government technology™
gt
Solutions for state and local government.
OCTOBER/NOVEMBER 2019

CYBER SIEGE

Attacks on elections and the growing scourge of ransomware are raising the stakes on cybersecurity. How can tech leaders stay ahead of the threats?

Faster Smarter Safer



A government executive's guide to understanding the **network of the future** and its role in transformative change.

Get your copy at
bit.ly/**GovFuture**

AT&T

© 2019 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.

CONTENTS

Vol 32 | Issue 7



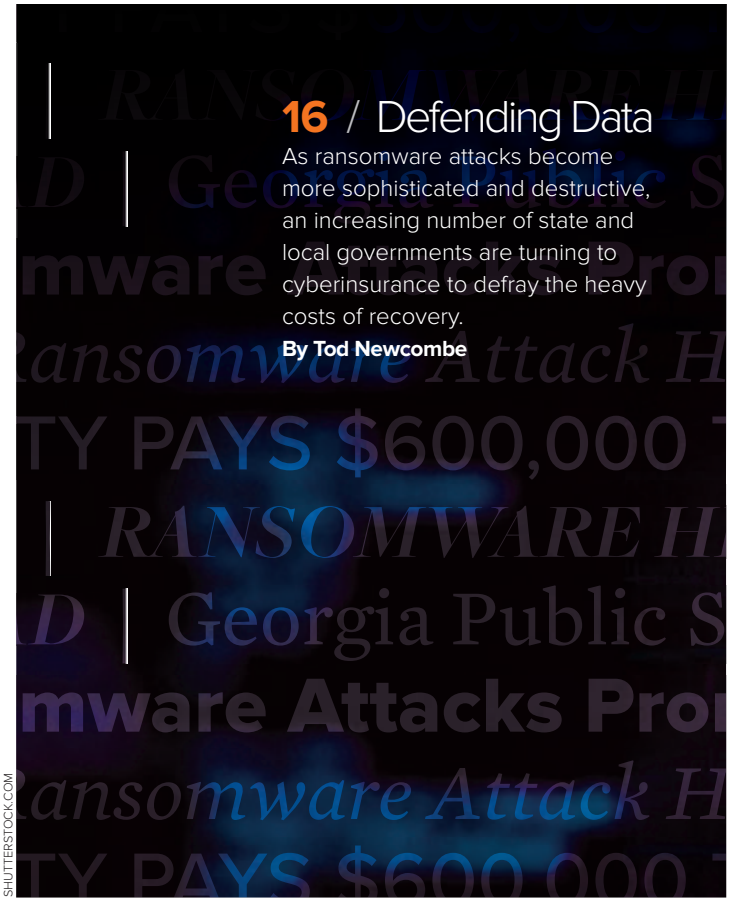
APIMAGES.COM

COVER STORY

10 / Securing the Vote

The virtual guarantee of foreign meddling in the 2020 election poses a challenge to state and local officials, IT staff included, to protect American democracy. Experts say the keys to success will be cybersecurity, paper trails, risk-limiting audits and inter-agency communication.

By Andrew Westrope



SHUTTERSTOCK.COM

16 / Defending Data

As ransomware attacks become more sophisticated and destructive, an increasing number of state and local governments are turning to cyberinsurance to defray the heavy costs of recovery.

By Tod Newcombe



38 / Patch Work

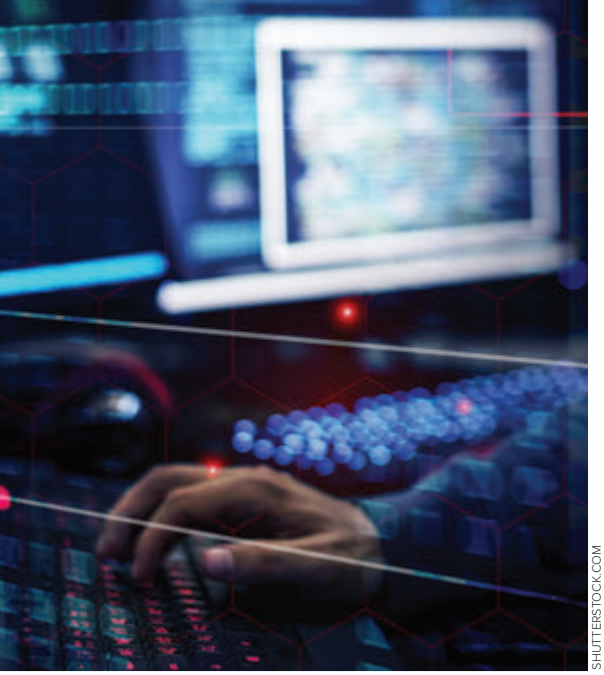
Patch management is a cornerstone to information security in today's highly digitized environment. So, why is it still such a vulnerability?

By David Raths

Government Technology (ISSN# 1043-9668) is published monthly except February, May, August, and November by e.Republic Inc, 100 Blue Ravine Rd, Folsom, CA 95630. Periodical Postage Paid at Folsom, CA and additional offices. POSTMASTER: Send address changes to: Government Technology, 100 Blue Ravine Rd, Folsom, CA 95630. 916-932-1300.

Copyright 2019 by e.Republic Inc. All rights reserved. SUBSCRIPTIONS: Subscription inquiries should be directed to Government Technology, Attn: Circulation Director, 100 Blue Ravine Rd, Folsom, CA 95630.

COVER IMAGE: SHUTTERSTOCK.COM



SHUTTERSTOCK.COM

COLUMNS

6 Point of View
Ready for 2020?

8 Data Points
Virtual reality can make smart cities even smarter.

9 Four Questions
Jonathan Feldman on his 15 years as Asheville, N.C., CIO.

50 Cybersecurity Strategies
How security chiefs can cyberproof for future tech.

54 GovGirl on Social
Why government should be wary of Instagram's restrict function.

DEPARTMENTS

44 / Hygiene Help
A federal program is helping a growing number of IT shops tune up their cyberposture.

48 / Who Is the State CISO?
A data-driven look at who's keeping us secure.

NEWS

7 govtech.com/extra
Updates from *Government Technology's* daily online news service.

51 Spectrum
More research, more science, more technology.

52 CIO Central
Career changes across tech-driven roles in government.



FOLLOW US ON

IN OUR NEXT ISSUE:

End of an Era
2019 closes out another decade of gov tech.

Digital Cities
Our annual look at local governments at the head of the class.

Hindsight Is ...
GT asks state and local CIOs what they see for 2020.

government technology

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, Data & Business: **Ben Miller,** bmiller@govtech.com
Assistant News Editor: **Zack Quaintance,** zquaintance@govtech.com
Staff Writers: **Skip Descant,** sdescant@govtech.com
Patrick Groves, pgroves@govtech.com
Jed Pressgrove, jpressgrove@govtech.com
Lucas Ropek, lropek@govtech.com
Andrew Westrope, awestrope@govtech.com
Editorial Assistant: **Moriah Chace,** mchace@govtech.com

DESIGN

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

PUBLISHING

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 Roebbelen, lroebbelen@govtech.com
Carmen Besirevic, cbesirevic@govtech.com
Lynn Gallagher, lgallagher@govtech.com
Kelly Schieding, kschieding@govtech.com
ACCOUNT EXECUTIVES:
Rebecca Regrut, rregrut@govtech.com
Joelle Tell, jtell@govtech.com
Lisa Blackie, lblackie@govtech.com
Kristi Leko, kleko@govtech.com
Mark Androvich, mandrovich@govtech.com
BUS. DEV. MANAGER:
Sheryl Winter, swinter@govtech.com
Brittany Hopkins Siebel, bsiebel@govtech.com
INSIDE SALES:
Paul Dangberg, pauld@govtech.com
Katrina Wheeler, kwheeler@govtech.com
Dana Kansa, dkansa@govtech.com
SALES ADMINISTRATORS:
Jane Mandel, jmandel@govtech.com
Lien Largent, llargent@govtech.com
Sharon Penny, spenny@govtech.com
Tara Holm, tholm@erepublic.com
Heather Earney, hearney@erepublic.com

Sr. Dir. of Sales Operations: **Andrea Kleinbardt,** akleinbardt@govtech.com
Event Sales Operations Mgr: **Alison Del Real,** adelreal@govtech.com
Chief Customer Success Officer: **Arlene Boeger,** aboeger@govtech.com
Dir. of Content Studio: **Jeana Bigham,** jbigham@govtech.com
Dir. of Digital Marketing: **Zach Presnall,** zpresnall@govtech.com
Web Advertising Mgr: **Adam Fowler,** afowler@govtech.com
Subscription Coord.: **Eenie Yang,** subscriptions@govtech.com

CORPORATE

CEO: **Dennis McKenna,** dmckenna@govtech.com
President: **Cathilea Robinett,** crobinett@govtech.com
CAO: **Lisa Harney,** lharney@govtech.com
CFO: **Paul Harney,** pharney@govtech.com
Executive VP: **Alan Cox,** alanc@govtech.com
Chief Innovation Officer: **Dustin Haisler,** dhaisler@govtech.com
Chief Content Officer: **Paul W. 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 2019 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.

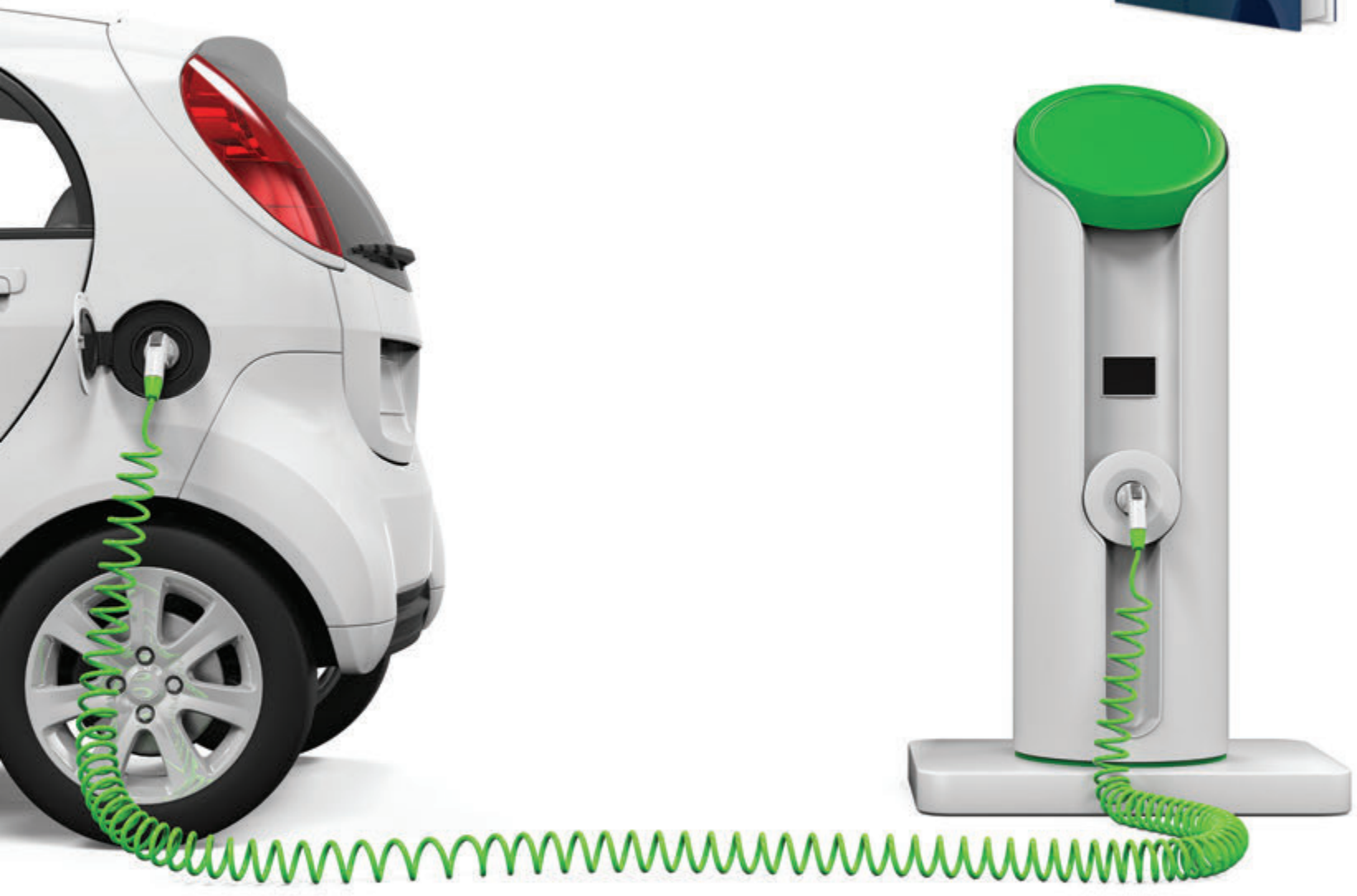
e.Republic BPA WORLDWIDE

It’s time for your fleet to go green.

With government targets to cut carbon emissions, now is the time for fleets to implement an EV strategy. Geotab’s electric vehicle product suite leverages your existing telematics data to help you choose the right vehicles to electrify, and then helps you ensure return on investment.

Learn more by reading our white paper “Going electric: What you need to know about EV fleet management” at www.geotab.com/gov.





GEOTAB®
management by measurement

www.geotab.com/gov
government@geotab.com

© 2019 Geotab Inc. All rights reserved.

By Noelle Knell / Editor



Ready for 2020?

I am a part of the 24 percent. According to a CNN poll, that's how many Americans read at least part of the report from Special Counsel Robert Mueller on Russian interference in the 2016 general election. It's been broadly reported that the report is a dense read punctuated by plenty of redaction. That said, there were many concerning takeaways.

What became secondary (if that) in the political fireworks display surrounding the report's release is the intentional, systematic interference in our democratic process by foreign powers that it uncovered. There's nothing like a compromised presidential election to shine a national spotlight on the importance of cybersecurity.

And this is one of those cases where even the appearance of impropriety is as damaging as if votes are actually altered.

"When it comes to the adversary, they're not necessarily looking to explicitly change votes or change results, but create the perception that something might have happened," said Ben Spear, director of the newly established Elections Infrastructure arm of the Information Sharing and Analysis Center (EI-ISAC).

As is covered in detail by *GT* Staff Writer Andrew Westrope in *Securing the Vote* (p. 10), there are myriad efforts to secure election infrastructure underway. From Washington, D.C., to state capitols to county registrars' offices, professionals whose livelihoods revolve around preserving the integrity of the vote are collaborating to close gaps and resolve vulnerabilities.

While many states were wary at first, the Department of Homeland Security classified election systems as "critical infrastructure" in 2018. In addition to laying the foundation for EI-ISAC, the move brought more resources, coordination and threat-sharing among officials across the country.

Secretaries of state similarly report a better condition of preparedness now than for the last election cycle, with some funding flowing toward tools like malware detection and staff to assist smaller local governments. Sensors were deployed in order to keep an eye on traffic to election websites and detect intrusions into voter databases.

There are ample reasons to remain vigilant.

In late August, a voter in the Mississippi gubernatorial election captured video of a voting machine repeatedly changing her vote from the candidate she selected (Bill Waller Jr.) to Tate Reeves. Several other instances of the malfunction were reported, leading to calls to technical staff, taking the questionable machines out of commission for the moment.

While this case reportedly only affected a couple dozen votes in an election that was decided by a spread of more than 26,000, undermining voter confidence can have sweeping effects. Add to that the proof in the Mueller report that voter registration databases in all 50 states were probed by bad actors. No evidence was found that information was altered, but again, it threatens voter confidence in the democratic process.

