain," he said.

The cloud also provides security vendors with a stream of data from their customers about the size, scope and type of threats

in privacy, data protection and information security practices. "It was once considered sacrilegious to put government data in the cloud," he said. "But in reality, the cloud is even more safe than on-prem. That's important, especially for small governments that don't have the resources for security."

IN 2017, ORGANIZATIONS SPENT **\$120 BILLION** ON CYBERSECURITY TOOLS AND PRODUCTS.

Gartner also highlights some specific trends as far as cybertechnology:

- Security products are rapidly exploiting cloud delivery to provide more agile solutions.
- Machine learning is growing to perform simple security tasks and can elevate suspicious activity for human analysis.

Peter Firstbrook, an analyst with Gartner who co-authored the report, pointed out that traditional, on-premise cybersecurity tools suffered because updates were often delayed for months, if not years, not by the vendors, but because IT departments were slow to

and hacks in real time, allowing them to respond faster. "They can provide services quickly, such as whether there's an intruder, what should be done next and how to solve the incident," said Firstbrook, who cited a service from CrowdStrike called Falcon Overwatch that does just that.

The cloud's ability to deliver high-end security without the need for a robust, on-premise, digital infrastructure gives it a special value in the public sector, especially among small government entities, explained Larry Ponemon, founder of the Ponemon Institute, a research think tank specializing

The emergence of the cloud has not only changed the agility of cybersecurity technology, but it has also impacted how hackers go after data, according to Firstbrook. As workloads and the productivity tools that run them have shifted to the cloud, the level of security from the major vendors, like Microsoft, has increased significantly. As a result, it has become harder for attackers to find a way to break into a PC and steal data. "Instead, they go after your authentication," said Firstbrook. "So, now they go after your [cloud] account by sending a phishing email, trick you into giving them your credentials and then lock you out and steal your data."

To counter this kind of threat escalation, many organizations have stepped up their awareness training for employees, to educate them on how to spot a phishing campaign and avoid having their credentials stolen. But there are other things that governments can do. First, by using multi-factor authentication solutions, government can make it harder for the attacker to take over the account, especially when work is increasingly in the cloud. Multi-factor authentication forces the hacker to steal not just a login and password, but also the person's unique token.

But Firstbrook said that organizations also need to monitor their accounts for suspicious activity. To do that requires threat analytics, part of a new trend that mirrors the growth of data analytics. In Georgia, threat analytics has evolved into an important cybersecurity strategy, according to Stan Gatewood, Georgia's chief information security officer (CISO). "We want to use threat analytics, user analytics and predictive analytics on all that data that's moving through our networks. We want to look at it and be able to predict what might happen."

It's the same reason Florida is using threat analysis along with more traditional security practices, such as security information management (SIM) and firewalls. "Threat analytics is about using the information you gather internally from SIMs and combining it with external sources as well as some of our own capabilities," said Thomas Vaughn, the state's CISO. "The data enriches what we are seeing in our environment and allows us to see threats that are impacting our environment," he said.

Analytics can also be brought to bear on user behavior. "Behavioral analytics considers how a user performs certain actions, and then by looking at the patterns created by certain individuals, we can determine if their actions may be dangerous for the network or may indicate something nefarious," he explained.

Ponemon calls threat analytics one of the smart investments his organization sees happening in both the public and private sector as a way to thwart the rise in cybercrimes and -attacks. "Threat intelligence or analytics is about getting

SHUTTERSTOCK.COM



CYBERSECURITY MARKET

One measure of just how important cybersecurity has become is to look at the number of startups that are investing in the field and where they are putting their money. CB Insights, a market intelligence firm, identified 106 cybersecurity startups in 2016, and mapped them to 11 main categories for security:

NETWORK AND ENDPOINT SECURITY

This is the largest startup security market, according to CB Insights, and includes firms that specialize in protecting enterprise computer networks from vulnerabilities.

IOT/IIOT SECURITY

This category includes firms that provide protection for connected vehicles and industrial control systems.

THREAT INTELLIGENCE

Startups in this category focus on targeting malicious activity on the deep Web to uncover potential threats and thwart attacks.

MOBILE SECURITY

This security category includes firms that provide enterprise mobile threat protection for Android and iOS devices.

BEHAVIORAL DETECTION

Companies are developing technology to detect abnormal behavior in order to identify threats and manage risks.

CLOUD SECURITY

This category of startups offers enterprise solutions for secure application delivery across all types of cloud technology.

DECEPTION SECURITY

Companies in this category can identify, deceive and disrupt attackers before they cause harm.

CONTINUOUS NETWORK SECURITY

Solutions in this category visualize network activity and response to attacks in real time.

RISK REMEDIATION

Companies look for vulnerabilities in technologies, people and processes and then give recommendations on how to plug the gaps.

WEBSITE SECURITY

Security firms offer website developers the ability to identify and police malicious website traffic.

QUANTUM ENCRYPTION

Using the science of quantum mechanics, startup firms in this category offer encrypted wireless and data communications technology.

SOURCE: CB INSIGHTS

more information from different sources about risk and threat vectors, what kinds of vulnerabilities an organization faces — the big picture,” he said. “Analytic tools are very effective in helping organizations manage their security in a systematic way that optimizes the budget.”

To make the most of threat analytics, states have hired analysts to carry out this critical cybersecurity function. But as Gartner’s 2018 trend report shows, machine learning presents an opportunity to automate some of the simpler threat intelligence tasks, such as identifying a problem and then elevating suspicious events for human analysts to evaluate. Machine learning can solve multiple security issues, such as authentication, insider threat, malware and advanced attacks, according to Gartner. By 2025, machine learning is expected to be a normal part of security practices.

This form of artificial intelligence, in which computers look for certain types of patterns, learn from them and refine their ability to detect anomalies in the data, is beginning to catch on. Ponemon Institute surveyed companies and found that 15 percent have either partially or fully deployed AI technology. “That’s higher than we thought,” said Ponemon, who pointed out that companies are increasing their purchases of AI security tools because they see value in those investments. However, the new technology is not replacing existing systems so much as augmenting them.

Gartner warns that applying machine learning well enough so that it actually detects something new and different in terms of a threat can be difficult. “There are gradients of machine learning,” said Firstbrook. “It’s not a perfect identifier of a threat. The technology tends to cause more false alerts and false positives.” For example, intruders can camouflage themselves in what appears to be normal activity. They can also evolve quickly and move in directions not addressed by existing machine learning algorithms.

Gartner recommends machine learning for addressing narrow and well-defined problems, like classifying executable

THE MARKET FOR CYBERSECURITY TOOLS IS EXPECTED TO GROW AT AN ANNUAL RATE OF 12 TO 15 PERCENT FOR THE NEXT THREE YEARS.

files. And it can help short-staffed security teams be more efficient, “find threats they couldn’t before, perform investigations more efficiently, and better anticipate future threats and risks.”

Gartner’s assessment of machine learning, AI and automation fits with how Florida’s Vaughn views the technology. “We tend to talk about AI and machine learning as topics unto themselves, but from my perspective, these technologies are enhancements that are being added to tools we already have,” he said. Vaughn pointed out that his team has been doing correlation searches for a long time, using data from the state’s firewall as well as data from SIM and malware tools. But with AI and machine learning, he can automate that correlation effort. “But it doesn’t change the core functionality of the SIM when you do that, it just adds an enhancement.”

