GCN

TECHNOLOGY, TOOLS AND TACTICS FOR PUBLIC SECTOR IT

SEPTEMBER 2015 • VOLUME 34, ISSUE 9

CAN MULTITASKING TURN YOU INTO AN INSIDER THREAT?

Survey finds unintentional insider is biggest cause of insider threats.

READ THE FINDINGS AND A WHITEPAPER AT:

WWW.RAYTHEONCYBER.COM/SPOTLIGHT/PONEMON

NEGLIGENCE IS THE #1 CAUSE OF INSIDER THREATS

All workplaces share the same security threat: the well meaning but careless employee who may be more focused on productivity than protecting the company's sensitive or confidential information.

BIGGEST RISK

CHARACTERISTICS OF GREATEST RISK EMPLOYEES

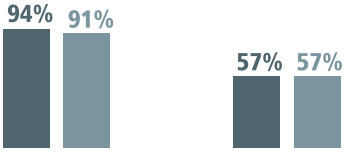
CAUSES

NEGLIGENCE #1 CAUSE OF INSIDER THREATS

UNINTENTIONAL NEGLIGENCE SEVERELY DIMINISHES IT FUNCTION PRODUCTIVITY

INCIDENTS ARE CAUSED MORE BY MISTAKES THAN BY INTENTIONAL OR MALICIOUS ACTS

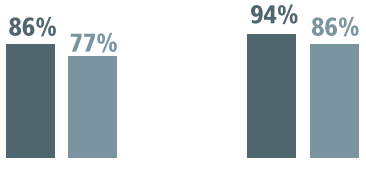
COMBINING BUSINESS AND PERSONAL DATA ON OWN DEVICES



THE LIKELIHOOD OF THIS HAPPENING IN ORGANIZATIONS

THE RISK THIS POSES TO ORGANIZATIONS

EMPLOYEES DUPED BY PHISHING SCAMS



THE LIKELIHOOD OF THIS HAPPENING IN ORGANIZATIONS

THE RISK THIS POSES TO ORGANIZATIONS

Read the full Ponemon report, The Unintentional Insider Risk in United States and German Organizations at: http://www.raytheoncyber.com/spotlight/ponemon

Ponemon INSTITUTE

Raytheon | websense

GCN

TECHNOLOGY, TOOLS AND TACTICS FOR PUBLIC SECTOR IT

SEPTEMBER 2015 • VOLUME 34, ISSUE 9

TECH IN CONTEXT:

Why SDN matters

Page 26

CASE STUDY:

A five-state collaboration on benefits data

Page 28

INSIDE DOD'S GLOBAL GRID

What DISA is doing to strengthen security and improve situational awareness

PAGE 18

105 MEDIA

Take the complexity out of CDM.

Think beyond compliance. Think ahead. HP Enterprise Security Products offers a complete solution to maintain secure data environments and meet agency missions. Our approach to CDM reduces compliance to four simple, integrated steps. We provide industry leading best-of-breed cybersecurity products to modernize agency infrastructure for improved efficiency and increased protection of networks and information systems.

Our easy to deploy and use security management products test assets for vulnerabilities before they launch, identity evolving risks in assets already in use, find and resolve threats across the network at machine speed, and reduce the number of events requiring manual management.

HP takes the complexity out of CDM. See how it strengthens your mission. To learn more visit: **hp.com/go/pubsecsecurity**

INSIDE

FEATURES

TECH IN CONTEXT

CASE STUDIES

HOW TO

GCN (ISSN 0738-4300) is published 11 times a year, monthly except Dec by 1105 Media, Inc., 9201 Oakdale Avenue, Ste. 101, Chatsworth, CA 91311. Periodicals postage paid at Chatsworth, CA 91311-9998, and at additional mailing offices. Complimentary subscriptions are sent to qualifying subscribers. Annual subscription rates payable in U.S. funds for non-qualified subscribers are: U.S. $125.00, International $165.00. **Subscription inquiries, back issue requests, and address changes:** Mail to: *GCN*, P.O. Box 2166, Skokie, IL 60076-7866, call (866) 293-3194, outside U.S. (847) 763-9560; fax (847) 763-9564 or email GCNmag@1105service.com. **POSTMASTER**: Send address changes to *GCN*, P.O. Box 2166, Skokie, IL 60076-7866. Canada Publications Mail Agreement No: 40612608. Return Undeliverable Canadian Addresses to Circulation Dept. or XPO Returns: P.O. Box 201, Richmond Hill, ON L4B 4R5, Canada.

