BODY CAMS: WHAT YOU NEED TO KNOW
SECURITY: IS CLOUD THE FUTURE?
WHAT’S NEXT: SOFTWARE-DEFINED EVERYTHING

UN-MASKING HACKTIVISM

HOW TO PREPARE FOR CYBERCRIMINALS WITH A POLITICAL AGENDA.

PLUS:
WE PICK GOVERNMENT’S BEST WEBSITES
ATT 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

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

ATT 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

When managing security in an all-IP network, it helps to see the big picture.
29 / What you need to know about deploying body worn cameras.

COLUMNS

4 Point of View
A few things to think about.

10 Becoming Data Smart
Keeping innovation on track.

14 Four Questions
Jane Holl Lute, CEO, Center for Internet Security

16 Open Gov
Opening up Congressional Research Service reports.

20 Data Points
Can data impact the drought?

46 Cybersecurity Strategies
Why we need both breach prevention and response strategies.

50 GovGirl on Social
How to get real-world impact from online input.

NEWS

6 govtech.com/extra
Updates from Government Technology’s daily online news service.

8 Best of the Web
See who ranks in our 20th annual government website survey.

47 Product News
Lenovo storage, Keyboardio ergonomic keyboard, MOTA Samsung battery case.

48 Spectrum
More research, more science, more technology.
A Few Things to Think About

A year ago the shooting of Michael Brown in Ferguson, Mo., by a local police officer helped touch off a national conversation about race and police brutality. Now the Ferguson tragedy—and others like it—are driving several issues that could have a big impact on government IT departments. Perhaps the most directly related of those issues is a looming requirement to store and manage huge amounts of video. Brown’s death last August put new attention on police body cameras. And it’s likely that more and more government IT professionals will be wrestling with how to comply with evolving policies around video captured by these devices. Earlier this summer, we reported that lawmakers in 36 states were reviewing approximately 100 bills related to body worn cameras, according to data from the Security Industry Association. The quantity of video that will be produced by body worn cameras is staggering. A police department with several hundred officers is likely to generate upward of 30 terabytes annually, according to some sources, and warehousing that data could cost millions, depending on how long agencies are required to retain it. In addition, they’ll need to implement processes and tools for finding the video evidence they need in that mountain of material and managing it appropriately.

We take an in-depth look at what all of that means for technology professionals in this month’s Digital Communities special report. These issues are coming your way as policymakers react to nationwide concerns over the use of deadly force by local police. Our report identifies the key IT challenges behind body camera initiatives and gives advice for solving them.

Our cover story examines a related issue: politically motivated hacking aimed at government agencies. During the protests that followed Brown’s shooting, some of that frustration was aimed at state of Missouri computer systems and networks. The state was hit with DDOS attacks to disable websites, SQL injections to infiltrate databases and a phishing campaign to obtain security credentials. These kinds of attacks are becoming more common. We talked to IT and security professionals about lessons learned from the Ferguson protests and other recent events.

Video management and hacktivism are issues that could be heading your way. Now is the time to prepare.
The best value in procurement has a new name.

WSCA-NASPO purchasing cooperative is now NASPO ValuePoint

The National Association of State Procurement Officials’ Purchasing Cooperative

www.naspovaluepoint.org
Innovation Interrupted
In late July, a Senate appropriations committee approved a spending bill that cuts roughly three-fourths of President Obama’s $20.2 million funding request for IT initiatives. Much of the money was tied to the operating budget of the U.S. Digital Service (USDS), the White House tech consulting team. The setback was preceded by yet another in June, when the House of Representatives whittled away the president’s request for $105 million to establish USDS branches in 25 major agencies. In a June 1 statement, the White House and OMB responded by calling the denial in funding a “failure” and “a missed opportunity to improve key agency services.” The larger issue is whether the potential lapse in funding will derail a campaign by USDS to reform federal IT projects.

Details on Diversity
Nashville is digging deeper into its data — the city’s Metro Human Relations Commission and Code for Nashville have unveiled a new data visualization platform that allows the public to view and track diversity within the Metro Government of Nashville and Davidson County, Tenn. The online platform is part of a larger project by the Metro Human Relations Commission to analyze the Metro’s workforce diversity and ensure transparency following the January 2015 release of the commission’s “IncluCivics Report,” which revealed a lack of diversity and a pay equity gap within the government workforce.

WHO SAYS?
“Could go back to flex Fridays and teleworking as our big idea, but if you really think that’s going to make a difference, you’re on crack.”

409
The number of callers met with a busy signal when calling 911 in Las Vegas during an hour-long outage in July, blamed by Metro Police on aging technology.
AN INFRASTRUCTURE FOR THE FUTURE

Building a Strong Foundation for a Scalable Education Environment

From 1:1 tablet deployments to digital content to massive open online courses, innovative technologies are driving student achievement. These solutions and strategies are pushing education institutions into the 21st century, helping them meet new standards and fulfill staff and student expectations. However, unless attention is paid to IT infrastructure first, these new technologies can present more of a challenge than a solution.

The most recent CDE Special Report offers strategies, tools, and real-life examples of challenges and successes experienced by institutions to help others create a strong IT infrastructure foundation.

To download a complimentary copy, visit: www.centerdigitaled.com/reports/q2-2015
Web Royalty
Our picks for the best state and local government websites were released this month in the 20th annual Best of the Web survey. When it comes to delivering online information and transactions, these sites were ranked at the top.

1st Place:
Independence, Mo.
www.independencemo.org

2nd Place:
Louisville, Ky.
www.louisvilleky.gov

3rd Place:
Fort Lauderdale, Fla.
www.fortlauderdale.gov

After the 2014 Best of the Web winners were announced, top-ranked agencies convened to put together best practices to help other jurisdictions achieve similar online success. Here are some snippets of their collective intelligence.

SITE STANDARDS

MOBILE-FIRST
Mobile is the starting point for constituents. Government sites should follow suit.

SIMPLICITY
Eliminate complexity and make it easy to find the most requested information quickly.

ACCESSIBLE
Keep content 508-compliant, consistent across operating systems and support other languages if needed.

RESPONSIVE
A modern government website embraces responsive design.

SEARCHABLE
A sophisticated search function should always be at users’ fingertips.

SECURE
Citizens’ personal information should be protected by strict adherence to the latest cybersecurity standards and practices.

Our picks for the best state and local government websites were released this month in the 20th annual Best of the Web survey. When it comes to delivering online information and transactions, these sites were ranked at the top.

After the 2014 Best of the Web winners were announced, top-ranked agencies convened to put together best practices to help other jurisdictions achieve similar online success. Here are some snippets of their collective intelligence.
1st Place:
Sacramento County, Calif.
www.saccounty.net

2nd Place:
Baltimore County, Md.
www.baltimorecountymd.gov

3rd Place:
Los Angeles County, Calif.
www.lacounty.gov

EARLY BUY-IN
Cast a wide net for stakeholders and start talking early.

DEVELOP THE BUSINESS CASE
A holistic program solves today’s problems and addresses tomorrow’s too.

EXECUTIVE SPONSOR
High-level support is critical to smoothing inevitable bumps in the road.

USER TESTING/QUALITY ASSURANCE
Catch the bugs before launch day by getting user feedback early and often.

AGILE DEVELOPMENT
Embrace iterative, collaborative development practices.

PROJECT GOVERNANCE
A well defined management framework streamlines decisions and oversight.

WINNING TACTICS
Big data can produce big operational and policy breakthroughs. And if not carefully addressed, it can produce even larger privacy concerns or a backlash. To date, most cities have been fortunate to avoid the backlash, but more as a result of good intentions than specific policies.

Preempting problems like these requires explicit policies and deliberate and continuing processes to update them. Cities need to consider data security, rules about guaranteeing anonymity, archival procedures and the ability to conduct forensic internal audits. As Seattle rolls out a citywide digital privacy initiative of unprecedented scale, which is expected to be fully in place by this fall, it looks to integrate the aforementioned measures to prevent such a backlash. Seattle proposes to control the way it collects, uses, retains and deletes data across departments. Leading the initiative is the city’s Department of Information Technology, headed by Chief Technology Officer (CTO) Michael Mattmiller.

To inform the effort, the city created an inter-departmental team (IDT) with members from 11 departments across the city’s government. Seattle also created a Privacy Advisory Committee composed of privacy experts from a broad swath of disciplines to guide the drafting of policies by recommending best practices to the IDT.

The IDT aims to develop policies that allow the city’s privacy practices to evolve as quickly as the ever-changing landscape of digital privacy dictates. As Mattmiller explains: “We can’t legislate or control for every new piece of technology coming into the market. Things are just changing too fast, and often regulation is lagging behind what the market can do.”

Instead, the CTO and his team compiled a list of principles that outline the ways the city wants to consider the public when using data. This ethical framework unites city departments under a shared commitment to processes and policies intended to keep data secure, transparent and accurate, while still allowing them to adapt their practices to the times.

In the next few months, Seattle will provide departments with a “privacy toolkit” to help them comply with these principles. As part of this kit, the city will require departments to complete annual online privacy and security awareness classes to help keep city officials up-to-date on the latest practices. It will also provide them with a Privacy Impact Assessment protocol that requires departments collecting new types of data, embarking on new programs or introducing new technologies to go through a process to self-assess any privacy risk that innovation may entail.

Seattle created a publicly accessible Web page on which departments will be required to share these assessments — part of a larger effort to be transparent about digital changes. By informing citizens of the heightened privacy measures that protect their data and the services the city delivers with that information, this initiative should allay residents’ anxieties about government use of their data, and in doing so, pave the way for future innovation.

Protecting Big Data

Seattle’s digital privacy initiative aims to keep innovation on track with new data safeguards.
When Parks & Recreation Goes High-Tech
Cobb County Modernizes Network to Boost Citizen Satisfaction

Active Citizens Require an Active Network
Most parks and recreation departments in the U.S. are charged with keeping ball fields and green spaces open and groomed for the recreational pleasure of their citizens. But Cobb County, Ga., takes its civic offerings a step further. Serving a population of over 714,000 in the region northwest of Atlanta, the Parks, Recreation and Cultural Affairs department oversees 77 parks that include baseball and soccer fields; tennis centers; two golf courses; a water park; centers for gymnastics, aquatics and the arts; a black box theater; an amphitheater and a civic center — not to mention the classes and events that hundreds of thousands of citizens register for annually.

Those numbers represent a populace that is physically active, appreciative of nature, and consumers of arts and performance. It also reveals a department working hard to provide a diverse set of programs to the best of its ability — but until 2014, there was a major roadblock hindering this.

The county’s legacy network infrastructure could not accommodate the demands of the department’s rich array of services and offerings. Many of its parks and venues are in remote locations, where broadband connectivity can be challenging. And the onslaught of Internet-based and hosted applications required more throughput than the network could provide.

Eddie Canon, Director of Cobb County Parks, Recreation and Cultural Affairs, says the worst part of limited connectivity was wasted time for staff and citizens. “When people tried to register for a class or make a payment, it took a long time,” Canon says. “Even for our staff trying to put information on our website or pull it up for people was causing issues.”

Ed Biggs, the county’s Technical Operations/GIS Manager, says, “If staff had to access documents from the central server or create a financial analysis report, it was slow. All of it was sketchy.”

Ticketing transactions at theaters were a lost cause. Citizens struggled to register for classes online. Information entered into Web-based forms often took a while. To make matters worse, the Parks, Recreation and Cultural Affairs department was just one of many agencies Ed Biggs’ division served county wide. “The county’s Information Services Department handles everything, including 300 to 350 business applications, the data center, database administration, network security, and the technology in police cars and fire trucks. The network is the biggest application we have in the county,” Biggs says. “Whenever there was a slowdown or hiccup in the network, we heard about it pretty quickly.”