In August, a research team from IBM revealed during a Black Hat security conference in Las Vegas that it had built a machine learning program that could slip past some of the most sophisticated cyberdefense measures. According to Reuters, the announcement could foreshadow a new generation of AI software that can be “trained to stay dormant until they reach a specific target, making them exceptionally hard to stop.”


Because the cost of AI software continues to drop — and in some cases can be used for free — the likelihood of

some bad actors creating these sorts of next-generation cyberthreats is a growing concern, according to experts. For state and local governments, strained by lack of resources and already exhibiting a wide range in the quality of cybersecurity, a further leap in the sophistication of cyberthreats comes at a bad time.

In 2017, the Ponemon Institute researched the challenges in public-sector IT operations and found that confidence in current IT performance has declined, with survey respondents pointing to an ongoing lack of tools, skills and resources that has degraded performance since 2016. One key point was that the majority of IT decision-makers and staff in the public sector are unsure or “don’t think the data sets they are using can solve multiple challenges, such as IT troubleshooting, service monitoring, security and mission analytics.”

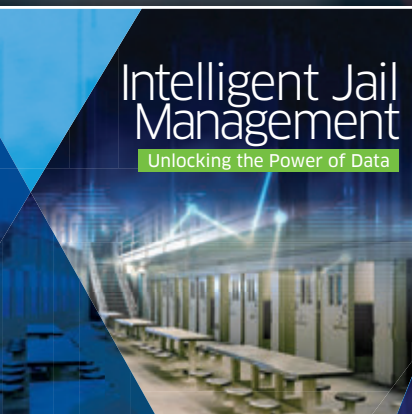
While that’s a problem that extends to all aspects of government IT, it is a particular challenge in IT security, where intruders and hackers are exploiting new vulnerabilities daily, making it vital that government build up the right resources against cyberattacks, whether they come from the next town, the next state or half way around the world, such as Iran or North Korea.

Firstbrook laid out the dilemma government faces as cyberthreats grow while investments in the latest IT security products and strategies continue to stagnate. “Government is stuck with legacy systems, so it’s unlikely they can wipe everything out and start over with an entirely new IT system that is entirely secure,” he said. To counter that problem, government needs to be cognizant of how hackers, intruders and data thieves operate.

“Attackers go after vulnerabilities that are generally well known. Their business model is built around a known vulnerability, where there are lots of potential victims,” he said. “You don’t have to be the Department of Defense [when it comes to cybersecurity], but you do have to be better than the next guy. You don’t want to be an obvious victim. That’s how they get you. If you have an open or exposed vulnerability, you are an easy target.” 

tnewcombe@govtech.com

Stay up to date on the latest trends and gain insights into some of your most pressing challenges.




Intelligent Jail Management

Unlocking the Power of Data

Incarceration is one of the costliest components of the criminal justice system.¹ And even though jails and other detention facilities are 24/7 data factories — generating volumes of information about offenders, booking, housing, health care, correctional officers and more — many are unable to harness that data to help control costs and manage facilities effectively.

Business intelligence solutions enhance the value of data by providing clear, accurate and actionable insight into what has happened and what's likely to happen in a facility. Using dashboards, operational reporting, data modeling, predictive analytics and other business intelligence tools, jail managers can go beyond basic record-keeping to not only reduce incarceration costs, but also track trends, predict outcomes, set short- and long-term goals, inform policymaking, minimize liability, and ensure compliance with federally imposed population caps and other government requirements.



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's client time is set.

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 Scott 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 build a prebuilt template that reflects a typical records request workflow and automates task routing, document forwarding and due date reminders.

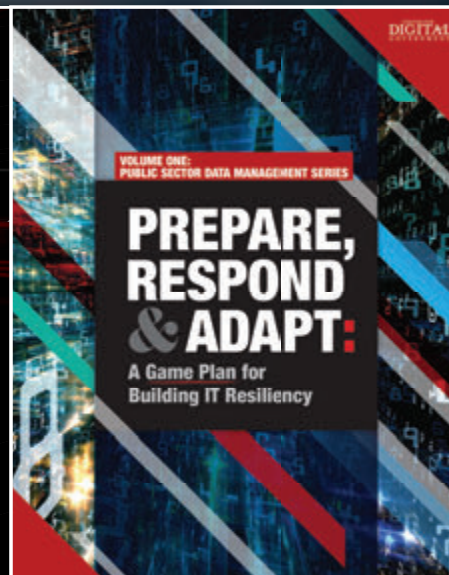
Using Laserfiche to create online forms and automate workflows is a significant part of this county's initiative to mitigate declining tax revenues by reducing direct costs and working with lower expenditures.

"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 \$5 to \$6 million in FY 2018. A program that employees still find to have 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 firing up quickly and involves:

- Tracking the status of required actions for each department and automatically sending reminder emails about items due
- Supporting retention 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 department request
- Holding 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 sending an invoice when the response work is finished



PREPARE, RESPOND & ADAPT:

A Game Plan for Building IT Resiliency

VOLUME ONE: PUBLIC SECTOR DATA MANAGEMENT SERIES



A ROADMAP TO INTEGRATED CYBER DEFENSE IN GOVERNMENT

A NEW APPROACH STRENGTHENS CYBERSECURITY AND MAKES BETTER USE OF BUDGET AND STAFFING.

Visit our website for some of our most recent work!
www.govtech.com/library

CLOUD-POWERED BACK OFFICE PAVES WAY TO MODERNIZATION IN ST. CROIX COUNTY



Although small local governments are under pressure to modernize operations, the budgets and resources needed to do so are often out of reach. St. Croix County, Wisc., is one of many organizations pursuing a strategy to rapidly bring their financial and human resource (HR) systems up to speed, deliver new services and prepare for the future, all by using applications powered by cloud computing.

Like many smaller entities, St. Croix County (population 89,000,¹) is working to meet the rising expectations of citizens who look to their local government to provide the same convenient, innovative digital services as a private company — whether that's using a computer or smartphone to pay property taxes, obtain a license, report potholes, check on the status of a contract bid or do other city business. Citizens also want financial transparency so they can see how their tax money is being spent.

A popular destination for outdoor enthusiasts, St. Croix County is also an attractive location for residents who may work in the nearby Minneapolis/St. Paul hub but crave a more affordable, suburban lifestyle. Similar to their big city counterparts, leaders in such counties and smaller towns recognize the potential of smart city implementations to streamline operations, deliver innovative services and generate revenue from the data they collect.

St. Croix County implemented cloud-native Oracle Enterprise Resource Planning (ERP) and Human Capital Management (HCM) services to integrate data across the organization and change the way that every department does business. In doing so, the county has laid a foundation for modernization. Central to its implementation success is Oracle Platinum partner CherryRoad Technologies, a full-service consulting firm with more than 30 years of experience in modernizing, optimizing and managing complex back-office processes and technologies for the public sector.

Mobile procurement is just one example of the solution's impact. For instance, when social workers conduct in-home or facility visits, they no longer need to come back to the office to order supplies for their client. In addition, information about vendors and other services is at their fingertips. The same is true for parks and facilities workers, highway crews and others in the field who can now order parts from the job site.

On the HR side, employees can submit their time cards electronically, and managers can approve expense reports and handle other HR-related tasks from their mobile devices.

STANDING STILL IS NOT AN OPTION

St. Croix faced challenges familiar to many government leaders. Before adopting Oracle's cloud-native services, the county used a legacy financial system with limited functionality.

