

# GOVERNMENT TECHNOLOGY

SOLUTIONS FOR STATE AND LOCAL GOVERNMENT

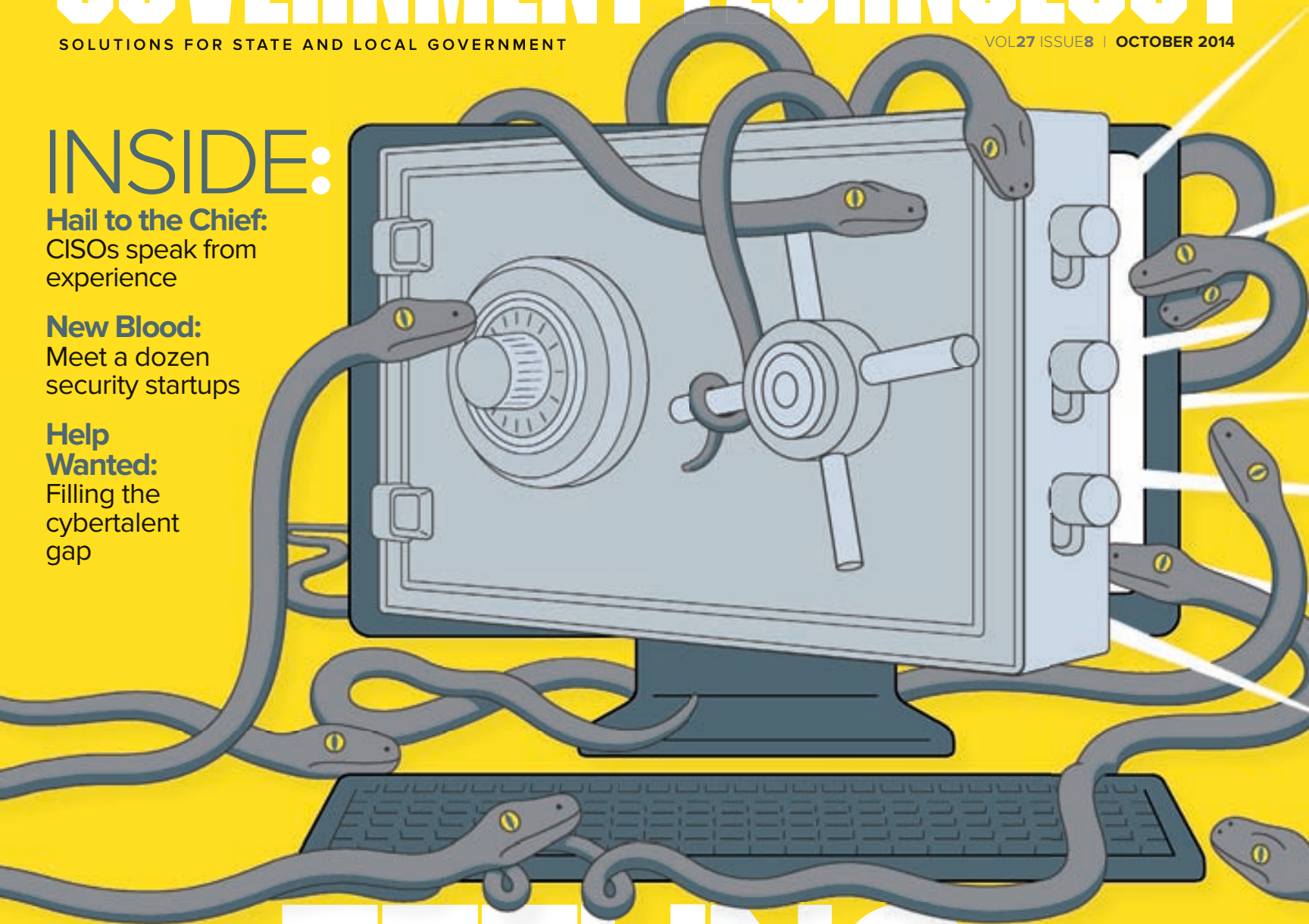
VOL27 ISSUE8 | OCTOBER 2014

## INSIDE:

**Hail to the Chief:**  
CISOs speak from experience

**New Blood:**  
Meet a dozen security startups

**Help Wanted:**  
Filling the cyber talent gap



# FEELING VULNERABLE?

CYBERATTACKERS AREN'T INVINCIBLE BUT  
YOU PROBABLY NEED TO RETHINK SECURITY.

# Dreaming of an easier, faster, safer customer payment experience?



First Data® has helped hundreds of government agencies reduce the risks associated with payment and information processing. We can do the same for you. Our experts will help you safeguard data, improve customer experience and reallocate resources ... all without increasing your overhead. That's why many of the nation's largest private companies turn to First Data.

Find out more about how solutions like TransArmor®, First Data's industry-leading payment card security, can help you reduce your overall risk.

William (Bill) Rogers, Vice President of Sales, Government Solutions

512.633.1118 • [william.rogers@firstdata.com](mailto:william.rogers@firstdata.com)



©2014 First Data Corporation. All rights reserved.



## COVER STORY

### 16 / Mission Impossible?

Cyberattackers aren't invincible but you probably need to rethink security.

**By Colin Wood**

COVER ART BY KLAUS MEINHARDT

### 22 / Can We Talk?

Federal framework aims to create a common language for security — and it's gaining support from security pros.

**By Brian Heaton**

### 28 / Security Leaders Sound Off

The role of chief security officer may look different in every organization — but in an increasingly connected and open society, it's more vital than ever.

**By David Rath**



TOLBERT PHOTO

### 34 / Help Wanted

The shortage of cybersecurity experts is well documented. So what are agencies doing to fill the gap?

**By Adam Stone**

### 40 / The Best Defense

The market is prime for a new class of startups that can decipher tomorrow's cybersecurity threats.

**By Jason Shueh**



SHUTTERSTOCK.COM

DAVID KIDD





Publisher: **Alan Cox**, [acox@govtech.com](mailto:acox@govtech.com)

## EDITORIAL

Editor: **Steve Towns**, [stowns@govtech.com](mailto:stowns@govtech.com)  
 Associate Editor: **Elaine Pittman**, [epittman@govtech.com](mailto:epittman@govtech.com)  
 Web Editor & Photographer: **Jessica Mulholland**, [jmulholland@govtech.com](mailto:jmulholland@govtech.com)  
 Managing Editor: **Noelle Knell**, [nknell@govtech.com](mailto:nknell@govtech.com)  
 Chief Copy Editor: **Miriam Jones**, [mjones@govtech.com](mailto:mjones@govtech.com)  
 Senior Editor: **Tod Newcombe**, [tnewcombe@govtech.com](mailto:tnewcombe@govtech.com)  
 Staff Writers: **Hilton Collins**, [hcollins@govtech.com](mailto:hcollins@govtech.com)  
**Jason Shueh**, [jshueh@govtech.com](mailto:jshueh@govtech.com)  
**Colin Wood**, [cwood@govtech.com](mailto:cwood@govtech.com)  
**Brian Heaton**, [bheaton@govtech.com](mailto:bheaton@govtech.com)  
 Senior Writer: **David Rath**, [drath@govtech.com](mailto:drath@govtech.com)  
 Contributing Writers: **David Rath**, [drath@govtech.com](mailto:drath@govtech.com)  
 Editorial Assistant: **Maggie Cabrey**, [mcabrey@govtech.com](mailto:mcabrey@govtech.com)

## DESIGN

Chief Design Officer: **Kelly Martinelli**, [kmartinelli@govtech.com](mailto:kmartinelli@govtech.com)  
 Senior Designer Pubs: **Heather Whisenhunt**, [hwhisenhunt@govtech.com](mailto:hwhisenhunt@govtech.com)  
 Senior Designer Custom: **Crystal Hopson**, [chopson@govtech.com](mailto:chopson@govtech.com)  
 Production Director: **Stephan Widmaier**, [swidm@govtech.com](mailto:swidm@govtech.com)  
 Production Manager: [production@govtech.com](mailto:production@govtech.com)

## PUBLISHING

### VPs OF STRATEGIC ACCOUNTS:

**Jon Fyffe**, [jfyffe@govtech.com](mailto:jfyffe@govtech.com)  
**Stacy Ward-Probst**, [sward@govtech.com](mailto:sward@govtech.com)  
**Noel Hollis Hegwood**, [nhollis@govtech.com](mailto:nhollis@govtech.com)  
**Arlene Boeger**, [aboeger@govtech.com](mailto:aboeger@govtech.com)  
**Shelley Ballard**, [sballard@govtech.com](mailto:sballard@govtech.com)  
**Liza Mendoza**, [lmendoza@govtech.com](mailto:lmendoza@govtech.com)

### SALES DIRECTORS:

**Melissa Sellers**, [msellers@govtech.com](mailto:msellers@govtech.com)  
**Tracy Meisler**, [tmeisler@govtech.com](mailto:tmeisler@govtech.com)  
**Mary Noel**, [mnoel@govtech.com](mailto:mnoel@govtech.com)  
**Stephanie George**, [sgeorge@govtech.com](mailto:sgeorge@govtech.com)  
**Alice Okali**, [aokali@govtech.com](mailto:aokali@govtech.com)

### ACCOUNT EXECUTIVES:

**Paul Dangberg**, [pauld@govtech.com](mailto:pauld@govtech.com)  
**Mari Carr**, [mcarr@govtech.com](mailto:mcarr@govtech.com)  
**Lara Roebbelen**, [lroebbelen@govtech.com](mailto:lroebbelen@govtech.com)  
**Rozaida O'Neill**, [ronell@govtech.com](mailto:ronell@govtech.com)

### ACCOUNT MANAGERS:

**Karen Hardison**, [khardison@govtech.com](mailto:khardison@govtech.com)  
**Ashley Whalen**, [awhalen@govtech.com](mailto:awhalen@govtech.com)  
**Carmen Mendoza**, [cmendoza@govtech.com](mailto:cmendoza@govtech.com)  
**Deanne Stupek**, [dstupek@govtech.com](mailto:dstupek@govtech.com)  
**Kelly Schieding**, [kschieding@govtech.com](mailto:kschieding@govtech.com)  
**Vonna Torres**, [vtorres@govtech.com](mailto:vtorres@govtech.com)  
**Lindsey Alberty**, [laberty@govtech.com](mailto:laberty@govtech.com)  
**Kelly Campbell**, [kcampbell@govtech.com](mailto:kcampbell@govtech.com)

### BUS. DEV. MANAGER:

**Maggie Ransier**, [mransier@govtech.com](mailto:mransier@govtech.com)

### SR. SALES ADMINISTRATOR:

**Christine Childs**, [cchilds@govtech.com](mailto:cchilds@govtech.com)

### SALES ADMINISTRATORS:

**Alexis Hart**, [ahart@govtech.com](mailto:ahart@govtech.com)  
**Valerie Gallup**, [vgallup@govtech.com](mailto:vgallup@govtech.com)  
**Colleen Espinoza**, [cespinoza@govtech.com](mailto:cespinoza@govtech.com)  
**Kelly Kashuba**, [kkashuba@govtech.com](mailto:kkashuba@govtech.com)  
**Sharon Mooningham**, [smooningham@govtech.com](mailto:smooningham@govtech.com)  
**Alicia Scott**, [ascott@govtech.com](mailto:ascott@govtech.com)

Sr. Dir. of Sales Operations: **Andrea Kleinbardt**, [akleinbardt@govtech.com](mailto:akleinbardt@govtech.com)

Sr. Dir. of Cust. Events: **Whitney Sweet**, [wsweet@govtech.com](mailto:wsweet@govtech.com)

Dir. Custom Media: **Rebecca Johnson**, [rjohnson@govtech.com](mailto:rjohnson@govtech.com)

Dir. of Web Marketing: **Zach Presnall**, [zpresnall@govtech.com](mailto:zpresnall@govtech.com)

Web Advertising Mgr: **Adam Fowler**, [afowler@govtech.com](mailto:afowler@govtech.com)

Subscription Coord.: **Ennie Yang**, [subscriptions@govtech.com](mailto:subscriptions@govtech.com)

## CORPORATE

CEO: **Dennis McKenna**, [dmckenna@govtech.com](mailto:dmckenna@govtech.com)  
 Executive VP: **Cathilea Robinett**, [crobinett@govtech.com](mailto:crobinett@govtech.com)  
 Senior VP of Sales: **Kim Frame**, [kframe@govtech.com](mailto:kframe@govtech.com)  
 CAO: **Lisa Bernard**, [lbernard@govtech.com](mailto:lbernard@govtech.com)  
 CFO: **Paul Harney**, [pharney@govtech.com](mailto:pharney@govtech.com)  
 Senior VP: **Alan Cox**, [acox@govtech.com](mailto:acox@govtech.com)  
 Chief Marketing Officer: **Margaret Mohr**, [mmohr@govtech.com](mailto:mmohr@govtech.com)  
 Chief Content Officer: **Paul Taylor**, [ptaylor@govtech.com](mailto:ptaylor@govtech.com)

*Government Technology* is published by e.Republic Inc. Copyright 2014 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](mailto: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](http://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

## DEPARTMENT

### 46 / Wages of Fear

Ransomware, once a small-time malware problem, has exploded in use, affecting state and local governments. And the extortion software is becoming more sophisticated.

## COLUMNS

### 6 Point of View

Cybersecurity hits the boardroom

### 12 Becoming Data Smart

How social media listening can improve public health.

### 14 Four Questions

Brian Engle, chief information security officer, Texas

## NEWS

### 8 govtech.com/extra

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

### 10 Big Picture

Locking down cyberspace

### 50 Spectrum

More research, more science, more technology.



FOLLOW  
 US ON



## IN OUR NEXT ISSUE:

### Breaking In

Entrepreneurs describe their struggles to enter the government technology market.

### E-Government Revisited

Experts weigh in: Have early visions for online service delivery been realized?

### Raising Innovation

There are many different ways to incubate tech startups. We look at five models.

WWW.GOVTECH.COM





## Global Network Operations Center



When managing security in an all-IP network,  
it helps to see the big picture.

AT&T security experts analyze more than 310 billion flow records each day for anomalies that indicate malicious activity. It's what makes us uniquely qualified to help state and local government agencies address the security challenges they face. Our proactive network-based approach to managed security delivers some of today's most powerful weapons to combat cyber security attacks – helping to safeguard all the elements of your IP infrastructure. To learn more, download the CIO Security Guide at [att.com/govsecurity](http://att.com/govsecurity)







# Cybersecurity Hits the Boardroom

**W**hen we asked state IT professionals to rank their priorities for the next two years, one issue stood far above the rest: cybersecurity.

Given the seemingly endless parade of high-profile attacks, their concerns are understandable. This year began, of course, with Target reeling from the news that attackers had stolen credit card information for some 40 million of the retailer's customers. As this issue of *Government Technology* went to press, Home Depot was investigating what could be an even bigger theft of its customers' credit and debit card data, and Apple was struggling to explain the unauthorized release of celebrity photos from its iCloud service.

Events like these can cost CIOs and CISOs their jobs, so it's little wonder they're paying attention. Sixty-five percent of respondents in our 2014 Digital States Survey put cybersecurity among their top three priorities. Cloud computing was a distant runner-up at 28 percent.

But while technology officials have worried about security breaches for years — cybersecurity was a top concern in our 2012 Digital States Survey, too — the issue hasn't been on the radar of top management. Instead, cybersecurity was viewed as a problem for the technology guys to fix, not a risk for leadership to address.

That's changing now as more and more of us become victims of data theft. A recent report from CNNMoney estimates that nearly half of all adults in the U.S. have had personal information stolen by hackers in the last 12 months, and it's reasonable to think that many of them are asking why top execs aren't taking better care of their data.

The Target breach didn't just cost CIO Beth Jacob her job. Company CEO Gregg Steinhafel resigned in May as the retailer struggled to regain the trust of shoppers. The event sounded a warning that repercussions from identity theft can ripple all the way up to the boardroom. Cybersecurity is getting more attention from state and local political leaders too. Late last year, the National Governors Association released a call to action urging governors to take steps to prevent cyberattacks.