Comcast Connectivity Project: A Whole New Ball Game
In 2014, Biggs and Canon outlined these pain points and presented the cost and potential benefits of upgrading the network to the county manager. After receiving the green light and interviewing several vendors, Cobb County ultimately hired Comcast Business to assess and address its network challenges.

Dubbed the “Comcast Connectivity Project,” Comcast Business began by replacing the county’s sluggish legacy DSL lines with 8 Megabits per second (Mbps) Ethernet Virtual Private Lines over Hybrid Fiber/Coax, utilizing a robust cable technology that provided savings on piping and construction costs. A fiber-based 100 Mbps Ethernet Dedicated Internet service boosted speed and capacity for the county’s email and VoIP phone system, as well as other back-office functions such as tax, finance, asset management, HR, courts case management — and parks registration. Following a four-month installation, each Parks, Recreation
The civic center and theaters — as part of an $83 million renovation of the county parks — are being outfitted with new wiring and routers. Additional technology will provide advanced visuals for stagecraft, artwork display and teaching. Event revenue has increased as a result of this improved customer experience.

“This new connectivity has helped us tremendously — it stopped all of our problems,” Canon says. “Just being connected to the rest of the county has helped every facility greatly. It makes a huge difference every day.”

Biggs says the big winners are really citizens, who can now quickly and efficiently interface with the department.

“The quality of our citizen experience is now stable,” he says. “As a citizen of Cobb County, I’m really proud of our parks. The Comcast Connectivity Project was a good solution.”

A Solid Foundation for a High-Tech Future

Recently, Cobb County citizens approved a one-cent Special Local Option Sales Tax that will create a $750 million fund for modernizing technologies in various agencies, including the Parks, Recreation and Cultural Affairs department.

“We have a program for IT to modernize technology over the next six years — to go Web-based and utilize the cloud for a lot of infrastructure needs,” Biggs says. “But connectivity is the main part of that. Having a solid network contributes to the success of all these projects.”

The Ethernet Advantage

Many government entities still recovering from the recession work within the restrictions of slow T1 or DSL networks. However, Ethernet can help these agencies increase employee efficiency and save dollars — while also improving the customer experience and reducing their tax burden.

1. With slow T1 or DSL throughput, the mixed video, data and voice traffic demanded today slowed Internet connections to a crawl — particularly when spread among disparate locations.
2. Ethernet utilizes wide area networks (WAN) to connect separate offices as if they were one network. Heavy traffic to one doesn’t affect the Internet access or speed of the others.
3. DSL is distance sensitive, which can affect speed. Ethernet Dedicated Internet provides a reliably fast connection.
4. T1 has a one-size-fits-all approach, unable to scale up or down. Ethernet Dedicated Internet offers scalable bandwidth with speeds ranging from 1 Mbps to 10 Gbps.
5. Dedicated Ethernet is easily configurable, reliable and secure — important elements for every public agency.

Sponsored by:

COMCAST BUSINESS

Comcast Business offers Internet, Ethernet, Voice and TV for businesses with Internet speeds up to five times faster than DSL, super fast Ethernet, a variety of Voice options and TV. Built for business, customers value the diverse, private network and 24x7 dedicated business support.

Speed comparison between Comcast Business Deluxe 100 Internet and standard 1.5 T1 or DSL (downloads only). Actual speeds vary and are not guaranteed.

© 2015 eRepublic. All rights reserved.
GOVERNMENT TECHNOLOGY™
EVENTS

NETWORK.
LEARN.
INNOVATE.

35 cities... to connect with your peers

Albany, NY  Honolulu, HI
Atlanta, GA  Indianapolis, IN
Augusta, ME  Jackson, MS
Austin, TX  Jefferson City, MO
Boston, MA  Lansing, MI
Brooklyn, NY  Las Vegas, NV
Charleston, WV  Linthicum, MD
Columbus, OH  Little Rock, AR
Denver, CO  Los Angeles, CA
Detroit, MI  Madison, WI
Frankfort, KY  Montgomery, AL
Harrisburg, PA  Nashville, TN
Phoenix, AZ  Richmond, VA
Sacramento, CA  Salem, OR
Salt Lake City, UT  Springfield, IL
St. Paul, MN  Tacoma, WA
Tallahassee, FL  Trenton, NJ

Attend or Sponsor

govtech.com/events
FOUR QUESTIONS

Jane Holl Lute brings a resumé packed with high-ranking government roles to her new position as CEO of the Center for Internet Security (CIS). Lute took the helm in May, following the retirement of longtime cybersecurity champion Will Pelgrin. The Council on CyberSecurity, where Lute most recently served as president and CEO, integrated with CIS in January 2015.

William Pelgrin and I recognized that both organizations had very similar missions and values, and were focused on inclusiveness, transparency and ethics, so integration was a natural next step to building a stronger platform for widespread public access to best practices in cybersecurity.

1. What are some highlights from your years in government service?
My service in the Army represents my first deep, personal appreciation for public service — in particular, as signal officer of the Berlin Brigade during the Cold War, as commander of the Signal Company at Arlington Hall Station and my deployment during Desert Storm. As a U.N. peacekeeper too, I had the extraordinary experience to see both the best and the worst humanity has to offer. Later, as deputy secretary of Homeland Security, especially having been in New York on 9/11, I had the opportunity to work with the country’s finest professionals to help prevent terrorism, strengthen national resilience in the face of disasters and ensure the cybersecurity of the nation’s critical infrastructure. It was amazing to work alongside some of the brightest and most passionate leaders all driven by the same goals.

2. Why did you found the Council on CyberSecurity (CCS)? Why did it make sense to merge with CIS?
We started the council to help identify, validate, promote and sustain best practices in cybersecurity. The game-changer for all of us in cybersecurity will be widespread adoption of basic cyber hygiene as a minimum standard of due care. We stewed the Critical Security Controls for this purpose — not as the only things to do, but as the most important things to do first for sound cybersecurity. CIS and CCS had been collaborating closely for more than a year on a number of different programs and initiatives, including with the National Governors Association’s Homeland Security Advisors Council on the national Cyber Hygiene Campaign.

3. What excites you most about the opportunities ahead as CEO of CIS?
I am excited to be part of an effort to lead the global community to secure our connected world. With the combination of our programs, like CIS’ Security Benchmarks and the Critical Security Controls, our amazingly talented staff and committed partnerships — we want to change the way the world approaches cybersecurity.

4. What are the biggest cybersecurity challenges for state and local governments moving forward?
No single enterprise or government at any level can do all that needs doing to protect themselves in cyberspace — and all that needs doing can’t be done alone. State and local governments, like small and medium-sized businesses, must orient their cybersecurity practices to begin with basic hygiene — the Critical Security Controls are a proven place to start. State and local governments, in particular, are challenged to find the money and talent to stay current as they move more heavily to consolidate operations, mobile platforms and cloud services. CIS will deepen its support to state and local governments, for example, by engaging with them to stand up Information Sharing and Analysis Organizations (ISAOs). Widespread success is good for everyone, and we are in this for the long haul.

— Dan Lohrmann, Government Technology contributor
ARE YOUR DATA SOLUTIONS A PUBLIC DISSERVICE?

New digitization mandates. Sensors. Video surveillance. The proliferation of devices. Big data is putting a big strain on government agencies everywhere. Comcast Business offers robust data services, through a far-reaching Ethernet network, that provide the security, scalability and performance that governments need to power today’s initiatives.

Visit business.comcast.com/government or call 866-429-2241.
TODAY ANY GOVERNMENT CAN SUDDENLY FIND ITSELF THE CENTER OF WORLDWIDE ATTENTION AFTER A DIVISIVE EVENT, DRAWING THE UNWELCOME ATTENTION OF HACKERS WITH A POLITICAL AGENDA. HERE’S HOW TO PREPARE.

COLIN WOOD | STAFF WRITER
"Tim Robertson" has a nice house. It’s a three-bedroom, two-bath American Craftsman, built in 1906, with an American flag flapping on the porch under a canopy of trees that are nearly as old as the house itself. His lawn is neat, just like his neighbors’ yards. Tim seems like the kind who does for himself, so the lawnmower is probably stored in the detached garage, which is out back. You can see it in the satellite image of his property, which is just an 18-minute drive to his office in the city. Yes, it’s just the brand of classical beauty that every American is raised to believe he will one day own.

Tim’s second wife has dropped a few hints that they might move closer to her sister, but he’s moved 12 times in the past 20 years, and at 47, with the kids out of the house, he’s ready to settle down. And besides, when Tim finds something he likes, he tries to stick with it. It’s why he’s had the same phone number for 19 years, the same email address for 16, and it’s why he still uses AOL as his Internet provider. At least, that’s what his IP address shows.

Tim doesn’t have the patience for social media and seems to have gone out of his way not to air any personal business online. And although he’s well educated, having attended two of America’s most esteemed learning institutions, what Tim may not be aware of is that with just two hours of research and $22.31 invested, a journalist from the other side of the country was able to compile a comprehensive profile on his personal life, family, work and criminal history (Tim ran a red light in 2012, but is otherwise clean). Such an investigation is harmless only because the experimenter harbors no ill intent where the mostly law-abiding father of two is concerned, but if a hacktivist group like Anonymous were to decide, for whatever reason, that Tim Robertson was the enemy, all it would take to destroy his life is a little bit of gumption.

TOOLS OF THE TRADE
Scouring the Internet for information about a target and then publishing it to defame or intimidate — doxing — is one of the hacktivist’s most powerful tools. Unlike distributed denial-of-service (DDoS) attacks, network breaches and misinformation campaigns led via social media, doxing is invasive, unstoppable and legal. Most people don’t mind having pictures of their families, homes and pets online for all to see, tagged by date and geographic coordinates, because most people don’t have malicious enemies fueled by political indignation and a sense of justice informed by the Old Testament.

When Michael Brown was fatally shot by a police officer in Ferguson, Mo., late Saturday, Aug. 9, 2014, state and local governments there had more problems than they could handle by Monday morning. Before mistakenly doxing an innocent bystander, Anonymous released St. Louis County Police Chief Jon Belmar’s home address, phone number and a photo of his house. Photos of the chief’s daughter and wife soon began circulating on Twitter, accompanied by veiled threats against his and his family’s safety.

The Anonymous vigilante assault also included DDoS attacks, SQL injection attacks and a phishing campaign launched against the digital infrastructure of Missouri state government, law enforcement agencies and regional governments that weren’t necessarily related to Brown’s death. It doesn’t matter who a person is or what he or she believes — the hacktivist’s shotgun approach to retribution means that anyone might wake up to find they’ve become collateral damage in the next big furor.

The targets of Anonymous’ ire all share in common some violation of the group’s...
moral code, usually a perceived abuse of power, but its targets are so diverse and far-flung that it’s difficult to say who might be next. Since cutting its hacktivist teeth in 2008, Anonymous has rallied against Sony, PayPal, Visa, MasterCard, the Motion Picture Association of America, ISIS, Koch Industries, the Westboro Baptist Church, the New York Stock Exchange, and the federal governments of the U.S., Australia, Uganda, Israel, Canada, Tunisia and Egypt, along with assorted private individuals and smaller companies that each transgressed against the group’s sense of propriety in some fashion.

MISSOURI UNDER ATTACK

When Missouri was attacked by Anonymous, it was half ready. Michael Roling, the state’s chief information security officer, said Missouri did an impressive job minimizing the impact of the attacks, but if he could go back in time, there are a couple of things he would do differently.

The attacks came in three forms: DDoS attacks to disable websites, SQL injections to infiltrate databases and a phishing campaign to obtain security credentials. The state had a security plan in place when the attacks struck, but it hadn’t been fully implemented and staff weren’t quite ready, especially for the DDoS, Roling said, which started in the middle of the night on the weekend.