There's a role for tech leaders in government here to help underscore the importance of needed resources, for both technology and training around voting systems. We cover another critical issue — patch management — in a separate feature (see p. 38), but its importance bears repeating. Aging systems are only as good as their last patch. And keeping those current takes resources too.

But even with "foolproof" technology in place to safeguard fair elections, experts broadly point to the importance of a backup plan — namely the availability of an auditable paper trail — if something goes awry on Election Day.

Chris Krebs, the inaugural director of DHS' Cybersecurity and Infrastructure Security Agency, backed up this widely held belief at a conference in August, underlining the need for the marriage of modern election technology with manual tools. "Gotta get auditability," he said. "I'll say it: Gotta have a paper ballot backup."

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.

tech/**bytes**

$1M

The amount Maine plans to spend on new software following Microsoft's announcement that it will no longer support Windows 7 after 2020.

11

The number of community digital literacy projects in which Seattle will invest $320K total in grant money.

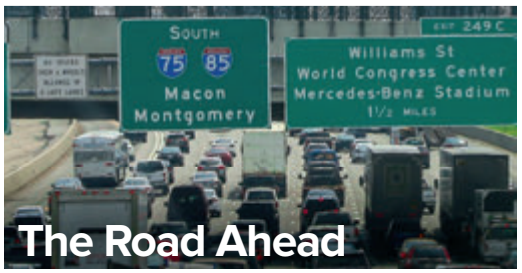


40

Las Vegas reports that as many as 40 cars each week drive the wrong direction down one-way streets, a problem it's working to solve with data analytics.

10K

The number of water bills Baltimore began printing each day in August for the first time following a system outage in connection with the city's devastating ransomware attack in May.



The Road Ahead

The Ray, an 18-mile section of Interstate 85 in Georgia, will be outfitted with connected vehicle technologies as part of a two-year project organized by the Georgia Department of Transportation and Panasonic. Six roadside units will send information from the vehicles to a traffic management platform, and four DoT vehicles will be equipped with onboard technology to send speed, location and direction data, along with info about vehicle operations such as windshield wipers or hard braking. The project is a test bed for future expanded connected vehicle infrastructure.

Biz Beat

When planning an update to its citizen engagement platform, Australian company **Bang the Table** announced a strategic partnership with Denver-based Engaged Public, makers of the software **Balancing Act**. Bang the Table's EngagementHQ platform, currently used by about 500 clients worldwide, will integrate Balancing Act's ability to let citizens participate in local government budgeting with simple graphics and simulations. The addition will replace the Budget Applicator tool within EngagementHQ.

STICKER SHOCK

The Kansas Bureau of Investigation painted a dire picture for legislators when its agency CIO informed an IT committee of a possible $8 million price tag to upgrade the state's Automated Fingerprint Identification System or run the risk of statewide failure. The vendor, IDEMIA, notified KBI in 2016 that it would no longer provide maintenance for the product after the contract expires mid-2022. The upgrade will enable Kansas to continue sharing biometric data with the FBI.



WHO SAYS?

"The private sector invests more than $42 billion each year in executive development, but there is no equivalent in the public sector."

govtech.com/quoteOctober2019

MOST READ STORIES ONLINE:

- Amazon's Ring Video Camera Alarms Privacy Advocates
- Texas Towns Slammed in 'Coordinated' Ransomware Attack
- Why School Systems? The Rise of Ransomware in Public Schools
- New York State CIO Robert Samson Announces His Retirement
- How Texas Cities Are Handling Recent Ransomware Attacks
- Social Engineering Attack Nets $1.7M in Government Funds

SHUTTERSTOCK.COM



Planning in Virtual Reality

Digital twin technology can make smart cities even smarter.

Imagine the potential benefits of having a nearly complete digital replica of a city — a virtual model of its roads, buildings and public spaces — combined with real-time information feeds from sensors and other data sources. Residents could visualize the impact of new construction before breaking ground. First responders could run computer simulations to prepare for potential emergency scenarios. And city planners could better analyze and respond to local energy and environmental changes.

The advancement of several technologies, including the Internet of Things, artificial intelligence, and augmented and virtual reality (AR/VR), has made it possible to create "digital twins," or virtual replicas of objects, processes or places from the physical world. The concept of creating "twins" to serve as tools to improve decision-making has long been used in engineering. For example, NASA developed two identical space vehicles for its Apollo program to mirror the conditions in space on Earth for training and flight preparation. More recently, the manufacturing sector has embraced digital twins to optimize production. As of 2018, GE had 1.2 million digital twins for 300,000 different types of assets from individual pieces of equipment to entire power plants. By analyzing real-time and historic data, the company can identify maintenance issues and reduce downtime and costly repairs.

Now cities around the world are beginning to use this same technology. Digital twins can help cities plan transportation systems, prepare for flooding and warn pedestrians about areas with high pollution.

In India, the state of Andhra Pradesh is building the first city created from the start with a digital twin as it establishes its new capital, Amaravati. The system will allow government officials to manage the permitting process, monitor construction progress and evaluate design plans, enabling them to understand things like how buildings will respond to the hot and humid climate.

Singapore has invested $73 million in its Virtual Singapore project, a digital three-dimensional city model that can be used as a test bed by government agencies, businesses and researchers to build a more resilient city. The digital model will allow telecom companies to experiment with different wireless network deployment models to optimize coverage, help building owners identify the best places to install solar panels, and allow city planners to analyze pedestrian patterns to improve parks and evacuation routes.

While most of these digital twins are designed to serve the local population, some are already thinking about how to create a network of these cities. The Association of Southeast Asian Nations has established a pilot project to build a network of digitally twinned smart cities, which, in addition to Singapore, will include Jakarta, Indonesia, and Cauayan City, Philippines. The goal is for participating cities to use their shared resources and capabilities to collaborate on solutions to key urban challenges.

Falling costs will eventually make digital twin technology feasible for all cities. And while more advanced cities are mapping out the entire urban landscape — including fine-grained details of buildings, vegetation and water bodies — some are starting more simply, such as by creating digital representations of key infrastructure like bridges and schools to track usage and carbon emissions.

Cities in the U.S., however, have been slow to adopt digital twins, even as many American firms have been leading providers of the technology. But some U.S. cities seem to be waking up to the technology. For example, 13 U.S. cities launched the Open Mobility Foundation in June 2019 to explore how digital twin models can enhance urban mobility.

Cities should continue to explore how to use digital twin technology to make their communities smarter, safer and more efficient. Investment in technical enablers, especially smart infrastructure and other smart city technology, would increase the availability of data necessary for cities to reap the benefit of digital twin technology. While much of this direction and leadership will come from the local level, U.S. cities should also work with their peers to create interoperable systems, support communities of practice and build national support for more smart city initiatives.

Chelsea Han, a fellow at the Center for Data Innovation, contributed to this article. gt

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



Jonathan Feldman

CIO, Asheville, N.C.

Asheville, N.C.'s CIO, Jonathan Feldman, is a bit of an outlier. He's been the city's IT chief for almost 15 years and has seen tech that was state-of-the-art at the start of his tenure become outdated. He's seen the rise of cloud services, endured the growing threat of ransomware, phishing and other cyberattacks, and used his experience to keep bad actors away from Asheville's data.

1 **With ransomware attacks affecting cities nationwide, what is your cybersecurity strategy?** It's an error for anyone to say that it could never happen here because it can happen anywhere, but we're doing our best. We were fortunate to have our city council approve a full-time cybersecurity coordinator, but that's not a magic bullet; it doesn't fix everything, and everyone is still responsible for security. Like a lot of other cities, we rely a lot on education, because we have had those social engineering attacks. When employees are empowered with information and they understand that bad things can happen, they tend to take this seriously and think before they click.

It's hard once you publish data to get it back. It's a lot like radiation that way because it sticks around a long time. If you don't have the data, you can't have a data breach around it. You have to be very mindful about what data you store, especially as a local government.

2 **How have cloud services enhanced local government in Asheville?** One of the major things that the Google Suite has done for us is enable folks to serve themselves when it comes to fielding questionnaires, building sites and that kind of thing. They can tailor it to their line of business needs and they don't need us for the little stuff, which means we can focus our efforts on the hard stuff.

One thing that pushed us toward Google was not having to maintain a server. An agency our size needs a pretty beefy exchange server, which means you're buying hardware every four years and somebody is the administrator. We've been able to reprogram those resources to do other things and that's one of the important things about cloud: You inevitably end up paying less.

3 **What have been your greatest achievements during your 15 years as Asheville's CIO?** Probably the biggest thing is that I have a quality of staff that is unmatched in local government. We can't pay as much as the private sector, but we can offer people a sense of mission and a sense of meaning in their work, and every time we do something, we're doing it for our community, where we live. We serve everyone in Asheville. That's one of the ways the mission has really morphed because when I first got here, it was a mission statement about how we serve city employees. Now we recognize that everyone in Asheville is our customer and everyone in Asheville has the potential to be a partner for us. We haven't adopted technology for the sake of adopting technology. We've done it so that we can get the mission accomplished in a better way.

4 **What is your long-term goal for the city?** A 1,200-person organization should not have a data center. There are so many other options if we do need on-premises gear, and there are data centers that we can rent space from. The goal is to try and get most of our portfolio either as software as a service or infrastructure as a service. gt

— Patrick Groves, Staff Writer

Securing the Vote

The virtual guarantee of foreign meddling in the 2020 election poses a challenge to state and local officials, IT staff included, to protect American democracy. Experts say the keys to success will be cybersecurity, paper trails, risk-limiting audits and inter-agency communication.

By Andrew Westrope

When asked at a congressional hearing if Russia would attack U.S. election systems again in 2020, Special Counsel Robert Mueller was unequivocal: "It wasn't a single attempt," he said. "They're doing it as we sit here, and they expect to do it during the next campaign."

Presidential campaigns are now underway, and election systems are still vulnerable. From voter registration databases to result-reporting websites to the voting machines themselves, researchers have identified soft spots across the system for hackers to exploit, meaning cybersecurity is now a front line of defense for American democracy.

There are many parties working on this problem — secretaries of state, the Department of Homeland Security (DHS), EI-ISAC (Elections Infrastructure Information Sharing and Analysis Center), various nonprofits and private companies — and a few common refrains between them. They're all pushing for paper ballots, vulnerability screenings, staff training, contingency plans, audits and, above all, more consistent funding. And they all have the same basic message for state and local officials: The security of our elections is riding on you.

New hacks, old systems: Lessons of 2016

The day after Mueller's testimony in July, the Senate Intelligence Committee released a 67-page report parsing Russia's calculated attacks on election infrastructure, reinforcing Mueller's conclusions at length. The good news was, the committee did not believe Russia manipulated vote tallies on Election Day, although it conceded that its actual insight into that determination was "limited."

The bad news: The scope and precision of Russia's attacks were worse than what had been widely reported. DHS now believes all 50 states were

REUTERS



DHS election security staff monitor myriad data sources at the National Cybersecurity and Communications Integration Center on Nov. 6, 2018, the day of the midterm elections.

systematically studied for vulnerabilities, in a Russian operation that started in 2014, if not earlier. This involved surreptitiously retrieving data from voter registration databases, scanning state election systems and gaining access to at least two of them.

According to international reports, Russia has used a similar playbook of cyberwarfare on Ukraine, Bulgaria, Estonia, Germany, France, Austria and elsewhere in recent years. The overarching objective, as far as DHS can tell, has been to influence results, sow discord and undermine people's faith in democratic elections. A declassified Intelligence Community Assessment from January 2017 found that Russian diplomats had even planned to publicly challenge the validity of the 2016 election if Hillary Clinton won, preparing a social media campaign centered around the hashtag #DemocracyRIP. It also found that Russians maintained access to certain elements of several state or local election systems up to that point, although none involved vote tallying.

Suffice to say Russia succeeded in causing widespread concern, to the extent that agencies like DHS and EI-ISAC have spent the past three years planning for 2020 and pinpointing vulnerabilities. They found many.

In a briefing before senators in August 2018, then-DHS Undersecretary for the National Protection and Programs Division Chris Krebs said top vulnerabilities included the administration of voter registration databases and the tabulation of data, the former being easier to attack.

The Senate Intelligence Committee's report in July offered several examples. In April 2016, a malicious cyberactor accessed a state's voter registration database because a county employee had opened an infected email attachment, which then stole the employee's credentials and posted them online for hackers to use. In another instance, in late 2018, Russian cyberactors penetrated Illinois' voter registration database, accessed up to 200,000 registration records and retrieved an unknown amount of voter data. They could have deleted or changed the data, but investigators found no evidence they did so.

With examples like these in mind, EI-ISAC Director Ben Spear emphasized to



APIMAGES.COM

Government Technology the importance of considering the whole election ecosystem when assessing its pressure points.

"When it comes to the adversary, they're not necessarily looking to explicitly change votes or change results, but create the perception that something might have happened," he said. "And while we talk about nation-state threats and things like that, the most common threats that anyone is going to see are the same across the SLTT [state, local, tribal and territorial] sector, so they're dealing with the same ransomware, the same financially motivated malware, the same phishing ... so [officials] should be collaborating with each other."

Voting machines

Assessing voting machines, the Senate report contains an almost entirely redacted section on Russian activity directed at vendors, noting that malicious cyberactors had "scanned ... a widely used vendor of election systems." The fact that most voting machines come from the same handful of manufacturers doesn't help, because it means the compromise of just one or two manufacturers could have a massive influence.

Of course, weaknesses differ depending on the machine and how the adversary accesses it, but the consensus today is that electronic voting machines, or direct recording electronic systems (DREs), are most vulnerable. Susan Greenhalgh, vice president of programs for the advocacy group National Election Defense Coalition, said DREs came into favor after the Help America Vote Act (HAVA) in 2002, aimed at improving access for the disabled and elderly.

"There were a lot of computer scientists who said, 'Hey, that's not a good idea, because these machines could be hacked and you might never know, if somebody



In congressional testimony earlier this year, Special Counsel Robert Mueller recommended "swift" action to protect the integrity of U.S. elections systems.

knows what they're doing,' so there's been a movement for a while to urge states to adopt paper voting machines. This happened well before 2016," she said. "We're told over and over again that voting machines aren't connected to the Internet. That is not correct. Voting machines have wireless modems that connect to the Internet, and election officials say, 'We only do it briefly at the end of the night,' but that doesn't matter. If you know anything about cybersecurity, you know that is enough for somebody to plant malware in a system."

One computer scientist raising warnings has been J. Alex Halderman of the University of Michigan, who warned a Senate committee in 2017 that cybersecurity experts found a wide range of "severe vulnerabilities" in both DREs and optical scanners that would allow saboteurs to alter votes. Earlier that year, an annual hacker conference in Las Vegas found that WinVote machines were most easily manipulated.

"When it comes to the adversary, they're not necessarily looking to explicitly change votes or change results, but create the perception that something might have happened.

Voting equipment manufacturer ES&S has also disclosed that election-management systems, not specifically voting machines, in close to 300 jurisdictions contained software that made them vulnerable in 2016. The software hadn't been installed in new machines since 2007, but the company said 41 states and more than 50 percent of voters use ES&S equipment.