Data came from disparate databases, spreadsheets and other sources, and had to be gathered and entered manually into the finance system. The process was time consuming and unwieldy, which hindered reporting and limited transparency as well as the timely delivery of important information to citizens and business decision-makers. It was not unusual for project management teams to be weeks behind in knowing how much money had been spent on a project. When citizens needed information, they would have to come into the government center, file a public records request and wait for the small office staff to fulfill the request. Another persistent problem was keeping the system updated — never mind modernizing it.

County leaders knew they could not meet stakeholders' needs without up-to-date technology. They realized that with the old system, standing still was not an option, as it was impossible to catch up with advances in technology.

SELF-SERVICE FOR EVERY DEPARTMENT

St. Croix County leaders wanted a cloud-native solution that would allow them to capture data more efficiently. The county needed to start fresh with a system that integrated everything, was easily accessible and had every employee working on the same system. And, of course, the solution needed to fit within the county's tight budget.

With Oracle's cloud-native ERP and HR services, staff can access data and programs from anywhere. Moreover, staff can avail themselves of the industry-standard workflow built into the system, which also helps ensure painless future upgrades.

Prior to modernization, the county was not able to encumber funding because it lacked a purchase order system. Through Oracle's procurement functions, budgetary and purchasing controls are built into the workflow. When an employee makes a purchase, it now flows automatically to the correct cost center and account.

Take the highway department, for example. The county builds and maintains its own roads, and can easily spend one million dollars in a single day. Staying on track is now possible, and finance managers now know how much money

is encumbered. The solution also helps with compliance and reporting on state-regulated services such as the county's nursing home.

The service's intuitive reporting features have also been a huge boon in terms of expediting decision-making and reducing reliance on analysts and IT staff. In the past, departmental employees had to depend on IT or the finance department to pull reports, and often waited one or two days for results. Today, these employees can immediately generate their own reports with easy-to-use tools and a user-friendly interface.

And, as a wave of workers retire, Oracle's HR reporting and talent management tools will expedite the hiring and onboarding of new employees.

However, the built-in functionality and ease of use weren't the only advantages that attracted the county. Because the service is cloud-based and maintained by Oracle, the county's back-office systems will always be on the leading edge of innovation and technology. System updates are organic, and the county no longer bears the operational and financial burdens of maintenance. In addition, systems can easily expand to accommodate the county's growth.

A NEED FOR EXPERTISE

St. Croix had never implemented any kind of system of this magnitude, and needed a partner who knew the Oracle system and had public sector experience. CherryRoad was instrumental in providing the expertise, services and long-term support that St. Croix County needed to be successful.

The CherryRoad team could predict how certain decisions would impact the county in the future.

"We saved St. Croix a lot of time and heartache," says Stephen Lange, CherryRoad president and chief operating officer. "We helped navigate new workflows and processes that made sense for them."

The smaller scale of St. Croix County was ideal for a cloud-based solution.

"Five years ago, St. Croix would have purchased a Tier 3 system that would not be able to change with its needs," says Lange. "Today, cloud can revolutionize the way local

government does business by ensuring that their systems will always be up to date with the latest software."

Best Practice Tips from St. Croix County

Besides teaming up with a partner like CherryRoad, the following are some recommendations from St. Croix County officials to help their peers throughout the country transition to the cloud:

- **Get help with the RFP** – The county enlisted the Government Finance Officers Association (GFOA) to help draft the RFP and review responses.
- **Review data early** – Organizations should decide what data they want to move to the cloud and remove or update data that is obsolete, redundant, incomplete or improperly formatted.
- **Supplement staff** – The county brought on temporary staff to help backfill key positions during set up and throughout the process. Testing and training can consume a lot of time from the regular workload of employees.
- **Manage change** – Involve employees and obtain their buy-in as a vital component to success.

READY FOR THE FUTURE

Moving forward, the county plans to bring in more employee self-services and overhaul its point-of-sale (POS) system to make it more user friendly. The opportunities will continue to unfold as the county rolls out new features and more data is added to the system. In the meantime, migrating finance and HR applications to the cloud is already paying off by bringing insights, efficiency and innovation to the workplace and the community — without the costs, complexity and built-in obsolescence of an on-premises solution.

1. https://factfinder.census.gov/faces/nav/jsf/pages/community_facts.xhtml?src=bkmk



Learn more at **ORACLE.COM/PUBLICSECTOR**

SETTING THE CYBER SCENE



HOW IT RANKS

Here's how CIOs rank cybersecurity on their priority lists.*



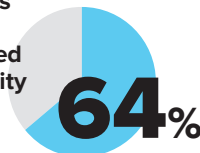
**HALF OF THE
PASSWORDS OF
GOVERNMENT
EMPLOYEES,
INCLUDING
MILITARY,
CAN BE HACKED
IN LESS THAN
TWO DAYS.**

Source: WatchGuard Technologies

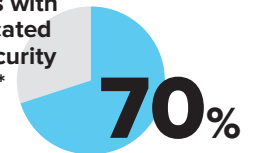
RISE OF THE CISO

States responding to the 2016 Deloitte-NASCIO Cybersecurity Study unanimously reported having an enterprise-level chief information security officer (CISO). In September 2017, Alaska joined their ranks with the appointment of the state's first-ever CISO, **Shannon Lawson**.

Counties with dedicated IT security staff:*



Cities with dedicated IT security staff:*



MORE, PLEASE

Increased need for cybersecurity workforce over the next few years:*



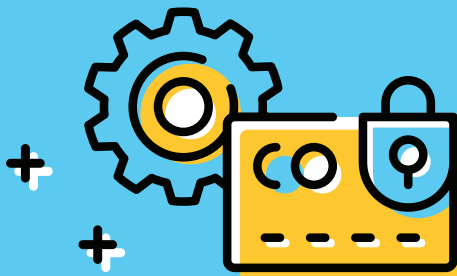
+ According to the National Initiative for Cybersecurity Education, **285,000 cybersecurity positions went unfilled in 2017**. *Cyber Defense Magazine* reports that by 2022, 1.8 million additional people will be needed to fill open jobs in cyber.

*Source: Center for Digital Government



21%
OF ALL FILES
ARE NOT
PROTECTED IN
ANY WAY.

Source: Varonis



**THE MEDIAN DWELL TIME
(NUMBER OF DAYS BETWEEN
FIRST EVIDENCE OF A
COMPROMISE AND DETECTION)
IN THE UNITED STATES WAS
75.5 DAYS IN 2017, COMPARED
WITH 99 DAYS IN 2016.**

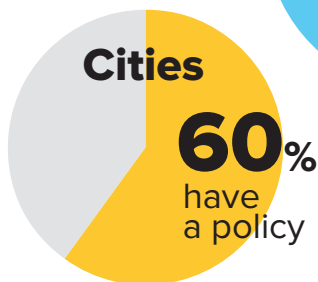
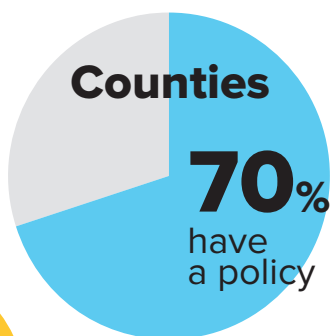
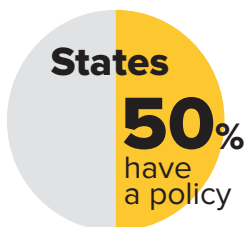
Source: Mandiant M-Trends 2018

\$120B
IN 2017



PROTECTED?