“Some of our better partners were sleeping,” he said. “The large DDoS partners, we had a difficult time reaching them, so that was one instance where I wish we’d have had those relationships in place much sooner. Some of the vendors wanted a $20,000 or $40,000 emergency setup fee. We had to figure out, ‘Do we want to go that route?’ Do we want to wake up our attorneys? Do we want to wake up purchasing?"

Ultimately, Roling said, the attacks improved the state’s security posture. Even today, the baseline for attacks against Missouri remains elevated compared to before Brown’s death, and the state now contracts with several new vendors to manage security operations. Missouri uses a managed DNS provider, border gateway protocol and application-layer protection to mitigate DDoS attacks.

Groups like Anonymous attack their enemies to prove a point. They want to show the government, or whomever, that evil deeds don’t go unpunished. It’s out of a perceived lack of legitimate recourse that hacktivists disable websites and make personal threats, but of the 10,000 arrows fired, many land on innocent villagers. Roling didn’t shoot anyone, but he and the rest of the state’s IT team are the ones left picking up the pieces. The more time and money the state spends on its cybersecurity, the less taxpayer funding there is left for citizen services. The people Anonymous wants to advocate for are the same ones footing the $40,000 emergency setup fees and new vendor contracts. Anonymous might mean well, but pestering the state won’t stop the next race riot. It’s just another thing that poorly funded state and local governments must worry about.

“The biggest shame in all this is just seeing some governments doing nothing, and they just get pounded over and over again,” Roling said. “Anonymous goes after the easy, soft targets, and it’ll continue to go after those soft targets until they have hardened. I think the biggest thing is it impacts the citizens’ trust in their government.”

As of 2015, Anonymous has become synonymous with serious, grass-roots political movements, but the group’s more puerile roots continue to color its activism. Tens of thousands of angry street activists in Guy Fawkes masks are unlikely to be convinced anytime soon that their efforts are less constructive than imagined, because their actions do generate a lot of attention, if nothing else. And those more sensible participants who would concede that point are not the ones government is worried about, anyway. The biggest threat posed by any group lies in the most extreme elements of its membership.

ANSWERS IN THE FORM OF BEST PRACTICES

Preparing for hacktivist attacks is similar to preparing for any other kind of cyberattack, said Bret Brasso, vice president of state and local government sales at security firm FireEye. “One of the key challenges, right at the outset, is the unpredictability,” he said.

Using the American legal system’s “means, opportunity and motive” device is a useful starting point for understanding hacktivists, Brasso explained. States face sophisticated attacks from other nations that have more means than hacktivists and organized crime groups might develop, and connections that create better opportunities than what hacktivists have, but hacktivists are the most motivated.

“How does one prepare for that? It’s almost impossible, because you never know when an incident like that is going to occur or if someone says something publicly that’s going to create an outrage,” Brasso said. “It puts state and local entities in a very reactive situation, and about the best the can do when something is going on like that and the media starts to focus on it is [recognize] that’s probably a good indicator that they should start to consider the possibility that hacktivist groups might take an interest.”

Preparing for hacktivism differs little from other forms of cyberdefense. Control frameworks like the one outlined by the National Institutes of Standards and Technology are good road maps for governments, Brasso said. Even if organizations aren’t ready to implement every piece of the framework, they can know where they stand compared to where they should be. Tools include things like firewalls, advanced malware protection, intrusion prevention tools, vulnerability assessment tools and education to prevent simple mistakes by employees.

In March 2014, Albuquerque, N.M., faced attacks from Anonymous after police fatally shot James Boyd, a schizophrenic homeless man who had been camping in the wilderness. Albuquerque CIO Peter
Luke Stowe, digital services coordinator for Evanston, Ill., said one of the best things governments can do when it comes to any disaster is to prepare and plan ahead. Fake social media accounts, for instance, have more influence when the government being spoofed doesn’t have a legitimate online presence to begin with.

“Make sure you have a robust social media presence up and running, because a lot of these government agencies are slow to adopt and waiting until after that natural disaster hits to start a Twitter account, [but] it’s too late,” Stowe said. “You want to build up those relationships ahead of time.”

There are many basic measures governments can take, Stowe said, like getting verified status on Twitter and using two-factor authentication, but when it comes to avoiding the release of someone’s family photos, there may not be a good answer.

“It’s the million-dollar question,” he said.

An official from the FBI’s Cyber Division, who asked to not be identified, said it’s the small and medium-sized organizations that are hit hardest by hacktivism because they’re not ready. State and local governments should expect DDoS attacks and have a mitigation plan and vendor relationships in place, he said. Governments should monitor how often their networks are being pinged so they can quickly recognize when an attack has begun.

“There are many basic measures governments can take, Stowe said, like getting verified status on Twitter and using two-factor authentication, but when it comes to avoiding the release of someone’s family photos, there may not be a good answer.”

“It’s the million-dollar question,” he said.

An official from the FBI’s Cyber Division, who asked to not be identified, said it’s the small and medium-sized organizations that are hit hardest by hacktivism because they’re the ones that aren’t ready. State and local governments should expect DDoS attacks and have a mitigation plan and vendor relationships in place, he said. Governments should monitor how often their networks are being pinged so they can quickly recognize when an attack has begun.

Because the minute it starts happening, it’s kind of too late,” he said. “If you don’t already have that set up, you’re going to be victim of it and there’s not a whole lot that the federal government can do to help you during the actual attack. … The simple fact of it is if someone wants to get into your system, if you get someone who has the skill set, it’s just a matter of persistence. They’re going to find a way.”

Once due diligence has been done, the most realistic advice — both for the hacktivists who rail against immutable forces of human nature and the governments that increasingly fall victim to their flailing — comes from the author of Treasure Island, Robert Louis Stevenson, who wrote that, “Our business in life is not to succeed, but to continue to fail in good spirits.”

Ambs said that cyberattacks like those are essentially tests of how well you’ve been maintaining your security posture all along. As in Missouri, the biggest challenge, he said, is establishing all the right relationships before your city’s name starts appearing in the headlines. The attacks brought down the Albuquerque police department’s website for a few hours, and by working with groups like the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the FBI, the city was able to mitigate the attacks, Ambs said.

“I think any state or local organization is just one step away that you can’t predict, in terms of hacktivism, that a threat will appear,” he said. “It doesn’t have to be a police brutality situation. It can be anything that’s perceived as a social injustice.”

Ambs admitted that where doxing is concerned, there’s little anyone can do except not to release any personal information in the first place. “If I want to promote and tweet city information, I use the city Twitter account. We’ve got a robust social media presence with the city, and so it is a conundrum. We’re expected to be very active in the social media environment, and you just have to be smart about what’s being publicized.”

Albuquerque considers itself a leader in open data and transparency too, Ambs said, but those issues, in combination with emerging technologies like police body cameras, make the line between good practice and threat to the public servant a thin one.

“Everybody’s demanding transparency and open government, as well as establishment of the right relationships before your city’s name starts appearing in the headlines,” Ambs said. “In the online world, everything that has a good motive also can be exploited.”

“EVERYBODY’S DEMANDING TRANSPARENCY AND OPEN GOVERNMENT, AS WELL WE SHOULD, BUT IN THE ONLINE WORLD, EVERYTHING THAT HAS A GOOD MOTIVE ALSO CAN BE EXPLOITED.”

Ambs said that cyberattacks like those are essentially tests of how well you’ve been maintaining your security posture all along. As in Missouri, the biggest challenge, he said, is establishing all the right relationships before your city’s name starts appearing in the headlines. The attacks brought down the Albuquerque police department’s website for a few hours, and by working with groups like the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the FBI, the city was able to mitigate the attacks, Ambs said.

“I think any state or local organization is just one step away that you can’t predict, in terms of hacktivism, that a threat will appear,” he said. “It doesn’t have to be a police brutality situation. It can be anything that’s perceived as a social injustice.”

Ambs admitted that where doxing is concerned, there’s little anyone can do except not to release any personal information in the first place. “If I want to promote and tweet city information, I use the city Twitter account. We’ve got a robust social media presence with the city, and so it is a conundrum. We’re expected to be very active in the social media environment, and you just have to be smart about what’s being publicized.”

Albuquerque considers itself a leader in open data and transparency too, Ambs said, but those issues, in combination with emerging technologies like police body cameras, make the line between good practice and threat to the public servant a thin one.

“Everybody’s demanding transparency and open government, as well as establishment of the right relationships before your city’s name starts appearing in the headlines,” Ambs said. “In the online world, everything that has a good motive also can be exploited.”

Luke Stowe, digital services coordinator for Evanston, Ill., said one of the best things governments can do when it comes to any disaster is to prepare and plan ahead. Fake social media accounts, for instance, have more influence when the government being spoofed doesn’t have a legitimate online presence to begin with.

“Make sure you have a robust social media presence up and running, because a lot of these government agencies are slow to adopt and waiting until after that natural disaster hits to start a Twitter account, [but] it’s too late,” Stowe said. “You want to build up those relationships ahead of time.”

There are many basic measures governments can take, Stowe said, like getting verified status on Twitter and using two-factor authentication, but when it comes to avoiding the release of someone’s family photos, there may not be a good answer.

“It’s the million-dollar question,” he said.

An official from the FBI’s Cyber Division, who asked to not be identified, said it’s the small and medium-sized organizations that are hit hardest by hacktivism because they’re the ones that aren’t ready. State and local governments should expect DDoS attacks and have a mitigation plan and vendor relationships in place, he said. Governments should monitor how often their networks are being pinged so they can quickly recognize when an attack has begun.

“Because the minute it starts happening, it’s kind of too late,” he said. “If you don’t already have that set up, you’re going to be victim of it and there’s not a whole lot that the federal government can do to help you during the actual attack. … The simple fact of it is if someone wants to get into your system, if you get someone who has the skill set, it’s just a matter of persistence. They’re going to find a way.”

Once due diligence has been done, the most realistic advice — both for the hacktivists who rail against immutable forces of human nature and the governments that increasingly fall victim to their flailing — comes from the author of Treasure Island, Robert Louis Stevenson, who wrote that, “Our business in life is not to succeed, but to continue to fail in good spirits.”
Five cities enter the City Accelerator to adopt new practices that better engage low-income residents in civic life and public decision-making.

Follow their progress at www.governing.com/cityaccelerator
Is security the next as-a-service offering you’ll be sending to the cloud?

Washington state uses a mix of hosted and on-site security solutions, says CISO Agnes Kirk.
As IT leaders have grown more comfortable with the security of software-as-a-service offerings and cloud storage, they also have started turning to cloud-based managed security services. For both commoditized basic services such as vulnerability testing and cloud security gateways to more sophisticated identity management and threat analysis, public-sector chief information security officers are growing more willing to consider managed security service providers (MSSPs).

Cost savings are one obvious consideration, but so is the fact that state and local governments are finding it next to impossible to compete with the private sector for cybersecurity talent. In a 2015 NASCIO state government IT workforce study, 67 percent of respondents said security was the most difficult position to fill and retain.

“Security is becoming highly specialized, and we are having a very difficult time finding appropriate people to do in-house security,” said Ralph Johnson, chief information security and privacy officer of King County, Wash., whereas a managed security services team often has the expertise and concentration he needs. For example, King County uses a managed security service for its network log and security event management. “For me to appropriately run that with an in-house solution, I would have had to hire three staffers and that would have been their sole function,” Johnson explained. “That would cost me $1.5 million over five years. I got a managed security product from a vendor that cost me $850,000 over the same time period.”

The decision to consider managed security services is akin to other outsourcing decisions, in that the most generic pieces are the easiest to give away, said Wolfgang Kandek, chief technical officer of Qualys Inc., which offers a suite of Web-based security and compliance applications. “Email is an example,” Kandek explained. “It’s important in terms of productivity, but not a distinguishing characteristic of your organization, so why devote your IT resources to running the best email system possible? “You can easily outsource and free up some people to work on more noble things in IT,” he said. “The
same thing is happening with security. A bunch of things in security can be automated and given away to third parties.”