Elevating the stature of cybersecurity is good news for CIOs and CISOs, who are now getting more resources and better executive backing for data protection initiatives. It also puts pressure on technology and security professionals to develop better and more sophisticated responses to cyberchallenges — and that's good news for all of us. **GT**

## RAISE YOUR VOICE

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

AN AWARD-WINNING PUBLICATION



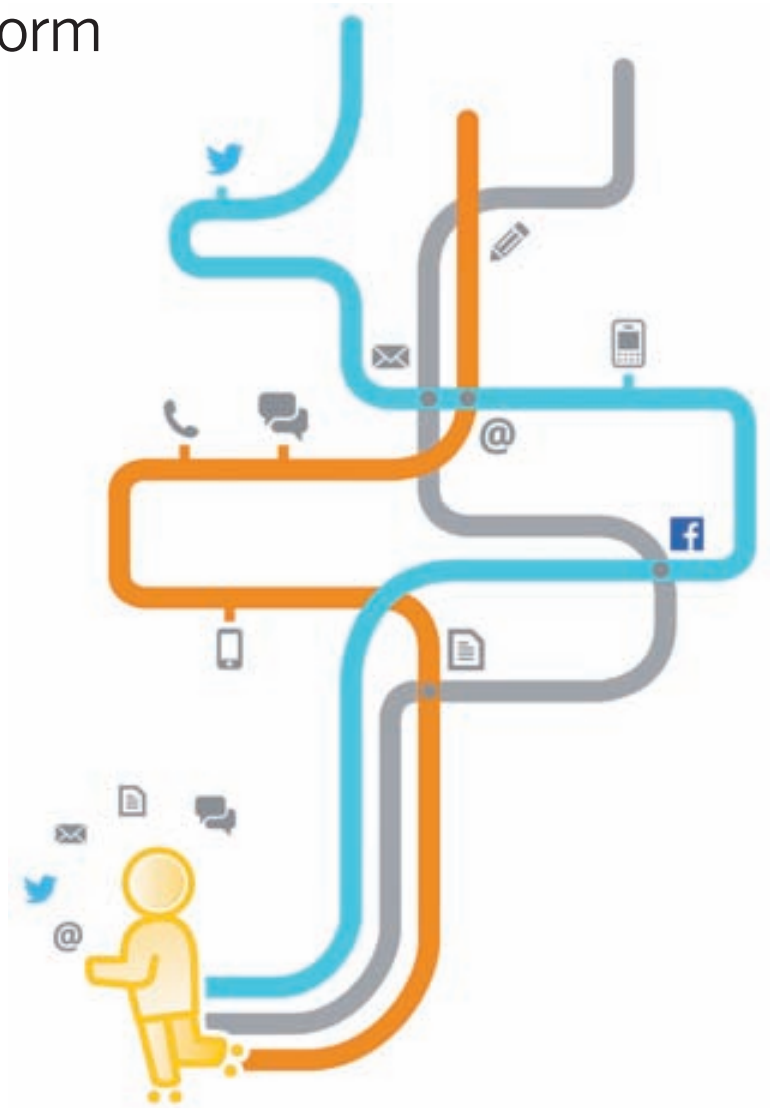


**TAME CONTENT. HARVEST INSIGHT.  
ACHIEVE INTELLIGENCE**



## **Kodak** Info Insight Platform

- Handles all your input channels with a single platform process
- Save time, money and resources by automating your business processes
- Integrates seamlessly with existing systems and databases
- Improves quality and consistency of your customer interactions



**Kodak alaris**

Learn more at: [kodakalaris.com/go/infoinsight](http://kodakalaris.com/go/infoinsight)

©2014 Kodak Alaris Inc. The Kodak trademark and trade dress are used under license from Eastman Kodak Company.

## Buckle Up

Can crowdsourced traffic data help a city re-time its traffic lights on the fly? Austin hopes so, approving a plan that will use the data to improve traffic flow by reducing bottlenecks on a minute-by-minute basis, especially following major events. The technology will track how fast motorists are going, how many motorists are in a certain location and which directions they're traveling. According to Austin's deputy CIO, Teri Pennington, the core system is in place. "Currently we are working on the connectivity, as well as how the mobile apps will communicate securely into the core system," she said.

## WHO SAYS?

*"The new face of the CIO in every industry is not someone who understands everything about technology, although that's useful. It's about being a leader, being a part of the business, trying to get people to try new things."*

[www.govtech.com/quote-oct14](http://www.govtech.com/quote-oct14)

### MOST SHARED STORIES

Which States Have the Best Technology?

**751**  
SHARES

Los Angeles Undertakes Massive Website Relaunch with Drupal

**565**  
SHARES

How the Sharing Economy is Strengthening Emergency Response and Recovery

**381**  
SHARES



## Procurement Power

Purchasing groups exist to negotiate competitive rates and help public-sector organizations buy everything from auto parts to notepads. But when it comes to procuring IT products, Oklahoma and Texas may have found a winning formula. Oklahoma's statewide Information Services Division and the Texas Department of Information Resources have partnered in a multistate procurement cooperative for technology equipment and services. The one-year pilot specifies that Texas will be Oklahoma's "preferred source" for buying tech items. The contract was signed in June and can be extended in perpetuity if both parties agree.

## MOST READ STORIES ONLINE

Which States Have the Best Technology?  
**5,914 VIEWS**

How Anonymous Hackers Changed Ferguson, Mo., Protests  
**4,615 VIEWS**

Hard-Won Experience: Lessons from America's Biggest Disasters and Emergencies  
**2,786 VIEWS**

Data Breaches in the Cloud: Who's Responsible?  
**2,230 VIEWS**

How the Cloud is Changing Everything for Govt. IT  
**2,137 VIEWS**

Los Angeles Undertakes Massive Website Relaunch with Drupal  
**1,953 VIEWS**

# 10

The number of seconds before the Aug. 24 **earthquake** in Napa Valley, Calif., that researchers received an alert about the event via the ShakeAlert early detection and warning system.

## reader/comments:

“People forget that most of the big innovations of the last 100 years came from government-funded innovation. The Internet? DARPA and ARPANET. Jet airplanes? Air Force-funded research and development. To name but a few. Government has always led the way with major innovations, either by doing or by funding the doing where no private-sector player would ever have done it because there wasn't a viable business model in it.

**joelracicot** in response to *The Big Leagues: Government Must Reclaim its Role as a Driver in the Innovation Economy*

“The question of the business case for open data should definitely be asked because you are going to be diverting some level of resources to set it up and management that could be used elsewhere. However, I don't think you have to look far/hard to find an ROI, and in fact I believe open data has provided the best ROI I've ever seen on a technology project.

**rob\_giggey** in response to *Can Open Data Find a Business Model?*

“Transparency is a huge administrative and financial cost that is not built into the cost of private business. I, too, have seen a disconnect between administrative agencies and legislatures in terms of appreciation of this burden that makes it hard to reform or tailor transparency procedure. Any attempt by an agency to call for a change in the procedure is seen as an attempt to hide something.

**Gabriel Epstein** in response to *Government Procurement Protests: There Are No Winners*

“It's no surprise that so few are interested in this program. The vetting process, the cost and the technical talent needed puts this out of reach of most local government IT shops.

**Andy** in response to *DHS Cybersecurity Program Finds Few Takers*



# Freedom of Information/Public Records Request

**Part I:** I hereby request to: ☒ Inspect ☐ Copy the following records:  
(please be specific and include names, dates, keywords, and name of record type where possible).

Please provide all Everton City and Police Department social  
networking content from May of 2012 regarding special notices  
and street closures related to the Everton Memorial Day parade

**Part II:** What format do you request? ☒ Electronic ☐ Paper

**Part III:** Name of individual(s) requesting information: John A. Reizer

Address: 1076 Freedom Way City: Everton State: TX Zip: 72996

Phone: (210) 867-5309 Email: jpublic1@gmail.com



## For Internal Office Use Only

Date Request Received: July 1, 2014 Request Status: Pending

**Notes:** Staff has invested more than ten hours scrolling through social media pages and collecting stored screenshots from department hard drives. Citizen comments no longer available, City Attorney issued subpoena to social network - response still pending after four weeks.

# HOW WILL YOU RESPOND?

ArchiveSocial automates the capture and retrieval of records from social networks including Facebook, Twitter, YouTube, Instagram, and LinkedIn for compliance with state and federal public records laws.

<http://archivesocial.com/respond>



## Locking Down Cyberspace

The National Guard is uniquely positioned to take on the ever-growing challenge of cybersecurity, since it is the only branch of the military at the service of both the president and the nation's governors.

Brig. Gen. Michael Stone (standing) of the Michigan National Guard, works with members of the guard's 110th Communications Flight, 110th Airlift Wing in Battle Creek, Mich. The facility serves as the hub of the Michigan Cyber Range, which offers educational courses and exercises aimed at strengthening public- and private-sector cyberdefenses.







# The New Urban Noise

Citizen-generated data obtained by social media listening is becoming a valuable public health tool.

Cities are notoriously noisy: The more people, activities and events condensed in a given space, the louder it is. Today, people are sharing everyday experiences at an enormous scale, and their pictures, videos, geotagged posts and check-ins create a new kind of urban noise. A new image of the city emerges from this collection of citizen-generated data and presents an opportunity to better understand urban activity. But in order to distill meaningful insights from all the noise, you need a good listener. Some government officials are beginning to catch on.

Diners who suffer food poisoning rarely report it through official channels, even though foodborne illness is a public health concern. However, sick, unhappy customers have incentive to vent their complaints on Yelp, a popular app and website for local business reviews. New York City's Department of Health and Mental Hygiene recently completed a pilot project in partnership with the company aimed at identifying unreported outbreaks of foodborne illness. Working with software developers at Columbia University, city researchers converted nearly nine months of Yelp reviews into machine-readable data. They were then able to pinpoint potentially hazardous establishments by reviews that included


terms such as "sick," "vomit" or "food poisoning." Scanning 294,000 restaurant reviews in New York, the software flagged three restaurants that together produced 16 documented illnesses. When health inspectors subsequently visited these establishments, they discovered astonishing health code violations: improperly sanitized surfaces and bare-hand contact with ready-to-eat food at the first two, and live roaches and evidence of mice at the third.

Food poisoning is not the only public health issue that goes severely under-reported. In order to report the side effects of prescription drugs, patients must fill out and submit a lengthy four-page form. The FDA, in partnership with Boston University and Harvard Medical School, analyzed 6.9 million Twitter posts generated over the course of seven months. In a *Drug Safety* paper published this April, researchers identified 4,401 tweets that described side effects worth reporting to the FDA. In fact, the complaints about gastrointestinal problems and psychiatric effects mirrored the FDA's independent data sets on such conditions.

Aware of this critical hole in its current database, the FDA helped fund the launch of Epidemico, a health data collection and analytics startup. The company then developed MedWatcher, an app that allows people to access and easily navigate the FDA's database, which is integrated with data from thousands of other sources, for information on drug side effects. It also provides an

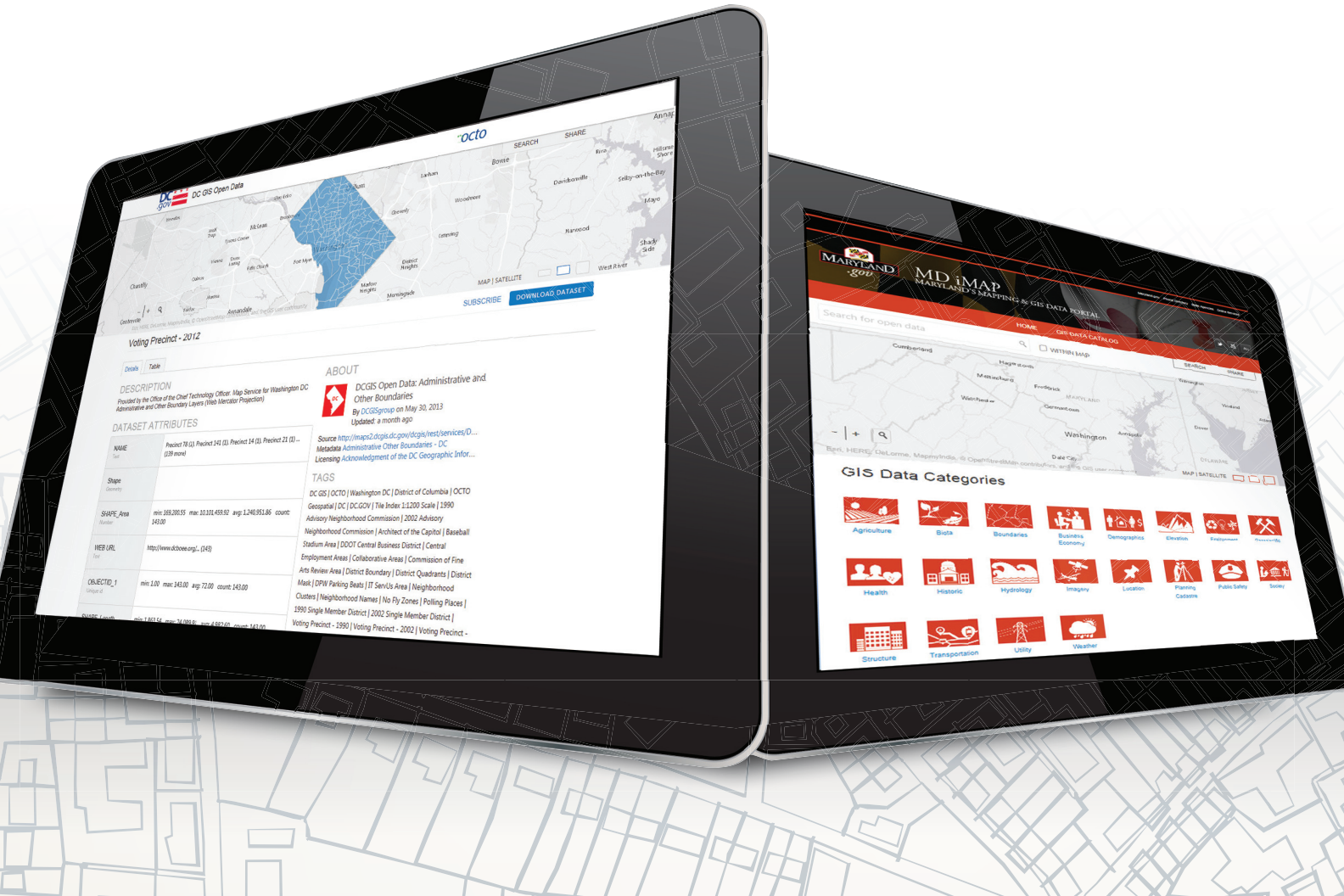
accessible avenue for patients to relay their experiences with drugs back to the FDA.

These examples illustrate two important points. The first is that urban airwaves are becoming increasingly proliferated with actionable public health data. According to a 2013 report from Pew Research Center's Internet and American Life Project, city dwellers are 50 percent likelier to use Twitter than their rural and suburban peers, and increasingly geotagged social media, in the face of the rising importance of "where" in government, marks the future of hyper-local data aggregation tools. The second point is that in each example, a government agency partnered with a research university and private company. The imperative for government action to be based on data-smart strategies is gaining ground. Companies, universities and nonprofits offer a trove of data and analytical methods that government cannot afford to ignore.

Yelp and Twitter offer users intuitive social interfaces that are easy to use. They generate data because people enjoy using them. Public agencies have begun to listen in, but as cities become increasingly responsive, such third-party mediation should become unnecessary. Existing channels for communicating with the government — whether about drug side effects, food poisoning or anything else — must be improved so that instead of just listening, they can be responding in real time. 

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





# Unlocking Open Data for the Public



## Bringing Data to Life

Take a look at a city calendar and you're likely to find words that didn't exist in the government lexicon a few years ago. "Hackathons," "datapaloozas" and even "code-a-paloozas" are popping up across the country as local government and states use the collective power of the public to create better government services.

But hackathons are only one component of a much bigger trend marked by transparency and government efforts to better communicate and collaborate with citizens: open data. Open data is powerful, allowing states and municipalities to share a wealth of information on the Web, and enabling citizens and government agencies to share a

common picture of intelligence that drives decisions across the nation.

For decades, government agencies have relied on Esri to support mission-critical tasks and daily operations. Now, after supporting the open exchange of geospatial data, geospatial analysis, data models, and workflows for many years, Esri launched a new open



"The site gives us the ability to search and discover data, to explore that data interactively right within the Web page, and download that data in multiple formats. Users can also build solutions off of live data feeds."

Tim Abdella, Geographic Information Officer, Washington, D.C.

## One Site, One Source: Washington, D.C., Simplifies Open Data

Washington, D.C., has been a front runner in data dissemination — its Data.dc.gov site was one of the first open data catalogs in the United States and predated even the federal government's Data.gov.

However, in the past, the city had several different websites dedicated to open data but lacked one site that included a robust search capability and the ability for users to explore information spatially.

"This was our challenge," says Geographic Information Officer Tim Abdella. "We had all of these different avenues to find data, but did not have a singular point of view that made sense for the GIS consumer."

Now the city is moving forward with the perfect fit — an open data site leveraging ArcGIS Open Data — which will wrap around the city's existing infrastructure and allow it to expose its data to the public in a simple and intuitive way.

"The site gives us the ability to search and discover data, to explore that data interactively right within the Web page, and download that data in multiple formats. Users can also build solutions off of live data feeds," says Abdella.

Importantly, the ArcGIS Open Data platform also allows the city to keep the data where it already resides — which is a critical sticking point for Abdella. "I am a big advocate of storing data one time, in one place,

and then exposing that data," he says. "The issue with loading data in multiple places is maintaining the data. If I only have one place where the data is loaded, I only have one place to maintain the data."