BRIEFING

COMMENTARY

WISH LIST

GCN

Technology,
Tools and Tactics
for Public Sector IT

SALES CONTACT INFORMATION

MEDIA CONSULTANTS
Ted Chase
Media Consultant, DC, MD, VA,
OH, Southeast
(703) 944-2188
tchase@1105media.com

Bill Cooper
Media Consultant, Midwest, CA, WA, OR
(650) 961-1760
bcooper@1105media.com

Matt Lally
Media Consultant, Northeast
(973) 600-2749
mlally@1105media.com

Mary Martin
Media Consultant, DC, MD, VA
(703) 222-2977
mmartin@1105media.com

EVENT SPONSORSHIP CONSULTANTS
Stacy Money
(415) 444-6933
smoney@1105media.com

Alyce Morrison
(703) 645-7873
amorrison@1105media.com

Kharry Wolinsky
(703) 300-8525
kwolinsky@1105media.com

MEDIA KITS
Direct your media kit
requests to Serena Barnes, sbarnes@1105media.com

REPRINTS
For single article reprints (in minimum quantities of 250-500), e-prints, plaques and posters contact:

PARS International
Phone: (212) 221-9595
Email: 1105reprints@parsintl.com
Web: magreprints.com/QuickQuote.asp

LIST RENTALS
This publication's subscriber list, as well as other lists from 1105 Media, Inc., is available for rental. For more information, please contact our list manager, Merit Direct. Phone: (914) 368-1000
Email: 1105media@meritdirect.com
Web: meritdirect.com/1105

SUBSCRIPTIONS
We will respond to all customer service inquiries within 48 hours.
Email: GCNmag@1105service.com
Mail: GCN
PO Box 2166
Skokie, IL 60076
Phone: (866) 293-3194 or (847) 763-9560

REACHING THE STAFF
E-mail: To e-mail any member of the staff, please use the following form: *FirstinitialLastname@1105media.com*.

CORPORATE OFFICE
Weekdays 8:30 a.m.–5:30 p.m. PST
Telephone (818) 814-5200; fax (818) 936-0496
9201 Oakdale Avenue, Suite 101
Chatsworth, CA 91311

GSA makes awards for long-awaited agile BPA

BY ZACH NOBLE

After a long wait and multiple delays, the General Services Administration's 18F agile blanket purchase agreement is up and running.

In announcing the awards on Aug. 28, 18F's consulting team praised 16 successful vendors for their delivery of "amazing, working software" in response to a request for quotations.

Unlike typical contract vehicles, the agile BPA sought to pool GSA Schedule 70 vendors for rapid agile or DevOps work on 18F and partner agency projects, and would-be vendors had to offer a functional project, not just a proposal, to seal the deal.

The process was not entirely smooth, however. Overwhelmed by questions about the novel BPA, 18F pushed back the deadline for the RFQ not once but twice.

"Before the RFQ release, we held a presolicitation conference so we could preview the RFQ to vendors and answer questions, with the goal of reducing the questions during the official Q&A period," the 18F team wrote. "Despite that, after the release, hundreds more questions still poured in — mostly on technical or contracting issues. To respond to this volume, we missed our own answer deadline, and that ended up pushing back the vendors' deadline to respond."

> **"We think we were successful in demonstrating some solid innovation with the award process, but we've got a long way to go now before we can declare success on what really matters."**
>
> **18F TEAM**

The team thanked the Federal Acquisition Service for working through the issues with them.