Cyberinsurance has reached the tipping point.*



A GROWTH INDUSTRY

ACCORDING TO RESEARCH FIRM
CYBERSECURITY VENTURES, IN 2017,
TOTAL SPEND ON CYBERSECURITY TOOLS
AND PRODUCTS WAS \$120 BILLION, UP
FROM \$3.5 BILLION IN 2004. AN ANNUAL
GROWTH RATE OF 12 TO 15 PERCENT IS
EXPECTED FOR THE NEXT THREE YEARS.

+ They also
estimate that
cybercrime-
related
damage will
hit \$6 trillion
annually by
2021.

\$3.5B
IN 2004



ACCORDING TO CISCO, FILE
FORMATS FROM MICROSOFT,
NAMELY WORD, POWERPOINT
AND EXCEL, ARE THE MOST
COMMON MALICIOUS FILE
EXTENSIONS, REPRESENTING
38 PERCENT OF THE TOTAL.

Source: Cisco

THE “PUBLIC ADMINISTRATION” SECTOR HAS THE HIGHEST RATE OF EMAIL-BORN MALWARE ACCORDING TO SYMANTEC, WITH 1 IN 120 EMAILS CONTAINING MALWARE. IN 2017, THAT TRANSLATES TO EACH USER AVERAGING A LITTLE MORE THAN ONE EMAIL CONTAINING MALWARE PER WEEK. PHISHING ATTACKS ARE MORE COMMON, WITH USERS IN PUBLIC ADMINISTRATION GETTING ONE PER 38 EMAILS RECEIVED.



4%
**OF PEOPLE
WILL CLICK
ON ANY GIVEN
PHISHING
CAMPAIGN.**



Source: Verizon

BREACHED

Several notable breaches impacted government in the last year — by no means an all-inclusive list.



CONFIDENTIAL BASE INFO EXPOSED

Fitness app Strava made an effective case for its far-reaching user base in November 2017, putting out an interactive map that plotted 13 million data points showing how people used the app to work toward their health goals. But some of those users were active members of the military. In January, the Institute for United Conflict Analysis uncovered the fact that by putting out the map, Strava revealed the locations of U.S., Turkish and Russian military bases.

to secure a set of customer data containing personally identifiable information, passwords and payment information, exposing data on 1.3 million customers. The exposure spanned several months in early 2018. First discovered by a security firm, the breach was broadly reported by the New Jersey Cybersecurity and Communications Integration Cell, the state's threat-sharing network, aimed at protecting public, and private, organizations from cyberthreats.

Management System lasted just 30 minutes one February afternoon. During the incident, blamed on employee error, the personal data of current and former teachers was exposed.



STATE CYBERCENTER GETS THE WORD OUT

A jewelry company with a very high-profile retail partner, Walmart, failed



TEACHER DATA BRIEFLY VULNERABLE

Education systems are rich targets for would-be data thieves, so thankfully the breach of the Pennsylvania Department of Education's Teacher Information



VOTER DATA NOT SECRET

An unidentified hacker obtained two databases that the *Sacramento Bee* (Calif.) had stored on third-party servers, demanding a bitcoin ransom to recover them. Along with personal information from more than 50,000 subscribers, the hack also included voter registration data from 19.4 million California voters: addresses, phone numbers and party affiliations, as well as places and dates of birth. The newspaper didn't pay the ransom.

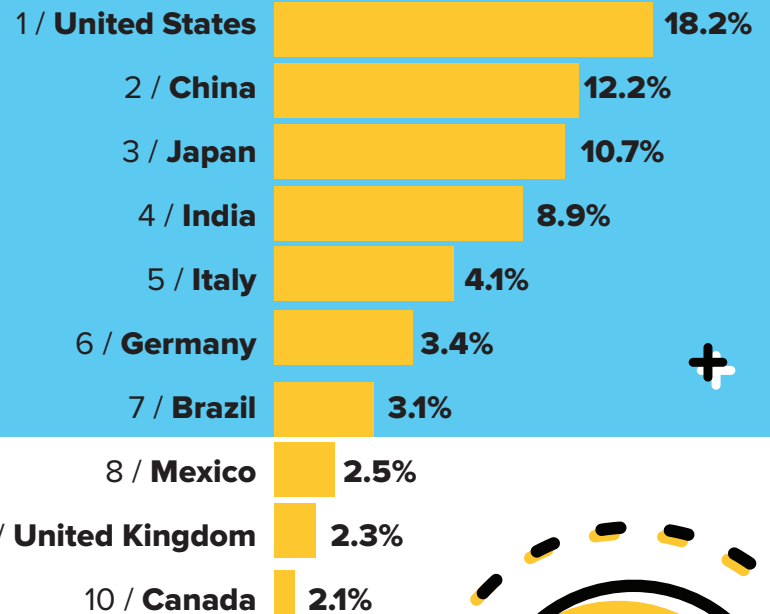


SYMANTEC REPORTS A 600% INCREASE IN ATTACKS ON IOT DEVICES BETWEEN 2016 AND 2017. THE BIGGEST SOURCES OF THE ATTACKS WERE CHINA (21%), UNITED STATES (11%), BRAZIL (7%) AND THE RUSSIAN FEDERATION (6%).



ACCENTURE REPORTS THAT THE COSTLIEST PART OF A CYBERATTACK IS **INFORMATION LOSS**, WHICH IT PEGS AT 43 PERCENT OF THE TOTAL COST. THE AVERAGE GLOBAL COST OF CYBERCRIME INCREASED BY MORE THAN 27 PERCENT IN 2017.