Abdella says the beauty of ArcGIS Open Data is that it leverages a central repository of content. "Every time I make a change, it's automatically cascaded as a change in the open data site. It's brilliant and simple."



data initiative, ArcGIS Open Data, which is an addition to ArcGIS Online.

ArcGIS Open Data leverages an organization's GIS investment, enabling agencies to simply and efficiently deliver their data in an easy-to-consume format. More than that, it provides a way for the thousands of governments that already use Esri to quickly and seamlessly deploy open data sites. This tool allows its users to create a custom website that helps citizens find data and view it in a spatial context.

## Opening Data with the Power of the Platform

As with any emerging practice, there have been limitations with open data.

Today, government agencies and constituents are increasingly realizing the benefits that can come from highly organized, simple-to-access open

data. Governments create a significant amount of map and spatial data that could be put to good use.

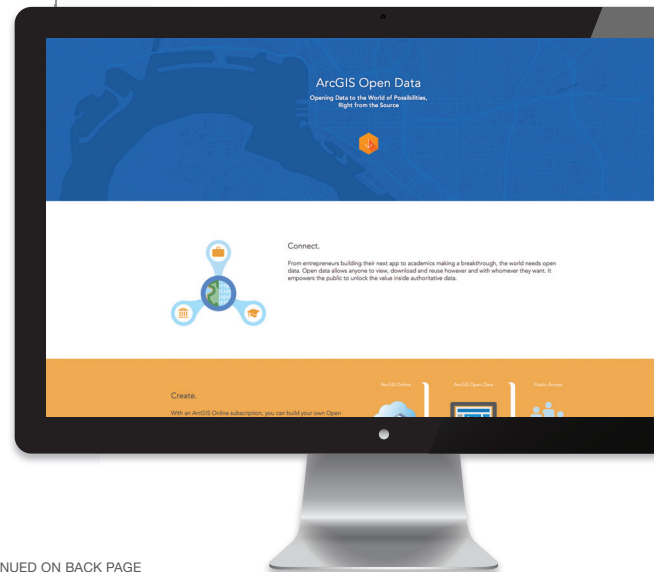
For the thousands of governments that already use ArcGIS Online, ArcGIS Open Data is part of their online account — allowing these agencies to leverage their investment in Esri's ArcGIS platform. This open data capability, combined with Esri's smart community solutions to governments, ArcGIS for Local Government and ArcGIS for State Government, provides a powerful foundation for government agencies to not only easily expose data to the public in an accessible, user-friendly format, but to share data across government agencies and jurisdictions to enable better communication and collaboration.

## An Open Data Strategy That Just Works

ArcGIS Open Data provides the piece of the puzzle that was

### ArcGIS Open Data

leverages an organization's GIS investment, enabling agencies to simply and efficiently deliver their data in an easy-to-consume format.  
<https://opendata.arcgis.com>



• CONTINUED ON BACK PAGE

## Coding with Open Data in Charlotte

Charlotte, N.C., relies heavily on Esri's ArcGIS platform to manage the city's daily public service activities.

"We could not run the city to the degree that we do without Esri's GIS technology," says Twyla McDermott, Charlotte's corporate IT program manager. "It's used for everything from predictive crime analysis to recycling pickups. It helps us determine eligible services by geography and manage our water and wastewater systems. We just couldn't do it without the software that models the real world from our office."

Charlotte also has a vibrant civic tech community that the city encourages and embraces. In order to make innovation thrive in Charlotte, the city's data needed to be more readily available and work with the technology infrastructure the city uses in the back office.

In order to better serve the civic tech community and promote government innovation, Charlotte created an open data site through ArcGIS Open Data so it can ensure the community is receiving the most current data the city produces.

This site has been a beneficial addition to the community as Charlotte is a 2014 host city for the Code for America Fellowship program. The Code for America Fellows are using the ArcGIS Open Data Portal to source data as they build an app for the city, called Citygram. In its initial implementation as a demonstration project for the Open Data Portal, the application will help citizens stay up to date on city activities (land development, street closures, reported traffic accidents, etc.). This app relies heavily on the City of Charlotte's ArcGIS Open Data portal as it pulls information from

systems of record and makes it easy for residents to understand the information. Citizens also have the option to go to the open data site itself and search for information.

The Charlotte civic tech community has shown they are excited about the city's open data site. "In February, Esri set up an open data portal to expose what was possible to the community," says McDermott. "It was the first time as a government employee that I ever received applause for anything we have produced. This positive and enthusiastic response was astounding to me."

# Powering Performance with Open Data in Maryland

Due to its popular StateStat website implemented by Gov. Martin O'Malley, Maryland has become synonymous with performance management and efforts to increase transparency and openness in government.

In 2014, O'Malley signed into law an Open Data Act. The new law combines the state's GIS capabilities with its open data initiatives and

open data and GIS are now managed as two closely parallel efforts.

To maximize geospatial collaboration, the state is leveraging ArcGIS Open Data for its mapping and GIS portal, MD iMap ([data.imap.maryland.gov](http://data.imap.maryland.gov)), which will increase search capabilities, make data available for download, and expose more application programming interfaces (APIs) for developers.

The state's open data site ([data.maryland.gov](http://data.maryland.gov)) provides similar capabilities for alphanumeric data.

For Maryland, making data available for download is paramount. "It's very important that people are able to access the raw data," says Barney Krucoff, Maryland's geographic information officer. "For a significant number of citizens, the power is in going to see the data themselves."

However, the state's open data components extend beyond the MD iMap site. "Our GIS capabilities allow us to provide a user interface that is embedded in our websites. Users may be exposed to the open data from a state government website and not necessarily realize all that is going on in the background," says Krucoff.

• CONTINUED FROM PREVIOUS PAGE

previously missing from open data efforts, allowing government agencies to communicate complex data in easy-to-understand geographic, tabular and chart formats. In doing so, they are better engaging with citizens, increasing transparency and improving accountability.

As Charlotte's Corporate IT Program Manager Twyla McDermott said, "I think this changes the conversation because data will be so readily available in map tabular forms and as visualizations that we will have a more empowered citizenry."

It's an open data strategy that just works.

## California Dreamin': Endless Possibilities on the West Coast

Washington, D.C., Charlotte, and Maryland aren't the only governments opening data. These counties are also maximizing open data's potential with ArcGIS Open Data:

- In June 2014, Riverside County, Calif., was the latest municipality to combine the power of the public with open APIs, hosting its first hackathon (aka RivCodes). The county took advantage of its open data site, powered by ArcGIS Open Data, to connect innovative software developers, designers, and other techies to open information and empower them to create simple solutions to common municipal problems.
- In San Bernardino, Calif., the county Public Works Department is leveraging open data to enable constituent self-service. The county has lowered costs by simply and efficiently providing information to citizens, alleviating the amount of requests for county employees to provide this data.

**Interested in how your agency can use open data more effectively?**

**Try ArcGIS Open Data for yourself at [esri.com/GTopenData](http://esri.com/GTopenData) and sign up for your 30-day trial of ArcGIS Online.**

**With a subscription to ArcGIS Online you will have the ability to build your own open data site, allowing the public to explore your data through interactive maps and charts that they can search and download.**

Sponsored by:



Part #141654



# GOING THROUGH PROCUREMENT PAINS?

The Center for  
Digital Government  
is pleased to present its  
**Best Practice Guide for  
Cloud and As-A-Service  
Procurements.**

Developed with input from state and local government leaders, as well as industry experts, the guide is intended to be a go-to resource for government leaders as they take advantage of modern technologies and create more flexible and agile procurement processes.

The guide includes Model Terms and Conditions for SaaS, PaaS and IaaS contracts as well as lessons learned from past cloud and XaaS contracts.



Procurement doesn't have to be painful.  
**Download the guide at [govtech.com/procurement](http://govtech.com/procurement).**

## Brian Engle

CISO, Texas

*Brian Engle became chief information security officer of Texas last year, after serving as CISO for the state's Health and Human Services Commission. He spoke with Government Technology about how the cloud and the Internet of Things are impacting cybersecurity.*

**1 How does the cloud change cybersecurity?** When organizations say they're "going to the cloud," that oversimplifies it. You start to see business processes happening in a lot of different places. An organization may have applications running in Salesforce. It may have an outsourced HR solution somewhere else in the cloud, and it may have an ERP solution somewhere else. So it's not adding one thing; it's adding numerous things into the equation.

How do I detect an attack across this very diverse set of environments — I see that as our next challenge. Most of our work around event monitoring and response addresses things inside the data center. Now we need to correlate things that happen in outside environments run by cloud

providers that aren't necessarily going to send raw data to us.

**2 So you need a different tool set?** A different tool set and perhaps someone who has a different observation perspective — the catbird seat — to see all of these things isn't necessarily within our organization. Bits and pieces of this are available, and they're starting to come together. But the rate of maturity for many things in security is a bit slow, and I just don't think they'll spring up ready to go. They'll need to go through a continuum of maturity, and that means growth pains for us.

**3 As the Internet of Things emerges, how does that impact your thinking?** It's another complexity, but I'm not sure

that it dramatically changes the threat landscape, except for the fact that we need to make sure that we're considering it and we may have overlooked it in the past. In this world of scarcity, we've focused on what we consider the most important items — critical business systems, etc. But the fact that those don't operate in isolation means we need to broaden our perspective.

Other types of devices have been connected by the Internet for a while — everything from controllers in critical infrastructure to road devices used by the highway department. Now the types of connected devices are potentially anything. Yet we continue to design these devices as we did in the past. We expect that something upstream

is in charge of protecting them, and that's not always the case.

**4 With all of the attention on cybersecurity now, is this a good time to be a CISO?** It's an awesome time to be a CISO, but you really need to be ready. There are a lot of people looking for answers now. A lot of the things that we normally do have been under the radar. But when things go wrong — and a number of things have hit the news — questions are being asked, and we've got to be able to answer them for executives and board members. Those answers don't come with speculation. They need to come with facts. People who can answer those questions and have those conversations will be in high demand.

— **Steve Towns**, Editor



# Accepting Nominations for the Innovation Award

for outstanding achievement in technology project innovation



PRESENTED BY



**IJIS Institute**

**EMERGENCY**  
MANAGEMENT

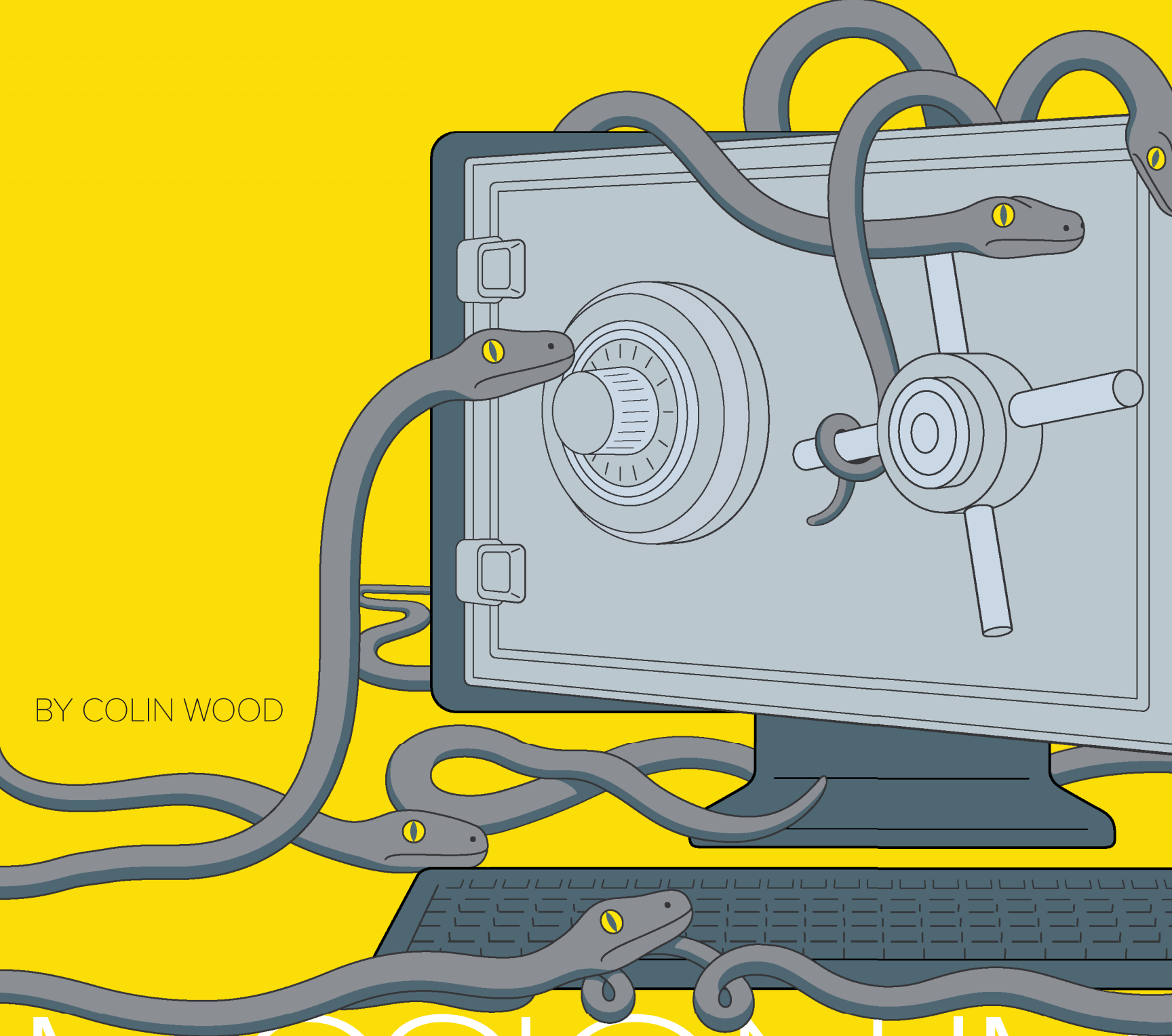
The IJIS Institute Innovation Award honors team achievement in information technology that contributes to the advancement of integration and interoperability for justice, public safety, or homeland security projects.

Nominations are open to successful partnerships between industry and federal, state, local, territory or tribal agencies.

**Award nominations due  
by November 5, 2014.**

For more information, visit the  
IJIS Institute web site at:

[www.ijis.org/\\_about/awards.html#innovation.](http://www.ijis.org/_about/awards.html#innovation)

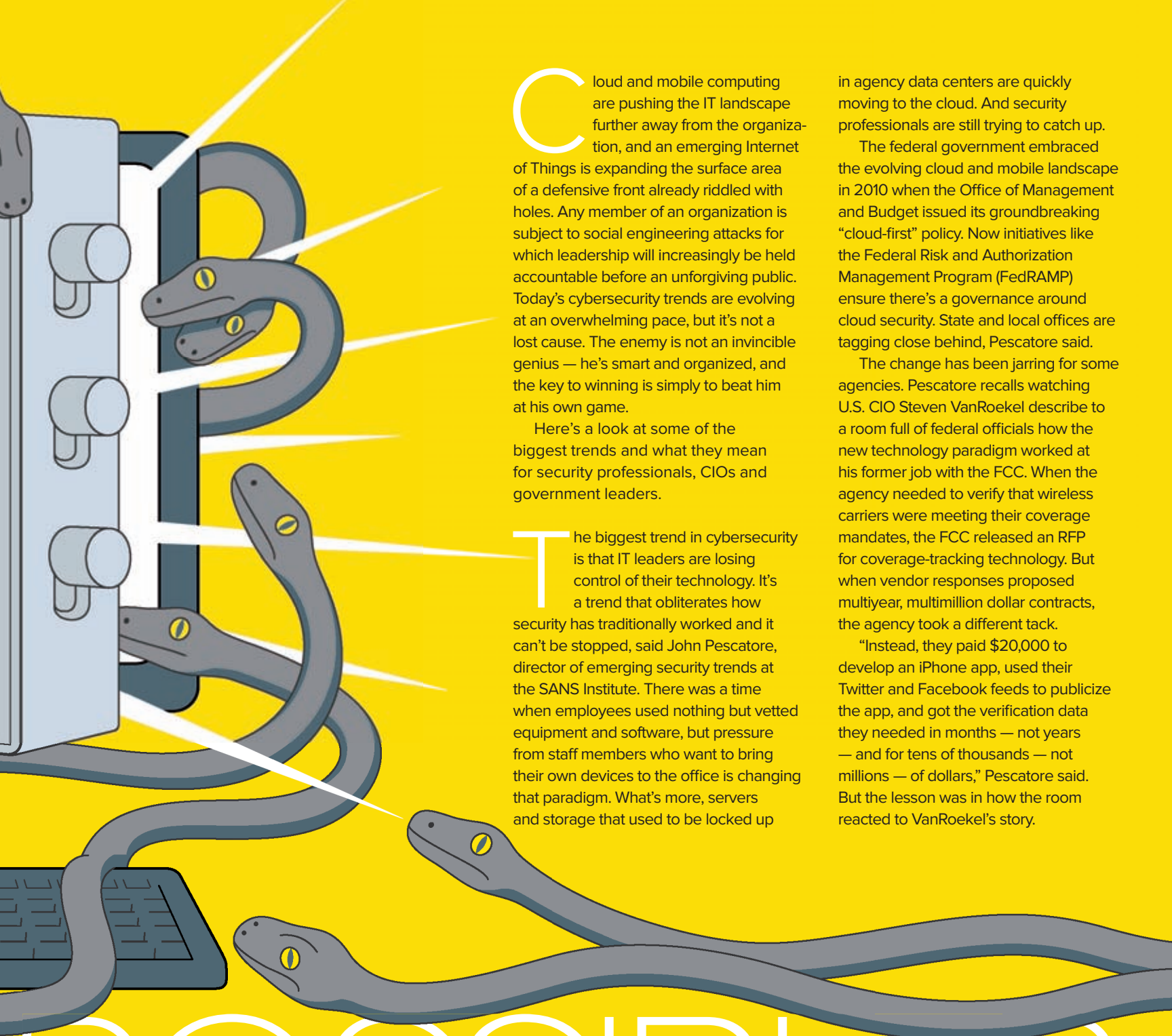


BY COLIN WOOD

# MISSION IM

CYBERATTACKERS AREN'T INVINCIBLE BUT





Cloud and mobile computing are pushing the IT landscape further away from the organization, and an emerging Internet of Things is expanding the surface area of a defensive front already riddled with holes. Any member of an organization is subject to social engineering attacks for which leadership will increasingly be held accountable before an unforgiving public. Today's cybersecurity trends are evolving at an overwhelming pace, but it's not a lost cause. The enemy is not an invincible genius — he's smart and organized, and the key to winning is simply to beat him at his own game.