18F officials admitted to being frustrated by the delay but claimed to have learned valuable lessons from the process.

"We think we were successful in demonstrating some solid innovation with the award process, but we've got a long way to go now before we can declare success on what really matters: demonstrating the ability to partner with industry to deliver successful digital services to our customers using agile delivery practices," they wrote. "In other words, as with the rest of 18F, delivery is the strategy, and now we're looking forward to shipping under the BPA."

Officials also pledged that other vendors would be afforded on-boarding opportunities in the future. •

The 16 vendors to win a slot on the BPA are:

- Acumen Solutions
- Applied Information Sciences
- Booz Allen Hamilton
- DSoft Technology
- Environmental Systems Research Institute
- Flexion
- NCI Information Systems
- PricewaterhouseCoopers Public Sector
- SemanticBits
- TechFlow
- TeraLogics
- Three Wire Systems
- True Tandem
- Vencore Services and Solutions
- Ventera
- World Wide Technology

Iowa tests digital driver's licenses

BY DEREK MAJOR

For agencies at all levels of government, the driver's license is the de facto standard for identification. But the wallet card might soon be replaced by a digital version that resides on a smartphone.

The Iowa Department of Transportation launched a trial program of a mobile driver's license with technology vendor MorphoTrust in August. The company said Iowa DOT employees are the first in the nation to use its secure, smartphone-based mDL software.

A test version was delivered to a group of Iowa DOT employees who will assess and validate its use in situations in which physical licenses are typically presented.

According to MorphoTrust, the mDL software carries the same level of trust as its physical driver's license counterpart. The software has visible and covert security features that are

layered into the digital image seen on screen. Those features allow the mDL to be quickly authenticated and protect it against reproduction.

Iowa officials will also work with MorphoTrust to test updates to its customer records, with the changes rendered on a smartphone in real time. With mDL, information such as name, address, over/under-21 status and organ donor status can be changed and posted on an individual's phone immediately.

In addition to the PINs and fingerprint-based security features built into the phones used in the pilot, the mDL app can be secured with MorphoTrust's facial recognition technology, which requires the user to take a selfie and use a custom PIN to unlock the app.

"Although we're not yet ready to release the mDL for customer use, the lessons learned in this pilot will demonstrate the use case for our mDL application to be offered in the future as an option to all citizens across the state," Iowa DOT Director Paul Trombino said. The pilot also "may help guide other states who want to launch similar digital identity programs." •

NYC gets serious about searchable public notices

BY DEREK MAJOR

New York City has released an online, searchable version of the daily City Record newspaper, the official publication for notices on public hearings, auctions and sales, solicitations, and rules proposed and adopted by city agencies.

The new City Record Online is a fully searchable database of all those notices, including schedules for more than 750 public hearings and contract awards for the $1.2 billion of goods and services that the city acquires each year.

Previously, only a small subset of information was searchable through the daily PDF versions of the newspaper. Now solicitations and awards are searchable as far back as 2003, and non-procurement notices are searchable from 2013 to the present. People can sign up for email notifications in their areas of interest and can download bid documents when available.

New postings appear first on City Record Online at 12:00 a.m. The newspaper is published at 9:00 a.m., and that's when the PDF version is posted online.

"Mayor de Blasio is ushering in a new era of government transparency as his administration puts online one of the oldest print publications in the country," said Minerva Tantoco, CTO for the city of New York. "By enabling real-time email notifications and posting this information in the Open Data Portal, we're planting the seeds of increased civic engagement and new business opportunities." •

DHS outlines its biometric future

BY SUSAN MILLER

The Department of Homeland Security has released its vision of how enhanced biometrics capabilities will transform the agency's operations over the next 10 years.

DHS has several biometric-based programs underway, including the Automated Biometric Identification System and various research and development activities in its Science and Technology Directorate and operational components. The new DHS strategic framework, released in August, will be used to align initiatives to meet strategic goals and objectives, and identify gaps where action plans must be initiated.