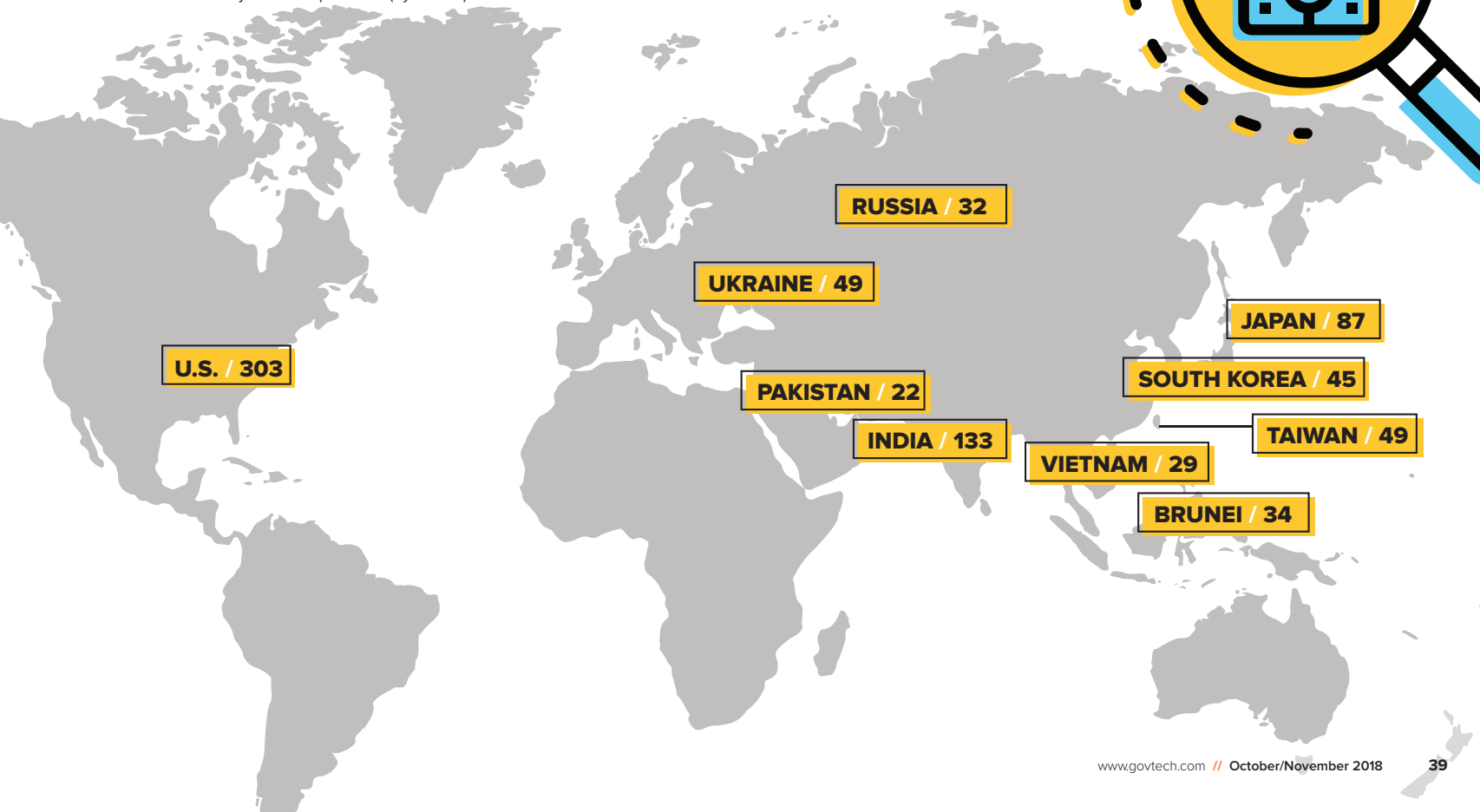
RANSOMWARE DETECTIONS BY COUNTRY



Source: Internet Security Threat Report v. 23 (Symantec)

TOP 10 COUNTRIES AFFECTED BY TARGETED ATTACKS BETWEEN 2015 AND 2017

Source: Internet Security Threat Report v. 23 (Symantec)



SECURITY BREACH

A Place for Cyber

Utah launches a multi-agency cybercenter — an idea whose time is overdue. **By Noelle Knell** / Editor

Michigan. Georgia. Colorado. New Jersey. And now Utah. The list of states with a broad coalition of cybersecurity stakeholders united in one physical space has grown steadily over the past few years. Surveys from a wide array of organizations reveal that the No. 1 priority on the minds of tech leaders in state and local government is cybersecurity. Nobody wants news of a breach to break in their jurisdiction. And as cyber has worked its way to the top of the agenda, so has the realization that the CIO's office can't tackle it alone.

Increasingly, cybersecurity has become a concern that transcends the CIO's office. *Government Technology* has tracked the growing frequency with which cybersecurity is now a part of the biggest policy speech most governors give each year: the State of the State address.

"We're doing all we can within our existing management structure to defend our state resources, and more importantly to keep our citizens' personal information safe from hackers, criminals or worse," said Idaho Gov. Butch Otter, pointing to the appointment of the state's first director of information security, Jeffrey Weak. Among Weak's activities, as outlined by Otter, is enacting strict cybersecurity standards, Internet security controls and training for every employee. In another common practice, Idaho's efforts, which include a partnership with the Idaho National Laboratory's Cybercore Integration Center, are also aimed at luring cybersecurity-related industry to the state.

As for models to emulate, many, including officials in Utah, refer to the recently opened Hull McKnight Georgia Cyber Center for

Innovation and Training as "the gold standard." A pet project of Gov. Nathan Deal, now nearing the end of his second term, the \$100 million center stands as a physical monument to the ever-broader way government is approaching cybersecurity. The 17-acre campus, when complete, will offer more than 330,000 square feet of space for various government and law enforcement agencies, academia and the private sector. It's just this kind of broad collaboration that will position states to take on the enormity of the cybersecurity challenge.

"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 and Georgia Technology Authority Executive Director Calvin Rhodes, tasked by Deal with overseeing the undertaking.



SHUTTERSTOCK.COM

Utah's Take

As for Utah, its cybercenter uses office space in the basement of the capitol building on State Street in Salt Lake City. It opened on the eve of the state's primary election in June — just in time to help ward off the influx of intrusion attempts that Utah, and so many other jurisdictions, are experiencing this election season. It's a proof of concept, of sorts, CIO Mike Hussey explained, estimating that the current space represents about 20 percent of what they need.

In answer to the question of "why now?" Utah Chief Information Security Officer Phil Bates admits that the state feels a bit behind the curve. "Five years ago was the right time," said Bates.

Long lauded as a digital leader among state governments, Utah consistently receives an "A" grade in the Center for

Digital Government's* bi-annual survey of state technology practices. With a consolidated IT environment, a lean state workforce (smaller today than in 2002), transparent, data-driven operations, and an openness to experimenting with emerging technologies, other states routinely consult Utah's example in making tech-driven improvements.

But when it comes to a multi-agency cybersecurity facility, funding has proven a challenge. Hussey estimates that the new space, about 25,000 square feet in total, would cost between \$15 million and \$18 million. If his team can secure support from the governor's office, they'll make the pitch to the Legislature early next year. Even with the funding in hand, building on Capitol Hill requires the approval of the Capitol Preservation Board, hesitant to

make any changes to the area's historical facilities. It won't be a simple process.


For now, the small-scale center unites the Department of Technology Services, the Department of Public Safety and the State Bureau of Investigation. It recently played host to a tabletop exercise that cast a much wider net: elections staff, public safety, Homeland Security and the Department of Emergency Management and more.

Ultimately, though, they envision a number of additional uses for a larger cybercenter on Capitol Hill. A bigger space would allow the state to develop partnerships with academia, establish internships to contribute to the workforce pipeline and share expertise with local governments. One place where the need is particularly acute is with counties, which are responsible for administering elections in the state.

"Counties have expressed interest in getting into the cybercenter and learning how to improve their cyberposture ... and we think that's a good idea," Hussey said.

An expanded cybercenter would also better position the state as a one-stop resource for Utah businesses needing guidance on their cybersecurity practices in order to prevent or respond to a breach. A few larger jurisdictions have started to serve this role as cyber-related concerns have increasingly permeated the private sector. Los Angeles, for example, opened its Cyber Lab in August 2017 in a partnership with Cisco to share threat information with local businesses.

"Every state needs to be looking at something like this," Hussey said, adding that when he came on board as CIO in late 2015, the state was blocking 130 million intrusion attempts daily. That number is closer to 1 billion today.

"It's not going backward. It's going to continue on this trajectory, and we need to get in front of this as soon as possible," he said. "We really need to respond now." 

nkneil@govtech.com

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



Unrelenting Threats Inspire a New Model in Texas

A managed security services contract with AT&T offers agencies prescreened cybersecurity tools — an arrangement that could take off across the country.

By Zack Quaintance / Staff Writer

The view that everybody pretty much adopts nowadays is, it's not whether or not you'll have a penetration, but how are you going to respond to it?" said Texas Chief Information Officer Todd Kimbriel at the Texas Digital Government Summit earlier this year. IT leaders in government are universally challenged by this and other questions about cybersecurity, like how to develop an effective cyberstrategy and how to find the budget to pay for it.