Here's a look at some of the biggest trends and what they mean for security professionals, CIOs and government leaders.

The biggest trend in cybersecurity is that IT leaders are losing control of their technology. It's a trend that obliterates how security has traditionally worked and it can't be stopped, said John Pescatore, director of emerging security trends at the SANS Institute. There was a time when employees used nothing but vetted equipment and software, but pressure from staff members who want to bring their own devices to the office is changing that paradigm. What's more, servers and storage that used to be locked up

in agency data centers are quickly moving to the cloud. And security professionals are still trying to catch up.

The federal government embraced the evolving cloud and mobile landscape in 2010 when the Office of Management and Budget issued its groundbreaking "cloud-first" policy. Now initiatives like the Federal Risk and Authorization Management Program (FedRAMP) ensure there's a governance around cloud security. State and local offices are tagging close behind, Pescatore said.

The change has been jarring for some agencies. Pescatore recalls watching U.S. CIO Steven VanRoekel describe to a room full of federal officials how the new technology paradigm worked at his former job with the FCC. When the agency needed to verify that wireless carriers were meeting their coverage mandates, the FCC released an RFP for coverage-tracking technology. But when vendor responses proposed multiyear, multimillion dollar contracts, the agency took a different tack.

"Instead, they paid \$20,000 to develop an iPhone app, used their Twitter and Facebook feeds to publicize the app, and got the verification data they needed in months — not years — and for tens of thousands — not millions — of dollars," Pescatore said. But the lesson was in how the room reacted to VanRoekel's story.

# POSSIBLE?

KLAUS MEINHARDT

## YOU PROBABLY NEED TO RETHINK SECURITY.



## SECURITY MISCONCEPTIONS

**Oversimplification:** “You’ll hear people say, ‘Security is really a \*blank\* problem,’ like, ‘it’s really a people problem.’ Well, so are gambling and alcoholism and so is crime. If you could just get people to stop committing crime, there would be no crime,” said John Pescatore of the SANS Institute. “Nobody ever says, ‘When will bank robberies be over?’” The best people can hope to do is eliminate vulnerabilities, he said. “If people lock their car doors, car theft goes down.”

**Attackers are invincible:** McAfee’s Scott Montgomery said news coverage — and some industry advertising — dwells on data breaches instead of security successes, creating a false portrayal of the enemy. “Our adversaries and criminals are not omnipotent,” he said. “They don’t have more resources than we do. They aren’t evil geniuses. They’re very, very careful project managers. They manage their projects the same way we do. It’s not like they went to different Ph.D. programs than everybody else. Their responsibilities are easier, therefore they’re able to generate more success.”

**Misunderstanding defense in depth:** “Many times organizations are using technologies that all use the same defensive approach. So for example, maybe you’ve got a firewall, you’ve got an IDS [intrusion detection system] and you’ve got anti-virus. All three of those use the same fundamental principles to do their job: static rules for policy or detection. It’s just that one’s on the edge, one’s in the middle and one’s on the endpoint,” said FireEye’s Dave Merkel. “Well, that’s not actually defense in depth because an attacker is going to use the effort and same technique to bypass all three of those so you don’t really get any additive defensive capability in terms of seeing an attack you otherwise might miss.”

Real defense in depth counts a firewall, IDS and anti-virus as one layer, and then adds a behavioral layer and maybe a data analytics layer, he said. “In each layer in that architecture, we’re using a fundamentally different approach, so the attacker has to use fundamentally different methods to not be detected by them and he has to use three different methods.”

“On one side of the room you had agencies like Census Bureau, Agriculture and many others that were cheering because of the potential for cost reductions and more agility,” he explained. “On the other side, you had the DISAs [Defense Information Systems Agency] and intelligence agencies aghast that such a lightweight, uncontrolled process was used. It was nearly identical to 20 years ago when the Internet first hit business.”

Like the Internet before them, cloud and mobility are genies that aren’t going back in the bottle — the business value is simply too compelling. And user attachment to mobile gadgets will drive growing acceptance of bring your own device policies.

But the new environment reshuffles the deck for security professionals — shifting the focus from prevention to response. Now organizations need plans and technologies that let them rapidly detect and react to threats that the vast IT landscape has made nearly impossible to stop. In February, Gartner analysts Neil MacDonald and Peter Firstbrook published a paper contending that by 2020, 60 percent of enterprise information security budgets will be allocated toward rapid detection and response approaches to cybersecurity. In 2014, that figure is less than 10 percent.

“The problem with most security technology today is that it assumes it’s going to win,” Firstbrook said. “It doesn’t tell you what it doesn’t know, and it assumes it’s always right. And in every major breach that we’ve seen, that’s obviously not been the case.”

Verizon’s 2014 Data Breach Investigations Report shows that it usually takes weeks for an organization to discover a breach, and increasingly, it’s a third party or law enforcement agency that informs the organization that a breach occurred. In many well publicized breaches — like the one in South Carolina’s Department of Revenue in 2012 or Target’s breach last year — detection took much longer than it would have with a more comprehensive cyberstrategy. The flaw of today’s security technologies often is mirrored in the mindsets of security professionals — most organizations have no plan B, Firstbrook said.



**As more devices and infrastructure connect to the Internet, their associated cybervulnerabilities aren’t always thought through by manufacturers.**

Predicting and detecting attacks means shifting an organization’s security mindset from one of what Firstbrook calls “incident response,” to one of “continuous response.” The way that’s accomplished, he said, is by developing a security architecture that integrates prediction, prevention, detection and response.

New cybersecurity architecture requires new technologies, and they probably won’t be cheap. Firstbrook’s report predicts that 40 percent of enterprises will have security data warehouses by 2020, up from less than 5 percent today. Gaining faster response time through big data and mathematical analysis is the new frontier of cybersecurity.

“To do this right, you have to collect a huge amount of information,” Firstbrook said — end-point and network events can generate terabits of data daily. “To be





SHUTTERSTOCK.COM

useful, you're going to have to build this database, or buy this database, that will be able to store at least six months' worth of data so you can go back and see what happened in the past. And you can also apply what-if scenarios to the data."

Most state and local governments will struggle to find the funds and talent to do this themselves, Firstbrook said, but as Target and others have learned, refusing to adapt is more costly than investing in a flexible new approach.

**A**s cloud and mobile technologies push the defensive front away from home, a growing number of Internet-connected devices expand the battlefield. According to the International Data Corp. (IDC), the Internet of Things is expanding at a compound

annual growth rate of 17.5 percent. If IDC is right, there will be 100 billion devices on the Internet by 2020, each one representing a possible route of attack.

Hacking a network via a microwave oven or through a smart light bulb isn't just paranoia. White hat hackers are already demonstrating that such vulnerabilities aren't being thoroughly considered by manufacturers.

"Most folks don't know a lot about Internet security, but the more things we throw onto the live Internet, the more we're going to have these problems," said McAfee's Scott Montgomery. "The challenge is that there's no standard, there's no oversight, there's no regulation, there's no certifications, there's no accreditation."

Standardization efforts are under way, but there are too many factions, he said.

Dell, Intel, Samsung, Broadcom and others formed the Open Interconnect Consortium with the aim of bringing interoperability and scalability to the Internet of Things device industry. Meanwhile, the Medical Device Innovation, Safety and Security Consortium is working on guidelines to protect patients with wirelessly connected pacemakers and insulin pumps.

"I'm not suggesting that one set of standards would cover everyone, but I do believe there is an 80/20 rule, where 80 percent of what's good for the goose is good for the gander, 80 percent of the time, for 80 percent of the applications," Montgomery said.

With or without standards, security professionals will need to defend against attacks. To do that, they'll need to think as creatively as attackers, said Mark Seward, senior director of public sector at operational intelligence firm Splunk.

"The solution is to be able to hire people who have an imagination," he said. "That's something I find lacking in customers in general, not specific to any particular segment." The thing that makes organizations weak is that they depend on vendors to tell them what to do, rather than thinking beyond which product they want to purchase, Seward said.

"If everyone would simply open their eyes and use their imagination a bit more about how the service they have can be used to take advantage of their particular system, I think they'd be better off, and that's something that's hard to teach," said Seward.

Attacks that sound outlandish happen, he said, because it was the attackers who were creative and imaginative enough to think of them first. Opportunities for creativity and imagination will grow along with the Internet of Things.

**M**obile technologies and an expanding Internet of Things are making everyone and everything a network gatekeeper. The burden of protecting organizational infrastructure that was once left to experts is now in the hands of every secretary, firefighter or clerk with a smartphone. A security architecture designed to handle failures in attack prevention ameliorates the technology problem, but

patching holes in an employee's brain might be a problem without a solution, and is one for which management ultimately will be held responsible.

One of the fastest-spreading malware attacks in recent history was enabled by unsuspecting users who opened an email promising information about a storm that was ravaging Europe. The Storm Worm, discovered in early 2007, piggybacked on a storm that smashed buildings and power pylons, shut down Germany's railway system, and killed 47 people across Europe. The worm originated in emails with the subject line "230 dead as storm batters Europe." People opened the emails amid the chaos, and the worm quickly accounted for 8 percent of all malware infections globally.

Attacks that capitalize on social events are made more effective by today's growing network of devices controlled by non-experts. Hurricane Sandy left a trail of destruction in 2012, and also forged a path for opportunistic crooks to take advantage of the event's many victims through avenues like fake charity websites.

As organizations of all types spread their infrastructure across more entry points and outside vendors, it's critical that leadership does its due diligence — and leaders increasingly are being held accountable for security lapses.

"I think there is a reasonable expectation that when you share your data, no matter who that is with, if there is personal information involved, you should, as a user of a service, understand how that information is going to be used and how that data is retained, stored and destroyed," said Jayne Friedland Holland, chief security officer and associate general counsel for e-government provider NIC. "The new reality is that you have an obligation to protect that data."

The 2013 Target breach that compromised millions of credit card numbers and personal records put cybersecurity in the public spotlight. Once initial confusion subsided, people wanted to know why Target didn't have a chief information security officer on its payroll and why security wasn't a primary focus of executive leadership. The public felt its trust had been betrayed.

## IS FIRSTNET SECURE?

Could the planned nationwide communications network for public safety agencies also become a conduit for new forms of cyberattack? Some security experts worry that it might.

The First Responder Network Authority's (FirstNet) system is being designed to allow communication across agencies and jurisdictions, and to let first responders integrate modern apps and devices into their operations. The network's everyday users will be the National Guard, firefighters, police, emergency and medical technicians, most of whom are not security experts. And that could lead to vulnerabilities, said McAfee's Scott Montgomery.

He notes that disasters attract opportunistic crooks who take advantage of victims. In the wake of Hurricane Sandy, scammers created fake charity websites, posed as repair men and Social Security agents, and stole property, vehicles and identities. These attacks have become more effective thanks to today's growing network of devices controlled by non-experts.

"In my information security background, paranoia, suspicion runs rampant," Montgomery said. "My concern is that attackers will utilize this when there is a significant event. Whenever there's a tragedy, I see FirstNet networks potentially being really good vectors for this kind of thing, because what will FirstNet be used for? Mudslides, wildfires, earthquakes, tornadoes, hurricanes — a whole range of multistate and national catastrophes."

But FirstNet Deputy General Manager T.J. Kennedy said the organization's top priorities are making the network resilient, available and secure. A draft RFP for the network is scheduled for release in early 2015. There also are plans, Kennedy said, to create a security operations center that constantly monitors for threats.

"Security will be designed into all of our radio access networks," he said. "It will also be designed into our evolved packet core. It will be designed into our service platforms as well as any devices that use the network, so we're looking at it pretty holistically."


Target CEO Gregg Steinhafel resigned in May and there were previously calls for the company's board members to be held legally accountable for the breach.

Holland said there's a huge reputational risk in not protecting data. Making security a cultural focus of the organization is a big part of the solution, she said, adding that her company trains employees to be security-minded from the moment they're hired.

"You should be doing everything you can to educate your personnel about how to comply with the policies that you have established to better protect those devices from miscreants or from malware," she said. "Your employees need to understand the significance of that device and what can happen with that device."

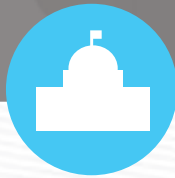
Although the outcome was unpleasant for Target's Steinhafel, mounting pressure on top-level officials could be an advantage for security professionals, said Dave Merkel, chief technology officer for security firm FireEye.

"It's a great opportunity to have a conversation with the head of your organization" and ensure that leadership has the right amount of visibility and all the right things are being done, he said. That way, if something goes wrong, leadership will be able to show, at the very least, that they're not being negligent. "The more senior in the organization you can have your conversations about information security posture and what you're doing, the better."

Understanding how an organization's technology works and what kind of exposure that creates is a crucial first step, Merkel said, and after that, leaders need to understand what vendors can offer. "You have to be a very educated buyer," he said. "The language we use to describe what products in that space should do is changing and morphing. You have to really talk to vendors and almost interrogate us to make sure that we're giving a very clear accounting of what we can do and what we can't do in terms you can understand so that you can map them to your needs." 



# Best Practices for a Converged IP-enabled Network



## Download ...❖❖❖

a complimentary copy of  
the Guide today at  
[www.govtech.com/converged-network-strategy](http://www.govtech.com/converged-network-strategy)



Produced by: **GOVERNMENT TECHNOLOGY**

In partnership with:  **at&t**

# CAN WE TALK?

By  
Brian  
Heaton

Federal framework aims to create a common language for security — and it's gaining support from security pros.

**A**s hacking attempts become more complex, governments continue to improve their cybersecurity presence through sophisticated firewalls and expanded procedures. But while high-profile data breaches have focused more state and municipal attention on cyberintrusions, a decidedly old-school problem continues to plague efforts to beef up security — communication.

With a variety of security options available, public-sector agencies often are deploying tools and using strategies that utilize different terminology and principles. These differences can lead to frustration when trying to compare cybersecurity programs and address the latest digital threats across agencies or jurisdictions. Without a standardized language, it's difficult to gauge how strong another organization's cybersecurity is.

To illustrate the concept, consider an advertisement for a new hotel. The hotel boasts that it has superior service, amenities and security. The only way to know that for sure, however, is for those claims to be verified. In the lodging industry, organizations like AAA visit hotels and rate them — five-star, four-star, etc. Customers then read those ratings and make a decision on where to stay based on the commonly understood vernacular.

A similar universal baseline evaluation for cybersecurity environments didn't exist in years past. But experts are hopeful that a new framework released by the National Institute of Standards and Technology (NIST) will give agencies a method to evaluate the security of their computing environments against their peers.

State chief information security officers (CISOs) say the effort to integrate the 41-page federal initiative — officially

called the Framework for Improving Critical Infrastructure Cybersecurity — will deliver significant benefits for government agencies in the years ahead. If the majority of organizations adopt the framework's principles, they'll be speaking the same language and have an easier time contracting with one another and protecting against cyberthreats.