The framework has three components:

1. Enhance the effectiveness of subject identification. By upgrading its outdated biometric collection systems with current technology, DHS will be able to more efficiently collect high-quality biometric data. The updates will also centralize access to federal and international biometric databases to reduce complexity, eliminate duplication of effort and standardize communications with partners.

Other objectives include improving real-time access from field locations and using a layered identity verification approach that expands the use of biometrics beyond fingerprints.

2. Transform identity operations to optimize performance. By automating identity verification, DHS officials expect to reduce processing time and enhance security. Shifting from an encounter-based to a "person-centric" view will make collected data available to more applications, thereby improving decision-making across the agency.

DHS will also identify and exploit ways to expand the use of biometrics to verify identity and reduce vulnerabilities and fraud.

3. Refine processes and policies to promote innovation. DHS officials plan to develop joint requirements to more efficiently address overlapping mission needs and oversight issues, establish departmentwide biometric authorities and implement standardized solutions to minimize maintenance of duplicative services.

An integrated, enterprise biometric framework that uses the latest technologies can help DHS ensure national security and public safety while improving the efficiency and effectiveness of agency operations.

The vision statement for the framework is available at **is.gd/GCN_DHS biometric**. •

EDITOR'S NOTE

Recognition for those who are doing it right

Too often, it seems the emphasis in public-sector IT coverage is on the projects that have gone wrong: the data breach, the cost overrun or the long-awaited system that makes a mission harder, not easier.

Those stories have their place, to be sure – and GCN covers them frequently. Important lessons can be learned from mistakes, and sometimes a problem project needs some public attention to get the remediation efforts rolling.

The success stories, however, are often treated like the dog that didn't bark. Lacking conflict or drama, even high-impact programs and projects can get passed over in favor of the latest train wreck.

The GCN Awards are one attempt to address that imbalance. You'll learn more about the 2015 winners in the October issue, and we will honor them at our Oct. 14 gala, but they deserve an advance shout-out here. Great teams have much to teach us – and these 10 should be celebrated and studied.

Here are the 2015 GCN Award winners:

1. Biomedical Research Informatics Computing System: National Institutes of Health

2. Child Care Fraud Detection Solution: Los Angeles County, Calif.

3. eDIVO Mobile App: Department of the Navy

4. FBI Next Generation Identification System: Justice Department

5. Fiscal Note Agency Response System: Utah

6. Global Combat Support System: Department of the Army

7. National Child Victim Identification Program: Department of Homeland Security

8. Non-Emergency Contact Center: Philadelphia

9. Pennsylvania Treasury Transformation Project: Pennsylvania

10. Swipe to Donate Life Program: Ohio Department of Public Safety

– Troy K. Schneider

tschneider@gcn.com / @troyschneider

TURN YOUR CURRENT DESK INTO A STANDING DESK

VARIDESK® users report experiencing an increase in energy and productivity*. The height-adjustable VARIDESK lets you move from sitting to standing quickly and easily. It's simple to adjust, ship fully assembled, and works with your existing desk. Feel better and work smarter with VARIDESK. **Order online or call 800-207-2881.**

*According to December 2014 Customer Survey; N=2166
US Patent #8671853 | US & Foreign Patents Pending,

VARIDESK.com
WORK ELEVATED™

READ ME

What: Forrester Research's 2015 U.S. Federal Customer Experience Index

Why: Political opinion, the effectiveness of legislation and the efficiency of agency operations are all influenced by people's experiences with government transactions.

Forrester's CX Index found that 18 federal agencies and programs ranked significantly lower for customer satisfaction when compared to the private sector.

On average, the government agencies ranked "poor," with the National Park Service and U.S. Postal Service tied for best of the bunch and the Department of Health and Human Services' HealthCare.gov portal placing last.

Compared to companies in 17 industries, the federal agencies overall had the lowest average CX Index score, worst reported experiences and uneven quality from one agency to another.

TAKEAWAY Forrester suggests agencies focus on key components of CX quality: making the customer feel important and valued, resolving customers' problems quickly, using clear communication and making efforts to fully understand customer needs.