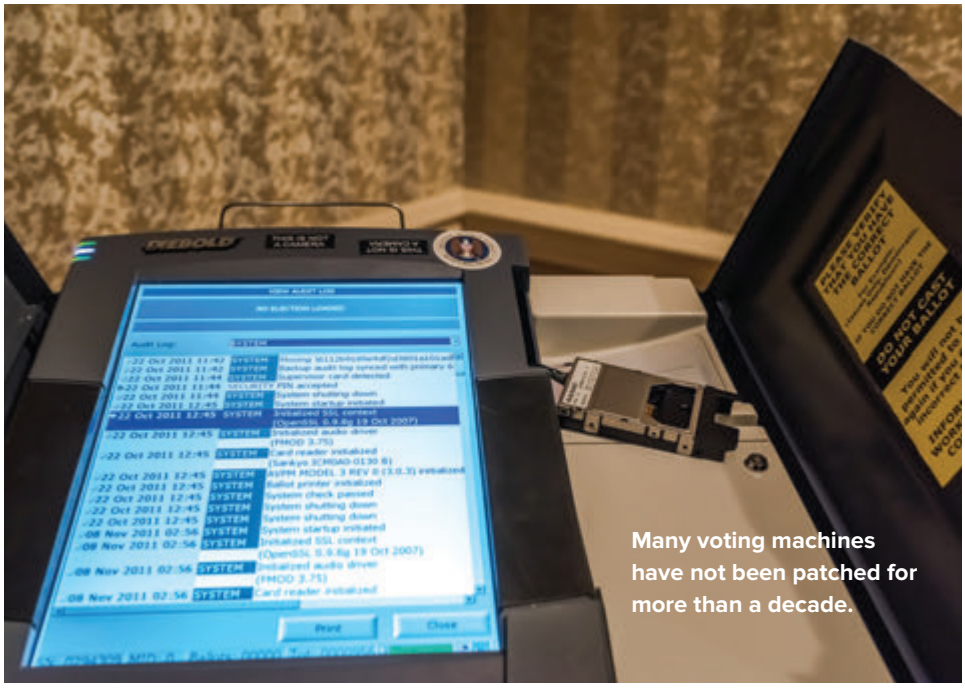
In 2016, five states were using only DREs with no paper trail, and another nine states were using at least some DREs with no paper trail. Experts consulted for this story were unanimous that every voting system going forward should have a paper trail.

All hands on deck

The potential upshot of cyberattacks is a productive reaction. Iowa Secretary of State Paul Pate, who is also president of the National Association of Secretaries of State, said he feels like he saw one, as election cybersecurity became an "all hands on deck" issue nationwide.

"Probably the biggest change since 2016 [is] that we had focused so much of this on the top, meaning federal and state centralized, but now what we've seen is definitely an expansion to the most local level of government," he said. "It's pretty clear that it's a high priority of ours, and it's clearly become a major issue in the last two election cycles, and it's not going to go away. What you're seeing is a lot more public dialog about it than in the past."

In 2018, Congress appropriated $380 million through HAVA for states to improve cybersecurity and replace vulnerable voting machines. In Iowa, that has meant rapid deployment of malware detection systems, traffic-detecting "Albert" sensors from DHS, and other protective technologies and system reviews. Pate's department also hired a cyberservices coordinator to work with CIOs and local jurisdictions, especially ones with limited resources, to connect them with services they need.



Many voting machines have not been patched for more than a decade.

SHUTTERSTOCK.COM

Lock It Down

A Senate Intelligence Report released in July offered a laundry list of recommendations for state and local election systems:

- ✓ *Work with DHS to identify weak points in networks*
- ✓ *Undertake security audits of voter registration databases*
- ✓ *Institute two-factor authentication for user access to state databases*
- ✓ *Install monitoring sensors like DHS' Albert on state systems*
- ✓ *Make voter registration database recovery part of continuity-of-operation plans*
- ✓ *Update software in voter registration systems*
- ✓ *Create paper backups of registration databases*
- ✓ *Consider a voter education program to make sure voters check their registration info before Election Day*
- ✓ *Replace outdated and vulnerable voting systems*
- ✓ *Re-examine safeguards against people inserting fraudulent paper ballots*



Forty-one states and more than half of U.S. voters use equipment from ES&S Systems, shown here at a 2018 National Secretaries of State convention in Philadelphia.

AP/IMAGES.COM

"With ... the final payment of the HAVA money we just received a little over a year ago, that has been focused on cyber. In our case, in Iowa, we are using more than half of that to provide support services directly to the counties," he said. "That money has been very productive in that regard."

Speaking for DHS, Cybersecurity Strategy and Integration Program Manager Geoff Hale said after the 2016 election, his department took steps to ensure state and local officials had the ability to receive up-to-date information and alerts about threats and vulnerabilities of their systems.

In 2018, despite the initial protestations of most states, DHS declared U.S. election infrastructure "critical infrastructure," making the federal government partially responsible for it. As part of this designation, DHS launched a Government Coordinating Council focused on elections, which made a list of IT and election officials to notify in case of a threat. DHS also started working with states on trend analysis, threat intelligence and vulnerability testing, deploying Albert sensors to monitor Web traffic and provide intrusion detection for voter registration databases.

DHS' critical-infrastructure designation also led to the creation of EI-ISAC, a branch of MS-ISAC that handles information for election officials and provides no-cost cybersecurity services to state and local governments.

Director Ben Spear said EI-ISAC started with conversations with election officials, then system assessments, then Albert sensors in all 50 states.

"That's been a great accomplishment ... having a better understanding of the threat landscape," he said. "We also provide forensic response. We provide a lot of free information and vulnerability profiling, which is different from the vulnerability assessments DHS provides. It's not as deep but provides some great information from folks."

Separate from EI-ISAC, Spear said the Center for Internet Security also has a best-practices unit that collaborated with local election officials, federal partners and advocates on a handbook for election infrastructure security.



How to reinforce the front lines (and the back)

With governments, nonprofits and technology vendors on high alert going into 2020, the list of ways for state and local officials to "improve cyberhygiene," as DHS puts it, is long and diverse.

DHS' Geoff Hale said his department's efforts at the local level will be focused on helping people understand their susceptibility to phishing scams, as well as incident-response planning and vulnerability scanning. First and foremost, he said, local governments should sign up to become members of EI-ISAC if they're not already, and avail themselves of its resources.

EI-ISAC's Spear stressed the importance of having an emergency response plan, which is required for election officials in many states, and for IT officials to start building a communicative relationship with their local election officials if they haven't already.

"At the local level, it's more common for the local IT to be the actual IT responsible for elections, and we encourage that they are engaged with their election officials," he said.

Consistent with DHS' efforts, Secretary of State Pate said the most needed investments are not hardware or software, but training and awareness. He also recommended that larger counties with more in-house expertise adopt a "good neighbor" policy, helping smaller jurisdictions around them, which he said has benefited rural communities in Iowa.

Pate added that all states should utilize the designated Homeland Security liaison to which they are entitled, and ask Congress for a more consistent source of funding.

"The best advice I can give Congress is that they should be working with the state jurisdictions to identify where we need to prioritize our resources," he said. "I think most of us secretaries are in agreement — it would be ideal to have a more consistent funding stream for these types of cyberprotections. ... What happens in five years when the money's not there? The state will have to ... raise taxes or whatever they need to do to pay for that cybernavigator that I hired, because the HAVA money will be gone."

In lieu of funding, several nonprofits, advocacy groups and private companies are stepping up to offer resources such as free software tools. Microsoft, for example, launched its own Defending Democracy Program and partnered with Galois, a security tech company, on an open-source software development kit called ElectionGuard. Available for free on GitHub, ElectionGuard proposes to help election officials and technology vendors make voting systems end-to-end verifiable (E2E-V), meaning they cannot be cheated without detection because they allow voters and third-party organizations to confirm that votes were unaltered and properly counted.

Protect Democracy, a nonpartisan nonprofit in Washington, D.C., has also released a free app called VoteShield, now used by more than a dozen states, which uses basic statistics and machine learning to analyze changes in voter registration databases and flag unusual activity.

Susannah Goodman, director of election security for the grass-roots watchdog organization Common Cause, praised these tools but stressed the importance of a legible paper trail no matter what.

"Unless the voter reviews the ballot, then that ballot isn't useful in becoming the permanent record of that voter's choices. You want to create a situation where the user interface is easy, and it's user-friendly for the voter to review the physical paper ballot. That's a step that usability experts across the board have [supported]," she said. "If the state law allows you to have backup paper ballots, have emergency ballots on hand. Understand that the e-poll books are great, but they do fail. ... There always needs to be a plan B, and that resilience needs to be baked into everything. Not only does that help with run-of-the-mill problems ... but it absolutely helps with the nation-state threat, because these systems are so resilient, if something happens that screws it up, and there's a plan B, it's fine."

With the idea of procedural security and backups in mind, the Senate Intelligence Committee report released in July gives a series of recommendations. For the federal government, it wants a policy of serious retaliation for future attacks, more discussion about cybernorms, and creating clear channels of communication with state and local officials. (See sidebar, p. 14.)

The committee also recommended that states commit to risk-limiting audits, and require their machines to be certified by the U.S. Election Assistance Commission or compliant with the EAC's Voluntary Voting System Guidelines. It said the components most in need of immediate cybersecurity fixes were voter registration databases, and election-night reporting websites run by the states — again, to prevent hacks that wouldn't affect vote tallies but might cause confusion.

To sum up the responsibilities that now lie with state and local governments, Gen. John Allen of the Brookings Institution said this to the National Association of Counties in 2017: "I always felt pretty proud, being a Marine, that I could say I was part of the first line of defense of the United States of America, and that I had spent most of my life defending the institutions of American democracy ... I now think that you, the leaders of the counties of America, in many respects are the front line of defense of the most profoundly essential institution of American democracy." gt

awestrope@govtech.com

DEFENDING DATA

As ransomware attacks become more sophisticated and destructive, an increasing number of state and local governments are turning to cyberinsurance to defray the heavy costs of recovery. **BY TOD NEWCOMBE**

In February 2016, the town of Medford, Mass., paid a $300 ransom to get access to its data from cyberextortionists. Outside of the local media, the incident attracted little attention. Three years later, hackers collected a combined $1.1 million bitcoin ransom from two small cities in Florida. The payout made national news.

The size of the recent payouts startled just about everyone, but in some respects, it's not surprising. Government continues to be a major target, with only the most prepared jurisdictions able to stop ransomware from disrupting information technology. And the demands aren't the only thing that is growing. So too is the sophistication of the attacks. Cities that have refused to pay ransoms have found it extremely difficult to restart their systems, in some cases having to rebuild from scratch.

The city of Atlanta was hit with a $52,000 ransom demand in April 2018, refused to pay and has been left with a $17 million cleanup bill that includes the cost of lost business to the city. Extortionists crippled Baltimore's IT systems this April and demanded $100,000 in bitcoin. Like Atlanta, the city refused to pay, and like Atlanta, it has found that the recovery has proven far more daunting and expensive than expected — $18 million and growing.

Many governments, especially small to mid-sized local cities, lack the funds to build up a robust cyberdefense. Limited budgets are also the reason why so many jurisdictions continue to run aging and outdated IT systems, which further hampers attempts to thwart the rise in ransomware attacks. The solution for many jurisdictions is to turn to cyberinsurance to limit the costs that come from an attack. The policies can help cities and counties respond and recover, bring in cyberexperts to evaluate the damage and even help pay the ransom as a last resort.

But not all cyberinsurance policies are the same, and large numbers of local governments don't carry the insurance at all. Baltimore did not have a policy that could have helped the city offset some of the costs for what has been paid out in terms of recovery and lost business. And with costs exploding — both for recovery from an attack and for the size of the ransom demands — it's possible the cyberinsurance market is due for a shakeup.

Ransomware: "A Daunting Problem"

First, the good news. Ransomware incidents are actually declining, according to cybersecurity firm Symantec. But that's primarily because high-volume attacks using basic ransomware software have been easy to block using anti-malware tools or work-arounds involving backup data. Instead, professional criminals are using sophisticated malware, such as Ryuk, to go after fewer, but larger, targets. The cybersecurity consulting firm Crypsis points out that rather than attack a single machine, criminals are using enterprise malware that can spread virally throughout an organization, making it harder to respond and recover.

Enterprisewide ransomware attacks mean higher extortion demands, with some organizations receiving ransoms for 20 to 50 bitcoins (the preferred method of payment in ransomware attacks). When criminals attack with the Ryuk malware, the impact is large and the payment demands average $288,000, compared to just $10,000



Ransomware Attacks Prompt Louisiana to Declare State of Emergency

SHUTTERSTOCK.COM

Louisiana Gov. John Bel Edwards declared a state of emergency in the state following a series of malware attacks on multiple school districts in July.

with other types of malware, according to Coveware, a ransomware recovery firm.

"Ransomware has become a notorious problem in the last two to three years," said Dave Chatfield, vice president of NetDiligence, a cyber-risk and response service that works with insurance companies and their clients. "There has been a striking uptick in the number and percentage of cyberclaims that have been the result of ransomware."

Tim Francis, enterprise cyber lead at Travelers Insurance, also sees a growing trend with ransomware attacks. "The [extortion] demands are getting larger, unfortunately, and it's not unique to the municipal sector," he said. "It is a phenomenon borne out of the fact that the software the bad actors are using is much more sophisticated than it used to be." Early on, ransomware software wasn't that good, which meant attackers only asked for a small amount of money, according to Francis. "The problem was a nuisance and it was easy to bring systems back online," he said.

Today, however, the complexity of the malware has made the attacks much more serious and potentially harmful to an entire organization. "There are times that if you don't pay [the ransom], your systems are not going to come back online, leaving you having to rebuild from the ground up," he said. "If you are a government with legacy systems, that's a daunting task."

As Francis and other experts point out, ransomware is a problem affecting both the public and private sectors. It tends to impact small to mid-sized firms that don't have the robust cyberdefense capabilities typically found in large firms and governments. But cities and counties have also become soft targets for ransomware attacks, thanks to their limited budgets and reliance on out-of-date technology.

Alan Shark, executive director of the Public Technology Institute, believes the problem will get far worse before it gets better, given the history of tight IT budgets and the limited control CIOs have over their systems and the changing nature of technology. "The problem for CIOs is that they cannot control all the end points in their systems; so much of government is mobile communications," he said. "Meanwhile, the political forces are against spending more on protection. Elected officials don't want to put the extra money into IT. Governments are stressed for capital."

The Expanding Role of Cyberinsurance

For years, states and localities have had access to cyberinsurance policies to help cover the costs of any damage or disruption to their IT systems. Most organizations look at cyberinsurance as a product that is meant to deal with compromised confidential information. Think of data breaches and the lawsuits that can ensue once personally identifiable information is exposed.

But the rise in ransomware has expanded the role of cyberinsurance, taking it in new directions, according to Francis. "Cyberinsurance would not only pay to deal with an event [involving ransomware], but we would be able to provide the insured with access to a network of professionals, including forensic investigators who deal with these types of incidents all the time," he said.

The investigators can quickly evaluate whether a ransom needs to be paid, or if a system backup or reboot will fix the problem. Insurance investigators might advise paying only a portion of the ransom, said Francis. "They will work with the bad actors and say something like, they will not pay all the money up front on the premise

they will act in good faith. Instead, they might negotiate to pay 10 percent and have them turn over 10 percent of the data, just to see if they are willing or have the ability to turn over the data under ransom."

Beyond helping negotiate with ransomware attackers and paying for the cost of recovering from an attack, insurance firms and the brokers that work with them can act as risk managers for clients. Mike Volk, vice president of cyber-risk solutions at PSA Insurance and Financial Services, says his firm can review an organization's IT ecosystem to help a client understand what they currently have and what needs protecting.