Will Pelgrin, president of the Center for Internet Security (CIS), a nonprofit group that helps states and localities improve cybersecurity, sees the framework as a cornerstone and common path forward for agencies. He calls the framework a valuable tool for helping organizations identify risks, priorities and gaps, and addressing them methodically.

Instead of a linear plan, the framework uses common fundamentals and a cyclical approach designed to help governments and businesses establish a cybersecurity baseline, find their most glaring vulnerabilities and tackle them at the outset using whatever method works for them. Then further steps can be





Virginia CISO  
Mike Watson was  
an early adopter  
of the NIST  
cybersecurity  
framework.

taken as priorities are outlined and financial resources are available.

“It’s about not reinventing the wheel; there are plenty of good strategies out there — pick one,” Pelgrin said. “Figure out what works best for your organization and move forward.”

## HOW IT WORKS

The framework is a living document of best practices that users can reference to establish a risk-based approach to improve cybersecurity. It provides a series of actions to anticipate and respond to attacks on systems. Five basic core functions are the foundation of the framework — Identify, Protect, Detect, Respond and Recover.

The functions are meant to be worked on concurrently and continuously. Within them are “implementation tiers” designed to show how mature an organization is in each of the five areas. The tiers range from the lowest level of Partial, followed by Risk Informed, Repeatable and Adaptive. Each tier describes the level of sophistication an organization has with performing each particular cybersecurity practice.

The next level of the framework is “profiles,” which align all the core functions with an agency’s business requirements, resources and risk tolerance. Profiles give organizations a way to describe their current cybersecurity condition and set a goal for where they want to be in the future. That shows where gaps exist, enabling users to address shortcomings and make improvements.

For a state or local government already running a cybersecurity program, adopting the framework may require aligning individual terminology and processes to match what’s in the core functions. But nothing has to be adopted all at once. Agencies can take parts of it and apply them as appropriate.

Work on the framework kicked off with President Obama’s Executive Order on Improving Critical Infrastructure Cybersecurity on Feb. 12, 2013. Section 7 of the order charged NIST with incorporating industry best practices and standards “to the fullest extent possible.”

To that end, NIST conducted five workshops throughout the U.S. to gather infor-



mation and ultimately create the current framework. It took a full year to develop, according to Adam Sedgewick, senior information technology policy adviser for NIST.

Sedgewick explained that the goal was to develop a common cybersecurity language for public- and private-sector organizations to communicate and pull people together to provide analysis and reach agreement on best practices.

“There has been a degree of fracturing where different sectors and organizations rely on different standards, regulations and requirements,” he said. “So what the framework does ... is allow people to communicate what their cybersecurity programs look like, and that makes it easier for those organizations to manage risk.”

## EARLY ADOPTERS

Virginia’s cybersecurity program has been in place for a while, but the state was one of the initial framework adopters. Mike Watson, the state’s CISO, said integrating the NIST Framework was a smooth process for the state, primarily because it had already implemented NIST Special Publication 800-53 from a few years ago, which

contained similar principles. The 800-53 document outlines recommended security and privacy controls for federal agencies.

Watson explained that the state chose to use the federal standards because a number of vendors in the area had begun marketing themselves as compliant with 800-53. As a result, Virginia took steps to map and align its existing standards back to those recommended in 800-53, so that communication was clear between the parties.

## CORE FUNCTIONS

The NIST Framework defines these functions as important parts of an operational culture that acknowledges the dynamic nature of cybersecurity

**IDENTIFY**  
Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.  
**Outcome categories** include asset management; business environment; governance; risk assessment; and risk management strategy.



Virginia took the same approach with the NIST Framework. Watson said the strength of the framework is that it gives decision-makers a clear understanding of where their cybersecurity program is in comparison to other agencies or entities.

"I want to make sure to use this as a way to see how secure our environment is with all the different pieces and parts," Watson said. "Adopting a standard language is really the first step in being able to do that."

Pennsylvania is in a similar position to Virginia, as it had already been complying with 800-53 as well. But when adopting the NIST Framework, Pennsylvania CISO Erik Avakian also made it a priority to take note of the cybersecurity call for action the National Governors Association (NGA) announced last year.

The NGA debuted a five-point plan to help states better protect themselves from cyberattacks, which includes states establishing an authority structure to handle cybersecurity issues; conducting risk assessments; implementing vulnerability assessments and threat mitigation practices; complying with current security methodologies; and creating a culture of risk-awareness.

Avakian threw everything into a blender and developed a cybersecurity road map for Pennsylvania that aligns with both the NIST Framework and the NGA's principles. He agreed with Watson that the biggest benefit of the NIST Framework is that it supplies a standard language for all parties across multiple industries

to use. But he's also enamored with the flexibility the framework provides.

"The NIST Framework is not trying to change what you're doing from a cybersecurity perspective — it augments it," Avakian said.

## IMPLEMENTATION

Watson said the first step for Virginia was just refining its process for gathering information and identifying the major metric points and risk indicators to support both what the state had in place previously and the NIST Framework.

The path for Pennsylvania was similar. Avakian and his team took everything in the framework, mapped it and then implemented it into the state's enterprise governance, and risk and compliance solution. Avakian said the move has been successful and sees a similar approach working well for other public-sector organizations.

The Pennsylvania CISO noted that because the framework shows on a granular level where an agency is, and where it needs to get to, it helps everyone stay ahead of cyberthreats. The key, he added, was a two-pronged communication approach.

"You need something for both the technical and the business sides of the organization," Avakian said, regarding what cyber-risks exist and how to mitigate them. "If you only do one or the other, you're not going to be able to clearly communicate to either of those groups."

Sedgewick admitted that the framework's overall complexity was one of the

major developmental challenges early on. Because the goal was to create a framework that can be adopted by companies and organizations of all different sizes and preparedness levels, providing the appropriate level of detail was critical.

If the framework was too detailed, then it would run counter to the basic tenets of Obama's executive order, as not all organizations have an advanced cybersecurity plan in place. But the framework still needed to have enough guidance to also help agencies and companies that were already at a high level.

But Sedgewick said NIST and its stakeholders struck the right balance that considers small local government operations and other potential adopters that may not have the funds to invest in cybersecurity efforts.

"One thing that we want to be clear about is that we don't necessarily think this is just about finding the resources — it's about general practices that people can do with the resources they already have," Sedgewick said. "And so if you look at the framework itself, part of the structure that stakeholders came up with, was an effort to help simplify and better articulate what the essential elements of a good cybersecurity program are."

## FUTURE CHALLENGES

While there are plenty of benefits in adopting the NIST Framework, it still presents a number of challenges for

### PROTECT

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

**Outcome categories** include access control; awareness and training; data security; information protection processes and procedures; maintenance; and protective technology.

### DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

**Outcome categories** include anomalies and events; continuous monitoring; and detection processes.

### RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

**Outcome categories** include response planning; communications; analysis; mitigation; and improvements.

### RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

**Outcome categories** include recovery planning; improvements; and communications.

# Privacy has never been this easy.



## 3M™ Easy-On Privacy Filter

Introducing the first removable privacy filter for tablets.

Choose privacy with a fast, bubble-free application every time. Stay private when needed, share content when wanted. Privacy is the best policy.

# 3M

Purchase today at  
[3Mscreens.com/easy-on](http://3Mscreens.com/easy-on) ►

3M is a trademark of 3M. © 3M 2014. All rights reserved.

CAN WE TALK?



**Pennsylvania  
CISO Erik  
Avakian adopted  
the NIST frame-  
work and cyber-  
principles  
released by  
the NGA.**

DAVID KIDD

organizations. The most obvious is financial investment to establish a baseline and have a minimum level of threat monitoring, particularly for agencies that don't have an active cybersecurity program.

For Pennsylvania and Virginia, there wasn't a significant cost outlay, as both states already had security measures and response systems in place. But Watson said agencies should expect to spend some dollars to get up to speed.

Avakian agreed that doing things like risk assessments — which the framework relies on — takes resources. But he noted that unlike years past, there now are a number of free services available for public-sector agencies to be proactive regarding cybersecurity.

For example, the Multi-State Information Sharing and Analysis Center (MS-ISAC) offers free managed security and advanced monitoring services, while the U.S. Department of Homeland Security provides cyber-resiliency assessments at no cost, according to Avakian. Those opportunities didn't exist years ago, and Avakian thinks agencies should take advantage of them as they consider adopting the NIST Framework.

Watson is concerned about just how much the federal government is going to push the private sector to adopt the framework. It could be an important factor in the long run, since working from a common language is one of the framework's largest benefits. Watson added that he also thinks

NIST should give agencies more guidance on how to measure compliance within each of the framework's categories.

Sedgewick was aware of the concerns, but noted that the framework is not a checklist, but rather a living document intended to be built upon by users. He said the idea is for people to look across the entirety of the framework and think about advanced capabilities that can support the outcomes that make organizations more secure.

In addition, Sedgewick explained that people shouldn't go through the framework and think they have to "implement every single word." Instead, they should use it as a tool to improve the cybersecurity position of their organizations.

Avakian called the NIST Framework a great start that encompasses most cybersecurity needs. He said that time will tell whether additional components are needed, but so far, there are no glaring omissions.

Pelgrin agreed, adding that there's something in the framework for everyone regardless of where an organization is on the cybersecurity maturity spectrum.

"It's really an opportunity to raise the bar across all sectors," he said. "The breadth and depth of sectors using it is impressive. It's not about the technology; it's about the behavior of implementing an effective process." **GT**

[bheaton@govtech.com](mailto:bheaton@govtech.com)  
[twitter@govtechbrian](https://twitter.com/govtechbrian)



Good News: your employee used the 2 hour commute to get work done.



Bad News: the person sitting next to them was a visual hacker.

Keep visual hackers in the dark. With today's mobile workforce, organizations can't afford to take chances. Help protect confidential data from prying eyes by requiring 3M™ Privacy Products on all your devices. Learn about all our products to prevent visual hacking at [3Mscreens.com/VisualHacking](http://3Mscreens.com/VisualHacking). Privacy is the best policy.

Privacy Solutions  
for Organizations



3M is a trademark of 3M. ©3M 2014. All rights reserved.

**3M**





**Delaware Chief  
Information  
Security Officer  
Elayne Starkey**





By David Rathes / Contributing Writer

# SECURITY LEADERS SOUND OFF

The role of chief security officer may look different in every organization — but in an increasingly connected and open society, it's more vital than ever.

**R**alph Johnson had some great conversations with CIOs at the National Association of Counties annual conference in July. But the chief information security officer of King County, Wash., did notice one odd fact: “I was the only CISO at the entire conference,” said Johnson. “A lot of large urban counties on the East Coast seem to have CISOs, but the sense I got was that in the Midwest and Western states, that was not the case.” In talking to the IT chiefs, he learned that the counties that do have a CISO have a very small information security staff.

While the role has been inching its way into local government, the view is very different at the state level. As more state governments have recognized the importance of securing information and assets — and high-profile breaches put them in the public eye — there has been a gradual increase in the number of chief security officers (CSOs) and CISOs over the last decade. Today every state has a CSO, CISO or equivalent, according to security experts, which historically hasn't been the case.

And while the titles include “security,” the job definition varies widely. Some incorporate privacy and audit functions, for example, while others house those responsibilities elsewhere. The

role also can differ depending on whether the state takes a centralized or decentralized approach to cybersecurity. In addition, the reporting structure varies, but experts stress that it's crucial for security officers to report to a senior-level official.

Dan Lohrmann, who recently stepped down as Michigan's CSO, was in charge of both information and physical security, including badges, cameras and building security, for the state. “The physical security aspect was a huge learning curve for me, but that was great.” He thinks these responsibilities will inevitably merge. “An ID is an ID is an ID,” he said. “You have a picture ID or a badge, access to certain buildings and not others. You have the same things in cyberspace. You can access certain files and not others. There's provisioning and de-provisioning. If you get to a certain level of sophistication, it is the next natural step that you have to bring these together.”

Many factors influence whether these two functions would be merged. But it's clear that the interdependencies between cyber- and physical security must be understood, no matter whether an individual's role covers both or a government has them listed separately on the org chart.

*Government Technology* spoke with five CSOs and CISOs at the state and local levels about their roles, greatest challenges and lessons learned on the job.

TOLBERT PHOTO


**JAY WHITE**

*director of the  
Information  
Security Services  
Division, Mississippi  
Department of  
Information  
Technology Services*

**In the position  
since: 2011**

**BIGGEST CHALLENGE:** IT in Mississippi is very decentralized. We haven't gone through a consolidation process. We have responsibility for policy and governance, but the operational aspects of security reside in the agencies. They all pay attention, but the availability of resources differs. There are pros and cons to both environments. Centralization doesn't resolve all the issues. But the more diverse the technology infrastructure is, the more challenging it is to have one set of policies and guidelines.

**SIGNIFICANT DEVELOPMENTS:**

Last August we had our first multiagency tabletop exercise, and it was an eye-opening experience for information technology services and the agencies. It gave us an opportunity to train for a cyberincident: How would we communicate? How would we respond?

**FORMING A RELATIONSHIP WITH THE CIO:** I have been fortunate enough to work with a CIO, Craig Orgeron, who


**RALPH JOHNSON**

*chief information  
security and privacy  
officer, King County,  
Wash.*

**In the position  
since: 2005**

**JOB RESPONSIBILITIES:** Executive leader of King County's information assurance program. Spearhead and manage initiatives to provide a proactive approach to information security.

**BIGGEST CHALLENGES:** Things were difficult in the early days because we were trying to introduce a governance model, not just for security, but also for IT as a whole, and we were changing the culture, changing the way IT is done.

We always had departmentally focused pockets of IT. For instance, we had the same anti-virus system across county workstations, but some departments would set up their own central management console. Some would manage each workstation individually. There was no overall picture. We combined all of that into a single management console so we could get a picture of endpoint protection across the entire county. Also, some operational functions that in a corporate


**AGNES KIRK**

*CISO, Washington*

**In the position  
since: 2005**

**JOB DESCRIPTION:** I have a dual role of being the state CISO and also having responsibility for delivering enterprise security services. My team doesn't manage the networks, but we have established a Security Operations Center, which handles logging, monitoring and analytics, as well as alerting and incidence response statewide. I also have operational responsibility for firewalls, remote access, gateways, Web filtering, etc. I have a close relationship with the state CIO, whose office is the policymaking arm of state government for IT. I work with

him on developing strategy for the state in terms of security policies and standards and implementation strategies. I also represent the state at Department of Homeland Security, MS-ISAC and other national forums. I do a lot of public-private collaboration.

**BIGGEST CHALLENGE:** Staying ahead of emerging mobile technologies. Everything is accessible now all the time. Because there are so many options available one click away, including collaboration sites and social media, it is a challenge for



started working for the state at roughly the same time I did. I have known him a long time, and we speak on a weekly basis. Craig is president of NASCIO and has given a number of presentations on this topic, so I know he is well aware of cybersecurity issues.

**VALUE OF MENTORS:** As part of the Multi-State Information Sharing and Analysis Center's (MS-ISAC) mentor program, I have been a mentee for two years and will be a mentor this year. In the first year, I was paired

## "THE MORE DIVERSE THE TECHNOLOGY INFRASTRUCTURE IS, THE MORE CHALLENGING IT IS TO HAVE ONE SET OF POLICIES AND GUIDELINES."

up with Michigan CSO Dan Lohrmann and we spoke at least once a month. I enjoyed it while we were doing it, but only afterward did I realize just how much I did learn. For instance, a tabletop exercise process we did in Mississippi developed from a conversation I had with Dan about how important it was in his state.

**LESSONS LEARNED:** You can have the best policy in the world, but if you can't get groups to collaborate, I don't know how policy requirements are going to work. Also, the CISO can't be an expert on everything, because this is such a complex topic. You have to rely on the expertise of people in specific roles and help them find training to stay up to date.

world would be turned over to information security tend to be handled by operations groups in government. I have oversight of the network team and I am involved with them, but my team doesn't actually manage them.

### ADVICE FOR NEW CISOs

**AND CSOs:** Learn your organization's culture before trying to make changes. Consider organizational culture and focus on risks to the data. Don't focus on the technology. You can

## "LEARN YOUR ORGANIZATION'S CULTURE BEFORE TRYING TO MAKE CHANGES."

buy lots of boxes with pretty blinking lights that are going to make your data center look really good, but if you can't incorporate what they do into that environment, because of the culture, you just spent a lot of money for nothing.

**LOOKING AHEAD:** We have four core initiatives in King County IT to support: mobility,

modernization, service maturity and e-government. All four are intermingled, and all have security elements. We are also looking at a multiyear identity and access management project. It would not only allow you to access the information you have permission to, it would also offer automated provisioning and de-provisioning.