CX leaders should assess which drivers most directly affect the quality of a specific experience and start with the ones that show the highest importance but the weakest performance. Agencies should then insist that CX improvement proposals directly address those drivers so that decision-makers can allocate funding appropriately.

SHUTTERSTOCK

DARPA wants to take the sting out of DDoS attacks

BY MARK POMERLEAU

Distributed denial-of-service attacks can be a minor inconvenience compared to more malicious cyberattacks, but they pose enough of a threat that the Defense Advanced Research Projects Agency is looking for innovative approaches to mitigate their effects.

According to a recent broad agency announcement, DARPA's Extreme DDoS Defense (XD3) program is seeking private-sector input on "fundamentally new DDoS defenses that afford far greater resilience to these attacks, across a broader range of contexts, than existing approaches or evolutionary extensions."

DARPA lists five technical areas for which contractors can submit responses that focus on lessening the effect of DDoS attacks and improving recovery time, including:

- Devise and demonstrate new architectures that physically and logically disperse these capabilities while retaining (or even exceeding) the performance of traditional centralized approaches.
- Develop new cyber agility and defensive maneuver techniques that improve resilience against DDoS attacks by overcoming limitations of preconceived maneuver plans that cannot adapt to circumstances and exploring deceptive approaches to establish a false reality for adversaries.
- Produce a response time of 10 seconds or less from attacks and at least a 90 percent recovery in application performance compared with hosts that do not have XD3 capabilities.

DARPA officials believe the military, commercial network service providers, cloud computing and storage providers, and enterprises of all sizes can benefit from XD3 concepts.

Responses should consider a wide range of network and service contexts, such as enterprise networks, wide-area networks, wireless networks, cloud computing and software-defined networks. The announcement does not include detection and mitigation of DDoS-related malware on hosts or networked devices.

Responses are due by Oct. 13. To read the announcement, go to **is.gd/GCN_DARPA**. •

Army health platform embraces fitness-tracking

BY MARK POMERLEAU

The Army is adapting its ArmyFit personal health, resilience and performance platform for smartphones and mobile fitness devices.

ArmyFit will store, track and integrate data from those devices, and provide real-time feedback on users' health-related activities, including how far they run or walk, what they eat and even how well they sleep.

ArmyFit works with Fitbit and Jawbone, and will soon have the ability to sync with Garmin and Withings devices.

"Tracking all of those behaviors increases awareness, increases mindfulness and also can prompt behavioral change, such as being more aware of what you're eating and how much you're working out," said Capt. Kristin Saboe, an Army research psychologist. "That alone can lead to change and increase resilience."

ArmyFit also added an "Ask the Experts" feature in which professionals confidentially respond to questions on a wide range of topics, such as physical fitness, sports medicine, nutrition, relationships, and mental and emotional health.

In addition to ArmyFit, the Army's Global Assessment Tool has also been made mobile-ready. The annual requirement for non-deployed soldiers helps evaluate fitness and is a prerequisite for accessing ArmyFit content. Soldiers reach the services by using an Army Knowledge Online username and password; a Common Access Card is not needed.

"Soldiers have a personal responsibility to manage and maintain their overall health and resilience," Saboe said. "ArmyFit is a platform to help soldiers do that." •

RETRO TECH

NAVAL IMAGING COMMAND

In government IT and everywhere else, it's been a decades-long march toward smaller, faster and more powerful. Although this Marine's mission during a 1988 Ocean Venture exercise would be familiar to his 2015 peers, the smartphones in their pockets would have more computing power than the machine he's using.

DISA's best practices for cloud migration

BY MARK POMERLEAU

The Defense Information Systems Agency recently released a Best Practices Guide for Department of Defense Cloud Mission Owners for those planning to migrate existing systems from physical environments to the cloud.

The guide is not meant to make policy or vendor recommendations, and although it is not official DOD policy, it offers advice intended to help Pentagon components avoid mishaps as they adopt cloud-based services.