To make this defense easier, in July the Texas Department of Information Resources launched what it's calling a Managed Security Services (MSS) contract in collaboration with AT&T. What the MSS does, in the simplest of terms, is give state agencies, local governments, school districts and other public entities the ability to opt into a broad and comprehensive selection

of cybersecurity services, essentially using and also paying for them as needed.

The list of available services includes security monitoring for breaches, device management, risk assessments and much more. With the MSS system, governmental organizations within Texas can access those services on an individual pay-as-you-go basis via the state's master contract, rather than having to build their own cybersecurity expertise and infrastructure from scratch. The state, rather than individual users of services, is also responsible for tracking vendor performance.

The new pact with AT&T will also enable agencies to comply with House Bill 8, the Texas Cybersecurity Act, approved during the last legislative session. The bill requires state agencies to do a cybersecurity assessment every two years. But DIR, which typically funds around 15 of these assessments

through administrative fees, received additional general revenue from the Legislature — and will now fund as many as 40 assessments per year through the new contract.

"We are absolutely focused on injecting a risk mitigation evaluation strategy, so that every dollar that we invest is really targeting the high-probability, high-impact risk that we have," Kimbriel added.

All indications are that the MSS concept will likely spread to other states, with independent cybersecurity experts saying the cost-efficient nature of the system — as well as the searing importance of guarding against cyberthreats — indicates this move will be worthwhile.

Understanding MSS

The MSS' offerings can be split into three major components: security monitoring and device management, incident



response, and risk and compliance. Each of those areas then includes a subset of more specific cybersecurity-related services for jurisdictions to choose from, wrote Nancy Rainosek, Texas' chief information security officer, in an email.

Security monitoring and device management include services such as Web application firewalls, intrusion detection and prevention, and end-user device management. There is also a threat research component. Basically, this is the most practical of the three areas, containing the tools that keep actual threats at bay.

Incident response, meanwhile, is made up of a subset of services that jurisdictions can use to prepare, and respond to an attack after it has occurred. These include security incident management and digital forensics to identify in detail what happened. Risk and compliance is the final category,

and it includes testing and assessment tools that jurisdictions can use to evaluate the maturity of their cyberposture.

Texas officials reported that roughly six weeks into the life of the MSS contract system, the state had almost 30 state agencies participating so far, as well as five universities, one community college and one local government entity. All told, there had been 55 requests for cybersecurity services, several of which have already been completed.

An Effective Approach

Cybersecurity experts are bullish on this new system, citing its seeming ability to make better protections affordable for public agencies, as well as its potential to eventually be tailored for and adapted by other states.

Cory Fleming is a program director with the International City/County Management Association. Fleming said that for smaller organizations, jurisdictions or agencies, cybersecurity is just as important as it is for larger counterparts, yet smaller entities often have fewer resources with which to defend themselves.

With that in mind, the MSS model's inherent ability to foster the sharing of resources has the potential to be a major benefit for individual agencies, said Fleming, who noted this was a new and unique approach.

Strength-by-sharing benefits are certainly a consideration for Texas and its corporate partners at AT&T. Texas has noted that some of its agencies have the resources to manage cybersecurity in-house but others do not. The ones that don't can trust that the state has already vetted the services available through the contract.

In addition, those handling the services can take a holistic view of the cyber-threats Texas faces. If one service detects a threat to one agency, that becomes instant intel about that same threat elsewhere.

Another benefit is that it all leads to a better price for protection. The agencies using the MSS system need only pay the costs for the individual services they use, rather than paying a larger bill for a holistic cyberdefense infrastructure.

For the agencies, simplicity of use is a benefit too. Staff and officials from

public organizations who use MSS just have to go to the DIR portal, select the services they need and place an order. This has the ultimate result of freeing individual organizations of the need to focus as much energy or expertise on cybersecurity, returning instead to their primary mission and business functions.

MSS Takes Off

The potential for this to be adapted in other states is high, according to stakeholders and outside experts.


Fleming said the public sector has a long and ongoing history of sharing ideas and services, given that the challenges and threats faced by one entity are often the same or similar to those faced by others.

"I can see this being something that pops up all across the public-sector radar screen," Fleming said.

Officials from AT&T echoed as much, noting that while no two jurisdictions or public agencies are exactly alike, they all tend to face the same landscape of threats. George Spencer, AT&T public sector assistant vice president for Texas, said that even the size of the agency is relatively immaterial, given that smaller agencies tend to have less expertise while larger agencies tend to face a higher volume of attacks. Both face challenges this system can alleviate.

Chris Roy, AT&T's vice president of government education client group, agreed, saying the company believes this is a solution that can and will spread to other states.

"There's no reason to think the states wouldn't share this, and that other states wouldn't see this idea and grab onto it," Roy said. "The discussions we're having with several other states, frankly, are in the discovery stage. They'd like to understand what the state of Texas is doing."

As Kimbriel shared in May, a new spirit of transparency has made its way into public-sector cybersecurity — a major shift from the status quo when he first came to the state's Department of Information Resources in 2008. Within Texas and beyond its borders, people now accept that organizations are "stronger by sharing." 

zquaintance@govtech.com

Reporting from Staff Writer Theo Douglas contributed to this story.



SHUTTERSTOCK.COM

CAN YOU HEAR ME NOW?

Two-way communication is about to get a whole lot more wearable. Thanks to a multimillion dollar contract with the Department of Defense, the “Molar Mic” is coming to the mouths of the U.S. Air Force. Created by Sonitus Technologies, the custom-fit mouthpiece fits onto the wearer’s upper molars and sends audio directly to the inner ear via a bone conduction speaker. The device includes a waterproof microphone and wireless charging, and will make communication among military personnel easier in scenarios like parachuting, open-water swimming and more. After the Molar Mic rolls out to the Air Force, other military branches may adopt the device as well, and Sonitus sees potential for its use by first responders. SOURCE: CNET.COM

Next-Gen Health Tracking

Smartwatches and fitness trackers are making many people more aware of their daily health and habits, but a professor at the Massachusetts Institute of Technology has developed something that could do the same thing without the bother of a device. The tech works sort of like a Wi-Fi router in the home, sending radio signals out that bounce off walls and bodies, and then return to the box, where they’re analyzed through a neural network working to learn more about our habits. By wirelessly tracking health in this way, doctors could potentially better treat patients with more tailored care. Currently the device is being tested in more than 200 homes of both healthy subjects and those with chronic conditions.

SOURCE: MIT TECHNOLOGY REVIEW



2 seconds

Smarter and more connected vehicles bring increased concerns around new ways bad actors will find to break into those high-tech systems. Even Tesla, which has gone to great lengths to protect its cars against cyberattacks, is not immune: Researchers at Belgium’s KU Leuven University figured out how to clone a Tesla’s key fob, enabling them to easily steal a car without damaging a single physical element. With equipment costing about \$600, the academic hackers created a system that could wirelessly read the signals from a nearby fob in just two seconds. When the researchers told Tesla of their find, the car manufacturer paid them a \$10,000 “bug bounty.”

SOURCE: WIRED



Creating Citizen-Centric Government



Today's citizens demand a better digital experience from government. They expect integrated services tailored to their unique needs and delivered via their preferred channels. To meet these expectations, government agencies need to implement technologies and processes that support a new way of doing business — one that's more seamless, data-driven, agile and collaborative. Ultimately, this is the foundation for putting citizens at the center of government services.