## "YOU CAN'T ASSUME THAT YOU CAN TREAT SOMEBODY ELSE'S DATA THE WAY YOU WOULD TREAT YOUR OWN."

organizations to know where all their data is to be sure it's being protected appropriately. The convenience of the services makes it hard for employees and citizens to remember the responsibility that hasn't changed. You

can't assume that you can treat somebody else's data the way you would treat your own. People are just trying to do their jobs, and they are picking the most convenient way. We are trying to keep track of that. It is an ongoing conversation I have with my private-sector counterparts.

**WHAT ABOUT THE IDEA OF MERGING PHYSICAL AND INFORMATION SECURITY RESPONSIBILITIES INTO A CSO ROLE?** It is a possibility, but I don't think it is imminent. It isn't that it would be wrong to merge it, but I don't

think it would be critical. We work very closely with the folks who handle physical security.

### DO YOU SEE THE NEED FOR A CHIEF DATA OFFICER OR PRIVACY OFFICER FOR THE STATE?

I don't think it would be a bad thing. We have just started looking at it, and we need to have a lot more discussion about it. Every agency has a privacy officer and public disclosure officer, sometimes one and the same. I see some benefits, but I also see the value of having it in the agency so that they understand the agency's business.

**ELAYNE STARKEY***CISO, Delaware***In the position since: 2006**

**SECURITY RESPONSIBILITIES:** At the time the CSO position was created, it was intended to encompass not just information security, but also physical security at our department. Since that time, we have reorganized a couple of times and physical security is no longer part of my purview. But I have strong partnerships with law enforcement and emergency management agencies. It is a critical part of my position to be well connected to those folks.

**MAJOR ACCOMPLISHMENT:** The cornerstone of Delaware's program is education and outreach. All executive branch employees go through an information security refresher training every year. We have a 99 percent completion rate. We are very proud of that number; it took a lot of hard work and a lot of prodding to make it happen. We count ourselves fortunate that we are one of a few states in the nation that requires every new employee who gets an email account to go through that training in the first 30 days.

**BIGGEST CHALLENGE:** One of the biggest things we have done is to empower departmental information security officers. There was a time when being an information security officer meant approving a few forms and resetting some passwords now and then. The threat environment has changed in such a major way that we have asked them to do much more. But I am not a fan of asking them to do more without training to go with that. We have subsidized boot camps to help them prepare to take Certified Information Systems Security Professional tests. Then when they achieve it, we make a

big deal of it and get the governor involved. It is an incredible motivator, we've found, that their ultimate boss cares about this.

**SUGGESTION FOR LOCAL GOVERNMENT:**

Every two years, we issue scorecards to all internal customers, even the smallest agencies, for them to do a self-assessment on their security posture. The hope is that the score keeps improving. If not, it is a vehicle to take to management to explain in a non-techy way the basics of why security is important and the risk of not investing. There are a lot of metrics-driven business leaders, and you can get a competition going among agencies. I don't see why that approach wouldn't work on the local level too.

**ADVICE TO NEW SECURITY**

**OFFICERS:** People think technical qualifications are important, and you do need to continue to hone technical skills, but I think you should place a huge emphasis on relationship building. The job is less about technical details and more about managing risk and describing risk in a way that a nontechnical person can understand.

**PATSY BOOZER***CISO, San Antonio, Texas***In the position since: 2012**

**CHANGES PUT IN PLACE:** I started in April 2012 and added physical security to my responsibilities in June of that year, although we didn't change the title to CSO. The city had a security understanding, but it needed to be broadened and fine-tuned. When I arrived there were 11 administrative security directives, and that is just too many for people to get their hands around. So I refreshed them and cut the number of directives to five.

**SETTING A NEW STRATEGIC**

**DIRECTION:** I saw that the internal auditor used the FISCAM (Federal Information System Controls Audit Manual), so it made

sense to me to use the National Institute of Standards and Technology SP 800-53 standard because that maps to the same controls. Of course, then you have to look at it from a cost-benefit perspective and see what type of data you are trying to protect. The main types of data the city deals with involve criminal justice and HIPAA (Health Insurance Portability and Accountability Act). We have 14 departments that fall under HIPAA, and we had to make sure the sensitive personally identifiable information was being handled correctly. We also had to look at the payment card industry, because all cities are starting to accept credit cards. I needed to start with a data-centric focus and look at all the requirements of those different mandated security policies and see where I can find commonality. We focused on the Council on CyberSecurity's Top 20 Critical Security Controls, and we have made significant progress on all 20 controls and mapped it so we are coming into compliance with all the mandatory requirements.

**SOMETHING UNIQUE ABOUT YOUR CITY:**

San Antonio is the seventh-largest city in the country, and it is also dubbed Cyber City USA. We have several military bases, and the city by its culture is very cyber-driven. I meet with other security directors and CISOs at a monthly meeting called the Security Leadership Forum. We talk about how we can be of help to each other and share lessons learned.

**LESSONS LEARNED:** One challenge is that a governmental organization can be so large and diverse that it essentially has all these vertical industries such as criminal justice and health care embedded within it. The key is to find a horizontal approach that works across all those areas. If you just look at it one vertical at a time, others are likely to get left behind. **GT**

draths@mac.com



**"Great conference. I took a lot away from all of the talks I attended."**

—David Hollis, Consultant, Raybeam Inc.

**"You will great insights and the speakers will put you on the fast track."**

—Chandrashekhar Vyas, Solution Architect, Diaspark

**"Big Data TechCon is a great learning experience and very intensive."**

—Huaxia Rui, Assistant Professor, University of Rochester

**"Big Data TechCon offers great technology depth."**

—Rahul Gupte, Associate Director, Deloitte



**There's Still Time to Register!**



# Big Data Gets Real at Big Data TechCon!

**Big Data TechCon is the HOW-TO technical conference for professionals implementing Big Data solutions at their company**

## Come to Big Data TechCon to learn the best ways to:

- Process and analyze the real-time data pouring into your organization
- Learn how to extract better data analytics and predictive analysis to produce the kind of actionable information and reports your organization needs.
- Come up to speed on the latest Big Data technologies like YARN, Apache Spark and Hadoop
- Understand HOW to leverage Big Data to help your organization today

**Choose from 55+ classes and tutorials!**

# BigData TECHCON

## San Francisco

**October 27-29, 2014**

**[www.BigDataTechCon.com](http://www.BigDataTechCon.com)**

**Enough talking about Big Data – learn how to DO IT!**

A **BZ Media** Event

Big Data TechCon™ is a trademark of BZ Media LLC.

**Special Pricing for Government Employees!**

**[www.bigdatatechcon.com/government.html](http://www.bigdatatechcon.com/government.html)**

# Help Wanted

Major retailers are not the only targets for cybercrime, despite what the recent headlines may suggest. State and county governments are equally at risk of attack, and it's a risk that many take seriously.

"We house information for payroll purposes for people's health insurance. We are dealing with confidential legal information, confidential criminal information. We have an obligation to do everything in our power to protect all the data that the state has in its possession," said Ann Visalli, director of Delaware's Office of Management and Budget.

For Visalli and her colleagues across government, that readiness to get in the game is sometimes thwarted by a lack of skilled players to help carry the ball. Workforce research firm Burning Glass Technologies reports the demand for cybersecurity workers is more than double the overall IT job market. An estimated 300,000 cybersecurity jobs are vacant in

The shortage of cybersecurity experts is well documented. So what are agencies doing to fill the gap?

By Adam Stone / Contributing Writer



# d



DELAWARE'S ANN VISALLI  
SAYS PAY CHANGES  
FOR TECHNOLOGY WORKERS  
HELPED THE STATE FIND  
CYBERSECURITY TALENT.

the United States, according to Symantec, and demand will likely rise as the private sector faces unprecedented numbers of data breaches and cybersecurity threats.

Government is hobbled here. With demand high and supply short, cybersecurity experts are commanding top dollar, typically \$120,000 and up in the private sector. Government struggles to keep up. State officials in Michigan report that their cybersalaries run about 20 percent below market rate.

"We really need to appeal to folks' sense of the nobility of public service," said Michigan CTO Rod Davenport.

But that'll only get you so far. As a result, states and localities are seeking more aggressive methods to woo top cybersecurity talent. Some are pursuing a two-pronged approach, implementing creative recruiting on the one hand, while simultaneously working with industry and academia on the other to build up the general pool of local cyberprofessionals, thus broadening the potential workforce all around.

**B**efore diving into state and local efforts, it helps to step back for a moment to look at the federal government's cyberagenda.

Programs at the federal level often help to set the tone for efforts across the states.

In 2013 the U.S. Department of Homeland Security launched the National Initiative for Cybersecurity Careers and Studies to spur development of a robust cybersecurity workforce. The organization aims to boost awareness, grow the pipeline and encourage advances in the field. For states, this effort comes with such benefits as an online cybersecurity workforce planner.

Working against this backdrop, which defines cybersecurity as a national priority, states have been eager to ensure that their cyber-resources are firmly in place.

In Delaware, recruitment efforts go well beyond the proverbial ad in the paper or online listing. To stretch its IT budget while simultaneously attracting top talent, the state made significant structural changes to its technology apparatus,

changes that in turn helped it find and keep skilled cybersecurity players.

The state gained efficiencies when it consolidated its diverse IT operations into a single Department of Technology and Information. One immediate effect was a reduction in duplicate roles: A single expert from the department could now be dispatched to multiple agencies as needed.

In the realm of cybersecurity, the overhaul gave recruiters a significant edge by exempting IT hires from traditional state pay scales. This opened the door to competency-based pay, pay-for-performance and other components aimed at giving state hiring a stronger chance in the face of private-sector competition.

"While we are pretty well positioned now, it is a constant battle," Visalli said. Under the revised system, "it's a little faster, it's a little more flexible, the pay is a little more competitive and it allows for promotion and retention for employees who do achieve what they need to be achieving."

In the bigger picture, Delaware is working aggressively to build a cyber-workforce throughout the state, reasoning as many do that a robust workforce will benefit government while also helping to ensure a strong economic base among local companies.

To this end, the state recently launched a \$3 million Delaware Cyber Initiative, intended to forge alliances between academia, workers and the private sector in order to develop a skilled and innovative cybersecurity workforce. The initiative — part research lab, part workforce development and part business park — includes the University of Delaware, Delaware State University, Delaware Technical Community College and private companies.

If Delaware is being especially aggressive in its efforts to bolster cybersecurity, it may have something to do with the nature of the local economic base. "As more and more data is managed electronically, the need to secure that information becomes critical. Staying ahead of the curve is something all states are dealing with," Visalli said. "But in



Delaware we also are home to a large number of financial institutions that have security as their No. 1 priority, and we need to be responsive to that."

**I**n Michigan, state IT leaders say they have two cyberpros on the payroll and need to fill five more openings — a hefty shortfall. In particular, they need people who possess not just security expertise but also a broader understanding of systems. "When you





ARLINGTON COUNTY'S  
DAVID JORDAN RECRUITS  
AD HOC SECURITY  
WATCHDOGS.

DAVID KIDD

are architecting a system at its inception, you need someone who understands all the applications and who also has the depth of knowledge in security,” said Jack Harris, director of network strategies.

Beyond the lack of readily available experts, part of the problem comes down to money. Often, the state just can’t afford to parallel what the corporate world is offering. The state may run a salary survey soon, Davenport said, but in the meantime his department has to work with the budget at hand.

Some internal recruiting may help to close the gap. “There is some interest from people here, just because it is a hot area and because IT people like diversity in their work. So that is something we are considering,” Harris said.

In the grand scheme, the state’s best hope for filling out its cyber-rolls may come from programs such as the Michigan Cyber Initiative. Besides raising awareness, the program also serves as an economic development vehicle, especially for companies with an interest

in security. For example, Michigan offers a beta test program for cybersecurity companies looking to deploy pre-release products within segments of the state’s IT infrastructure. All this in turn helps to build the overall pool of available cybersecurity talent.

At the county level, many IT managers find themselves facing the dual burden of stingy salaries, paired with volumes of digital activity

that rival those of some of the biggest corporations. So their workforce solutions need to be all the more creative.

Take for instance Arlington County, Va., population 250,000. There are about 4,500 users on the county network, which processes some 1 trillion events every day. To keep it all safe, the county employs an IT security staff of one: Chief Information Security Officer Dave Jordan. That's it. "The first thing I had them do is put in a small chapel at the end of the hall," Jordan quipped.

In the absence of a formal cybersecurity workforce, Jordan bridges the gap by enlisting the aid of others in the organization as ad hoc security watchdogs.

He briefs IT help desk workers constantly on issues related to security, sending out multiple alerts daily. "They are the first filter and then if there is something they can't answer, they send it to me," he said. "Everybody who works in the IT department has a security component."

Reaching out even further, Jordan leverages the combined power of the county workforce as a sort of extended security operation. "I've enlisted the aid of my 4,500 people. I talk to every single employee that is hired: I talk about the rules of the house, I talk about basic IT security, how you should use your email or not use it — basic things like that," he said. Security practices are written down, "but it's better to have the eyeball conversation. I will get in an elevator and someone will tell me I am the only one they remember from orientation. And I'm not even that funny. But I give them information that they care about, I make it relate to them in their personal lives. I give them information to protect their personal, private information at home, and that helps them to make the connection."

Jordan also collaborates with area peers through the National Capital Region Council of Government. Through its CISO subgroup, "we can instantly reach out to each other. In the event I see something peculiar and I want to share that with my colleagues, I can do that," he said. "By having this ability to question the community, we are able to provide added value to each other."

Even as states and localities struggle with their own cyberworkforce needs, some are looking beyond their own walls, sponsoring broad community partnerships meant to foster cybertalent for the coming years.

In Maryland, the Howard Tech Council teams with the Howard County Economic Development Authority and local tech incubator Innovation Catalyst to offer a CISO-in-residence program. The program gives more than 300 member organizations access to a range of security consulting services and expertise. This in turn helps to

## BEST CYBERSECURITY SCHOOLS

A recent survey asked experienced technology and information security pros for input on the best cybersecurity programs. Feedback came in on more than 400 institutions, from community colleges to programs granting doctorates in cybersecurity-related fields. Here's who came out on top:

- ☒ University of Texas, San Antonio, San Antonio
- ☒ Norwich University, Northfield, Vt.
- ☒ Mississippi State University, Starkville, Miss.
- ☒ Syracuse University, Syracuse, N.Y.
- ☒ Carnegie Mellon University, Pittsburgh
- ☒ Purdue University, West Lafayette, Ind.
- ☒ University of Southern California, Los Angeles
- ☒ University of Pittsburgh, Pittsburgh
- ☒ George Mason University, Fairfax, Va.
- ☒ West Chester University of Pennsylvania, West Chester, Pa.
- ☒ U.S. Military Academy, West Point, N.Y.
- ☒ University of Washington, Pullman, Wash.

SOURCE: 2014 BEST SCHOOLS FOR CYBERSECURITY, SPONSORED BY HP ENTERPRISE SECURITY AND INDEPENDENTLY CONDUCTED BY THE PONEMON INSTITUTE

build a culture of awareness — an important first step toward workforce development.

"Typically you don't see these firms really considering the implications of not protecting their intellectual property, protecting themselves from the undue harm associated with folks who may be looking to steal their goods," said Howard Tech Council Executive Director Patrick Wynn. In addition to providing access to experts, the program helps to put the issue of cybersecurity that much higher on the communal radar.

A similar effort can be seen at the state level in Florida, where the Legislature recently budgeted \$5 million to create the Florida Center for Cybersecurity at the University of South Florida. "There is a huge supply and demand problem in the marketplace. We need to create a workforce that can respond to the needs of the market," said Sri Sridharan, managing director of the online program, which conveys both degrees and certificates. "Our objective is to crank out thousands of qualified students."

Besides building up a cyberworkforce statewide, the program could provide state and local IT offices with a cost-effective way to fill jobs that today stand empty, Sridharan said.

"They can find people they already have, put them through a quick certificate program, get them knowledgeable in areas where they think there is a hole and then get them back to work," he said.

"For a state or county government with somebody earning \$65,000 or \$70,000, you can put them through a certificate program, you pay them another \$10,000 and they will stick around," he said. "That is a significant pay increase, so you get the need met and you don't have to budget \$120,000 to \$150,000 for that position."

Ultimately, though, it's a balancing act.

On the one hand, there's the immediate, short-term pressure to get people into chairs as the cybercrime wave continues to swell. Many IT leaders will

continue to struggle with the short-term need, an issue exacerbated by the fact that states can't match private-sector pay.

On the other hand, a rising tide floats all boats: When states invest in broad-ranging workforce development programs with an eye on cybersecurity, they likely will be creating a new potential pool of cyberworkers ready to take up places in state IT operations. **GT**

adam.stone@newsroom42.com





Helping clients improve how they buy, implement,  
and manage the technology infrastructure that  
support their mission critical business applications.