A 2014 Gartner market trend report predicted that the cloud-based security services market—which includes secure email or Web gateways, identity and access management, remote vulnerability assessment, security information, and event management—would hit $4.13 billion by 2017.

King County is just starting to redesign a security process around public key infrastructure certificate authorities. “My staff is not expert enough to do what I want to do,” Johnson said. This function should never be in-house unless an agency has staff members who can properly manage it, he added. There are service providers that have the expertise and the processes in place for revoking and issuing certificates. “We don’t have to build it,” he said. “They have already got it, and the prices are reasonable.”

In terms of what to outsource, organizations tend to start with reactive security, such as firewalls and intrusion detection systems, and then move to more proactive threat intelligence, seeking to gain visibility into their environment through security information and event management tools, said Christina Richmond, IDC’s program director for security services. Proactive security, she said, involves gathering threat intelligence not just from your network but also from a broader group of networks. Managed security services can help customers gain visibility into aspects of security that CISOs are comfortable outsourcing depend on the overall IT environment. “The first step is usually looking at commoditized security activities—things that are resource-intensive, costly and they don’t want to do them anymore,” said Montecillo, who once served as the vulnerability management coordinator in Michigan’s Office of Enterprise Security. He makes a distinction between very small organizations, like town governments, where typically there are a few IT staffers who work on network infrastructure and also are responsible for security, and a state agency that might have a CISO and a more mature approach. (IBM survey research found that organizations that have a CISO are likelier to adopt security as a service from the cloud.)

With more applications moving to the cloud and users increasingly mobile, cloud services will be the only way to do security.

Mike Montecillo, director of security intelligence for IBM Security, said that the aspects of security that CISOs are comfortable outsourcing depend on the overall IT environment. “The first step is usually looking at commoditized security activities—things that are resource-intensive, costly and they don’t want to do them anymore,” said Montecillo, who once served as the vulnerability management coordinator in Michigan’s Office of Enterprise Security. He makes a distinction between very small organizations, like town governments, where typically there are a few IT staffers who work on network infrastructure and also are responsible for security, and a state agency that might have a CISO and a more mature approach. (IBM survey research found that organizations that have a CISO are likelier to adopt security as a service from the cloud.)

**Services on the Road Map**

“When you have a CISO, you are developing a road map and identifying services you can outsource to maintain your capability or enhance it,” Montecillo said. “But in a smaller environment, you don’t have that road map, and the adoption of these services tends to be more ad hoc, which slows the adoption rate. You might have five issues in security, but the budget to only move one to an as-a-service model now. Which one do you pick?”

Jim Moore, IT director of Woodstock, Ga., is the type of IT executive who turns to security services out of necessity. With only a three-person department, he automates whatever he can. “We are 24/7 with police and fire, which you can’t really cover with three people,” he said. “Extending your staff with a service, you

The IBM Center for Applied Insights recently interviewed 138 security leaders, who indicated their likelihood of adopting one or more of the following security functions as-a-service:

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption/key management as a service</td>
<td>48%</td>
</tr>
<tr>
<td>Security monitoring as a service</td>
<td>46%</td>
</tr>
<tr>
<td>Application security scanning as a service</td>
<td>42%</td>
</tr>
<tr>
<td>Cloud security gateway as a service</td>
<td>41%</td>
</tr>
<tr>
<td>Identity as a service</td>
<td>31%</td>
</tr>
</tbody>
</table>

**With more applications moving to the cloud and users increasingly mobile, cloud services will be the only way to do security.**
have people who think about security all the time, deal with it rather than being one of the 40 or 50 hats we have to wear.” Woodstock implemented Microsoft Office 365 earlier this year and has turned to Web-based Centrify for Office 365 for Active Directory-based user provisioning, single sign-on and mobile management. Employees can access all Office 365 clients and other SaaS, mobile and on-premises apps through a Centrify user portal.

“The Human Resources Department uses several online resources,” Moore said. “One of our HR employees literally kept a notebook with all the various log-ins. If that person left or if they left that notebook somewhere, we could have had a security issue.” The city also uses Mimecast, a cloud-based email security solution that provides protection from malware, spam and data leakage, he added. Edward Block, CSIO of Texas, said small to medium-sized state agencies are more likely to turn to managed services. “The idea that they would have a firewall expert on staff is not really realistic,” Block said. “They don't need a firewall expert 40 hours a week. They need it 40 hours a month, or even a year. So if they go with an MSSP, they can procure someone who lives and breathes that technology for the period of time they need it. They are not sacrificing expertise by trying to find a jack-of-all-trades.”

*Identity as a Service*

Although its IT structure is federated rather than consolidated, the Texas Department of Information Resources is planning to do a feasibility study for a statewide identity access management solution. “We will look at whether it makes sense to do that internally or if it is better suited as an outsourced, cloud-based service,” Block said. But not all CISOs are comfortable with the idea of identity and access management in the cloud. “I don’t support outsourcing the keys to the kingdom,” said Agnes Kirk, CISO for Washington state. “That authentication and ID management are how we ensure we are protecting privacy and data entrusted to us.”

IBM’s Montecillo said identity and access management as a service could have a lot of benefits. “The caution is if you don’t have a strategy in place, and you don’t understand what some of the iterative steps are to be able to adopt that model, you could get in trouble if you try to jump from step one to step five without progressing along a maturity curve.” A good service provider will work with clients to help them develop the road map and integrate that capability in a model where they can avoid pitfalls, he added.

Security is becoming highly specialized, and we are having a very difficult time finding appropriate people to do in-house security.

Washington is both a customer of MSSPs for services like vulnerability assessments and a service provider itself. The central IT organization offers a variety of services to state agencies. The state provides a set of common security services that agencies use so they don’t have to duplicate the cost and effort of implementation. These include perimeter security, logging and monitoring, forward proxy services, a secure single sign-on portal to state applications, and vulnerability management. The cost is covered by the state through an internal transfer process. “We are finding a good mix between on-premises and cloud services, and we make that determination through a full risk assessment,” Kirk said. “We continually evaluate managed services offerings to determine when it makes sense to leverage a third party.”

Public-sector organizations have some challenges not faced by the private sector, Kirk added. As states move to provide services anywhere, anytime, it becomes harder to keep track of information and ensure it’s appropriately protected. As the state outsources various types of services, the requirement to find and retrieve information does not change or transfer to third parties, she noted. “That means you must have the ability to know where your data is, who touched it and when, retrieve all copies of it, and provide it in a timely fashion,” she said. “If the state does not manage its third-party relationships well, that could create unexpected risk.”

Like many other states, to augment its services and expertise, Washington turns to Multi-State Information Sharing Analysis Center (MS-ISAC) services such as log analysis and threat information sharing. “They provide information that is specific not only to our state but all the other states,” Kirk said. “That makes them a valuable partner in the security space. If we have an incident and need to quickly analyze logs to determine the extent, MS-ISAC has a free service to do that for us. They are great at that.” (MS-ISAC is funded by the U.S. Department of Homeland Security and provides most of its services at no cost to state and local governments.)

The need for security services is increasing because so much more data traffic from employees is bound for the Internet rather than the data center. “You still need to protect the data centers in a traditional way, but all Internet traffic needs to go through security checkpoints, and a Web service makes sense for that,” said Jay Chaudhry, CEO of Zscaler, a multi-tenant, cloud-based security platform. “We exist in a world where the Internet is the new data center.”

So for example, he said, New York now points the Internet-bound traffic of state employees to Zscaler, which also works with other states, counties and school districts. “We are acting as a checkpoint to make sure nothing bad comes in and nothing leaks out,” Chaudhry said. “Email security and vulnerability assessment are now done regularly in the cloud. The next natural step is to have the traffic headed to the Internet go through a checkpoint to be inspected. With more applications moving to the cloud and users increasingly mobile, cloud services will be the only way to do security.”
SOFTWARE-DEFINED EVERYTHING

Completely virtualized data centers may be the future for large, sophisticated jurisdictions. But they're still a few years away.

By Brian Heaton
Contributing Writer

Government agencies have been steadily consolidating and in some cases outsourcing their IT infrastructure over the last several years, seeking improved efficiency and better performance. And while that activity continues, some organizations have their sights set on the next phase of the technology evolution — the virtualization of entire data centers. While many would imagine the topography of data centers to consist of rows of server racks with cables snaking among hundreds, if not thousands, of machines, there’s a new vision of how those centers should be run and organized. Instead of having people physically plug in wires based on client needs, there’s a push to revolutionize data centers so those changes can be made remotely.
Welcome to the concept of software-defined data centers (SDDCs). The clinical definition sounds simple: a data center where all the infrastructure and four major layers — compute, storage, network and security — are virtualized and delivered as a service.

Thanks to software-defined networking, most data center tasks can now be done from a keyboard. Once servers are plugged in and installed, all the configuration that previously was done manually can be completed from a single desktop.

Chris McClendon, technology services officer for the Georgia Technology Authority, got a glimpse of the future during a visit to one of Microsoft’s Azure data centers in Virginia. The data center needed people to “run around with crash carts” replacing hard drives, but the real technical work was done at the company’s headquarters in Washington state, he said. “All the administration, all the logical stuff is done out in Redmond [Wash.].”

Although growing use of virtualization is pushing data centers in this direction, experts say fully functioning SDDCs are still a couple of years away for government agencies.

ADOPTION CHALLENGES

Utah and Georgia have started the transition toward running SDDCs, but neither state is close to full deployment. Utah completed the virtualization of its compute layer, but the state is still undergoing active testing of technologies in the other three layers. So it’s only about a quarter-mile down the road to completion.

Georgia’s data center is split in half. Steve Nichols, the state’s chief technology officer, explained that when you walk in the door, the left side is dedicated to legacy equipment and the right side is “all the new stuff” that’s controlled remotely. But like Utah, the state has only completed a fraction of the changes needed to launch a true SDDC. However, Georgia has been running a software-defined networking network for years.

Nichols said the new data center technology is a tradeoff. While the state doesn’t need personnel to physically stand up new servers because it can be done virtually, there’s been an increase in lead time and planning to determine just how to make it all happen remotely. “It hasn’t necessarily made things go faster for us,” Nichols said. “It’s just sort of shifted the work around.”

Bob Woolley, Utah’s chief technical architect, added that the subject is complex for government agencies, because there are policy and skill issues to address, along with the four separate layers IT personnel need to consider. It could take up to a decade for some governments to reach a full SDDC implementation. “You just can’t flip the switch,” Woolley said. “The compute layer is already happening, as virtualization is pretty common now. The storage layer will probably start happening this year, and the network layer isn’t going to be too far behind. But states have huge investments in network infrastructure. I think I have $16 million worth of switches; you just don’t throw that away. It’s a practical matter.”

Moving to an SDDC can provide a variety of benefits, but not necessarily immediate cost savings. The primary gain is the same as virtualizing any component of an agency’s IT environment — flexibility, according to Miguel Gamino, CIO of San Francisco.

Many experts use the word “scalability” to describe SDDCs, but Gamino thinks that’s too limiting a term. “I refer...
to it as 'elasticity'; because it also allows you to shrink your footprint as dynamically as you can grow it,” he said. “It’s a bidirectional opportunity that lets you be more efficient with how you’re using your infrastructure and resources.”

Financially the jury’s still out on whether governments will save a significant amount of money by moving to an SDDC. Utah has saved more than $4 million by virtualizing the compute layer and expects similar financial savings as it progresses to the others. But Georgia isn’t pursuing an SDDC thinking about the return on investment, said Nichols. Instead, it’s about getting the state’s data center in a place where everything can be managed remotely and homogenously.

Both Nichols and Woolley said the transition to an SDDC will have an impact on the IT workforce.

“We need smarter people who really understand routing and … we needed those people to begin with,” Nichols said. “But it sort of changes the work so that instead of them designing it and having some guys with screwdrivers in their back pockets running around on the floor, then they also become the guys who are typing the commands in the console to make it so.”