"We have a process to help figure out what data they have that is critical to business operations, the key IT systems they rely on, and if those become unavailable from an attack, how it will impact the mission," he said. "Then we map all that back to cyberinsurance coverage." Volk says that by showing clients how a cyberincident will impact their business, they can think up front about what needs to be done, rather than scramble on the back end. "Part of that ties into the right kind of insurance to buy," he said. "We provide recommendations based on those discussions."

While conducting these kinds of risk assessments seems obvious, in reality, the practice is not widespread. In a 2018 survey of both public- and private-sector respondents by Travelers Insurance, one of the nation's largest providers of cyberpolicies, 91 percent of respondents reported being confident their companies have implemented best practices to avoid a cyberevent. Yet, 55 percent admitted not completing a cyber-risk assessment; 62 percent had not developed a business continuity plan; 63 percent had not completed a cyber-risk assessment on vendors who have access to their data; and, most revealing, 50 percent had not purchased cyberinsurance.

Francis says the government portion of the cyberpolicy market at Travelers is growing. "The kind of coverage varies on the size of the municipality, and around how we assess the risk and the threat," he said. "When governments apply for cyberinsurance at Travelers, they are asked to identify the types of data they have, what their security controls are, their patching cadence [frequency] and how well prepared they are to deal with an event, should it take place."

"There has been a striking uptick in the number and percentage of cyberclaims that have been the result of ransomware.

'The Problem Will Continue'

When it comes to ransomware and cyberinsurance, everybody talks about Riviera Beach, Fla. After an attack in June encrypted the city's data, the Riviera Beach City Council voted unanimously to give in to the ransom demand and pay over $600,000 to recover its data and systems. Also in June, Lake City, Fla., paid $470,000 to extortionists. But the city only had to pay a $10,000 deductible; cyberinsurance covered the rest of the money owed to the attackers.

PTI's Shark called these substantial demands and record ransom payouts game changers. "That's the first time someone in the public sector has paid such a large



Baltimore ransomware attack will cost the city over $18 million

SHUTTERSTOCK.COM

Ransomware Attack Hits 20 Local Texa Government Agencies | FLORIDA CITY PAYS $600,000 TO RANSOMWARE



SHUTTERSTOCK.COM

The city council in Riviera Beach, Fla., unanimously voted to pay more than $600,000 in ransom to get their encrypted data back.

Florida city pays $600,000 to ransomware gang to have its data back

amount," he said. "The insurance company paid out the ransom, knowing that it would be significantly lower than the cost to rebuild the systems from scratch."

And that's what worries him. When cyberinsurance firms know it is cheaper to pay the ransom rather than pay for the cost of rebuilding aging government IT systems from scratch, the ransomware problem could spiral out of control with attackers demanding ever-larger payouts. As a result, attacks will continue against the weakest and least-prepared local governments. But Shark doesn't really blame the insurance companies for the situation. He understands that in the short term, ransom payments remain cheaper than system rebuilds. "This situation requires the feds and states to step up, otherwise the problem will continue."

Insurance firms say there's little they can do about making ransom payments a part of their policy. "Even if I philosophically disagree with the payment option, we have to provide our clients with what's available in the marketplace," said Mike Volk. "We don't want to encourage criminal activity, but it has become a necessary part of doing business as a cyberinsurance broker. Payment is a solution, and we have to offer it until the market changes or if there's some kind of legislation that prohibits it. Meanwhile, this is going to continue."

With the problem expected to grow, governments, especially small to mid-sized jurisdictions, need to obtain policies, Francis said. "From my perspective, not nearly enough municipalities are buying insurance. More are uninsured, and given the rise in ransomware attacks, the need is there to offset the cost of the ransom attacks."

In an ironic twist, government has helped the country wake up to just how pervasive and costly ransomware has become. The attacks are estimated to cost American businesses as much as $75 billion in lost business and ransom payments, according to Datto, a disaster recovery and business recovery firm. But few companies publicize when they are attacked and that ransomware is behind their lost data and failed IT systems. Not so with government.

"One thing municipalities have going for them is that when an event happens, it makes the news," said Francis. "It puts a lot of eyes on the problem that haven't been looking before. It's becoming more common for local government risk managers to understand that a ransomware attack can occur anywhere, against anybody." GT

"Payment is a solution, and we have to offer it until the market changes or if there's some kind of legislation that prohibits it.

tnewcombe@govtech.com

government technology

SPONSORED CONTENT

INNOVATION IN GOVERNMENT®

BEST OF WHAT'S NEW IN CYBERSECURITY

Technologies and techniques for combating growing threats.

2 Attackers Target Government

4 Using AI as a Cybersecurity Force Multiplier

6 Using Data and Machine Learning to Address Vulnerabilities

8 Using Threat Intelligence to Stay Ahead of Cyberattacks

10 Understanding and Controlling the Connected Device Landscape

12 Protecting Complex Environments With Integrated Solutions

14 Assessing and Managing Cyber Risk

16 3 Ways to Strengthen Cybersecurity as Technology Evolves

carahsoft



ATTACKERS TARGET GOVERNMENT

Public sector responds with new tools and growing cybersecurity sophistication.

Cyberattacks against governments, already a top concern for public sector IT professionals, took an ominous turn in August, when the Texas Department of Information Resources reported that 22 Texas cities had been attacked simultaneously by a single source.

Most of the targets were smaller, rural cities, according to the department, which in late August was leading recovery efforts in coordination with multiple state and federal agencies. Experts immediately pointed to the attacks as a new permutation in government's ongoing war with cyber crooks.

"What's unique about this attack and something we hadn't seen before is how coordinated this attack is," said Allan Liska, a threat intelligence analyst with security firm Recorded Future, in an interview with NPR shortly after the incident. "It does present a new front in the ransomware attack. It absolutely is the largest coordinated attack we've seen."

This latest ransomware evolution comes at a time when governments already face intensifying cybersecurity challenges.

States and localities have become a favored target for attackers, according to security experts. A new report from security firm Barracuda Networks says there have been more than 70 ransomware attacks on state and local governments in 2019, representing almost two-thirds of all publicly reported attacks this year.

In addition, new computing models are broadening and complicating the task of safeguarding government data and IT systems. The rise of mobility, increasing use of edge computing and IoT-connected devices, and migration to cloud platforms and services all expand the cyber threat landscape for public agencies.

New Attention on Risk

These and other factors are pushing states and localities toward more sophisticated cybersecurity approaches, including growing adoption of risk management tools, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework. These tools help agencies understand vulnerabilities, focus protection efforts on their most critical systems and implement security best practices.

Thanks to the risk management trend, cyberattacks increasingly are viewed as a business threat instead of a technology problem. As a result, cybersecurity is getting more attention from political leaders and agency management — and governments are responding to cyberattacks as they would other large-scale emergencies.

For instance, former Colorado Gov. John Hickenlooper declared an emergency last year when a ransomware attack impacted financial systems at the state's Department of Transportation, which processes around $100 million in monthly payments. Hickenlooper's executive action, thought to be the first in response to a cyberattack, enabled the state to use the same resources and processes that are triggered after a major natural disaster.

Louisiana Gov. John Bel Edwards took a similar approach this year when attackers hit several local school districts in his state, mobilizing the Governor's Office of Homeland Security, Louisiana State Police and National Guard, statewide Office of Technology Services, and academic and private sector experts. And Texas Gov. Greg Abbott ordered a "Level 2 Escalated Response" after the August coordinated ransomware attack in his state — the second-highest level of Texas' four-step emergency response protocol.

Growing attacks on local governments are also prompting more states to share cybersecurity resources with cities and counties. Michigan, for example, recently launched a CISO-as-a-Service program where state security experts provide maturity assessments and implementation plans for counties and cities.

"A few years ago, states started developing incident response teams, but states are now starting to say, how do we engage with locals before an incident," said Maggie Brunner, a program director for the National Governors Association (NGA), during a recent *Government Technology* webinar.

The NGA is working with states to strengthen their cybersecurity partnerships with local governments, she said. "States, having the cyber expertise that they do, are in a great position to create these economies of scale."

More Powerful Technologies

Along with new techniques and partnerships, governments are implementing sophisticated new technologies for cyber protection.

"Many of the technology tools and services that governments are buying now have some level of artificial intelligence capability built into them," says Teri Takai, executive director of the Center for Digital Government (CDG). "You can't deal with the number of cyber threats on an ongoing basis without it."

Results from CDG's 2018 Digital States Survey show broad adoption of cybersecurity technologies such as intrusion prevention, security patch enforcement and data encryption enforcement systems. States also are deploying emerging security solutions like microsegmentation, security policy orchestration and application visibility.

Many of these tools automate security processes and procedures, helping ensure that software vulnerabilities are quickly patched and equipment is properly configured. They can also scan for unusual activity, enabling agencies to detect potential intrusion into systems and data.

Like states, city governments also have broadly adopted intrusion prevention and patch management systems, as well as tools to monitor and analyze threats to endpoint computing devices, according to CDG's 2018 Digital Cities Survey.

The surveys also make it clear that government agencies continue to struggle to attract cybersecurity professionals into public service. State and city respondents both ranked cybersecurity as their biggest technology workforce need. The talent shortage is driving growing use of security services by government agencies.

A Continuing Challenge

Takai says the current spike in government-focused cyberattacks puts public sector CIOs and CISOs in a stronger position to argue for more security resources.

"The good and bad of it is that, as a CIO, I would be much more cautious and I would also be looking to highlight where I might need funding," she says. "And in highly decentralized organizations, security can be a powerful argument for adopting an enterprise view of technology to decrease vulnerability."

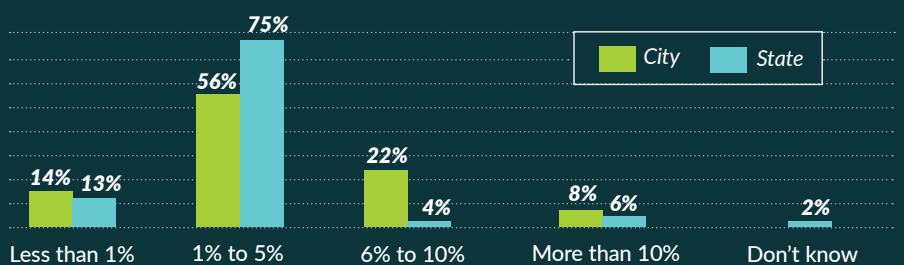
Even as states and localities have increased their sophistication around cybersecurity, these efforts must continue to expand and evolve. Indeed, one looming issue for CIOs and chief security officers is making sure advanced security tools can function together.

"The challenge is integrating these individual products into an enterprise framework now," says Takai, "and understanding the cybersecurity architecture of the future."

Addressing these issues and strengthening security capabilities will remain a top priority for CIOs — and increasingly their bosses — as cyber threats proliferate.

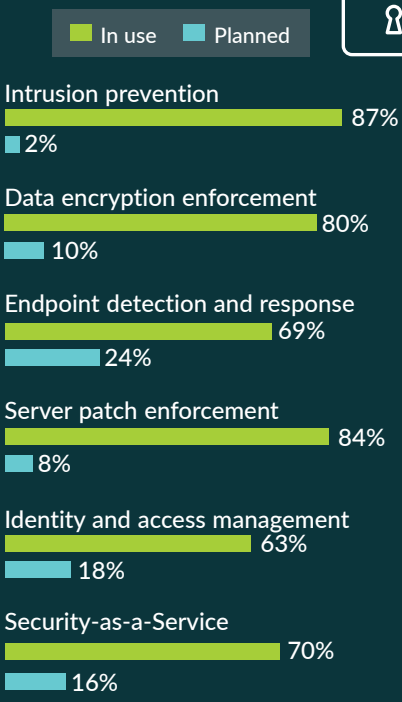
"I think we're entering an epidemic stage," said Alan Shark, executive director of the Public Technology Institute, in a recent interview with the *Washington Post*. "The bad actors have been emboldened."

Percentage of Technology Budget Spent on Cybersecurity



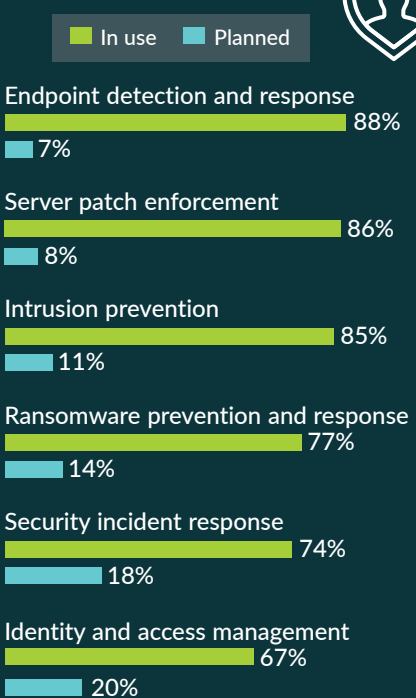
State Cybersecurity Measures and Initiatives





City Cybersecurity Measures and Initiatives





Source: CDG 2018 Digital States and Digital Cities Surveys



USING AI AS A CYBERSECURITY FORCE MULTIPLIER

Joseph Mara, vice president Americas, state and local government and education for Symantec, discusses technologies that not only improve cybersecurity but also help address cybersecurity staffing shortages.

The recent ransomware attack against multiple cities in Texas reportedly was a targeted attack. Does this indicate that the nature of these attacks is changing? If so, what are the implications for government agencies?

We recently published a special Internet Security Threat Report on targeted ransomware (https://www.symantec.com/security-center). These targeted attacks are very destructive and inclusive. Protecting the significant amount of personally identifiable information (PII) that organizations have in their systems is very important, and some municipalities — especially the smaller ones — don't have the appropriate resources in place to protect everything. That can make them easy targets for a ransomware attack. I don't want to say that smaller cities can't protect themselves, but they could be a potential target.

How are technologies like artificial intelligence (AI) and machine learning being used to improve security?

The strength of AI lies in the ability to analyze a huge volume of data across large networks. It allows state and local agencies to detect patterns and abnormalities; it signals potential threats; and it does so faster than any human could do alone. AI enables organizations to determine quickly and efficiently how to respond, so it's very important. Machine learning takes it a step further by enabling the solution to learn as it goes.

Where will AI and machine learning have the biggest impact?

The biggest impact will be in the security operations center, where these technologies act as a force multiplier. A lot of agencies face a shortage of cybersecurity professionals, so AI and machine learning can help augment their resources. The good news is that AI is rapidly becoming commercialized, meaning it's being embedded into existing products so state and local agencies don't have to worry about hiring experts in that area.

What emerging technologies should our readers be aware of?

Behavioral analytics is an interesting area. Leveraging AI, you can learn what constitutes normal behavior on the network, both in terms of the system and humans. Then, by monitoring for what is abnormal, you can take actions to help protect yourself. If something happens you can quickly remediate the threats targeting your system. In the past, organizations recognized cyber threats only after the damage was done, which is way too late. Today's technologies accelerate every aspect of the cybersecurity life cycle, from detection to response and mitigation.

What else can agencies do to strengthen their security stance?

Agencies can no longer approach cybersecurity in a fragmented way — meaning buying products to solve for a specific vulnerability without thinking about how they should be integrated together. They need to adopt an integrated cyber defense approach that unifies products, services and partners to drive down the cost and complexity of cybersecurity. This approach combines information protection; threat protection; identity management; compliance; and intelligence and automation across endpoints, networks, applications and clouds.

Learn more at **Carah.io/GT-Cyber-Symantec**

Integrated Cyber Defense for State & Local Government

Enhancing cyber capabilities to identify, protect, and respond to advanced threats.