**Better Data  
Centers,  
Better Business  
Outcomes**

*Cloud Computing  
IT Assessment & Planning  
Virtualization  
SAN/NAS Storage Solutions  
Networking*

**All Lines Technology**

791 Commonwealth Drive, Warrendale, PA 15086 | PH: 724-850-9190

**[www.alllinestech.com](http://www.alllinestech.com)**

BY JASON SHUEH / STAFF WRITER

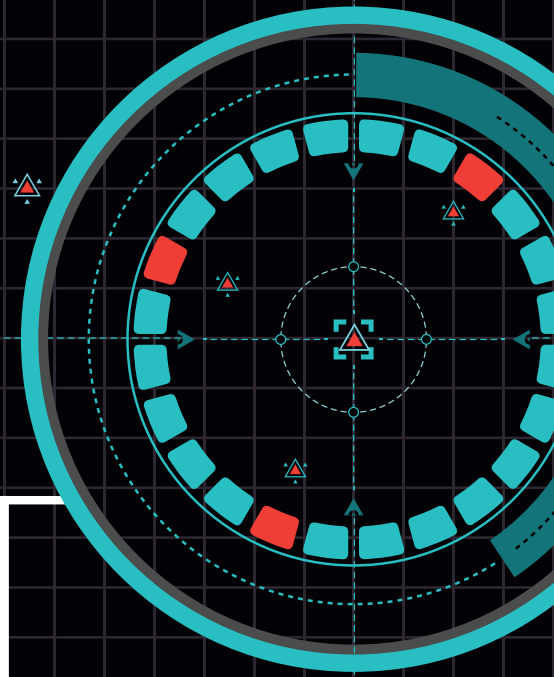
# THE BEST DEFENSE

The market is prime for a new class of startups that can decipher tomorrow's cybersecurity threats.

According to Gartner, by 2020, 60 percent of digital businesses will fall victim to devastating service failures due to their inability to handle the threats present in new technologies. Digital hazards are so pervasive that Gartner reports that the worldwide security software market grew 4.9 percent and totaled \$19.9 billion by the end of 2013.

Though dismaying statistics for government officials, the news is catalyzing IT entrepreneurs and venture capitalists to launch startups to meet demand. Research group PrivCo noted companies in the cybersecurity sector jumped by nearly 60 percent in early stage funding from 2012 to 2013, and worldwide, listed investments at \$244 million.

In light of the rising tide of cyberattacks, *Government Technology* interviewed 12 emerging security companies to hear about their strategies and tactics for protecting their customers' digital assets.





# SYNACK

[WWW.SYNACK.COM](http://WWW.SYNACK.COM)

Enterprise-level crowdsourced security testing for Web applications, mobile apps and host-based infrastructure. The company points to its Red Team, made up of security pros spanning six continents and 27 countries, as vital to the success of its security business model.

**Primary customers:** Retail, financial services, oil and gas, and health-care services.

**Founded:** January 2013

**Founders:** Jay Kaplan and Mark Kuhr

## WHAT'S THE MOST DANGEROUS THREAT AFFECTING ORGANIZATIONS?

"The most dangerous threats are those that organizations don't know about. Specifically, we find threats to mobile applications are on the rise. Every day organizations are getting compromised via a variety of attack vectors without ever realizing it."

## WHAT'S THE MOST DANGEROUS TYPE OF MALWARE TODAY?

"Malware with an extremely small footprint is difficult to spot and difficult to remediate against. Malware and malware detection solutions will continue to play a cat-and-mouse game for many years to come."

— Jay Kaplan, CEO

# AXON GHOST SENTINEL

[WWW.AXONGHOSTSENTINEL.COM](http://WWW.AXONGHOSTSENTINEL.COM)

The startup provides protection for mobile devices, enterprise networks and smart devices within the Internet of Things, such as home automation systems, smart cars and smart medical devices. Its unique process deploys lightweight software entities called "ghosts" to assess device status, processes and application activity and to classify abnormal behavior in real time.

**Primary customers:** Consumers, small and medium-sized businesses, and large enterprise networks.

**Founded:** January 2014

**Founders:** Kent Murphy, Sven Brueckner, Ravi Gupta, Andrew Yinger and Hugh Brooks

## WHAT'S THE BIGGEST MISCONCEPTION IT PROFESSIONALS HAVE ABOUT CYBERSECURITY?

"That existing approaches to security — containerization, centralized data analysis, firewalls and anti-virus — can deal with new threats and especially, can work on new types of smart devices."

## WHAT'S THE MOST DANGEROUS THREAT AFFECTING ORGANIZATIONS?

"The increasing reliance on more and different types of connected devices from phones to cars to thermostats to insulin pumps. These new devices are open to exploitation in ways never seen before and can pose a significant risk if not protected."

— Hugh Brooks, President

# SHAPE SECURITY

[WWW.SHAPESECURITY.COM](http://WWW.SHAPESECURITY.COM)

Shape says it challenges the traditional "detect and fix" model by adding a foundational layer of security to protect Web applications at the user interface level. Its flagship product, ShapeShifter, is a botwall that disables attacks from malware, botnets and scripts by mimicking the way malware evades anti-virus software, turning websites into moving targets, rendering malware, botnets and scripts unable to interact with them.

**Primary customers:** Emphasis on Fortune 50 companies with early adopters in financial services, health care and retail.

**Founded:** Stealth launch in 2011, official launch in January 2014

**Founders:** Derek Smith, Justin Call and Sumit Agarwal

## WHAT'S THE MOST DANGEROUS THREAT AFFECTING ORGANIZATIONS?

"Automation is the most dangerous threat and is what all attacks — from malware, botnets and scripts — have in common. These sophisticated attacks — such as account takeovers, application DDoS, database scraping and fake account creation — use automation to evade even the best security defenses."

## WHAT'S THE BIGGEST MISCONCEPTION ABOUT CYBERSECURITY?

"There are many big misconceptions, but one of the most pervasive is that 'fully patched' applications [software that's been updated with protection] are secure."

— Shuman Ghosemajumder, VP of Strategy

# CYLANCE

[WWW.CYLANCE.COM](http://WWW.CYLANCE.COM)

Next-generation endpoint security technology detects and blocks viruses, malware and spyware through machine-learning algorithms. Cylance says it's the first to bring a signature-less, 100 percent machine-learning cybersecurity product to market, using technology that spots previously undetectable advanced threats. The company calls itself proactive rather than reactive; its approach relies on advanced mathematics rather than reactive signature- or trust-based systems.

**Primary customers:** Focused on government, Fortune 1000 companies, tech-sector companies and enterprise-level financial services.

**Founded:** July 2012

**Founders:** Stuart McClure and Ryan Permech

## WHAT'S THE MOST DANGEROUS TYPE OF MALWARE TODAY?

"Malware that is targeted to steal a specific set of data from a customer, not compromise an entire system. It's the most dangerous type of malware today. Because it's an under-the-radar attack with a smaller scope and customized to the targeted environment, it can be easily underestimated by the IT departments built to defend it. This is a common threat, especially from Chinese and Russian hackers, who are looking to compromise core American businesses with greater frequency."

— Jon Miller, VP of Strategy

# BITGLASS

[WWW.BITGLASS.COM](http://WWW.BITGLASS.COM)

Bitglass offers enterprise-level data security, touting its ability to secure corporate data anywhere it goes — from the cloud, to the mobile device, and anywhere on the Internet.

Bitglass provides a combination of visibility and data security — access control, data leakage prevention, cloud encryption, file encryption, data tracking/fingerprinting, etc. — in order to provide the appropriate levels of access to cloud data.

**Primary customers:** Multiple industries with emphasis in government, health care, financial services and other heavily regulated environments.

**Founded:** January 2013

**Founders:** Nat Kausik, Anurag Kahol, Anoop Bhattacharjya and Chris Chan

#### WHAT'S THE BIGGEST MISCONCEPTION ABOUT CYBERSECURITY?

“That the cloud is insecure. It's the job of software-as-a-service application providers to ensure that their products are as secure as possible. Many SaaS vendors hire the best and the brightest in IT security, and buy the best security products in order to ensure the security of their customers' data. But they are solely focused on preventing breaches into their infrastructure — things like denial of service attacks, malware outbreaks and widespread data exfiltration events.

There's another set of security risks that cloud app vendors are less concerned with, risks that involve leakage of sensitive corporate data. When sensitive data stored in SaaS apps is not properly controlled, the result can be an inadvertent or malicious leakage of company data, theft of user credentials, regulatory compliance failure, etc. These types of risks are outside of the control of the SaaS application provider.”  
— *Nat Kausik, CEO*

## CLOUDLOCK

[WWW.CLOUDLOCK.COM](http://WWW.CLOUDLOCK.COM)

Offering cloud security for data in Google Apps, Salesforce and more, CloudLock bills itself as the world's only cloud-to-cloud security provider, enabling organizations to enforce regulatory, operational and security compliance easily and effectively. The company extends enterprise security controls to the cloud, responds to next-generation cybersecurity risk within public cloud platforms and increases adoption of SaaS apps.

**Primary customers:** Government agencies include the U.S. Naval Academy, National Defense University and more than 15 other federal departments. Commercial customers include Whirlpool, HBO, Seagate Technology and Pandora.

**Founded:** 2011

**Founders:** Gil Zimmermann, Tsahy Shapsa and Ron Zalkind

#### WHAT'S THE MOST DANGEROUS THREAT AFFECTING ORGANIZATIONS?

“The exponentially growing threat surface represented by mobile and cloud applications and services. Businesses are self-selecting cloud solutions and outpacing traditional IT and security. This means that there is a very large threat surface that is addressed with legacy mindset and solutions.”

#### WHAT'S THE BIGGEST MISCONCEPTION ABOUT CYBERSECURITY?

“That it is an inhibitor. Security is not just for saying no. When used correctly, security enables IT professionals to say yes, and ultimately leads to happier and more productive workforces.”  
— *Ron Zalkind, Co-Founder and CTO*

## FIREEYE

[WWW.FIREEYE.COM](http://WWW.FIREEYE.COM)

FireEye offers protection against targeted attacks aimed at individuals and companies for specific data assets such as national secrets and intellectual property. The company's proprietary hypervisor identifies multistage, multivector attacks.

**Primary customers:** Data companies, retail, financial sector, U.S. government and other governments protecting national secrets.

**Date founded:** 2004

**Founder:** Ashar Aziz

#### WHAT'S THE MOST DANGEROUS THREAT AFFECTING ORGANIZATIONS?

“I would say as you look across governments in general, not just the U.S. federal government, but when you go down to states and localities, the biggest problem they have is not understanding that the data they have is

valuable. ... Even if they think their data isn't important, they may be a steppingstone to another environment [or target].”

#### WHAT'S THE BIGGEST MISCONCEPTION ABOUT CYBERSECURITY?

“You hear the term ‘cyberwar,’ and regardless about how you think about it, it's something that's here, it's not going to change and it's going to be a continuous cat-and-mouse game for many years and for the foreseeable future. ... We have to be diligent 24 by 7.”

— *Tony Cole, VP and Global Government CTO*

## THREATSTREAM

[WWW.THREATSTREAM.COM](http://WWW.THREATSTREAM.COM)

The company enables threat intelligence through actionable advice, priority ranking of an organization's threat intelligence stream, real-time threat detection and algorithmic detection. Facilitating trusted collaboration between organizations, ThreatStream lets customers share threat intelligence findings both publicly or privately to better identify and defend against cyberattacks.

**Primary customers:** Fortune 2000 and government customers.

**Date founded:** 2012 launched in stealth mode, made public February 2014

**Founder:** Greg Martin

#### WHAT'S THE MOST DANGEROUS TYPE OF MALWARE TODAY?

“Password stealers — the low-lying, advanced, persistent threat waiting to capture password information or credit card details. It is inactive for long periods of time while watching network traffic and gathering information. The recently discovered theft of 1.2 billion usernames and passwords [by Russian hackers in August] is a great example. If security teams had a way to share threat information more quickly, these problems would not become such great successes and never make such headlines.”

— *Greg Martin, CTO*

## BITSIGHT

[WWW.BITSIGHTTECH.COM](http://WWW.BITSIGHTTECH.COM)

BitSight claims to secure corporate data anywhere it goes — from the



ARE YOU

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

SEX: F  
SSN: 123-45-6789  
9.5.6

I'M HOMEALONE  
RIGHT NOW

YOUR USERNAME  
YOUR PASSWORD

YOURNAME1234@EM.TL.COM

ID: 120345678

2345 ANYPLACE

ANYTOWN  
AVE, NY 12345

CC#: 47167167  
A2031071 EX: 6-13

YOURSELF?

## PROTECT YOUR IDENTITY BY PRACTICING SAFE HABITS ONLINE.

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

Visit [www.dhs.gov/stopthinkconnect](http://www.dhs.gov/stopthinkconnect) for more information on how to get involved with the Stop.Think.Connect. Campaign.



Homeland  
Security



STOP | THINK | CONNECT™

“New devices are open to exploitation in ways never seen before and can pose a significant risk if not protected.”

cloud, to the mobile device and on the Internet. The company describes its approach as “quantified and evidence-based,” using globally placed Internet sensors to detect malicious activity coming out of an entity’s network.

**Primary customers:** Finance, retail, education, utilities, health care, insurance and more.

**Founded:** 2011

**Founders:** Stephen Boyer and Nagarjuna Venna

#### WHAT’S THE BIGGEST MISCONCEPTION ABOUT CYBERSECURITY?

“Regularly updating [malware code] definitions in anti-virus and firewall systems will be enough to protect the organization from the changing threat landscape. Organizations need to have an active view of their security performance that tracks change over time and provides metrics that can be understood by business executives as well. This way, cybersecurity becomes a strategic business issue instead of a rote task of checking minimum requirements.”

— *Stephen Boyer, Founder and CTO*

## CONFER

[WWW.CONFER.NET](http://WWW.CONFER.NET)

Confer protects servers, laptops, mobile devices and other endpoint users from sophisticated attackers through cloud-based behavioral tracking. The company’s advanced detection and incident response uses a single sensor and gives administrators detailed information on malware — how it got there, when it got there, what it did, etc.

**Primary customers:** Both enterprise and public-sector institutions with deployments ranging from 100-person companies to Fortune 50 companies.

**Founded:** 2013

**Founders:** Jeff Kraemer, Paul Morville and Mark Quinlivan

#### WHAT’S THE MOST DANGEROUS TYPE OF MALWARE TODAY?

“In the past, we worried a lot about destructive attacks such as fast-moving worms, but we don’t see these as much lately and they are easy to detect. We worry a lot more about custom-developed, targeted attacks that are remote-controlled. They fly past anti-virus protection and are very hard to detect from the network. Meanwhile, they provide unfettered access to any information on that machine and can be a leverage point for a broader attack.”

— *Paul Morville, VP of Products*

## VERACODE

[WWW.VERACODE.COM](http://WWW.VERACODE.COM)

Veracode provides a cloud-based platform for application risk assessment and management. The company delivers a widely used cloud-based service for securing a variety of enterprise applications, including Web, mobile, legacy and third-party; identifying application-level threats before they can be exploited by cybercriminals.

**Primary customers:** Global enterprise companies, including three of the top four banks in the Fortune 100 and more than 25 of the world’s top 100 brands.

**Founded:** 2006

**Founders:** Chris Wysopal and Christien Rioux

#### WHAT’S THE BIGGEST MISCONCEPTION ABOUT CYBERSECURITY?

“The biggest misconception is around the need to block attacks from threat actors such as organized crime and nation states, and that protection alone can secure an enterprise. This has created an over-dependence on firewalls and endpoint security, as well as other tool-based security approaches. The reality is, more than 50 percent of attacks target the vulnerabilities in the application layer.”

— *Chris Wysopal, Co-Founder and CTO*

## TRUSTWAVE

[WWW.TRUSTWAVE.COM](http://WWW.TRUSTWAVE.COM)

Trustwave has three main areas of expertise: compliance and risk management, managed security services and threat intelligence research and services. Its 50-plus patents legitimize the company’s security on demand services, offered through its cloud-based portal platform, Trustkeeper.

**Primary customers:** Small businesses to Fortune 500 companies across industries, including government, with services touching 2 million customers in more than 96 countries.

**Founded:** 1995

**Founders:** Robert McCullen and Andrew Bokor

#### WHAT’S THE MOST DANGEROUS THREAT AFFECTING ORGANIZATIONS?

“Unfortunately there is no one single threat that affects all organizations. Every organization has its own unique threat profile based on its industry, business model, adoption of technology (for instance, an e-commerce presence) and internal security awareness. Some industries are more targeted than others, like retail and hospitality. According to Trustwave’s Global Security Report, retail was once again the top industry compromised, making up 35 percent of the attacks investigated in 2013. Food and beverage ranked second at 18 percent and hospitality ranked third at 11 percent.”