Woolley agreed that moving to an SDDC requires an upfront investment and an “upskilling” of IT staff. But he also said most public-sector technologists already have many of the skills necessary to make the move.

From an architectural standpoint, there’s opportunity to think very differently about what the IT agency does. That shift may already be happening, Woolley said, noting that most governments are going to wind up with hybrid computing environments that include both on-premises and cloud-based resources.

Thanks to software-defined networking, most data center tasks can now be done from a keyboard. Once servers are plugged in and installed, all the configuration that previously was done manually can be completed from a single desktop.

That combination begins to look “an awful lot like a software-defined data center if provisioned correctly,” he said. “I think the migration is more natural than unnatural, but it’s going to take time.”

It’s a mistake to consider SDDC and cloud strategy as separate issues, Woolley added. “CIOs are focusing on how they get their customers and themselves to use the cloud and how to make it make financial sense. They’re not thinking about rebuilding infrastructure on the SDDC level. They look at that as something to do later; I think that lends itself to a lot of potential errors.”

Gamino likened the transition to software-defined data centers to the transition to voice over Internet protocol (VoIP) phone service. He recalled that when VoIP went mainstream with government agencies, “classically trained” telecom engineers had to choose whether to retrain or retire. Those working for Gamino when that happened were able to not only make the change, but also to thrive in the new environment. “It’s a matter of the attitude and appetite of the workforce itself, rather than a question of whether the people are competent enough to learn new skills.”

GOOD CANDIDATES

So which governments should look to make the move to an SDDC? It depends on size and maturity. These deployments may make the most sense for very large, sophisticated organizations.

“We’re formal, but there are people a lot more formal than us,” Nichols said. “We’re large, but there are others hundreds of times larger than us. So we’re kind of on that border of getting some value, but we’re not in a situation of a Google, where they might have to do something like this because it’s the only way they can scale to being able to manage millions of servers.”

Woolley cautioned that there are other challenges to consider too. First and foremost are the impacts on an agency’s budgetary environment. Once services are automated, that will impact how chargebacks, metering and billing are done, because all the various IT pieces aren’t controlled in the same way.

Georgia’s McClendon said individual organizations either need to work toward moving their IT operations into a managed service provider environment or they need to keep it fairly simple. He added that pursuing an SDDC will depend on just how much an organization believes it can handle work-wise. Despite those questions, Gamino appears to be all-in. He plans to get there in the next couple of years, calling San Francisco’s IT maturity at the front edge of the curve: “We’ll let the private sector and other people nickel and dime the bleeding edge, but we’re right behind that.”

Utah and Georgia are moving closer to having operational SDDCs. But neither Woolley nor Nichols would reveal just when they thought their respective shops would get there. It’ll likely be a few years.
Health + Human Services:
Realizing Better Outcomes at a Cost Governments Can Afford

How do we provide effective, comprehensive care and services in a way that is fiscally sustainable? This is one of the biggest challenges HHS agencies face as they seek stable ground five years post-ACA. Read this Special Report from the Governing Institute and the Center for Digital Government for information on how HHS agencies can:

- Improve outcomes and reduce redundancies by integrating health and human services programs
- Increase access with smarter policies and technologies, including telemedicine
- Prevent costly health and social problems from occurring in the first place
- Gain insights from data to make better decisions and reduce fraud

Download a complimentary copy of the report at: governing.com/papers

A Special Report on Health and Human Services

SPONSORED BY:
FOR THE RECORD:
UNDERSTANDING THE TECHNOLOGY
BEHIND BODY WORN CAMERAS
INTEREST IN BODY WORN CAMERAS IS GROWING FAST. HERE ARE SOME ISSUES TO CONSIDER BEFORE YOU DEPLOY.

It’s been a year since the shooting of unarmed black teenager Michael Brown, which sparked riots in Ferguson, Mo., that lasted for days. In that short time span, a number of other deadly incidents involving young black men and police officers have occurred, triggering a national debate about the use of deadly force by police officers.

At the same time, another discussion has emerged, one that put forward the idea that creating a record of interactions between the police and the public might defuse simmering disputes, improve officer safety and mitigate allegations of racial profiling. The idea of using cameras to record interactions isn’t new. In the past decade, police departments have installed more than 17,500 cameras in police cars, according to the International Association of Chiefs of Police (IACP).

But a program where police wear body cameras to record their interactions is still a rather new, and little-tested concept. Two years ago, only a handful of police departments used body worn cameras (BWC). Today, there are various estimates that put the number of law enforcement agencies using, or investigating BWCs at as many as 6,000 out of 18,000 nationwide.

The huge jump in interest has elevated what was once a niche technology for public safety into a major growth market. The federal government has pushed it further with $20 million in grants to fund BWC pilot projects. The grants are part of President Obama’s proposal to invest $75 million over three years to purchase 50,000 body worn cameras for law enforcement agencies.

Driving the growth in BWCs are many benefits that go beyond the accountability of police officers and the public. They include transparency, increased professionalism, more peaceful civil interactions and even potential cost savings on internal affairs investigations into possible wrongdoing by officers as well as settlements of lawsuits stemming from the use of excessive force. Every year, law enforcement agencies spend hundreds of millions of dollars to settle claims. New York City spent $348 million on settlements and judgments between 2006 and 2011, according to the Huffington Post. Chicago spent a whopping $521 million between 2004 and 2014. The list goes on.

As quickly as interest in the technology has grown, so too have the questions surrounding both the policies needed to govern a workable BWC program, and the technology that would make recording and retaining these police interactions a feasible solution. Like any technology project, BWCs can impact a range of systems, and require project management skills in order to avoid failure. Besides evaluating the attributes of the cameras themselves, CIOs face a major issue in terms of video storage. The amount of data generated by digital video is huge, making storage...
The best defense against viruses, malware and bots? Anticipating them.

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 city and county 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 safeguard all the elements of your IP infrastructure.

To learn more, download the CIO Security Guide at att.com/govsecurity
costly. The use of cloud services as a storage option raises a host of issues that local CIOs are just begin-
ing to grapple with. BWCS will also impact other IT systems used by police depart-
ments, including but not limited to computer aided dispatch, records and
evidence management systems, content management systems and so on. There are concerns around security, support and training. Finally, and perhaps most importantly, there’s the question of cost. Data storage costs can reach $2 million annually for a
department, according to the Police Executive Research Forum.

Local CIOs will have a host of consider-
ations to sift through when their jurisdiction decides to implement a BWCS program in the police department. This report will walk through some of the key technological questions that confront local jurisdictions as they weigh the costs and benefits of body cameras.

IT STARTS WITH THE CAMERA

In 2006, police officers in the United Kingdom tested body cameras and found that the technology enhanced the collection of hard-to-refute evidence and resulted in fewer cases going to trial. In 2012, a similar field test took place with the Rialto, Calif., Police Department. The 12-month experiment randomly tested body cameras on officers during their shifts. The cops used cameras from Taser International, which were water resistant, captured video in full color and had a battery life of 12 hours. The test results were startling. When the cameras were turned on, use of force by officers dropped 60 percent and complaints against the police fell nearly 40 percent.

These early positive results have opened the floodgates to BWCS programs across the country. As CIOs and police departments begin to evaluate the systems that can capture and store video, the cameras themselves provide a glimpse at the complexity in options that have to be weighed, both from a field operations perspec-
tive as well as from the impact on policies that govern how and when cameras and videos are to be used. Overall, the camera hardware can be light (cameras used by Rialto police weighed just 4 ounces). Their light weight enables officers to wear cameras in a variety of positions: head, shoulder or chest, for example. In Rialto, the police tried different types of gear and eventually found they liked cameras that fit on their sunglasses or cap. One advan-
tage of a head-worn camera is that it will record what the officer is looking at, while chest or shoulder-worn cameras only record what’s in front of the body.

In 2013, the Phoenix Police Depart-
ment evaluated the impact of BWCS and used the following parameters when they procured cameras for the officers:

“Standard cameras are likely to have image quality issues (e.g., fuzzy pictures and poor quality at night) as compared to more high-end cameras due to technical compromises to manage costs. There can also be quality issues with stability. For example, when an officer is running or fighting, the video may be shaky and the camera may not be secure; this again links back to placement of the camera on the officer being extremely important. Some feel that head camera placement allows the head to act as a natural gyroscope to reduce some motion issues seen with cameras.”

DHS provides some more specific issues that police should consider when choosing a type of camera:

“Camera should provide a minimum of three hours of recording.

5 / The camera should have a low lux rating to allow for recording events in low light.

6 / System should have a minimum one-year warranty.

The Department of Homeland Security (DHS), which established the System Assessment and Validation for First Responders Program to objectively assess and validate commercial equipment, came up with the following recommendations for BWCS:

1 / An image resolution of at least 640 x 480 pixels.

2 / A frame rate of at least 25 frames per second.

3 / A battery runtime that allows a camera to record continuously for at least three hours.

4 / The camera’s onboard storage, set at the lowest video quality setting, should be able to capture a minimum of three hours of recording.

25 frames per second.
that police would have the ability to view the recently recorded video footage on the scene of an incident. The field of vision of the device needed to be at least 50 degrees. The department also wanted officers to have the ability to turn off the night vision function, if there was one, and to be able to change the placement of the device to several locations, including the ear, shoulder and lapel. Finally, there could not be more than two wires on the device, and it would need to have the capacity to automatically label video files with the date and time of the recording.

The Phoenix Police Department tested different camera models. Some of the findings showed officers could get confused with camera features like the pre-record option on some cameras, which retains 30 seconds of video prior to an officer activating a recording. Many officers found this option to be a liability, according to a 2015 report, Evaluating the Impact of Officer Body Worn Cameras. Officers also had reservations about cameras equipped with night vision capabilities. Apparently some officers believed courts and prosecutors would view much clearer images of what happened compared to what officers actually saw, putting their personal conduct at risk in terms of how it might be judged.

Findings from the PPD study showed officers were much likelier to agree that the camera is easy to use (61.8 percent), comfortable to wear (57.6 percent), and that its battery life is adequate (65.6 percent). The officers were much less likely to agree that it is easy to locate and retrieve a video for a specific event (26.5 percent) and that it’s easy to download data at the end of the shift (23.5 percent).

DATA STORAGE: THE GORILLA IN THE ROOM

When the Chula Vista, Calif., Police Department started giving body worn cameras to a handful of police officers, they quickly learned that a 30-minute video took about 800 MB of storage space. The department crunched the numbers and realized that if it equipped every one of its 200 sworn officers with cameras, they could potentially generate 33 terabytes of data every year, according to Police Chief Magazine.

When it comes to BWCs, data storage is the 800-pound gorilla in the room. Video, as every CIO knows, is a data hog. And BWC systems can produce vast amounts of video data, as well as the metadata to track and manage the video clips for retention and chain of custody purposes. Data storage is a technology issue and it’s one that CIOs try to address in the most cost-effective manner.

But in the case of BWCs, policy is inextricably linked to the question of storage. Retention policies can play havoc with the portion of a BWC budget that’s dedicated to storage. Some jurisdictions say non-evidentiary video should only be kept for 60 to 90 days. Some departments say it should be longer, others say less. The Oakland, Calif., Police Department, which currently has 600 BWCs deployed, retains video for a remarkable five years. As a result, storage needs have grown significantly over the past couple of years and the department now captures on average almost 7 TB of video data per month, according to Officer Dave Burke. And if a video becomes evidence in a court case, the retention requirements can be even longer. “What if there’s an appeal in the case 10 years down the road?” asked a CIO. “What are the requirements and policies for handling those scenarios?”