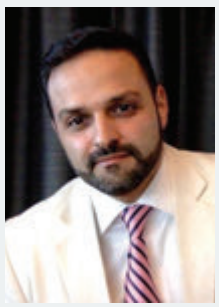
Learn more at: www.symantec.com/state-local-gov

Symantec™



Copyright ©2019 Symantec Corporation. All rights reserved.

USING DATA AND MACHINE LEARNING TO ADDRESS VULNERABILITIES



Adilson Jardim, area vice president for public sector sales engineering at Splunk, discusses analytics-driven security and the importance of a defense-in-depth approach in today's hyper-connected enterprise.

How has cybersecurity management become more complex as organizations move toward a more connected future?

Before the internet took off, our focus was on whether a single system or application complied with general security practices. Since then, the attack surface has exploded. We now have internet-facing applications, microservices, IoT devices, mobile phones and other elements that have to be interconnected to exchange data. Given the value of personal data and the ways that bad actors can use that information, the imperative to protect data — to secure access to the data, systems and services — comes with this complexity. Some of these elements didn't exist even 10 years ago.

How can organizations leverage machine learning, AI, automation and other tools to improve their cybersecurity stance?

There are a number of basic considerations. You need to gather and save log files and other data that's generated by devices across your enterprise about what's going on. Then you must implement ways to identify the low-hanging fruit, like using statistical methods to establish basic anomalies of behavior inside your environments. You want to be able to "template" activities so that you can automatically orchestrate an operation or response. Then you can move into a machine learning framework where you consider how those large data sets inform your cybersecurity operations.

What do organizations need to put in place to unlock the power of analytics-driven security?

You need a lot of data to support machine learning and ultimately AI. Organizations must capture and understand the machine data coming from all the systems, services and devices connected to their networks. They need a historical view into what has happened, as well as the capability to use that data for a more real-time response to threats. To establish the basis for machine learning, they also need that historical set of data to teach algorithms what to look for and what outcomes to enable.

But organizations can get started right away with applying analytics to aid their security mission. For example, do you have a good handle on trusted identities in your enterprise? How about known devices? Analytics can answer these types of questions quickly to help agencies prioritize and take action on security enhancements.

What questions should organizations ask as they assess their vulnerability to cyberattacks?

There are lots of levels where an organization might be vulnerable. With so many unknowns, the question is never are you 100 percent secure, but rather how do you respond to incidents and breaches, given certain conditions. This requires a defense-in-depth approach that uses multiple layers of controls to address security on every front: Do we have the right visibility; do we have the data to support decision-making when we respond to an incident; do we have the right automation, processes and standard operating procedures to address different families of vulnerabilities, threats or incidents; and so on. Organizations also have to ask what their risks are if, given their budget, they can't address certain actions or responses. They may have to make tradeoffs, but they should only do so when they understand what's going on in their environment and what exposure at different layers looks like.

Learn more at **Carah.io/GT-Cyber-Splunk**



WEAPON OF A SECURITY WARRIOR.

Machine data is the key to having happy customers and avoiding costly cybersecurity incidents. Like we do for more than 16,000 customers around the world — let Splunk turn your data into real-time visibility and insights that will streamline operations and provide a foundation for a robust security posture.

→ **splunk.com/get-value**

© 2019 Splunk Inc.

USING THREAT INTELLIGENCE TO STAY AHEAD OF CYBERATTACKS



The right threat intelligence rounds out the security arsenal so that state and local government agencies can stay ahead of threats. ***Sarah Geary,*** *manager of Intelligence for Executives at FireEye, explains how.*

Why are traditional defenses inadequate to protect against today's advanced cyberattacks?

Today's threat actors are very sophisticated. Many of them target state and local governments specifically, and if they're kept out one way, they'll try to evolve their tactics to get in through other means. Firewalls and other traditional defenses only focus on keeping the threat out. In today's environment, organizations need a more dynamic and sophisticated defense capability.

What is the key to addressing today's attacks effectively?

Intelligence. Technology by itself is not enough to protect the network. Focusing intelligence on the threat actor lets you see how the threat is evolving and stay ahead of the game. Take the recent Texas ransomware attack that targeted 20-plus cities. If that had been an espionage operation instead of a ransomware attack, the full extent of the targets would not have been so obvious, and the threat would potentially remain on their networks. Using intelligence to identify the source of the attack and understand the full extent of the problem would be key to remediating quickly and staying ahead of the threat.

What cybersecurity issues do state and local governments tend to overlook as they modernize their operations and services?

State and local governments usually have many disparate, decentralized systems that generate multiple alerts. This environment coupled with a shortage of cybersecurity staff who still need to deal with many alerts makes it difficult to prioritize response efforts. For example, the National Vulnerability Database annually ranks more than 1,000 vulnerabilities as critical — the highest level of severity — which makes prioritization difficult. Fortunately, the right third-party threat intelligence can act as a force multiplier that enables organizations to prioritize response efforts based on an analysis of how easily a vulnerability could be exploited, as well as what's being observed in other government networks and the global landscape.

How do technologies such as AI, machine learning and automation improve the detection, analysis of and response to security risks?

Coupled with intelligence, these technologies can be a game changer. To give you an example, our endpoint security tool recently alerted us to new APT34 malware on a customer's network. This sort of malware would have gotten past traditional defenses, but through behavioral monitoring, the tool enabled us to detect the malware. Over and above that, we used intelligence on top of that tool to explore the malware more. In doing so, we identified multiple completely new malware families associated with APT34. With that intelligence, we could protect the customer before the threat actor attempted to use the new tools to attack the organization.

Where should organizations start as they adopt new technologies such as AI and machine learning?

While these new technologies are very important, they are even more successful when integrated with an intelligence element that allows organizations to stay ahead of the threat. When state and local agencies know what threat actors are up to and what threats are coming, they can take a proactive posture.

FIREEYE™



BREACHES ARE INEVITABLE. BEING A HEADLINE ISN'T.

Secure your systems and manage your message with world-renown incident response services and cyber threat intelligence.

FireEye.com

www.FireEye.com | ©2019 FireEye, Inc. All rights reserved.



UNDERSTANDING AND CONTROLLING THE CONNECTED DEVICE LANDSCAPE



Shawn Taylor, senior systems engineer with Forescout, explains how continuous device visibility and automated controls enable organizations to take fuller advantage of emerging technologies.

How are network attacks against government organizations changing, and what are the implications for cybersecurity?

One of the biggest changes is the regularity of attacks. Ransomware and malware are for hire today, so adversaries don't need to be particularly skilled to execute an attack. In addition, state and local government entities are typically understaffed, underfunded and consequently underprepared from a tools and automation perspective. That puts a big bullseye on their organizations.

What unique challenges do smart cities, smart transportation and other enterprise-wide initiatives pose?

IoT devices, operational technology devices and other non-traditional computing devices are not inherently designed with security in mind, so security is often an afterthought in these initiatives. Organizations bolt these devices onto infrastructure that's providing PII, HIPAA, IRS 1075 and many other sensitive data feeds that traverse the enterprise. Organizations must ensure they're continuously aware of all these devices throughout their life cycle on the network, that they protect them and more importantly, that they protect the institutional data.

With high-value and PII data spread throughout the enterprise, how can organizations improve their security posture without impeding services or the free flow of information?

Two key aspects are dynamic segmentation and role-based access control that ties into the underlying infrastructure of hardware and software asset management. When I log in to a resource, you need to understand who I am, my user role and what data I'm authorized to see. At the same time, you must understand the device I'm using to log into the network and its context. For example, does the device have inherent authorization to see PII data? If not, there should be an automated segmentation process to deny that access, even if my credentials or group memberships would otherwise allow me to access PII data. So it's understanding the device itself as well as the user, and then using that information to automatically execute a permit/deny access decision.

What is device visibility and control, and why is it important to government security efforts?

It's a concept that says you must be able to understand the entire connected device landscape at any given point in time — what types of devices are on my network; who is logged in to them; are they a risk and so on. Then, along with that visibility you need an automated mechanism to execute control actions such as restricting, allowing or segmenting devices throughout the network after they connect.

What advice do you have for organizations as they consider emerging technologies such as AI and machine learning to improve their cybersecurity stance?

First, it's important to have continuous situational awareness of the device landscape and add that information into the overall picture. You need to understand the devices that are sending data to AI and machine learning technologies for analysis. Second, when your AI or machine learning detects an event, you need to know what action to take and how you can do that in an automated, orchestrated fashion without human intervention.

FORESCOUT®

The Leader in Device Visibility and Control
for State and Local Goverments

100% Device Visibility and Control

Across Your Extended Enterprise

- Gain Continuous Security Awareness
- Mitigate Threats with Policy-based Controls

"With the Forescout solution, we expect to save millions from exponentially faster audits that produce fewer findings and require less remediation effort."

– Phil Bates, Chief Information Security Officer, State of Utah

www.Forescout.com

PROTECTING COMPLEX ENVIRONMENTS WITH INTEGRATED SOLUTIONS



Matthew Schneider, vice president of sales, state and local government and education east for Palo Alto Networks, discusses the importance of integrating disparate security solutions to achieve the full potential of machine learning and other advanced technologies.

How are cyber attacks changing and what do these changes imply for government organizations?

What's really changing and creating challenges is the vast shortage of cybersecurity professionals and the complexities associated with moving into the cloud and new computing environments. Exploits today are taking advantage of disparate systems that rely on human interaction to prevent, detect and respond to attacks. By leveraging compute power, shareware and readily available malicious code, cybercriminals can find cracks in poorly architected systems and manipulate human weaknesses to get in. The way to resolve this isn't significantly different from what we already know. The biggest challenge is to correlate and integrate the solutions that we put in place. That means understanding our users, applications and data that's being accessed, as well as the contextual relationships among those users and applications.

What is data-centric cybersecurity and why is it important as organizations modernize?

Data-centric security acknowledges that the traditional perimeter no longer exists. Users, applications and data are dynamic in terms of where they live, so to defend the entire enterprise, we must bring security to the most sensitive aspects — and that's the data. Organizations must start by classifying their data and then understanding and controlling who uses it and how. There is great power in doing that. They can then take advantage of new opportunities around the cloud, direct citizen access and more. They can leverage massive amounts of data to their fullest, while doing so in a manner that ensures security.

How can organizations use AI and other advanced technologies to improve their cybersecurity operations?

Machine learning on its own is excellent, but it's even more powerful when used contextually in combination with a broad understanding of the enterprise, the cloud, users and applications. If we can bring all of our data into a common set of repositories where we can make context-based decisions, we can protect it at levels we never have before. This approach creates an opportunity to automate responses from a machine learning and AI perspective, so we can eliminate the need for human intervention and free up limited staff resources to go after the most critical attacks and response areas.

DATA-CENTRIC SECURITY ACKNOWLEDGES THAT THE TRADITIONAL PERIMETER NO LONGER EXISTS.

What should IT leaders consider as they integrate AI, machine learning and other emerging technologies into their defense?

The most critical aspect is to build as complete of a view as possible into the data sources that will be coming in. To make data actionable, organizations need to be sure they're not building disparate security systems that can't communicate. They need to integrate these systems — the endpoints, data center, networks and cloud — and bring in all their data collectively so the machine learning algorithms — the input feeds — can be as vast as possible to provide actionable output from the machine learning environment.

Learn more at **Carah.io/GT-Cyber-Palo-Alto**

Govern access, protect data and secure cloud applications with



- Visibility and compliance
- Threat detection
- Realtime prevention
- Secure DevOps and containers
- Secure data and SaaS
- Advanced detection and response

paloaltonetworks.com/cloud-security



ASSESSING AND MANAGING CYBER RISK



As organizations evolve and their reliance on technology increases, securing the enterprise becomes more complex. ***Robert J. Carey,*** *vice president and general manager of global public sector solutions at RSA, explains how a business-driven approach helps state and local agencies manage risk.*

How have security and risk management become more complex with the rise of mobile, edge, cloud and other innovations?
As the pace of innovation accelerates, government organizations may embrace new technologies faster than they are ready to secure them. The network carries the organization's mission "on its back," so as new technologies are introduced, digital risk management is critical. This means looking at how the technology provides a fundamental underpinning for a component of the business and understanding whether it introduces or reduces risk. Performing digital risk management is an ongoing journey as organizations continue to transform and their networks evolve.

What is a business-driven security approach and how does it help address growing complexity?
Business-driven security means understanding that the technology used to deliver on your mission and your business outcomes — servers, databases, mobile platforms, office productivity software and cloud — is wholly reliant on the network. It also involves identifying which technologies support your most mission-critical business functions and protecting them first. In the Department of Defense, we called it Mission Assurance, which means, can I perform my mission and how does the network support that mission. That analysis is really important because you might have to do something from a security point of view to give yourself the risk mitigation that allows the mission to succeed.

What tools or approaches can help organizations address workforce staffing and skills gaps?
One approach within the cybersecurity domain is to leverage AI, machine learning and quantum computing tools that help lighten the load on people in the security operations center. These blossoming tools can offload certain functions to machines so analysts can focus on higher-priority events. But we're not operating purely at machine speed today. Staffing and skills gaps must still be addressed outside of new technologies. The second part is strengthening the ability to hire, train and retain a workforce. To be competitive, people often look at the compensation only, but it also comes down to the "soft" aspects, such as making work meaningful for people, providing a path to grow and being a fun place to work.

How can organizations more accurately assess their cybersecurity maturity and begin moving toward a stronger defense?
Start by understanding the business or mission outcomes the network supports and taking an inventory of all the technology connecting to the network. Then benchmark your organization against an established framework — NIST and ISO have some — to assess your cybersecurity maturity. The assessment will help your organization develop a maturation path, prioritize where to invest and identify the controls needed to reduce or manage business risk. You must also understand your compliance requirements, but keep in mind that compliance does not equal security. It simply means sufficient controls are in place to comply with a specific regulation. Finally, devise a multiyear plan to move the business forward as new technologies emerge and additional funding becomes available.

Mission-Driven Security

Achieving Successful Cyber Outcomes

RSA delivers Mission-Driven Security so organizations across the Public Sector can take command of their evolving security posture.

Learn more by watching the RSA Threat Hunting webinar here: **carah.io/RSAWebinar**



RSA®

ISSUES TO WATCH

3 WAYS TO STRENGTHEN CYBERSECURITY AS TECHNOLOGY EVOLVES



Government Technology talks to Dan Lohrmann, former Michigan state chief security officer and one of the nation's leading cybersecurity experts, about how to confront evolving threats.

A growing volume of research indicates that cybercriminals are targeting state and local governments. But these reports often don't shed light on why it's occurring.

"There are a few reasons governments are being hit so aggressively," says Dan Lohrmann, an internationally recognized cybersecurity leader who led Michigan's cybersecurity and technology infrastructure teams from 2002 to 2014. "One is vulnerability — there tends to be more weaknesses in government networks. It could also be a lack of resources or a lack of IT talent, or the possibility that cybercriminals can generate more public attention by launching a government attack."

The good news is, emerging technologies like AI, machine learning, 5G and quantum computing could help governments improve their cybersecurity posture. However, Lohrmann warns that cybercriminals will also have access to such tools, so those new technologies could generate fresh cybersecurity challenges.

Lohrmann recently shared his thoughts on three things state and local government agencies can do to bolster their approach to cybersecurity both today and as newer technologies emerge tomorrow.

1 Adopt an enterprise view. Michigan was one of the first states to adopt an enterprise approach to security when it did so in 2002. Centralizing security functions provides a holistic view of an agency's security vulnerabilities and protections, Lohrmann says. It also can improve efficiency, cut costs, drive standardization and give jurisdictions a unified way to respond to cybersecurity incidents.