Here are four steps for moving your organization in a more citizen-centric direction:



Build a strong network foundation. High-performance Ethernet connections will support intra- and inter-departmental integration, data sharing and collaboration on a fast, secure and reliable network. Explore network solutions that can quickly respond to changing agency needs and scale to meet growing demands.



Use integrated data to understand citizen needs. To be more citizen-centric, agencies must gain a

360-degree view of their needs. Integrating data from multiple applications will help agencies develop this comprehensive view and enable them to offer portfolios of services that are customized to individual citizens.



Connect with citizens via digital platforms. Citizens expect to interact with government however and whenever they want. Meet this expectation by offering convenient self-service applications on the web, public kiosks or mobile apps.



Form partnerships to reduce operating costs. Take advantage of managed services for network connectivity and other IT infrastructure. Outsourcing IT infrastructure management to third-party experts enables your agency to cut technology expenses and free up internal IT staff to focus on mission-critical functions.

As government agencies strive to become more citizen-centric, a strong infrastructure partner can ease the transition and help ensure success.

For more information, visit
enterprise.spectrum.com/government

Spectrum
ENTERPRISE



Security in Transition

Best practices for cyberleaders anticipating administration changes this November.

Which candidate will win the election? How will cybersecurity strategies change locally? What technology projects will be funded, or cut, or mothballed? How can we prepare for the unknown? Can I move up, or back, or over, or into an incoming administration leadership role?

These are just a few of the hundreds of questions that are being asked in governments all over the country as we head toward Election Day 2018. The number of open and contested gubernatorial election races this year is staggering. Change is in the air, and there will certainly be new governors, mayors, legislators, commissioners and more coming soon to a government near you.

Regardless of their political leanings, civil servants in government technology and security roles are anxiously preparing for their new leaders to arrive. Those who have been through executive transitions before expect new visions with fresh goals and modified definitions of success.

So what can we learn from similar situations in the past? Are there best practices to help prepare for the future? Absolutely.

Learning from the Past

Back in 2002, change was also in the air. Michigan Gov. John Engler was term-limited, and we knew that new leadership would be arriving after the votes were in.

Our Michigan cybersecurity team started working on the

Secure Michigan Initiative in May 2002, with a full-court press to build a strong cybersecurity plan by Election Day. Despite losing staff to early-outs, we organized an enterprisewide cyber-risk assessment based on the latest NIST guidance. Our results made the case for new funding for cyber, including prioritized project lists with costs and benefits identified.

When Democratic Gov. Jennifer Granholm was elected, we presented the plan to top cabinet leaders. After initial disappointments, our new CIO Teri Takai, along with our new Homeland Security Advisor Brigadier Gen. Michael McDaniel, saw the benefits and provided grant funding for cybersecurity projects, even as other programs were getting cut. We implemented the majority of that IT security plan within the two terms that Granholm served.

A similar list of questions was formed prior to Republican Rick Snyder becoming Michigan's 48th governor in the 2010 election. As in most states, a formal transition plan was prepared to brief the incoming team on current IT projects and plans.

But our technology leaders went further, proposing a bold set of new cybersecurity strategies that would help shape the Snyder administration's priorities based on needed cyberprotections. Snyder not only embraced these security ideas once elected, he expanded them. He championed the Michigan Cyber Initiative for eight years.

5 Cybertransition Tips

So what can help prepare your cyberagenda for the incoming transition team and beyond?


✓ **Do your homework.** Know your enterprise's people, process and technology strengths and weaknesses. Use existing strategies, audit findings, risk assessments, penetration tests, phishing simulation results and more to prepare your proposals.

✓ **Segment your plans.** Not everything can get done at once. Offer 100-day milestones, along with six-month, one-year, two-year and four-year deliverables. Show past successes, but realize that the new team will want to highlight new opportunities addressing emerging cyberthreats.

✓ **After Election Day, know the incoming team's plans for tech and cyber.** Who was on the bus with the governor-elect? What do their speeches and website say about technology and cybersecurity? Adjust proposals accordingly.

✓ **Get on the "boats that are leaving the dock."** I often hear that "there is no money." But resources are always being allocated to something. Align plans with the new leadership's priority technology projects and join those efforts.

✓ **Don't give up.** Realign, reprioritize and reassess your cyberstrategy as necessary when new information becomes available. Our initial requests in 2003 were met with blank stares. But persistence led to grant funding and more resources applied to cybersecurity.

Cybersecurity is a (rare) bipartisan issue. No public leader wants to be the victim of a cyberattack that paralyzes government. Be proactive and position your team to have the right cybersecurity projects that are "shovel-ready." 

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.



◀ Pro Laptop

ASUS announced the ZenBook Pro 15, a 15.6-inch laptop with a 4K ultra high-definition (UHD) touchscreen, an Intel Core i9 hexa-core processor and NVIDIA GeForce GTX 1050 Ti graphics. The body is all-aluminum and is equipped with both Thunderbolt 3 ports and an integrated fingerprint sensor. The laptop also has up to 16 GB of high-performance 2400 MHz DDR4 RAM and up to 1 TB PCIe 3.0 x4 solid state drive. With speeds of up to 1734 Mbps — up to 12X faster than 802.11n — the dual-band 802.11ac Wi-Fi in the ZenBook Pro 15 has greater range and establishes more stable network connections for smooth streaming of 4K UHD online videos and more.

www.asus.com



▲ Solid Drive

Samsung Electronics unveiled its first NVMe-based portable solid state drive (SSD) — the Samsung Portable SSD X5 — designed for multimedia uses like editing 4K videos, creating real-time 3-D rendering images or compiling high-resolution photos. Thunderbolt 3 provides 40 Gb/s bandwidth, up to four times faster than USB 3.1. The X5 offers a read speed of up to 2,800 MB/s, which is up to 5.2 times faster than SATA interface portable SSDs and up to 25.5 times faster than external hard disk drives. The drive also has a maximum write speed of 2,300 MB/s, enabling users to transfer a 20 GB-sized 4K UHD video in 12 seconds. Designed for Macs and PCs with Thunderbolt 3 ports, the X5 gives users a lightweight and portable design, with capacity options of up to 2 TB.

www.samsung.com/us



▲ iPhone Protection

Pelican announced its complete line of cases for the new iPhone Xs, Xs Max and XR. The latest phone case line includes the Ambassador case, Adventurer case and Protector case, as well as the Interceptor glass screen protector. The cases are designed with dual-layer protection to absorb impact during a fall. They have been drop-tested to Military 810G Specifications and feature a non-slip grip for easy holding and staying put on various surfaces. The Interceptor screen protector is made of thin, high-definition glass for great clarity and low scratches. <https://pelican.com/us/en>

FirstNet CEO Departs for the Private Sector

After three years leading the First Responder Network Authority, CEO **Mike Poth** stepped down to take a position in the private sector. Poth led the effort to get state and local governments on board with the dedicated communications network for first responders, and saw all 50 states and six territories opt in. The board of FirstNet will appoint his replacement.



ED TECH LEADER NAMED ATLANTA CIO

Following many months without a permanent IT leader, Atlanta announced its new CIO is **Gary Brantley**, who spent the last seven years as CIO for the DeKalb County School District. His predecessor was Samir Saini, who left to become CIO of New York City earlier this year.