Many cities, under pressure to implement BWCs, have found data storage and related costs to be a major stumbling block. Last year, Baltimore Mayor
whether the system includes protections, such as audit trails and backup. The National Institute of Justice points out that as video becomes more important to a police department, storage adjustments will need to be made. “The length of storage time can cost numerous man hours in addition to the actual costs of the storage device.” It goes on to say that advanced data storage systems can provide end-to-end data management that includes safeguards to control data handling and assist in chain-of-custody control.

THE CLOUD OPTION

The use of cloud technology as part of a BWC storage solution really hasn’t been on the radar for police departments because most cloud computing platforms don’t meet the FBI’s Criminal Justice Information Services (CJIS) requirements. In a 2013 survey of state and local law enforcement officials by the International Association of Chiefs of Police, the Ponemon Institute reported that 15 percent were using cloud technology for storage; 35 percent were considering it; and 50 percent were not pursuing it at all. But the situation has changed recently as some big vendors — most notably Microsoft — now offer cloud storage that meets FBI requirements. With the standardization of cloud storage (and other capabilities) police departments have an opportunity to gain from some of the cloud’s more recognized benefits: cost-effectiveness, scalability and access to innovation. Savings estimates, when comparing cloud storage to an on-premises solution, can range between 30 and 60 percent, according to industry analysts. These benefits are buttressed by the IACP survey, which found that state and local law enforcement officials were comfortable using third-party storage solutions, but to consider the vendor’s technical capabilities and whether the system includes protections, such as audit trails and backup. The Police Executive Research Foundation (PERF) released a report on BWCs in 2014 (Implementing a Body-Worn Camera Program) that looked at existing BWC programs around the country and developed a list of key lessons learned when it comes to data storage:

✓ Consult with prosecutors and legal advisors.
✓ Explicitly prohibit data tampering, editing and copying.
✓ Include protections against tampering with the data prior to downloading.
✓ Create an auditing system.
✓ Explicitly state who will be authorized to access data.
✓ Ensure there is a reliable backup system.
✓ Specify when videos will be downloaded from the camera to the storage system and who will download them.
✓ Consider third-party vendors carefully.

For the final point, PERF reported that police departments, legal advisers and prosecutors were comfortable using third-party storage solutions, but to consider the vendor’s technical capabilities and whether the system includes protections, such as audit trails and backup. The National Institute of Justice points out that as video becomes more important to a police department, storage adjustments will need to be made. “The length of storage time can cost numerous man hours in addition to the actual costs of the storage device.” It goes on to say that advanced data storage systems can provide end-to-end data management that includes safeguards to control data handling and assist in chain-of-custody control.

BIPARTISAN SUPPORT FOR MORE BODY CAMERAS ON POLICE OFFICERS

More police officers wearing body cameras to record interactions would be...

<table>
<thead>
<tr>
<th></th>
<th>Bad idea</th>
<th>Good idea</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>100</td>
<td>77</td>
</tr>
<tr>
<td>White</td>
<td>100</td>
<td>76</td>
</tr>
<tr>
<td>Black</td>
<td>100</td>
<td>84</td>
</tr>
<tr>
<td>Hispanic</td>
<td>100</td>
<td>84</td>
</tr>
<tr>
<td>Republican</td>
<td>100</td>
<td>90</td>
</tr>
<tr>
<td>Democrat</td>
<td>100</td>
<td>90</td>
</tr>
<tr>
<td>Independent</td>
<td>100</td>
<td>90</td>
</tr>
</tbody>
</table>

Survey conducted Dec. 3-7, 2014. “Don’t know” responses not shown. Whites and blacks include only non-Hispanics; Hispanics are of any race. Source: Pew Research Study/USA Today

Stephanie Rawlings-Blake vetoed a BWC proposal after concluding that data storage costs and other details were not sufficiently taken into account. Baltimore city officials estimated video storage costs at as much as $2.6 million annually.

Experts agree that issues concerning privacy must be balanced with storage capacity, transparency and state laws. The Police Executive Research Foundation (PERF) released a report on BWCs in 2014 (Implementing a Body-Worn Camera Program) that looked at existing BWC programs around the country and developed a list of key lessons learned when it comes to data storage:
Harnessing the Power of the Cloud

Government agencies are striving to do more with less. By shifting to cloud computing, your agency can reduce infrastructure, equipment, software and staff resourcing requirements while giving your citizens access to the services they need.

The Accela Civic Platform and suites of cloud-based solutions can modernize the way your agency operates, communicates and shares information.

With Accela, you’ll spend less time worrying about your infrastructure and more time engaging your citizens to build more connected communities.

Connecting citizens and government

See how the power of the Civic Platform can work for you.

www.accela.com/cloudebook

©2015 Accela, Inc. All rights reserved.
(52 percent), and to take advantage of new innovations (31 percent).

The city of Oakland, which as more than 600 BWCS deployed, had been storing video in an in-house system for five years. But that retention policy had overburdened the department’s servers. The department considered reducing the number of years to three, but ended up opting for a CJIS-compliant cloud solution from VIEVU, a Seattle-based maker of BWCS that runs on Microsoft’s Azure Government Cloud platform.

The solution is expected to give the Oakland police almost unlimited room to store video. Officer Dave Burke told Government Technology in February. The platform will let the department use digital signatures to verify a video’s authenticity, should it later be used in court; it will also generate a running audit log of the video database and provide courtroom-ready transcriptions.

Other technical considerations for a video storage solution, whether cloud-based or on-premises, would be advanced search and analytical tools that include facial recognition to help narrow down the relevant video for evaluation. Storage tools should also support the redaction of visual content to protect the privacy of people who interact with police but are not part of any investigation.

PARADIGM SHIFT FOR EVIDENCE MANAGEMENT

Recently the New Mexico Supreme Court ruled that when a district attorney’s office opens a case, police departments must have all evidence in place within 10 days or less. In other words, documents, physical evidence, images, recordings and any video has to be turned over in that time. Such policies have put pressure on police departments to have consolidated evidence management systems that are up to the task.

The Albuquerque Police Department (APD) has a management system for physical evidence, but not one that can take into account all the new digital evidence the department now collects from more than 600 officers who are equipped with cameras. “We want to be able to package all that up in an electronic manner and provide it to the DA’s office without any delay in delivery,” said Rishma Khimji, interim director of APD’s tech services.

A BWCS system can touch a number of other critical police information systems, ranging from CAD and records management to content management. But evidence management is the one system that will experience the biggest impact from video. In Dubuhr, Minn., the city’s 11 BWCS are generating 8,000 to 10,000 videos per month, according to Police Chief Gordon Ramsay. The Rialto, Calif., Police Department generated 2.3 million videos over a three-year period. With that amount of video evidence entering a police department’s overall evidence database, the need for a robust, enterprise management system becomes more crucial.

An evidence management system automates search and retrieval, organizes evidence data, provides security safeguards, creates a workflow, and can report, track and audit evidence from the moment it is captured on the camera to the time of disposition. Well-designed evidence management systems automate much of the workload done by users, while expanding the effectiveness of the data, not to mention distributing it more broadly across a law enforcement agency. As the scope of evidence management expands, it presents certain IT challenges. First, backup and disaster recovery become critical as evidence management software and data assume a workload once managed by users and with paper. Second, security becomes more essential as the amount of digital evidence increases. In addition, IT can expect to develop an archiving strategy, including offline storage, and prepare for growth as the scope of BWCS undoubt-edly balloons. All of these factors can be further impacted by policies and future policy changes.

Albuquerque’s physical evidence management system creates an elec-tronic catalog of every physical item that gets barcoded and stored for later retrieval. The police department would like to create a similar process for its video evidence. “What we need is a video evidence system that allows for an easy way for officers to enter what they have captured both from BWCS as well as backup cameras carried by some personnel,” said Khimji. Besides images, video and physical items, the system also must capture and catalog 911 calls and other audio recordings as well. In other words, APD could use a sophisticated, consolidated evidence management system to meet its growing needs.

“The amount of evidence we have to give the DA’s office is so large that we have to come up with the right kind of evidence repository system that will contain all that information, based on the case and officer,” she added. The Santa Clara, Calif., Police Department has created an evidence manage-
Better security for a better organization.

Are you ready for an end-to-end IT security solution that enables your government agency?

Discover how IT security can enable growth at Dell.com/security.
ment system to catalog all of the digital evidence officers collect. IT provides a customized security level access, a documented chain of custody and a nearly automatic sharing of digital evidence. The system is used by approximately 100 people in the city’s District Attorney’s office and they have the ability to stream video or download files.

HOW PRIVACY DRIVES VIDEO SECURITY

The single biggest nontechnical issue dominating any discussion about the use of BWCs is privacy. Deciding when to record an interaction remains a controversial subject. Some advocates of BWCs say all interactions between police and the public should be recorded, while others would like to see officers use discretion in deciding when to record. Meanwhile, in 12 states there are laws that require all parties to consent before any recording can occur.

The policy considerations on this issue are lengthy and detailed, and to cover them effectively is outside the scope of this report. But it raises a fundamental IT consideration: security. The last thing any elected local official wants to see is headlines in the local paper about a data breach exposing hundreds or thousands of video files. For that reason alone, CIOs will need to practice due diligence in planning how the security of the video files will be handled.

When it comes to an on-premises solution, CIOs will have to weigh such questions as “how much” and “how good” along with access. For law enforcement agencies that are considering a regional storage solution, decisions will need to take into account the security implications of such a system. Cloud storage solutions can provide some law enforcement agencies, especially small ones, with a degree of security they may not be able to develop on their own. But as the Police Executive Research Forum points out, a cloud solution requires CIOs and law enforcement agencies to perform their due diligence in ensuring that chain of custody for the video is properly established. Other security points to consider when evaluating a third-party cloud storage solution include:

✓ Work with a reputable vendor.
✓ Enter into a legal contract that governs the vendor relationship and protects the agency’s data.

VIDEO’S HIGH COSTS (AND SOME COST-SAVING IDEAS)

More than three-quarters of the nation’s 20 largest city police forces use body cameras or plan to do so, but none are using BWCs with all of their officers, according to a 2015 survey by the news agency Reuters. Nearly all cited costs as the reason why BWC use isn’t more widespread.

In a national survey of law enforcement agencies last year, 39 percent said they had no plans to use BWCs primarily because of cost considerations, according to PERF. With so many cities still struggling to regain their fiscal footing after years of retrenchment and cuts that affected police departments, it’s not surprising that BWCs are having a rough time moving from plan to pilot to full implementation.

Cameras range in cost from $150 to $1,000, though most average around $300 to $500 apiece. But docking stations can easily cost more than $1,000, and then there’s storage and digital evidence systems to help automate the cataloging of what can become a flood of new data. It all adds up. For example, San Diego plans to equip 1,000 patrol officers with cameras by the end of the year; first-year costs are expected to hit $1 million, with a large portion of that going to data storage. In Duluth, Minn., the police department spent...
Sometimes it’s the things you can’t see that make all the difference. When citizens feel safe and secure, big, amazing, powerful things can happen in cities and across businesses. Citizens are free to create, to innovate and to celebrate.

As a global leader in Mission Critical communications, we understand the information flowing between citizens, businesses and emergency personnel is the intelligence that helps build safer cities.

We are building on Mission Critical Communications to bring you Mission Critical Intelligence, helping you avert, respond to and resolve incidents.

Visit www.motorolasolutions.com to learn more.
$5,000 for 84 cameras and charging bays. But its three-year contract for data storage cost the department $78,000.

Besides hardware and software costs, police departments report having to appoint at least one full-time officer to manage a BWC program. This person administers the BWCs, handles training, helps with tech support and even ensures BWC policy compliance among officers.

An indirect cost that can be overlooked is the extra time officers have to spend reviewing and categorizing videos, making sure they are properly tagged and loaded into the database. This is where the choice of evidence management or records management technology can play a role. More sophisticated solutions can automate some or most of the legwork that many officers currently have to handle manually.

When it comes to cost-saving strategies, there is little in the way of low-hanging fruit. But there are several ways that the overall expense of a BWC program can be reduced, according to PERF.