"You're not isolated by agency with firewalls between you, so you can work together more easily," says Lohrmann.

Although he sees some movement toward enterprise security among state and local governments, progress is uneven.

"It's a mixed bag," he says. "At the moment, I think a lot of organizations are still decentralized."

That's because adopting an enterprise view can be challenging — it creates turf battles and highlights inequalities between agencies, especially around budget and personnel.

"Different groups I've worked with went through these types of growing pains in Michigan," says Lohrmann. "The trick is to highlight the benefits of a centralized approach rather than focusing on the challenges involved in making it happen."

2 Conduct a thorough risk assessment. Strengthening cybersecurity means going back to the basics. While it's certainly not new advice, conducting a thorough risk assessment is a critical part of improving cybersecurity defenses.

"It's not about more equipment, more software or more people," says Lohrmann. "It's figuring out the risks. What are your crown jewels? What is the most important data you have? What are the most important services you have?"

Lohrmann says too many agencies lack these basis insights.

"An agency must have a good assessment of its systems, data and security defenses," he says. "Only then can it begin to build an adequate cybersecurity plan for the future."

3 Prioritize. One downside of conducting a thorough security assessment is the results can be overwhelming.

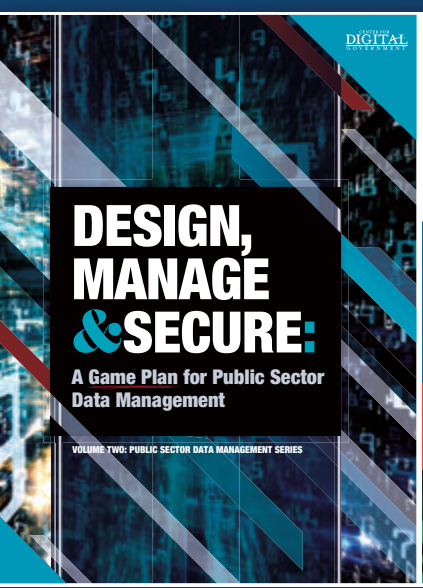
"A lot of people are afraid of a risk assessment because now they have a list of a hundred things they need to do to put their house in order," says Lohrmann. "Meanwhile, you're so busy putting out fires, nobody's even available to tackle the big picture."

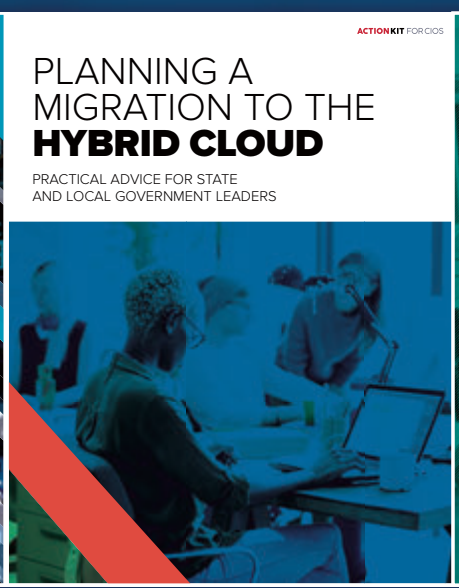
Lack of budget and staff to address security issues are other common hurdles. Lohrmann suggests agencies prioritize their list, develop a plan of action, ensure they follow through, and maintain a scorecard to show management and executives improvements made over time.

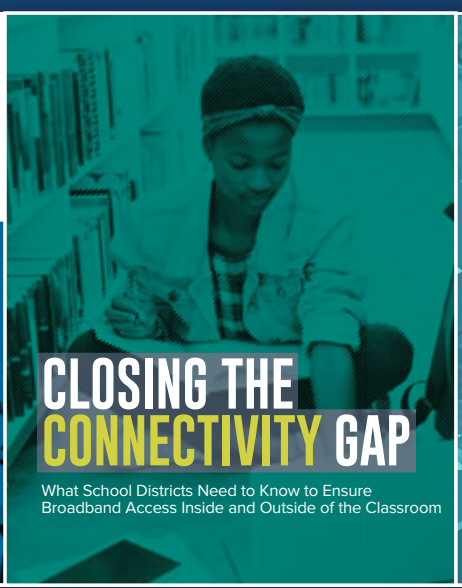
"The challenge is moving the ball down the field, so you are constantly working to build a solid cybersecurity base as technology and the skills of cybercriminals evolve."

© 2019 e.Republic. All rights reserved. Photos by Shutterstock.com

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









Visit our website for some of our most recent work!

www.govtech.com/library

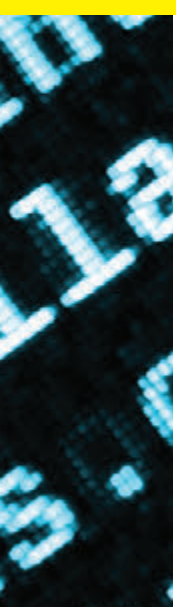
government technology

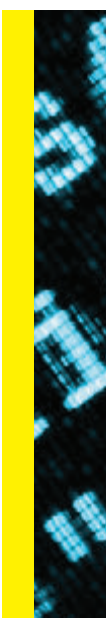

PATCH
WORK



BY DAVID RATHS

PATCH MANAGEMENT IS A CORNERSTONE TO INFORMATION SECURITY IN TODAY'S HIGHLY DIGITIZED ENVIRONMENT. SO, WHY IS IT STILL SUCH A VULNERABILITY?





The after-effects of a ransomware attack on government can be devastating. But in so many cases, the reason why it happened often comes down to a simple flaw: Government agencies are using outdated computer software, such as unsupported Windows operating systems, including XP and Windows 2003; they also are not applying freely available software patches and not creating effective backups.

A typical example of the problem can be found in a March 2019 audit of the Maryland Department of Information Technology (DoIT) by the state Office of Legislative Audits. The office found the department's customer agencies' workstations had not been updated with the latest releases for three application software products that are known to have ongoing security-related vulnerabilities. The report also pointed out that "workstations were not being regularly updated" with software patches, increasing the risk of security breaches "from attacks focused on the related vulnerable application software."

The problem faced by Maryland's DoIT is common throughout government and the private sector. In 2018, the Ponemon Institute, an international research organization, surveyed 3,000 cybersecurity professionals globally and found that more than half of the organizations suffered a data breach in the last two years. Of these, a majority attributed the breach to a vulnerability for which a patch was already available. The organizations that have been able to avoid a breach reported being able to detect a vulnerability quickly, and could patch vulnerabilities in a timely manner.

So, what is keeping government IT leaders from doing a better job of patching their systems and how are some IT organizations approaching the issue systematically?

THE HARD LESSONS OF DECENTRALIZED IT

Nicholas Andersen, former chief information security officer of Vermont, pointed out that traditionally, governments have not thought of themselves as prime targets for nefarious online actors. Obviously, they can no longer think that now. "It is a mix of a lack of resources and starting to recognize that the risk to them is as significant as it is to larger government organizations," he said.

The CIO or CISO must be able to set patch management standards and enforce compliance, according to Andersen. "If they can't do that, then they are not going to be able to succeed," he said. "Decentralized IT in a lot of ways does not lead to enabling that CIO or CISO to be successful in this regard."

Peter Romness, the cybersecurity solutions lead in the U.S. Public Sector CTO Office at Cisco Systems, noted that after a breach, you often hear people saying that if people would just patch and do basic hygiene, this wouldn't have happened. "Then if you talk to people responsible for doing this work, they say, 'That is true, and we do patch as much as we can, but it is not as easy as you make it sound,'" he said.

State and local governments are the most budget-constrained organizations in terms of cybersecurity that there are, Romness added. "When they need to do something on cybersecurity, it takes time to get the money budgeted for it," he said. "They also have a hard time getting cybersecurity staff."



Maria Thompson, North Carolina Chief Risk Officer

In a recent blog post, Romness pointed out that busy IT execs may be managing thousands of computers that need periodic updates and, in some cases, they may not even know all the systems in their environment. "Managing updates on so many different pieces of software, on so many systems, can be overwhelming and effective updates may slip through the cracks," he wrote. Of greater concern is that patches are only developed for known vulnerabilities. Once these zero-day vulnerabilities are found, it can take time to develop and distribute the patch. "But newer (or undiscovered) malware will slip right through the latest patch," he said.

Romness argued for taking a holistic, architectural approach to cybersecurity. "We used to talk about defense in depth,



SHUTTERSTOCK.COM



but I have come to see that as throwing good money after bad and piling up solutions that become hard to manage. Now I like to talk about effective defense that makes sense," he said. "That means you look at what you have, determine what is important to your organization and make appropriate defense decisions."

THE SPEED PROBLEM

One key issue around patching is speed. Hackers aren't just attacking more aggressively, they are doing it at a much faster rate, according to Ponemon's report, *Patch Work Demands Attention,* which was produced for ServiceNow, a cloud computing company. With the rise in AI-fueled attacks, the research organization believes the speed of hacking attacks will only increase. But many organizations rely on manual patching processes and have disconnected systems, making it harder to fight back in a cohesive way. That's especially true in state and local government, but strategies are emerging.

Vermont had a decentralized IT management approach until two years ago. When Gov. Phil Scott came into office, one of the first executive orders he signed created the Agency of Digital Services (ADS) as a cabinet-level department to support centralized IT management statewide. Andersen said that new centralized IT was key to how ADS approached patch management.

Previously, each agency or department had its own team to handle their own IT system deployment through the full life cycle, including patch management. Some agencies had only one or two IT people. They were focused on things that the agency needed (database administration or Web server management) and some didn't have people with security expertise or enterprise architects or cloud architects. Others were better funded and had invested money in their IT infrastructure, but that wasn't the case across the board.

"THE CIO OR CISO MUST BE ENABLED TO SET PATCH MANAGEMENT STANDARDS AND ENFORCE COMPLIANCE. IF THEY CAN'T DO THAT, THEN THEY ARE NOT GOING TO BE ABLE TO SUCCEED."

"Now [Vermont] can consolidate all of that, not only to generate savings for the state, but also to provide greater visibility into its security posture and better governance of patch management status," Andersen explained. Vermont now has an enterprise approach with a 30/60/90-day plan — 30 days for mitigating high vulnerabilities, 60 for medium vulnerabilities and 90 for low-risk vulnerabilities.

"Bringing everything under one agency allowed [Vermont] to build a shared services team to provide enterprise hosted options," Andersen said. With a centralized patch management system, the shared services department can find high-level patches that need to be applied urgently. The department can respond quickly to alerts from a vendor such as Microsoft, the Department of Homeland Security, or the Multi-State Information Sharing and Analysis Center (MS-ISAC).

One important task is identifying legacy operating systems and applications and the agency business processes they support. That includes the network infrastructure too. "Every networking device you might use has its own vulnerabilities, and the same for mobile devices," said Andersen.

Microsoft, in particular, does a good job of forecasting years in advance when they are going to end support for their systems, and when organizations are going to be able to purchase extended services to continue receiving critical patches even beyond their end-of-service date, according to Andersen.

An enterprise software solution provides patch management and patch status updates. A complementary vulnerability management system gives a comprehensive vulnerability management picture to ADS and department IT leaders.

If there is not a patch available, ADS wants to be able to see where an agency has a road map or plan to no longer use that end-of-service hardware or software

and get it off the network. In the interim, if there is something the business says is critical to its mission, and that is not supported any longer by a vendor, IT will work to identify compensating controls — to keep it relatively isolated on the network and turn off nonessential services to reduce potential attacks and isolate those systems that are no longer supported.

"Having that vulnerability awareness platform in place allows [Vermont] to have a single person on staff who has visibility into everything in the enterprise," Andersen said, adding that this visibility allows for conversations with IT leaders at the agency level about risks and needed updates.

UPDATE THAT OPERATING SYSTEM

One of the biggest complaints about information security — including patch management — is the need for more personnel to carry out the work. But more doesn't always equal safer, according to the Ponemon Institute. Improving an organization's security posture won't happen with more personnel as long as the patching process remains broken. States with lean IT staff have begun to figure that out.

In South Dakota, patch management is made somewhat easier by the fact that IT is highly centralized in the Bureau of Information and Telecommunications (BIT), where a small team of technology engineers oversees patch management. They use a tool from Ivanti for custom third-party patches, but also for patching Windows machines, according to Matt Guelde, technology engineer.

"Within the Ivanti endpoint management software, the patch definitions come to us with metadata that tells us how critical the patch is, both from Ivante's perspective and the vendor's perspective. We typically home in on those patches that have a critical or high vulnerability rate," he said.

Michael Hanson, technology engineer, added that the state is on a fast track to making sure that all workstations are running Windows 10. "We are sitting at 91 percent now. By the first of the year, we should be at 100 percent."



"THERE ARE ALWAYS GAPS IN YOUR ENVIRONMENT YOU CAN'T SEE,AND YOU CAN'T PROTECT WHAT YOU CAN'T SEE."

SHUTTERSTOCK.COM

BIT sets policies for how agencies deal with software vendors and IT service providers, according to Deb Dufour, LAN service manager. "If it involves technology purchases, we have a review process the agencies have to go through," she said. "Part of that review is they are required to have a maintenance agreement with the vendor. If a vendor is hosting a system for the state, we ask about how they do patch management."

BUILDING RISK INTO THE PATCHING EQUATION

One of the first things Maria Thompson, chief risk officer at the North Carolina Department of Information Technology (DIT), noticed when she moved to state government from the federal sector was the lack of visibility. "There are always gaps in your environment you can't see," she said, "and you can't protect what you can't see."

Thompson uses a practice common in the federal sector called Continuous Diagnostics and Mitigation (CDM), which has enabled DIT to take a risk management approach to patching. "We are trying to gain better visibility across the landscape. We need to understand what our capabilities are and the gaps so that we can better protect ourselves."

She described North Carolina state government IT as a hybrid model, with some agencies that are consolidated and some that are not. "We have to build relationships with decentralized organizations and help them understand that we are not trying to manage their environment," she said. "We are trying to enable them to do their job but also feed that enterprise visibility so we can collectively help protect ourselves from any type of cyberincident."

When she arrived, Thompson set out to expand the use of tools that scan for vulnerabilities. "What we have been working on is increasing our footprint to not just DIT but all the agencies that have a need for a solution similar to this and may not have anything similar in place." The state uses an enterprise version of Tenable, a security monitoring solution for large organizations.

DIT has provisioned accounts for all the agencies and identified points of contact, such as security liaisons or application owners and system administrators. "They have access to get into the system to run reports as needed," Thompson said. "We run a scan on a seven-day cycle."