It provides knowledge gained from DOD cloud pilots — specifically, DISA's Information Assurance Support Environment and the Army's DOD Environment, Safety and Occupational Health Network and Information Exchange.

The guide includes information on IP standards, domain name servers, storage capacity, assessment and authorization. It follows the release of three other documents in July regarding security requirements for cloud computing.

The best practices guide includes advice to mission owners not to worry about selecting the wrong type of cloud service for infrastructure as a service because providers offer several choices, and changing is easy.

The document also states that "estimating bandwidth usage-based billing can be difficult," and it recommends that officials multiply their initial estimates by four. Bandwidth is metered so overestimates are not an issue, but DISA's guide recommends that owners review their bandwidth use on a quarterly basis.

Read the full report at **is.gd/GCN_cloud**. •

CYBEREYE
BY BRIAN ROBINSON

Dumb and dumber: Shadow BYOD at government agencies

A RISING CONCERN for government organizations is the so-called shadow IT ecosystem — the unauthorized applications that employees download and use at work without formal agency permission.

That poses serious security headaches for network administrators, who don't know which applications are out there and who has them and therefore find it impossible to write effective security policies. It's similarly difficult to optimize network parameters when traffic is produced by unknown sources.

The bring-your-own-device movement has generated its own security headaches over the past few years, and agencies have struggled to come up with ways to let employees use their personal mobile devices for government work. A few agencies have done that, but most have simply barred employees from using personal phones and tablets to handle government data.

Case closed? If only.

Were there really that many IT executives who thought that, simply because they said so, people used to peering at their screens every few minutes outside work would meekly give that up at the office and switch to agency-sanctioned devices? Hillary Clinton is not the only one who doesn't want to swap phones to get email or other communications.

Mobile security company Lookout wanted to see what the reality of this "shadow BYOD" is, and it's not pretty. An analysis of records for Lookout-enabled devices found 14,622 associated with government networks. More than one in 10 of those devices registered a "serious mobile threat encounter" in the course of a year.

> The threat from mobile devices is not only real, it seems to be higher than that found outside government.

In a recent survey of more than 1,000 government employees at 20 agencies, Lookout discovered that half of them have used their personal devices to get email, and nearly as many have used them to download work documents.

And the threat from mobile devices is not only real, it seems to be higher than that found outside government. In the Lookout survey, 18 percent of federal employees claimed to have encountered malware on their personal and government-issued mobile devices. That's more than double the average percentage reported overall for iPhone and Android devices.

All this comes on the heels of a number of recent announcements of dangerous bugs found in the Android operating system. One was the so-called Stagefright vulnerability, which could affect up to 95 percent of Android devices. Some experts have likened it to the OpenSSL Heartbleed bug of 2014.

Now another bug has been found in an Android system-level app called Google Admin. The bug allows Android to accept URLs from other apps, which could be manipulated to give malware access to private data on the device.

The bad news for Android continues to pile on, with vulnerabilities also found in various browsers used with the operating system.

But don't make the mistake of thinking Apple's iOS is immune to cyberthreats.

The trick, of course, is making sure users install all the patches that come out for Android and iOS to fix those vulnerabilities — and do so in a timely manner. Perfect patching doesn't happen, so at any given time there will be vulnerable devices accessing government systems and data.

Then there's just the dumb stuff that no one can govern. The Lookout survey found that 58 percent of respondents were aware of the potential consequences of using their personal devices at work, but 85 percent admitted to using them for risky activities anyway.

It's back-to-school time for most of America. Maybe it's also time for the federal government to get back to basics with cybersecurity and put together formal policies to handle BYOD. The practice is only going to get more prevalent over time — and so will the potential risks. •

BY PATRICK MARSHALL

Augmented reality: Coming to a city near you

IT STARTED IN GAMES. Now it's coming to government services. Get ready for smartphone-based augmented reality.

Want to know when the next express downtown is coming to the bus stop on the corner? Just point your smartphone's camera at the stop and CivicAR can deliver the schedule.