One recommendation is to reduce the retention time for non-evidentiary video. Oakland currently holds all videos for five years, and some BWC advocates recommend that cops record every interaction they have while on the beat. But that’s a costly burden. The Greensboro, NC, Police Department has a less comprehensive recording policy, but still has managed to produce 40,000 videos in just seven months.

Another challenge is responding to records requests. As the use of video becomes more widespread, police organizations such as PERF and IACP expect that cops record every altercation with the police and post the images online. It makes sense to law enforcement leaders that the police do the same, to ensure there is a fair and objective record of what occurred.

It’s a great example of how technology keeps changing, forcing government policy makers and practitioners to play catchup. Technology has given the police a variety of tools to wage war on crime while providing the public with the kind of public safety they expect.

In recent years, police departments have put cameras on the dashboards of cruisers to record interactions with the public. They have mounted special cameras on their vehicles that can read license plates to look for possible matches with stolen cars and for drivers involved in a crime.

But once again, technology has leaped ahead and now the public can record incidents that the police once had control over. At the same time, BWCs also are having a very nontechnical impact on both officers and the public. As the study of BWCs in Rialto, Calif., revealed, when a camera is turned on, there is a certain self-awareness and conduct changes.

Everyone behaves better.

All of these factors have prompted public officials to push hard for BWCs. But what research and experience shows is that rushing toward a technological solution to a complex problem is fraught with potential failure. Setting down IT plans for BWCs before policies on privacy, retention and evidence management have been hashed out will make rollout harder and more expensive.

The public, local leaders and law enforcement agencies want to move rapidly on testing and deploying BWCs. The technology is hot and it works. But local CIOs and their counterparts in the police departments are in the middle. They have to make sure everything works and is cost-effective when the switch is turned on and cameras start recording. It will take a great deal of experience, leadership, even consensus-building, to make sure a technology program like this is done the right way.
Digital Communities are real places that understand and value the transformative power of broadband connectivity, core computing technologies and interoperable applications to improve the way government conducts business and interacts with citizens. The Digital Communities Program showcases solutions from leading technology companies that are specifically designed for communities and local governments that want to exceed the expectations of their citizens. In addition, the program provides a collaboration forum where community officials discover and share emerging best practices and innovative community technology deployments.
When Congress created the Congressional Research Service (CRS) in 1914, it envisioned a government entity that would gather and analyze data to inform the legislative process. In the decades since, the CRS has continued to produce hundreds of valuable, comprehensive, nonpartisan reports on legislative issues each year for members of Congress and their staffs. But CRS reports aren’t just an essential tool for policymaking. They’re also a valuable instrument for informing the public about issues that affect our country each and every day. CRS reports are unclassified and cover topics ranging from incarceration rates in the U.S., to economic impacts of individual budget and appropriations bills, to international responses to natural disasters, and everything in between.

After 100 years, it’s time to make this broad collection of information and analysis available and accessible to the public. Taxpayers spend more than $100 million each year to fund the CRS, and its unclassified reports belong in the public domain.

In a June editorial, The New York Times echoed the call of groups like the Sunlight Foundation that have been advocating for years for the reports to be made public. “As the Library of Congress, which will soon get a new leader, takes long-overdue steps to modernize digital access, lawmakers and library officials must find a way to make the service’s valuable work readily available,” The Times wrote. “Those expert reports give taxpayers a richer understanding of the issues and choices their representatives deal with.”

Legislation recently introduced in the House of Representatives would direct the Clerk of the House and the CRS to host the reports in a centralized electronic database that makes the information searchable and available for bulk download. The CRS could easily do this by hosting the reports on Congress.gov, which already serves as a central portal for legislative branch information. In fact, the agency does already make reports available to select audiences who know where to find them and who to ask. Some private companies with access to the reports have even started charging subscription fees for them. It makes little sense to withhold the reports from the general public, but to allow private companies to charge for access to research paid for by taxpayers.

But instead of being proactive and making the information readily available to anyone who wants it, the CRS has stalled efforts over the past 15 years to make its reports public by claiming that increased access to the information would impede its relationship with Congress and direct public comments and ire its way.

Over the last 100 years, CRS reports have become essential to the policymaking process: Members of Congress and their staffs rely on them for everything from basic research on a new topic, to writing legislation, to making decisions on how they will vote and more. The public deserves access to this window into the governing process in order to better understand how elected officials establish positions on, and make decisions about, vital policy matters.

Window into Public Policy
It’s time to make Congressional Research Service reports easily accessible to everyone.
Q&A: Why All-Flash Storage is the Next Step for Government Data Centers

It’s no secret that the amount of data government agencies must store is increasing at a rapid rate. What used to be measured in megabytes and gigabytes is now petabytes and exabytes — and this growth shows no signs of slowing. But government agencies can’t just build more data centers to house this data — there must be a more efficient and cost-effective solution. In this Q&A, Melanie Stevens, Director, State and Local Government and Education, discusses why all-flash is an important next step in the storage evolution for government agencies.

Q: What is all-flash and why is it important for government agencies to consider? Melanie Stevens: Many government agencies are facing a storage dilemma in their data centers. Their need for storage is growing, but there is insufficient funding to purchase new equipment and limited budget for IT staff, space, power and cooling.

Across the data center, we see increasing speed and lower cost in many networking devices, such as servers and switches. However, storage has failed to keep up because of the way mechanical disk works. Capacity and cost have grown, but performance has stayed flat. Because of this, the performance per gigabyte of disk is getting slower. Flash memory is faster, has more space and is much more power efficient than disk.

The Pure Storage all-flash storage array meets the availability, reliability and scalability requirements of government agencies. It reduces flash storage to a price point that makes it cost effective for distributed deployments. Our all-flash storage array is cost competitive and more efficient to administer than disk, so it’s a logical next step for government data centers.

Q: What are some of the major challenges all-flash can help government agencies overcome? Melanie Stevens: In the past decade, we’ve seen the widespread adoption of virtualization in the data center. This has had an amazing impact on the efficiency of how state agencies do business. Server consolidation now supports ratios around 20:1 per physical server, and that number climbs with every new release of a processor. For government agencies, this means being able to do more with less, and faster.

At the same time, virtualization creates its own challenges for storage. Virtualization is only as efficient as the storage on which it runs, and it requires more resources than the pre-virtualization era. This issue is compounded by applications such as virtual desktop infrastructure (VDI), which is commonly used to support kiosks, mobile workforces and online services offered by state agencies. While government agencies have realized ROI from server consolidation, they have to turn around and spend those savings on additional storage. As end users continue to virtualize more applications, disk arrays will only get more expensive and put government agencies further behind in the budget battle.

Pure Storage provides the technology that allows government to maximize the benefits of virtualization, without inflated storage costs. So, whether the application is to manage database requirements, virtual desktop or server infrastructure, our all-flash storage array allows for maximum performance without the usual backend cost.

Q: How is Pure Storage FlashStack Converged Infrastructure unique? Melanie Stevens: FlashStack is unique because it takes our all-flash storage array from a standalone solution, and combines it with a leading technology provider for an enhanced data center solution. FlashStack is built upon trusted hardware from Cisco and Pure Storage. FlashStack leverages Cisco’s flexible and expandable Unified Computing System (UCS) to provide the compute horsepower, Cisco Nexus for networking and Pure Storage’s own FlashArray 400 Series as the storage foundation. Managed by a single point of support supplied by FlashStack authorized support partners, FlashStack provides a modular and powerful infrastructure that is simple to use, deploy and maintain, while providing an architecture that suits a wide variety of application requirements.

Pure Storage FlashStack Converged Infrastructure provides a predefined, complete technology stack that is:

• Repeatable, creating a scalable building block that can be easily replicated at any customer site
• Virtualized, enabling every infrastructure component to run in a virtual machine (VM)
• Available, making the design resilient and not prone to failure of a single component
• Cost-effective, meaning agencies can take advantage of inline data reduction and low latency of the Pure Storage FlashArray by pushing the envelope on VMs per server density
• Simple, minimizing tweaks and configuration changes (from defaults) to streamline the deployment process

For more information, visit: www.purestorage.com
Can Data Impact the Drought?

Smart infrastructure can help policymakers make the most use of limited water resources.

Policymakers are pushing residents and businesses to cut back on their water use in response to the severe drought gripping many parts of the western U.S. California Gov. Jerry Brown has even gone so far as to declare a state of emergency and impose restrictions intended to reduce water usage by 25 percent across the state. While there is no silver bullet that will solve the water crisis, policymakers have many opportunities to use data from connected devices to improve conservation. In particular, states should accelerate water utilities’ deployment of smart meters to better manage water use and make communities more sustainable.

This would be a major improvement, considering how many homes and businesses have no metering at all and simply pay a flat rate for water. There were approximately a quarter-million last year in California alone, and those unmetered customers used almost 40 percent more water per capita than the state average. The problem is severe enough that California passed a law requiring utilities to install meters for all customers by 2025. But there is also the problem of legacy analog meters that many homes and business already have. They have to be read manually every few months, which is both expensive and prone to human error.

That is why utilities are now starting to replace them with smart meters. To cut costs and improve accuracy, utilities have begun installing meters with automatic meter reading (AMR) technology that transmits water usage data to the utility electronically. Workers collect usage data from these meters by driving around in vehicles equipped with specialized wireless receivers. In addition, some utilities have moved beyond AMR solutions and begun to deploy smart meters that not only allow utilities to collect detailed usage data — often in real time over a fixed network — but that also are capable of receiving information. For example, a utility can remotely shut off service to a customer that is moving. These meters further cut down on in-person service visits by utility workers and save the utility money — savings that can then be passed on to consumers.

The benefits of smart meters go beyond enhanced productivity. By providing consumers and utilities real-time data, the meters can help customers use water more efficiently. Utilities using real-time data can detect problems in their water distribution system or alert homeowners of potential leaks. Startups like WaterSmart Software work with utilities to analyze smart meter data and communicate personalized recommendations to customers about how they can improve water-use efficiency and save money. The potential payoff from automatic leak detection is substantial. Nationwide, household leaks waste more than 1 trillion gallons of water annually. For homeowners, real-time alerts can allow them to fix leaks sooner rather than months later, after receiving a high water bill or discovering water damage. Every year, water damage from leaks costs homeowners and insurers billions of dollars in property losses.

The U.S. is still in the early stages of deploying smart water meters. Nationwide, less than 20 percent of the 100 million metered water customers have smart meters. However, where smart meters have gained a foothold, communities have seen substantial savings. For example, after Mumbai launched an ambitious smart metering program, it was able to cut in half the 150 million gallons of water lost per day from leaks. Smart meters can also help spot businesses or homeowners who ignore mandatory water restrictions. For example, the water utility in Long Beach, Calif., has used smart meter data to enforce water restrictions on customers who previously ignored complaints about their waste. Longer-term, better smart meter data can help policymakers maximize limited resources, by prioritizing water efficiency grants for the most effective updates to businesses and homes or deploying pricing models that reward efficiency. Deploying smart infrastructure requires capital investments, tech-savvy public administrators and visionary regulators — all of which are too often in short supply. Yet the broader water problems are not going away. Communities that successfully navigate these obstacles will be best positioned to meet new water challenges in the years ahead.
Driving Performance and Improving Decision-Making

Data and analytics is the combination of two powerful computing trends in government. States and localities are beginning to amass huge amounts of structured and unstructured data, and are using the algorithms in analytics software programs to make more informed decisions. This is resulting in saved time and resources for agencies and citizens alike. The most recent Center for Digital Government Public CIO Special Report sheds light on the technology requirements for increasing amounts of data and the governance necessary to make sound judgements based on analytics — including the benefits, challenges and real-life examples of implementing big data analytics initiatives.