This helps the DIT team prioritize which things to target. The Tenable scanner is only one solution in a suite of tools that help complete this picture, she added. "We have other solutions to help monitor our external perimeter and give us a credit card score of how we look from an external perspective, and based on your score, there are points associated with the types of vulnerabilities and it helps you make a decision: If I make this change, which one will give me more bang for the buck and offer more protection? Prioritization is definitely key to this." gt

draths@mac.com



2019 SPECIAL DISTRICTS

Technology Innovation Award Winners

SOUTHEAST

CITIZENS CATEGORY

Housing Authority of the City of Prichard // Project SOAR
St. Johns River Water Management District // Water Well Construction Module
North Springs Improvement District // Advanced Metering Infrastructure (AMI)

OPERATIONS CATEGORY

Bonita Springs Fire Control and Rescue District // Technology Projects
Southwest Florida Water Management District // Data Consolidation Initiative
The Children's Trust // Trust Central
Housing Authority of the City of Fort Lauderdale // Neighborhood Master Plan

LEADERSHIP CATEGORY

Greater Naples Fire Rescue District // Shawn Hanson, Deputy Chief/Fire Marshal
Tampa Housing Authority // Cherrie Calloway, Neighborhood Networks Technical Trainer

SOUTHWEST

CITIZENS CATEGORY

Colorado Valley Transit District // GoFare Card
Fort Bend County Levee Improvement District No. 2 // Public Outreach

OPERATIONS CATEGORY

Brushy Creek Municipal Utility District // Plan for Unaccounted for Water
Capital Metropolitan Transportation Authority // Detour-Aware Real-Time GTFS Feed
Central Texas Regional Mobility Authority // State Highway 45 Southwest
Colorado Valley Transit District // Fare Cards
East Texas Council of Governments // GoBus New Fare System

LEADERSHIP CATEGORY

Orleans Parish Communication District // Tyrell T. Morris, MBA, CPE, Executive Director
Edinburg Housing Authority // Rene Torres, Information Systems Manager

MIDWEST

CITIZENS CATEGORY

SouthWest Transit (SWT) // SW Prime - Microtransit Service
Naperville Park District // Eight-Facility Wi-Fi Provision

OPERATIONS CATEGORY

Cleveland Metroparks // New Technologies Usage
Columbus Crossroads Special Improvement District // Collaboration for Increased Ridership
Des Moines Area Metropolitan Planning Organization (MPO) // Container Locator
Greater Cleveland Regional Transit Authority // Continuous Auditing Implementation
Indian Trails Library District // Transformation to Community Space
Naperville Park District // 311 Parks System

LEADERSHIP CATEGORY

Lucas Metropolitan Housing Authority // Demetria Simpson, President & CEO
Park District of Oak Park // Innovation Team
Metropolitan Water Reclamation District of Greater Chicago // John Sudduth, Director of Information Technology
Naperville Park District // Omar Sandoval, Director of Information Technology
Lexington Regional Health Center // Rob Hanna, CIO

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

govtech.com/districts

AN AT&T PROGRAM

government technology



SHUTTERSTOCK.COM

Hygiene Help

A federal program is helping a growing number of IT shops tune up their cyberposture.

By Lucas Ropek / Staff Writer

At a time when hackers target state and local governments more than ever before, proper cybersecurity practices are crucial. Some recent estimates have put the number of attacks against state governments at 150 million a day, making cyberhygiene — the task of analyzing system infrastructures to test for and correct vulnerabilities — an increasingly vital practice. But the costs of maintaining that hygiene can be out of reach for smaller communities.

That's why a special team within the Department of Homeland Security (DHS) is helping governments at all levels better secure their systems. The DHS Cybersecurity Assessments program offers its services free of charge to any organization that requests them.

Operated from within DHS' new Cybersecurity and Infrastructure Security Agency (CISA), the program has grown rapidly over the years from a handful of cyberprofessionals to a large team that provides hundreds of services per year to state, local and tribal government entities, as well as private-sector companies.

Don Benack is the program's former deputy director (he has since been promoted to another position within the program) who helped guide it from its inception in 2007. Benack said that the services, which are provided both remotely and with in-person technical support, are centered on identifying and analyzing system vulnerabilities.

The program includes cyberhygiene assessments, which analyze potential weak configurations in Internet-facing systems; phishing campaign assessments, which measure human susceptibility to lure emails; and remote penetration testing, which simulates a cyberattack to expose gaps in security. The program also has a red team, which utilizes social engineering efforts to understand intrusion methods and system flaws that adversaries exploit.

Benack said the program initially grew from a fairly limited federal compliance effort in the mid-2000s.

The Trust Internet Connections (TIC) initiative, mandated by the U.S. Office of Management and Budget (OMB) in 2007, was a large effort to reduce the risk of malicious intrusions to the federal government by drastically shrinking its external network connections. OMB authorized what was then called DHS' National Cyber Security Division to coordinate TIC for the federal civilian executive branch — establishing an assessment team called the Cyber Assurance Branch (CAB). CAB, which would eventually transform into the larger Assessments program, was initially tasked with what were essentially compliance efforts for federal agencies looking to secure their systems.

However, it soon became apparent that the scope of the program could be drastically expanded, Benack said.

"We quickly realized that there was an opportunity to do more than just be a compliance checker for meeting the specific mandate capability," said Benack, explaining that the focus transitioned to risk assessments and advancement of best practices. "Over time, the capabilities of the assessment team grew to help agencies better understand and manage the risks and vulnerabilities identified."

The team began to offer federal agencies optional assessments, including two new voluntary services that would eventually become program mainstays. These were the Risk and Vulnerability Assessments (RVA) in 2012 and Cyber Hygiene (CyHy) vulnerability scanning in 2013.

The program's federal scope was also greatly expanded by the discovery of the Heartbleed vulnerability in 2014, a significant weakness in OpenSSL encryption software on myriad websites and devices. The discovery spurred the OMB to mandate that all federal civilian agencies use the program's cyberhygiene services. DHS later followed the OMB mandate by issuing its own operational directive that obligated federal civilian agencies to mitigate critical vulnerabilities on their Internet-facing systems identified by CyHy services within 30 days of notification, Benack said.

In late 2013, the program ultimately pivoted from one with a singular federal focus to a national one — offering, for the first time, RVA and CyHy services to state and local governments and all 16 sectors identified by the federal government as "critical infrastructure."

Not surprisingly, the program continues to grow in popularity. Only 11 cyberhygiene tests were conducted for state and local governments during the first year, but four years later, the number of stakeholders had jumped to 208, before rising to 633 in 2019. Similarly, the phishing campaign assessments — first offered in 2018 — jumped from one test conducted last year to 30 tests conducted this year. The team's validated architecture design reviews — which help governments understand the relative design strength of their systems and networks — were requested 25 times by different state and local governments so far this year.

"The great thing about these services is that they're for everybody," said Erik Avakian, chief information security officer (CISO) of Pennsylvania. For larger organizations, the tests can serve to augment other security testing procedures, while for agencies and communities with more limited funding, they are an alternative to services that would otherwise have to be purchased from the private sector.



DAVID KIDD

Pennsylvania has been using DHS' cybersecurity services since 2016 to bolster its own testing practices, said state CISO Erik Avakian.

Avakian said his agency has been using the services since mid-2016 to complement its own security tests and that the state continues to receive regular reviews from the program. Pennsylvania gets both remote and in-person testing and reviews, he said, adding that the expertise DHS operators bring to the table adds a lot of value.

Similarly, North Dakota's Information Technology Department, which already conducts its own cyberhygiene tests — including phishing campaign assessments, and risk and vulnerability scans — has been receiving the DHS assessments for a little more than a year. State CISO Sean Wiese thinks of the DHS evaluation as "another set of eyes" on processes his agency is already responsible for.

"It's somebody else doing it for us — to validate [results] and for us to compare notes, really," Wiese said.

All of the services that DHS is offering should be a part of an agency's threat mitigation tactics, Wiese said. Of course, depending on a government's cybersecurity maturity level, they might not be able to be as thorough as they need to be, he added.

Indeed, the National Association of State Chief Information Officers released a report in 2018 arguing that while states have made significant progress in establishing cybersecurity programs, serious "shortages in both funding and cybertalent continue to exist." The report notes that risk assessments were one of the most routinely outsourced operations, and are an area where CISOs still have "room to improve."

Looking to the future, the program's operators see more clients, wider availability of their services, and the use of emerging technologies and automation to better deliver them.

"We have over 1,200 state and local and critical infrastructure customers leveraging the service and we hope to keep growing," Benack said. "Our message [over the years] hasn't changed, and the value statement hasn't changed. Every year, we get a few more resources," Benack said, explaining that he hopes there is increased funding in the coming years. gt

For more information on the DHS Cybersecurity Assessments program, visit www.dhs.gov/cisa/cybersecurity-assessments.

lropek@govtech.com

ADVERTISEMENT



HOW TO ENSURE A NATURAL DISASTER DOESN'T LEAD TO DATA LOSS

A carefully considered plan for offsite data backup makes information available when it's needed most.

Access to data is one of the first things a government needs following a natural disaster. Data in many forms is essential to bring back government operations, deliver emergency services and help the community rebuild.

Many governments follow solid practices for creating data backups but may not have an easy or secure way to store them offsite. In other cases, a government may have offsite storage in a nearby data center or service provider's colocation facility. However, that backup is vulnerable to the same tornado, hurricane, earthquake or other widespread and destructive incident as the primary storage.

In addition, traditional tools and processes for data backup and recovery are often manual — making them slow, cumbersome and vulnerable to human error. This challenge expands as governments store data across multiple, diverse applications and storage systems, both on premises and in the cloud.

A carefully considered choice for offsite backup, a documented data recovery plan, and the right management tools and processes can help ensure vital informaton is available after a disaster. Yet many governments have found developing these resources daunting given the large scope of data and applications.

THE NEED FOR OFFSITE STORAGE

To safeguard data in the event of a natural disaster, government agencies need to ensure they have strong offsite data backup, replication and recovery services. The offsite location should be far enough away to ensure it's not susceptible to the same natural disaster as the original location. For example, when Hurricane Dorian struck in September 2019, it caused widespread damage in the Bahamas, along the U.S. eastern seaboard and into Canada. Storing data in a neighboring city or county, therefore, may not always be enough.

Other offsite storage considerations:

- Weigh the use of other locations within the organization versus colocation, a managed cloud provider versus a public cloud provider, or possibly a combination of multiple providers. Other locations or colocation typically provide the utmost flexibility for disaster recovery options.
- Copy all backups offsite. A good offsite backup is automatic, consistent and reliable. Agencies should check their offsite files regularly to make sure backups are completed consistently and perform regular disaster recovery drills to ensure all data is accessible, usable and up to date.
- Use runbooks and orchestration when available. Orchestration ensures that critical servers, applications and their dependencies come online without incident. It's important to understand how a vendor plans to failover your applications, and then failback, and how much customization and control you have in the orchestration process. Some disaster recovery providers offer runbooks that describe the order in which your systems should recover. Runbooks can help enhance IT operations efficiency measures, reduce mean time to repair, increase mean time between failures and automate the provisioning of IT resources.
- A cloud-based offsite storage solution, when and where appropriate, can provide economical offsite data backups and a comprehensive recovery service for all data files, applications and servers. This can enable advantages such as backup redundancy and multiple recovery points for reliable restoration of critical data needed to continue operations, automation to assure fast and timely backups and restores, and improved visibility and management control for protecting data from all sources (including user endpoints and software-as-a-service [Saas] applications).

TIPS FOR CREATING STRONGER DATA PROTECTION

Consider the following three tips to implement strong data protection measures.

First, look for vendor software tools that help create a detailed disaster recovery plan and automation runbook. Make sure these resources are specific to the agency's applications and data, and schedule regular reviews to keep them up to date. The plan and runbook should specify the following:

- **What is covered by the backup.** Identify backup coverage for virtual

© 2019 e.Republic. All rights reserved.



and physical servers, data storage systems, desktops and laptops, cloud applications and infrastructure, and SaaS workloads. Current business and operational data may need a more stringent plan than archived data. In addition, consider the data recovery requirements of key departments and functions such as emergency management, police and fire, and public works.

- **Replication.** For each defined workload, determine whether server replication is needed to obtain an extra measure of protection and assure timely recovery through instant failover.
- **Compliance.** Evaluate how the backup solution and processes meet regulatory requirements. Factors such as restore time objectives (RTO) and restore point objectives (RPO) for specific systems and databases may be important compliance mandates.
- **Management.** Identify the capabilities needed for data protection monitoring, reporting and capacity planning. These capabilities are essential to balance data protection, backup and recovery performance, and costs.

Second, automate backup and restore processes. Automated processes improve the timeliness and consistency of backups and reduce the potential for human error that can impair full and accurate data restoration.

Finally, automate testing of all items in the data backup, replication and recovery plan, using multiple scenarios to verify complete backups and restores. These scenarios should include all anticipated natural disasters and running automated and manual data restores. Additional items to test include:

- Operation of needed systems, applications and network connections
- Documented policies and procedures
- Team, vendor and employee roles
- Achievement of the defined RTO and RPO metrics

DATA WHEN IT'S NEEDED MOST

Today's resources for offsite backups offer powerful tools to protect government data and applications used in both every day and emergency operations. With reliable availability of information, agencies can better maintain services, protect public safety and help citizens in times of need.

HOW YAKIMA COUNTY PROTECTS PUBLIC SAFETY DATA

Emergency personnel need immediate access to essential data to protect their community during and following a natural disaster. To solve this challenge, Yakima County, Wash., implemented a cloud solution for dependable and high-speed backup, replication and recovery of 50 TB of data. The new cloud solution eliminated the frustration of failed backups that occurred with the county's previous solution. It also eliminated the time the county's server administrator spent troubleshooting those problems each week.

Another benefit: A replication design under the previous solution wasn't feasible because it required a high capital investment. Using cloud, Yakima County can economically replicate critical data for quick failover and data access in an emergency.

With the hyper-growth and hyper-sprawl of today's data, traditional data management is not enough. Data must become hyper available. Getting there requires a new approach that merges the traditional disciplines of data backup and recovery, data protection and data security. Moving from policy-based to behavior-based management to make data both intelligent, and ultimately, self-governing. As the leader in availability across multi-cloud environments, Veeam® is uniquely positioned to help customers along their journey to intelligent data management. **www.veeam.com/sled**

Who Is the State CISO?

Though chief information security officers became a universal fixture in state government much later than CIOs, their importance has grown rapidly along with the expanding IT footprint of the public sector and the morphing threats against it. To better understand who these people are and what factors shape their work, we gathered data on as many state CISOs as we could find — which turned out to be 158 CISO terms. Where appropriate, we compared this with similar data we've compiled on CIOs in order to put the numbers in context. **By Ben Miller**

The Hot Seat

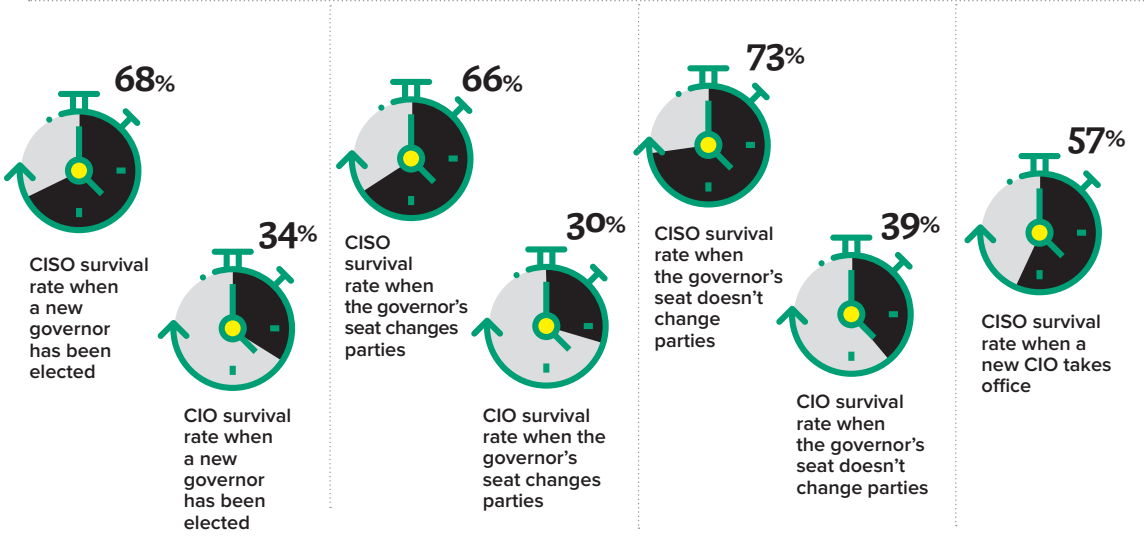
Average tenure of a state CISO:
3 years, 10 months

Longest-serving CISO:
Agnes Kirk, Washington state, 13 years, 2005-2018

Shortest-serving CISO:
Nicholas Andersen, Vermont, 9 months, December 2018-August 2019

Staying Power

We know that a new governor usually means a new CIO, but what does it mean for the CISO? As it happens, CISOs are much more sheltered from the political winds — it's when there's a new CIO that a CISO is more likely to leave. To get a better look at those dynamics, we calculated the "survival rates" when a new governor or CIO takes office — in other words, how often does a CISO stick around when there's a new leader?