By using a smartphone's location data and camera to detect points of interest, CivicAR can deliver virtually any data a city chooses to make available — including transit schedules, traffic reports, information about local events, emergency service facilities or available parking spots.

A visual search feature allows users to scan city assets such as subway stations, restaurants, signs and even trees for information. CivicAR's directional search feature uses the phone's camera to let users explore and engage with their current environment, and a virtual teleportation feature allows them to visualize distant points of interest.

"Everything in the public sector is so location-based," which makes it a natural sector for implementing augmented reality, said Greg Curtin, CEO of Civic Resource Group International, which developed CivicAR.

According to Curtin, two factors have recently made augmented reality feasible: the viability of the cloud as a data platform and the proliferation of smart mobile devices.

Curtin, who was a municipal government attorney before founding CRGI, said that "there was an opportunity here, specifically in the government sector, to pull together a platform that would offer multiple, ready-to-go applications." The goal was "a modular solution ready-made for all the various public sectors, including government services, utilities, emergency services and so on."

With the click of a smartphone's camera, CivicAR delivers a wealth of data on points of interest as diverse as subway stations and trees.

The CivicAR module joins several others in the company's cloud-based CivicConnect mobile-data platform, which can deliver integrated public and third-party data streams through a variety of digital channels. CivicConnect integrates and processes data feeds, and the company designs applications, although clients are free to write their own apps.

"We already have a wide range of pre-built, ready-to-go modules and applications," Curtin said. "All the organization has to do is plug in their data. But if an agency wants to take it on, they can gin up their own apps."

CivicConnect runs on Amazon Web Services and can handle data from all the major databases.

So far, he said, the early adopters in government have mostly come from a single sector. "A lot of it is being driven — no pun intended — by transit and transportation," Curtin said, adding that transportation agencies are likely to put a primary emphasis on communications with the public. "They've done some of the heavy lifting already in terms of 'smartening up' with smart technologies."

He said his company's government clients are particularly excited by the potential uses for augmented reality, which "has amazing applications and benefits in the public sector. When we sit down with the business folks, they'll come up with a 100 uses cases that we didn't even think of. It's not just another bell or whistle. It really changes the way that end users engage with the public sector." •

INDUSTRY INSIGHT

BY CHIP GEORGE

How to wring every ounce of performance from data center storage

MANY PUBLIC-SECTOR CIOs who are at the start of their cloud journey are uncertain how large a role the cloud should play in their overall storage strategies. As a result, they often find it difficult to know where to begin.

One of the first steps is conducting a thorough inventory of the current data center infrastructure, which is often a heterogeneous mix of server, network and storage platforms. Gartner estimates that storage capacity demands are growing at a rate of 50 percent a year, but storage budgets are expected to grow at less than 10 percent.

One way CIOs can address that challenge is by maximizing current investments in the storage infrastructure. Underutilization is inefficient and wasteful, and there are ways to wring every ounce of performance and disk space out of existing investments before considering the cloud for storage.

Three storage efficiency technologies can reap tremendous benefits in both cost and space savings. Making efficient use of existing storage capacity frees up resources for investments in new technologies, including cloud-enabled storage.

It also lets agencies compare the costs of cloud services to those of its own data center.

• **Deduplication.** Some of the biggest clogs in any data storage system are related to redundant data. By applying the intelligent compression made possible by deduplication, only one instance of the data is retained on disk. A pointer lets the system know where to find that single stored version. Depending on the workload, deduplication can mean massive savings in terms of disk storage and network traffic. It can also shrink backup windows.

But deduplication is not just for backup or archive workloads. In primary workloads, it can help agencies store more "hot data" — the business-critical information that needs to be accessed frequently — and deliver better performance. When looking for ways to maximize efficiencies within an existing storage architecture, deduplication is always a smart place to start.

• **Thin provisioning.** All enterprise applications are allotted a set amount of storage to operate, which is referred to as provisioning. Problems arise when those storage predictions are either too low (causing performance problems) or too high (resulting in underutilization on either end of the spectrum). The latter can also lead to fat provisioning, where IT shops buy more storage than they need.