Download your complimentary copy at: govtech.com/2015Q3report

SPONSORS:

OPENTEXT  workday  TERADATA

workday  TERADATA  redhat

VION  HITACHI  PURE

STORAGE

BLACK  YELLOW  MAGENTA  CYAN

®  CMY grey  T1  T2  T3
The Security Paradox
Why breach prevention and response strategies are both essential.

Are breaches inevitable? That simple question is dividing the technology world today. Depending on who you talk to within the cybersecurity industry, the answer is either a simple yes or a battle cry to fight international surrender in cyberspace. But be warned: Asking this “indefinite” question is a loaded with hidden traps. Your answer will likely affect your enterprise-wide cybersecurity priorities and overall security funding strategy.

Breaches Everywhere
First we have a sea of scary breach headlines along with consistent problems keeping sensitive data out of enemy hands. Late last year FBI Director James Comey proclaimed that Chinese hackers have invaded every major U.S. company. Comey also said the Chinese aren’t very good at covering their tracks. “Their strategy seems to be: We’ll just be everywhere all the time. And there’s no way they can stop us.”

There are also well known lines from leading technology CEOs like former Cisco head John Chambers, who said, “There are two types of companies: Those who have been hacked, and those who don’t yet know they have been hacked.”

One “security manifesto” lays out philosophical and technological arguments for why breaches are inevitable, including the way the Internet is built, problems with business partner connectivity, trouble with employee Web-surfing habits and even new technology deployments with vulnerabilities. But it doesn’t stop there. In fact, the “not if, but when” champions make the case that your IT security dollars should be spent on incident response and network redesign, and not on breach prevention.

Rick Holland, a security and risk management analyst at Forrester Research, told the BBC that companies must redesign networks to respond faster to the inevitable breach. “This involves separating one part of the network from another in such a way that if hackers get onto the network, they only get access to the data in that segment and no more.”

Not So Fast
But not everyone thinks breaches are inevitable. Invincia CEO Anup Ghosh told Washington news site DC Inno that breach prevention is possible, proclaiming “breach inevitability” is just marketing. Ghosh mocked competitors: “You cannot stop the breach. So don’t even try. … To me that’s a self-serving message. What you’re really saying is, ‘Don’t invest in prevention because you’ll never stop the threat.’”

And those arguing for more investments in new technologies to stop breaches point to the National Institute of Standards and Technology (NIST) Cybersecurity Framework to make their case. The framework includes five core functions: identify, protect, detect, respond and recover. As a Harvard Law article points out, agencies must demonstrate due care, “Organizations can potentially avoid the inevitable conclusion (or parallel accusation by a plaintiff’s attorney) that they were ‘negligent’ or ‘inattentive’ to cybersecurity best practices following disclosure of a cyberbreach.”

Is There a Middle Ground?
Back in early 2013, I was one of the first cyberpros to ask: “Are data breaches inevitable?” The context was slightly different at that time, as I was clearly placing myself in the “yes” camp. My goal was to encourage improved cyberincident response capabilities.

But the debate has evolved. Proponents of the “inevitable breaches” idea are now moving to almost throw in the towel against hackers. With Ghosh, I think this is a mistake.

Why? Consider banks, which despite knowing that robberies will happen, have numerous processes and procedures in place to stop criminals. From cameras to guards to timed vaults, banks have adapted to new threats to inhibit bank robberies, as well as respond to incidents when they do happen. No doubt the bad guys are ahead of the good guys regarding cybercrime today. But there is still hope. Some breaches, like bank robberies, may be inevitable. Nevertheless, your local branch getting robbed is not a foregone conclusion.

Bottom line: Build your security priorities around all five NIST Cybersecurity Framework functions. “All of the above” is a third option to prepare for inevitable cyberattacks.
For more product news, log on to explore Government Technology’s Product Source.

govtech.com/products

By Miriam Jones | Chief Copy Editor

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

Long Life

The MOTA Samsung S6 premium extended battery case helps protect and extend the battery of a user’s phone simultaneously by charging the phone and the extended battery case at the same time. Simply plug the case into your charger with your smartphone inside the case to save time and space. Four LED lights easily indicate the percentage of remaining power. The ultra-lightweight external battery case comes in black or white.

www.mota.com

Easy Typing

Keyboardio launched a Kickstarter campaign for its Model 01 ergonomic keyboard. Crafted with solid maple, the keyboard is divided into two independently adjustable halves featuring custom-sculpted keycaps to make typing comfortable. The Model 01 has programmable LEDs so users can create and share animation, or program the keyboard to react to computer events. The keyboard is compatible with MacOS, Windows, Linux, Android and iOS (limited LED support for phones and tablets).

www.keyboard.io

Supreme Storage

Lenovo announced its Storage S2200 storage array, which supports up to 96 drives to withstand storage growth. Designed for small and medium-sized organizations, the S2200 supports Fibre Channel, iSCSI and SAS connectivity. It offers Intelligent Real-Time Tiering, which automatically moves frequently accessed data to higher performing drives every five seconds, significantly increasing storage performance. Snapshot provides point-in-time copies of live data, eliminating the need for restore and performance hits. Rapid RAID Rebuild minimizes recovery time and risk factors with fast data restoration.

www.lenovo.com

Visit www.IntelliTime.com | Call 888-757-0337

IntelliTime Systems Corporation

IntelliTime is 100% dedicated to Public Sector workforce automation solutions including Timekeeping and Scheduling for State, County, City and Municipal organizations across North America.

‡ Web Timecards with advanced rules
‡ 24 x 7 Scheduling for Public Safety, Public Works etc.
‡ Time Clocks
‡ Mobile apps including our Mobile Crew Sheet
‡ Telephone Timekeeping (IVR)
‡ Activity Based Cost Accounting
‡ Interfaces to: Cityworks
‡ Open311
‡ All Popular ERP Finance HR and Payroll solutions.

IntelliTime Systems Corporation

Our modular solution includes:

© eRepublic

100 Blue Ravine Road
Folsom, CA 95630
916-932-1300
www.eRepublic.com

CMY grey
T1
T2

OK to go
Dutch researchers are testing new roadside barriers that combine multiple technologies into brightly colored walls that not only combat noise pollution in communities adjacent to freeways, but also collect solar energy. A year-long pilot is underway, exposing the Solar Noise Barriers to real-world conditions. If successful, highways across the globe could get much more colorful.

SOURCE: INHABITAT

Beware the Butt Dial
Now it’s not just the embarrassment of unintentionally phoning a friend or acquaintance that smartphone users need to worry about. A recent ruling from a U.S. Appeals court says phone calls resulting from inadvertent dialing are not protected by federal wire-tapping laws. Recipients of such calls can record them with impunity, the court declared, explaining that the responsibility lies with the caller who failed to lock the phone and prevent the call in the first place.

SOURCE: GIZMODO

Renaissance Sound Walls
Dutch researchers are testing new roadside barriers that combine multiple technologies into brightly colored walls that not only combat noise pollution in communities adjacent to freeways, but also collect solar energy. A year-long plot is underway, exposing the Solar Noise Barriers to real-world conditions. If successful, highways across the globe could get much more colorful.

SOURCE: INHABITAT

THE TRUTH ABOUT AIRPORT WAIT TIMES
Travelers at New York’s JFK Airport are getting a truer picture of the airport experience thanks to a new system that uses passenger cellphones to measure the length of time it takes to get through lines. Wi-Fi and Bluetooth signals are tracked by sensors as passengers maneuver through JFK’s Terminal 4. Wait times are displayed to passengers on monitors at security checkpoints, the customs area and the taxi queue. According to airport officials, the data not only keeps passengers informed, it also could help management make better staffing and operations decisions.

SOURCE: MASHABLE

SOCIAL GARBAGE
One Finnish startup is taking on an issue that wastes (pardon the pun) municipal dollars around the globe: Sending out trash collection trucks to nearly empty dumpsters. “E-containers” from Enovo are equipped with sensors that send a tweet to waste management officials when they need a pickup. The company reports that the containers are being used in 35 countries. Smart cities, indeed.

SOURCE: CITISCOPE
NASCIO is the Resource for What’s Happening in State IT

Visit www.NASCIO.org where you can access survey reports and issue briefs on topics such as cybersecurity, IT workforce, unmanned aerial systems, IT accessibility, enterprise architecture and more.

Follow us @NASCIO to stay informed on our newest research

TAKING OFF: Advancing Smart Government
Empowered CIOs • Strategic Partnerships • Engaged Citizens

NASCIO members will come together in Salt Lake City on October 11-14 for the 2015 NASCIO Annual Conference

Follow the conversation from the Annual Conference using #NASCI015
GOV GIRL ON SOCIAL

By Kristy Dalton

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

GOVERNMENT TECHNOLOGY

SOLUTIONS FOR STATE AND LOCAL GOVERNMENT

eRepublic

100 Blue Ravine Road
Folsom, CA 95630
916-932-1300
www.eerepublic.com

September 2015

Online Input, Real-World Impact

Governments can get valuable citizen feedback from social media, but there are keys to being successful.

In June, I started a biweekly chat on Twitter as a way to help government social media managers connect with one another. During one #GSMCHAT, the conversation focused on how to get meaningful citizen input through social media — input that agencies can actually use to aid decision-making. Here is some of the best advice shared by government staff members in the trenches.

Conduct Social Polls
Social polling is an effective way to boost engagement, get opinions and collect additional content for future posts or blogs. #GSMCHAT participants mentioned everything from Google Forms and polling on Facebook to text-ins and Wedgies (the social polling app, of course). Asking questions on social media is an easy and inexpensive way to gather feedback on areas such as policy changes, community issues and special events.

Live Tweet Events
Sometimes we are lucky to get even a handful of citizens attending a government open house or community meeting. One technique to get participation from more people than just an in-person audience is to “live tweet” these events.

First, establish and promote a hashtag for the event. Giving your audience a searchable term on Twitter will let them follow along and join the conversation more easily. “Don’t forget to research your hashtag first to make sure it’s available & the results are appropriate,” noted @KaitlinKeeler on #GSMCHAT. Retweeting comments and pictures from attendees will create more excitement, and the free Storify Web tool is a great way to recap the live tweet for anyone who did not participate. Another great tip from @JuanSVAS: “Use tools to ID the right people, then reach out via [direct message] asking them to invite 3-5 specific folks. Engage.” I also recommend preparing certain tweets in advance. The conversation happens fast and this allows you to copy and paste various tweets.

Share Input with Elected Officials
The key with soliciting input via social media is actually sharing those comments with elected officials and staff. So much public input via social seems to stay in the ether, so have a plan for using it. In January, Austin, Texas, publicized the hashtag #myatxgov the week before a town hall meeting involving a proposal for a new way to conduct council meetings. Staff organized the feedback (209 tweets using the hashtag) into categories and submitted them to both the city manager’s office and the city council so they could weigh and implement changes suggested by citizens.

In another example, the Neighborhood Commission Office of Honolulu held the agency’s first-ever #NCOTweetup in 2014. Officials needed to increase citizen engagement to reflect the true demographic makeup of the island. Participants had interactive discussions on the value and importance of civic engagement in the digital age. As a result of the event, the office received several ideas to implement and saw a marked increase in online interactions with both current and newly inspired constituents. Some attendees ultimately even became board members.

I love it when the online world has a meaningful impact on the offline world. #GSMCHAT

What: #GSMCHAT on Twitter
When: Every other Thursday at 1 p.m. PDT
Why: Connect with other government social media managers
Freedom of Information/Public Records Request

Part I: I hereby request to:  X 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 Doe

Address: 1076 Freedom Way  City: Everton  Zip: 86097

Phone:  (202) 867-5309  Email: jjohnson@email.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
VARIDESK® is an affordable, height-adjustable desk that lets you switch easily between sitting and standing as you work. It ships fully assembled and ready-to-use, so you can just place it on top of your existing desk and you’re ready to go. Order online or call 800-207-2881.