Looking Back

Previous job before becoming state CISO:

Private	21%
Public	70%
Education	2%
Nonprofit	2%
Military	6%
Retired	0%

Previous job before becoming state CIO:

Private	28%
Public	59%
Education	9%
Nonprofit	1%
Military	3%
Retired	0%

Looking Ahead

Next job after serving as state CISO:

Private	48%
Public	33%
Education	8%
Nonprofit	8%
Military	1%
Retired	4%

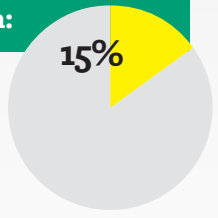
Next job after serving as state CIO:

Private	52%
Public	22%
Education	14%
Nonprofit	3%
Military	1%
Retired	8%

Declining Women

Just as with state CIOs, we found that the prevalence of women in state CISO roles has declined in recent years. Here's the data on female state CISOs as a percentage of all available information:

Overall percentage of state CISOs who have been women:



Most Common CISO Names

Michael/Mike: 9

Christopher/Chris/Kris: 8

John/Jack: 6

James/Jim: 7

Data was collected from LinkedIn profiles, coverage from *Government Technology* and other publications, state government websites, the National Association of State Chief Information Officers' (NASCIO) State Cybersecurity Resource Guides, and a couple very helpful public officials. Only permanent CISOs and interim/acting CISOs who served for at least a year were included on the list. Kris Rowley, who served as CISO of Vermont from 2008 to 2015, transitioned from female to male after leaving the government. For purposes of gender statistics, Rowley was counted among the women for his time as CISO. Data is current as of Aug. 23, 2019.

By Dan Lohrmann



Cyberproofing the Future

Five ways cyberchiefs can support emerging technologies in the coming decade.

As we head into the 2020s, emerging technologies are both exciting and a bit scary at the same time.

On the positive side, the definition of "government service" is changing before our eyes. From artificial intelligence and the Internet of Things to 5G apps and autonomous vehicles, the list of startup opportunities promises to revolutionize government (again) over the next decade. Plus, the smartphones in our pockets have the power to enable digital transformation in government on a scale that seemed like a far-fetched fantasy at the beginning of the millennium.

But, if history has taught us anything over the past two decades, the Achilles' heel to these advances in technology will continue to be cybersecurity. The Internet is an accelerator for both wonderful ideas for good but also bad actors, data breaches and privacy violations.

So what can be done? Here are tips to help enable the good and disable the bad.

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.

1 / Stop saying "no" when you are approached with innovative tools to improve customer service. Instead, security and technology professionals should strive to:

- Offer workable alternatives to provide deliverables on time and on budget, with the right level of security.
- Examine global best practices and innovative approaches to solve security and privacy concerns.
- Empower new capabilities that will maintain trust with citizens and staff.

2 / Mandate cybersecurity at the start. Executives need to build security into government solutions from the beginning of projects and throughout the entire life cycle. Cybersecurity is a tool that enables new possibilities to break down old barriers and you must provide resources to ensure security is done right. While security is a part of everyone's role, cybersecurity ambassadors need to be included on key strategic project teams. Oftentimes, cyberprotections are an afterthought for major projects, or security is added only after a data breach. This must change.

3 / Embrace new tech, like IoT, inside security shops. Too many organizations are leaving new technologies to business areas and/or "shadow IT" groups. They see these areas as not central to the mission.

For example, they don't see IoT deployments as part of their job. But according to a 2019 Microsoft study of more than 3,000 private-sector executives across the globe, IoT adoption is expected to accelerate with 94 percent of public- and private-sector organizations by 2021. Consequently, the top three security concerns on the minds of leaders are:

- 43 percent are careful about developing strong user authentication;
- 38 percent have a concern regarding tracking and managing each IoT device; and
- 38 percent are worried about securing endpoints for each IoT device.

4 / Partner with the private sector. Perhaps you're thinking that you just don't have the expertise to implement a new technology securely. There are plenty of innovative companies who would love to help and guide you, but who can you trust?

Most governments are not the first to deploy these new tech products and services. Look for case studies from other successful implementations and watch for success stories from groups like the National Association of State Chief Information Officers or Federal CIO Council.

5 / Good security is all about the people. It's tempting to always run to the latest and greatest new solution. But whether you are implementing a $150 million tax system, a $25,000 security appliance or a cloud-based server, most security problems come from people-related issues or processes that are inadequate or not regularly secured, updated or tested properly.

Ensure that your cybersecurity automation is implemented with people, process and technology in mind. Go back and double-check assumptions with your team.

The 2020s promise to be a decade filled with amazing new technologies that make government even more accessible to the masses in new ways. But cyber is left out of these projects at your peril. GT

spectrum

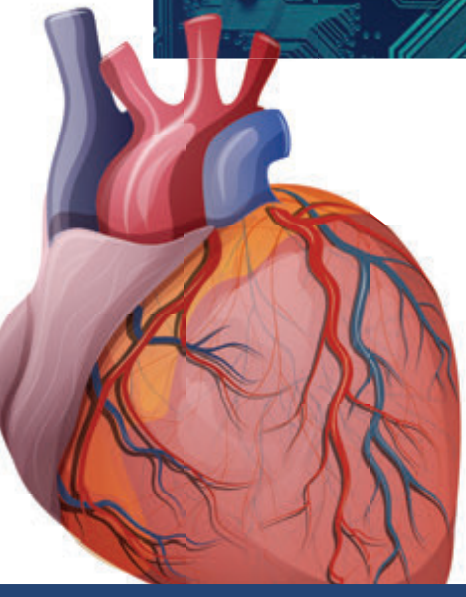
More research, more science, more technology.

BUILDING BIGGER

While the longtime trend has been for microchips to get smaller and smaller, thereby enabling ever-shrinking computing devices, a new chip from California-based startup Cerebras is going in a whole different direction. The company's WSE chip is about the size of an iPad at about 46,000 square millimeters and is specifically designed to power artificial intelligence processes with its 1.2 trillion transistors and 18 GB of memory. The idea is that a bigger, more powerful chip will stand up to the growing use of AI, enabling the software to learn faster. SOURCE: DIGITAL TRENDS

3,700

Toyota reports it will provide "3,700 mobility products and/or vehicles" for the Olympics and Paralympics in Tokyo next year, 90 percent of which will be electric, some powered by batteries and others by fuel cells. SOURCE: THE VERGE



50%

On average, about half of people undergoing heart surgery will need at least one follow-up procedure, and the Food and Drug Administration is planning a high-tech approach to combat that. Called Optimal Target Identification via Modelling of Arrhythmogenesis (OPTIMA), the procedure will create a virtual model of a patient's heart, use electrical pulses to see where it is experiencing an irregular heartbeat, and then perform simulated surgeries as many times as needed to get the correct fix. Once a surgeon performs the operation according to the plan, the patient likely will not need follow-up surgeries. SOURCE: ENGADGET

Jaws

Sand tiger sharks, a species with a declining population that's currently classified as "vulnerable" to endangerment, have been swimming around shipwrecks off the coast of North Carolina, and researchers there are using a futuristic way to study them: underwater robots outfitted with lasers. They use the bots to monitor water conditions and animal size, plus pick up signals from acoustic tags that mark individual sand tiger sharks. SOURCE: TREEHUGGER



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

cio central

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


Phil Bertolini

Bertolini Retires from Michigan, Joins Center for Digital Government

After announcing his retirement as deputy county executive and CIO of Oakland County, Mich., following a 31-year career with the government, **Phil Bertolini** was named co-director of the Center for Digital Government.* Together with Executive Director Teri Takai, he will lead the center's major programs, including a new initiative on cybersecurity. Bertolini led Oakland County IT since 2001, and his tenure was marked by accomplishments including a move to the cloud and the creation of the G2G Marketplace, which offers IT solutions from approved vendors to government agencies at all levels.

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

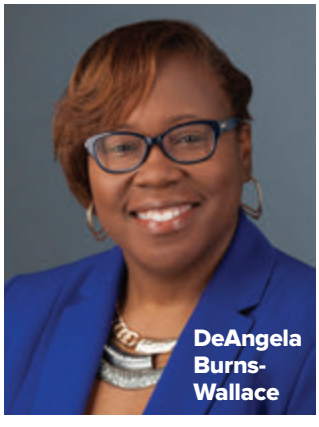

Tyler Kleykamp

Connecticut CDO Leaves for Academia

Tyler Kleykamp, Connecticut's first chief data officer, left for a position in the academic sector after serving the state since 2014. A leader in data work, Kleykamp helped found the State Chief Data Officer Network, which fosters collaboration among those in the role around best practices, inter-state projects and more. As of press time, his new position was unspecified, and his replacement had not been named.

New York State Appoints Interim CIO

Following the retirement of Bob Samson in mid-August, the New York State Office of Information Technology Services named **Joseph J. Rabito** interim director and chief information officer. "We will welcome new methods and approaches to enhance efficiency, and plan a responsible and effective investment of state resources," Rabito wrote in a message to ITS staff upon his arrival.


DeAngela Burns-Wallace

Kansas Gov. Replaces CITO

In August, Kansas Gov. Laura Kelly appointed **DeAngela Burns-Wallace** as the state's new chief information technology officer. Burns-Wallace will also continue in her role as secretary of the state Department of Administration. She replaces **Lee Allen**, who was named to the position by former Gov. Jeff Colyer in July 2018.



Enrique Martinez Jr.

El Paso CIO Leaves for Arlington

Enrique Martinez Jr., who led technology operations in El Paso, Texas, for six years, left that city for Arlington, Texas, in September. He cited standing up a second data center in partnership with El Paso County as one of his chief accomplishments. Martinez was replaced in an interim capacity by the IT department's assistant director, Araceli Guerra.


Jeff Nyberg

Minnesota Appoints CTO

Private-sector veteran of major companies like Target and Dairy Queen **Jeff Nyberg** was tapped to be Minnesota's new chief technology officer. He also previously worked for the city of St. Paul, and CIO Tarek Tomes said Nyberg will help oversee the state's new Data Performance and Management Program.


Matt Singleton

Oklahoma Names New CISO

In Oklahoma, Digital Transformation and Administration Secretary David Ostrowe and CIO Bo Reese tapped **Matt Singleton** as the state's new chief information security officer. Singleton previously spent many years in IT security at Oklahoma University, where he helped build the school's Cyber-Forensics Lab. His plans for the state include developing statewide cyberstrategy and privacy practices, among others.

Vermont CISO Departs

After a brief stint as Vermont's chief information security officer beginning in December 2018, **Nicholas Andersen** left his post with the state in mid-August. He returned to the Washington, D.C., area, where he was expected to hold a position in the Executive Office of the President at the White House. Deputy CISO Scott Carbee was named to the top security position on an interim basis.

By Kristy Dalton



Should Government Restrict Social Followers?

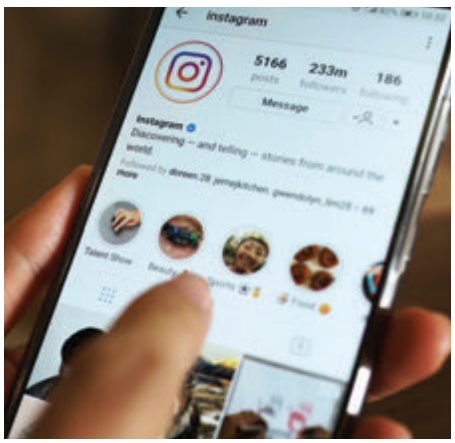
Instagram's new comment restriction tool may be helpful for some users, but it presents challenges for public-sector agencies.

Instagram is testing a new comment moderation tool, but government agencies might want to think twice about adopting it.

The image- and video-sharing platform has discovered that sometimes younger users are hesitant to report or block bullies because they don't want to risk retaliation. Enter the new "restrict" feature, which attempts to address this problem by giving users more control over the comments people can view on their posts.

According to preliminary details from Instagram, accounts will be able to restrict who can see comments certain users make on their posts. Because the person who makes the comment continues to see it, and isn't notified that it's no longer seen by anyone else, the "restrict" option feels similar to the "hide" option available for Facebook comments. The key difference is that hiding Facebook comments is done individually after the comment has been published. Comments made on an Instagram account by someone restricted by that profile would automatically be hidden to others.

Restricting is an action a user can take toward another Instagram profile, such as with "blocking." But unlike blocked profiles, restricted accounts aren't banned from finding the restricter's profile and can continue to view all the content that the person who has restricted them publishes. If your profile is blocked, you might know it because you can't view the profile that blocked you at all. However, restricted profiles would be unaware their comments have been restricted (which does make it useful for bullied people who don't want to make waves).



SHUTTERSTOCK.COM

The other important feature of restricting an Instagram profile is that users can choose to make the restricted person's comments visible to others on a case-by-case basis. This means all the offender's comments would start off as automatically hidden, and then the original poster can decide to let some of those comments be visible.

Why should government be cautious?

As soon as Instagram mentioned it was testing the restrict option, I heard from several government agencies eager to test it out as a way to manage profiles that repeatedly violate their official comment policies.

I've always cautioned government agencies against comment hiding and profile blocking. While the idea of restricting Instagram profiles may be a useful tool for private citizens, it raises concerns for government agencies.

Courts are being more consistent in finding that government profiles on social media are public forums, and that blocking profiles is a violation of citizens' First Amendment rights.

What if you restrict a profile with the good intention of reviewing the user's comments on a case-by-case basis, but you don't immediately review the comments, or you forget to? Relevant information (that doesn't violate your social policy) might never see the light of day.

Whenever government is in a situation where it is choosing which comments to allow and which to restrict, trouble is near.

The best advice on government social media comment moderation is always to get your legal staff involved, review your policy to see if any adjustments are needed in light of changing circumstances and avoid putting yourself in the situation of monitoring viewpoints. GT

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.



Simplified. Intuitive. Unified.

CGI Advantage®: ERP that works for me.

CGI Advantage is re-imagined with a mobile-first design that streamlines engagement and transforms your user experience. An ERP solution that delivers everything you need and nothing you don't — enabling digital insights through embedded analytics and backed by the scale, reach and delivery capabilities of a global IT champion.

cgi.com/advantage

CGI

Experience the commitment®

More first responders rely on Verizon.

Responder Private Core, part of Verizon's Response Solutions, is a dedicated lane for first responders on America's most reliable network. When you choose the network for first responders, your team is ready.
verizon.com/publicsafety

Are you ready?



verizon

Based on RootMetrics® by IHS Markit's RootScore® Reports 2H 2018 of 4 mobile networks. Results may vary. Not an endorsement.