Rod Davenport Leaves for Municipal Utility

Michigan CTO **Rod Davenport's** last day with the state was in mid-August as he moved to take the position of CIO with the Lansing Board of Water and Light. Davenport, one of *GT's* 2018 Top 25 Doers, Dreamers and Drivers, spent more than six years in his position. The state will conduct a nationwide search to fill the vacancy.



STU DAVIS STEPS DOWN

A stalwart of state IT since 2011, **Stu Davis** left his post as Ohio CIO on Sept. 7. The second-longest-serving state CIO in the U.S., Davis can count among his accomplishments a massive IT optimization, resulting in more than \$162 million in savings in tech spending, among many others. After 21 years in state service, Davis has not yet announced his next move.

Taking the reins in Ohio in an interim capacity is **Spencer Wood**, who served as deputy CIO under Davis. His interim status will remain in place through the upcoming election cycle to replace Gov. John Kasich.

DAVID KIDD



Missouri CISO Steps Down

Missouri's longtime Chief Information Security Officer **Michael Roling** announced in September he would be moving on from his role. "Mike Roling has been a tremendous leader and change agent for the state of Missouri and beyond our state borders," said acting state CIO Rich Kliethermes. Roling will next take the position of lead technical project manager for a private software company.

DAVID KIDD

NEW CHIEF INNOVATION OFFICER FOR RIVERSIDE, CALIF.

Riverside, Calif.'s new chief innovation officer took up the position at the end of August. **George Khalil** previously spent three years as the city's chief information security officer, and replaces Lea Deesing, who was named assistant city manager in June. "George Khalil is a leader in cybersecurity and is especially well-regarded in inland Southern California," Mayor Pro Tem Chuck Conder said in a release. "When he frequently brings regional IT leaders together to explore issues of common concern, we all benefit."

Philadelphia Makes CIO Permanent

After a national search, Philadelphia has named **Mark Wheeler** its new CIO. Wheeler had served as interim CIO since the dismissal of his predecessor, Charles Brennan, in January. He was also previously chief geographic information officer for the city, and first came to Philadelphia in 2010 to work on the City Planning Commission.



DAVID KIDD

LONGTIME MINNEAPOLIS CIO RETIRES

After seven years as the head of Minneapolis IT, **Otto Doll** announced that he will retire at the end of November. Doll helped usher the city out of the Great Recession and implemented digital strategies to improve equity and promote open data. He was formerly CIO of South Dakota for 15 years, and was one of GT's Top 25 Doers, Dreamers and Drivers of 2005.



JESSICA MULHOLLAND

SF Data Officer Departs

Joy Bonaguro, San Francisco's inaugural data officer, left the city after five years of service. A GT Top 25 Doer, Dreamer and Driver in 2016 as part of Team SF, Bonaguro created the city's first open data program. She will be succeeded by **Jason Lally**.

Kansas Names New CITO

In July, Kansas appointed **Lee Allen** as its new state chief information technology officer. Despite the potential for an administration change following the November election, he hopes to continue a project outsourcing data centers in Topeka and consolidating enterprise IT services. Allen's appointment comes after previous CITO Phil Wittmer's departure in February.

N.J. Names First-Ever Privacy Officer

Gov. Phil Murphy tapped **Carrie Parikh** to become New Jersey's inaugural chief data and privacy officer, as well as the chief operating officer in the state's Office of Information Technology. Formerly senior counsel for global privacy and data security for the Wyndham Hotel Group, one of Parikh's initial projects will be to redo the privacy notices that run on all state websites, with an emphasis on transparency.



DAVID KIDD

MAINE CIO RETIRES

Having served the state for more than six years, Maine CIO **Jim Smith** retired at the end of September. During his tenure, Smith was involved in several modernization efforts, and advocated for smart partnerships to help achieve outcomes, such as Maine's participation in the multistate unemployment insurance consortium ReEmployUSA.

Charlotte, N.C., CIO Returns to Private Sector

After more than 10 years as CIO of Charlotte, N.C., **Jeff Stovall** left his post to take over as chief operating officer of PMMC, a health-care software payment processing firm. A GT 2018 Top 25 Doer, Dreamer and Driver, Stovall was integral in developing the city's IT strategies and eliminating redundancies.



Total Transparency

Hiding rather than deleting unwanted comments from a social media platform can have negative consequences.

It's a fairly common practice for government agencies to "hide" social media comments for violating their social media policy, rather than delete them. There is a sense that hiding comments isn't as bad as permanently removing them. But hiding is actually far worse and can have unintended implications for government.

Citizens have a right to disagree with what your agency does and even to be downright angry, thanks to the First Amendment of the U.S. Constitution. Freedom of speech gives citizens the right to express opinions without fear of persecution or censorship by government. First Amendment protections also extend to certain statements made on social media. Therefore, your social media policy should be crystal clear about any circumstances that would give your agency the right to remove comments, such as the use of profanity, discriminating remarks or threats. It's common for governments to have a comment moderation policy such as this.

comment was hidden. Some social media administrators believe hiding is appealing because it feels less obtrusive for the commenter than entirely deleting their comment. Others believe that if the citizen has no idea, then they can't voice additional anger or post disgruntled rebuttals. It defuses the situation.

But here's the problem: The real trouble in hiding comments on Facebook is that the commenter, and his or her Facebook friends, can still view the comment. Not only this, but they can continue the conversation by replying to the comment, without knowing that the comment is no longer public on your page.

Why is that bad?

The problem with hiding comments is that it's a purposeful move by an agency's representatives to be secretive about displaying something a citizen wrote on their department's Facebook page. If your agency ever had to argue a position in court, you would likely need to fully disclose your intention in hiding the comment. Even if a comment egregiously violates your comment policy, and you hide it, what if someone in that person's friend list posts a reply to it? Maybe the friend's comment doesn't violate your policy and contributes to useful public discourse. Unknown to them, their reply is hidden from anyone outside their friends viewing it.

If you're dealing with a company or business in the private sector, hiding comments might not be a big deal. But

when you're a government agency, it's a whole different story. If a social media comment is worthy of deletion because it violates your official social media comment policy, then delete the comment while following your records retention protocols. Be cautious of looking to hiding as a less severe alternative. [gt](#)

Why is hiding comments different from deleting them?

When government social media administrators use Facebook's tool to hide a comment, no notification or other indication is sent to the person who posted the comment. The citizen likely has no idea that their

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.



HOW TO CREATE A MODERN RANSOMWARE SECURITY STRATEGY

Government and education leaders should focus on the three pillars of technology, people and policy to guard against sophisticated hackers.

READ OUR GUIDE TO LEARN MORE AT:

govtech.com/Ransomware-Security-Strategy



Every step of the way CentralSquare was there for you

As Jan watches her daughter play in the park, she reflects on their lives together.

And with each memory – from the 911 call, the ambulance and the emergency delivery that started her family's journey, to the new home they just built and the safe school where her daughter is enrolled – CentralSquare Technologies has been by their side.

So while Jan enjoys her Sunday with her daughter, we work behind the scenes to help Jan, and other families in her community, grow and thrive.

CentralSquare Technologies brings together four software powerhouses, and now serves 3 out of 4 citizens across North America

 aptean

 SUPERION

 TRITECH
SOFTWARE SYSTEMS

ZU-RCHER

911 | Asset Management | CAD | Citations | Citizen Engagement | Corrections | Finance | Human Capital Management | Mobile | Patient Management | Records | Utilities

WWW.CENTRALSQR.COM