— *Karl Sigler, Threat Intelligence Manager* **GT**

Trustwave was named in multiple lawsuits by financial institutions related to the company’s relationship with Target during its massive data breach discovered late last year. While the claims point fingers at Trustwave for failing to spot the retailer’s security vulnerabilities, CEO Robert McCullen called the claims “without merit” in an open letter to customers and business partners. “... Target did not outsource its data security or IT obligations to Trustwave. Trustwave did not monitor Target’s network, nor did Trustwave process cardholder data for Target,” he said.

**Editor’s Note:** Company responses have been edited for length.



# A CITY OF 8 MILLION PEOPLE NEEDS PROVEN SOLUTIONS.

From language to culture to customs, New York's diversity is unparalleled. That presents an enormous challenge to a city that serves over 8 million people. Using DiRAD call center, web, mobile and interactive voice response (IVR) solutions, many of the largest agencies in New York have dramatically improved citizen communication, emergency response and employee accountability.



If we can do it in New York, imagine what we can do for your city.



CONTACT CENTERS



UNIFIED COMMUNICATIONS



INTERACTIVE VOICE RESPONSE



NOTIFICATION AND ALERTING



(518) 438-6000



info@dirad.com



<https://twitter.com/diradtech>



Contract Holder



# Wages of Fear

Ransomware, once a small-time malware problem, has exploded in use, affecting state and local governments. And the extortion software is becoming more sophisticated.

By **Tod Newcombe** / Senior Editor

**D**urham, N.H., is a small college town, near the state's coastline. Aside from the activities on the campus of the University of New Hampshire, not too much happens there. But on the evening of June 5, a Durham police officer opened what appeared to be a legitimate email attachment. By Friday morning, the Durham Police Department's computer system was in serious trouble.

The officer had downloaded CryptoWall, an extortion malware program, more popularly known as ransomware, which encrypts a computer's files and then sends the user a digital ransom note, demanding money to decrypt the infected data. Despite having

the latest in spam filters and anti-virus software, CryptoWall bypassed these lines of defense, forcing Luke Vincent, Durham's IT manager, to take the police server offline, isolate it and recover the encrypted files.

Once a problem overseas and limited to individuals, the latest cybersecurity issue has grown quickly in the U.S. and spread to include businesses, institutions and, yes, government agencies. According to the Multi-State Information Sharing and Analysis Center (MS-ISAC), 26 states and nine local governments report that they have been impacted by ransomware.

"It's not a huge number, but it's not insignificant," said Will Pelgrin, chairman

of MS-ISAC. "It's very time-consuming to defend against, and it preys on the emotional side of the victim as well as the cyber-side of government computing."

Versions of ransomware have been around for years. The earliest types were labeled scareware and involved some mischief, but did little lasting damage and didn't involve financial extortion. But the attacks quickly morphed into financial extortion. Originally a problem in Russia, various types of ransomware began appearing in Europe and then in America by 2011. A report published in 2012 by the security firm Symantec identified at least 16





different versions of ransomware, each one run by a different criminal gang.

The tactics of each type of ransomware may vary, but all follow the same theme: Shame the victim into payment. When someone downloads the trojan software from an email attachment or from what appears to be a legitimate advertisement on a website, it takes over the computer, encrypts certain files and launches an image on the computer screen with a message purporting to be from law enforcement that declares a crime was committed. The message often alleges that the victim has browsed illicit material and must pay a fine.

The amount of the fine varies, according to Richard Stiennon, who has written extensively about cybersecurity. "These gangs are sophisticated; they have their own marketing practices and know the optimum amount to charge." On average the fine is several hundred dollars. But ransomware has proven to be highly profitable for the criminals who are behind the attacks. CryptoLocker, one of the best known extortion malware programs, has generated millions of dollars for the people who run it, according to Rahul Kashyap, chief security architect at Bromium Labs, a security firm.

In June, the Justice Department announced that an international law enforcement operation had successfully disrupted CryptoLocker and had filed criminal charges against the alleged administrator behind the trojan software. But other, more sophisticated versions of the ransomware continue to hit computers. The attack on the police

server in Durham took place a week after CryptoLocker was shut down.

Newer versions, such as CryptoDefense and CryptoWall, have been designed to infect a computer, but the actual attack doesn't occur for several days, allowing the malware to infect backup versions of files as well. When a victim takes down an infected computer, isolates it and then tries to clean and reboot it with backed-up data, the system remains infected.

Ransomware isn't just limited to desktop PCs and servers. The latest versions also infect smartphones, including Android devices, according to experts. "The criminals go where the money is," said Stiennon.

At first glance, it would seem odd that the criminals behind ransomware would choose to attack government computers. But apparently there is some profit to be found in the public sector too. Last year, the police department in the small town of Swansea, Mass., forked over \$750 to recover its files after an employee opened an email with a ransomware attachment.

But according to Kashyap, any organization with legacy computers that don't



**Rami Zakaria, CIO,  
Sacramento County**

JESSICA MULHOLLAND

the threats are time-based. If victims don't pay within a certain amount of time, they will lose the agency's files. There's a timer on the screen that ratchets up the sense of fear, said Kashyap.

But paying the ransom rarely fixes the problem. Victims are usually instructed to purchase an electronic PIN and to enter the number into a box on a screen. At this

**“When people see the ransomware notice on their work PC, they panic, afraid they might lose their job.”**

have the latest in cybersecurity defenses makes them more vulnerable than other computer users. Small towns and cities with older, less sophisticated computer equipment — like Swansea — are likely to be affected. Ransomware attacks tend to be scattershot. CryptoLocker was launched by a sort of drive-by exploitation involving downloads of Java, the software applets that run inside of Web browsers, said Kashyap.

But it's the psychological aspect of ransomware that makes the problem so malicious. "When people see the ransomware notice on their work PC, they panic, afraid they might lose their job," Kashyap said. "They think it's their fault for triggering the attack, so they pay." Adding another layer of fear is that

point, the victim is supposed to receive a decryption key to unlock the computer files. However, this rarely happens, according to the Symantec report. "In actuality, many of the ransomware variants do not even contain the code to uninstall themselves. All the attackers care about is obtaining the payment PIN."

Other experts agree that paying the ransom is a waste of time and money. "Don't pay the ransom, don't negotiate," said Stiennon. "If everybody stopped paying, this form of malware wouldn't continue."

In fact, Stiennon believes ransomware shouldn't be a problem for government at all. "We've had more than 15 years of best practices to learn how to

protect yourself from malware, and more than 50 years of learning that government needs to back up their data all the time,” he said. “That’s the ideal world. Unfortunately we don’t live in it.”

But even the best defenses aren’t perfect. Sacramento County, Calif., recently detected a ransomware attack by CryptoLocker, according to Rami Zakaria, the county’s CIO. “We didn’t respond to the ransom requests and ran our backups, so there was no problem,” he said.

Sacramento County takes its information security seriously, said Zakaria. “We also work with other governments to keep each other informed about what’s happening,” he added. “Good defense is also about good staff training and good [cybersecurity] software. You also want to promote security to your staff and the county employees.”

But Zakaria admitted that protecting a government’s information assets is time-consuming and challenging as the threats constantly evolve and become more

**“We’ve had more than 15 years of best practices to learn how to protect yourself from malware, and more than 50 years of learning that government needs to back up their data all the time. That’s the ideal world. Unfortunately we don’t live in it.”**

sophisticated. “I have four people who dedicate much of their time responding to potential threats and breaches,” he said. “This is the new reality. You have to invest in information security, just as you would an ERP system.”

Zakaria said Sacramento County constantly evaluates its investment in information security to ensure it has adequate protection. That’s an exercise every state or local government should practice. However, the reality is that most governments under-invest when it comes to cybersecurity. While it’s true that ransomware isn’t as serious a problem as a breach, which involves data leakage (once data leaves a government’s premises, it becomes a major security

issue), it nonetheless remains a problem that consumes public-sector resources.

MS-ISAC, which monitors and advises states and localities on cyberthreats, recommends that government agencies practice basic cyberhygiene, which means keeping software up to date, including, of course, anti-virus and anti-malware tools. Governments also need to run a strong awareness campaign to understand how attacks are morphing. But most important of all, is backing up the data.

“You want to minimize your risk,” said Pelgrin. “You need to evaluate how much data you can risk losing. If it’s one day, then your backups need to be daily.” **GT**

[tnewcombe@govtech.com](mailto:tnewcombe@govtech.com)

## When you’re ready for success in a changing world.

You are ready for American Public University.

Choose from more than 180 online degrees and certificates, and gain relevant skills that can be put into practice the same day. From Cybersecurity to Digital Forensics and Cloud Computing, you’ll find respected programs at American Public University—at a cost that’s 20% less than the average published in-state rates at public universities.\*

Visit [StudyatAPU.com/GT](http://StudyatAPU.com/GT)

\*College Board, Trends in College Pricing, 2013

We want you to make an informed decision about the university that’s right for you. For more about our graduation rates, the median debt of students who completed each program, and other important information, visit [www.apu.edu/disclosure](http://www.apu.edu/disclosure).





# NETWORK. LEARN. INNOVATE.

48 cities / Endless possibilities

Connect with your peers in your city.

Albany, NY  
Arlington, TX  
Atlanta, GA  
Augusta, ME  
Austin, TX  
Baton Rouge, LA  
Boston, MA  
Brooklyn, NY  
Charleston, WV  
Chicago, IL  
Columbia, SC  
Columbus, OH

Dallas, TX  
Denver, CO  
Des Moines, IA  
Foster City (Bay Area), CA  
Frankfort, KY  
Harrisburg, PA  
Honolulu, HI  
Houston, TX  
Indianapolis, IN  
Jackson, MS  
Jefferson City, MO  
Juneau, AK

Lansing, MI  
Las Vegas, NV  
Lincoln, NE  
Linthicum, MD  
Little Rock, AR  
Los Angeles, CA  
Madison, WI  
Montgomery, AL  
Miami, FL  
Nashville, TN  
Oklahoma City, OK  
Phoenix, AZ

Raleigh, NC  
Richmond, VA  
Sacramento, CA  
Salem, OR  
Salt Lake City, UT  
Santa Fe, NM  
Springfield, IL  
St. Paul, MN  
Tacoma, WA  
Tallahassee, FL  
Topeka, KS  
Trenton, NJ

**Register or sponsor**  
at [govtech.com/events](http://govtech.com/events)



## Monkey See, Monkey Do

Award-winning nature photographer Marsel van Oosten ventures to the hot springs in Jigokudani, Japan, every winter to capture images of wildlife, including cranes, swans, eagles and snow monkeys. Over the years, the once relatively unknown location grew in popularity, now bustling with visitors and photographers. As one tourist brought her iPhone ever closer to her subject,

a macaque monkey snatched it from her and made a getaway to the middle of the hot spring.

Van Oosten's picture of the event was nominated for the People's Choice Award in the U.K. Natural History Museum's 2014 Wildlife Photographer of the Year contest.

SOURCE: 500PX.COM. PHOTO BY MARSEL VAN OOSTEN

**Sleep in Peace.** Restful sleep often eludes caregivers of Alzheimer's patients, like 15-year-old Kenneth Shinozuka's aunt, who could rarely log much rest while caring for her ailing father at night. Kenneth fashioned a thin pressure sensor that adheres to a foot, sock or shoe and connects via Bluetooth to the smartphone app he designed. His aunt gets an audible alert when his grandfather gets out of bed, keeping her from having to get up every 30 minutes to make sure he is safe. Fueled in part by a \$50,000 Scientific American Science in Action Award, plans are to conduct larger tests at residential care homes and then bring the device to the mass market. SOURCE: CO.EXIST



## FINDING A SMARTPHONE IN A HAYSTACK:

Avalanche and earthquake victims could have a new lifeline in the form of a planelike drone developed at the Swiss Federal Institute of Technology. Even if the phone's owner can't make a call, the drone detects the phone's Wi-Fi signal, triangulating its location within 30 feet. The drone could give people trapped under rubble new hope, as it can pick up weaker signals too, helping direct rescue personnel's search efforts. SOURCE: GIGAOM



## CAPTCHA Gets Gamified

Researchers at the University of Alabama at Birmingham are threatening to make the text CAPTCHA code obsolete. Developed to differentiate human users from computers, CAPTCHA, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart, requires

users to reproduce letters and numbers that appear in distorted form. The method, however, is vulnerable to a relay attack in which people are paid to enter the codes.

Dynamic cognitive game (DCG) CAPTCHAs ask users to interact with images, and the technology shows promise in warding off relay

attacks as well as machine-based hacking attempts. DCGs ask users to grab a particular image, like a boat, and drag and drop it into a nearby dock. Research on the gamelike challenges is supported in part by Comcast and a National Science Foundation grant.

SOURCE: SCIENCE DAILY



# Classroom Management in the 21<sup>st</sup> Century

The last decade has been a whirlwind of evolving technologies, innovative initiatives and first-of-their-kind implementations. With more technology initiatives on the horizon, it's time to hone in on best practices for managing classroom technologies. Limiting botched rollouts, avoiding underutilized investments and smoothly integrating new tools into the classroom should be priorities. The most recent Center for Digital Education Special Report on classroom management tackles all of these issues from a variety of perspectives, by providing tips, best practices and effective strategies.

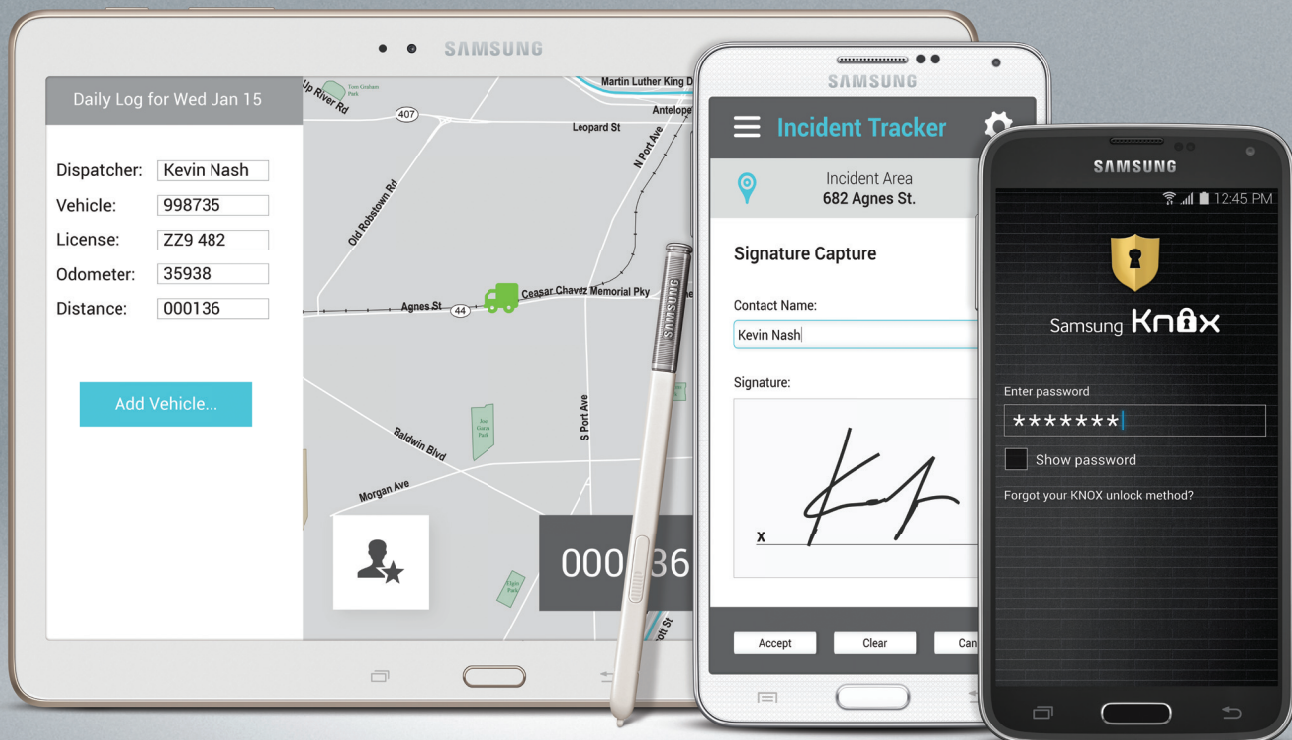
Download the  
Special Report now!  
[www.centerdigitaled.com/  
reports/q3-2014](http://www.centerdigitaled.com/reports/q3-2014)

**Jeremy Shorr**  
*Director of Educational  
Technology and  
Curriculum Innovation,  
Mentor Public Schools*



SAMSUNG

# INCREASE YOUR SECURITY DETAIL.



GALAXY Tab S

GALAXY Note 3

GALAXY S5

Samsung **Knox**

ENHANCED MOBILE SECURITY

LEARN MORE AT [WWW.SAMSUNG.COM/US/KNOX](http://WWW.SAMSUNG.COM/US/KNOX)