Thin provisioning lets organizations allocate disk storage space in a flexible manner among multiple users, which saves money by protecting resources from applications that ask for lots of storage upfront and then don't use it. When an organization plans for several years of predicted use, thin provisioning keeps it from locking or stranding storage where it isn't being used.

• **Compression.** Compression reduces the number of bits and bytes required to represent data by encoding information more efficiently. It can reduce a text file to half its original size. Smaller data is faster to transfer and cheaper to store, and it helps free up precious network bandwidth.

Those three technologies can combine to significantly reduce the total amount of storage needed, thereby lowering both capital and operating expenses. Total space savings can range as high as 87 percent from compression alone, depending on the application. Implementing all three approaches can take the savings even higher.

> Efficient use of existing storage capacity frees up resources for investments in new technologies, including cloud-enabled storage.

Although cloud-enabled storage can provide many avenues for savings, the best place to begin any cloud journey is with a comprehensive inventory of the data center to find places where the existing storage investments can do more. Getting back to basics is a great way to prioritize storage needs, maximize current storage assets and figure out how to eventually make cloud-enabled storage a key component of an overall storage plan. •

— Chip George is director of NetApp's state and local government and education business.

INDUSTRY INSIGHT

BY RODNEY CAUDLE

How to minimize the impact from DDoS attacks

IN EARLY 2000, one of the first known distributed denial-of-service (DDoS) attacks shut down Yahoo for three hours when an attacker repurposed a university's computers to flood the Internet portal's traffic. Such synchronized attacks from multiple sources against a sole target characterize DDoS attacks, a relatively new phenomenon compared to traditional denial-of-service attacks, which originate from a single source.

Thanks in part to the increasing number of devices on the Internet and the availability of high-speed Internet access, there's a larger pool of possible sources for all kinds of attacks. In the early 2000s, DDoS attacks reached a speed of approximately 4 gigabits/sec. Now they average 10 to 60 Gbps or even faster. A DDoS incident in February peaked at almost 400 Gbps, and the average DDoS attack now lasts 17 hours.

Three types of DDoS attacks have appeared in recent years:

• **Resource consumption**, in which attackers initiate a large number of bogus connection requests to a single destination. Attackers might also launch a resource consumption attack by attempting to exhaust the target server's disk space or another finite resource by using legitimate traffic to force the server to create large numbers of log files.

• **Bandwidth consumption**, in which attackers consume all available bandwidth on the networks leading to the targeted server by sending bogus traffic in quick succession. The resulting surge renders the targeted server unavailable. It can also take down other servers on the same network.

• **Keeping connections open**, which involves attackers completing numerous three-way handshakes to establish legitimate connections but then using Slowloris software to delay the process by designing each connection to instruct the target that it is "busy." The attackers can keep numerous connections open for extended periods by sending a data fragment to each connection every few minutes, thus tying up the server so it can't respond to legitimate traffic.

DDoS attacks on the public sector accelerated more than in any other industry in the fourth quarter of 2014. Commonly, opposition to legislation and political activism are motivators in DDoS attacks on government. Hackers aim to damage an agency's finances, reputation or both while gaining notoriety on social media.

Government agencies and the services they offer, by their nature, will always be targets. And because DDoS attacks can be launched with increasing ease — even by hackers with little technological expertise — agencies should operate as if a DDoS attack is inevitable.

> DDoS attacks on the public sector accelerated more than in any other industry in the fourth quarter of 2014.

DDoS attacks come without warning and, equally disconcerting, can escalate from start to peak effectiveness in as little as one minute. Some Internet service providers offer automatic responses, but they can cause outages and block legitimate traffic.

However, with some advance planning, agencies can reduce the perceived gains from future attacks.

What agencies can — and should — do is make themselves less appealing targets. Distributing services across various locations, instead of placing them in only one data center, is the first step. That way, a single DDoS attack cannot take the agency's entire suite of services off-line, and the agency won't have to rely exclusively on the Internet service provider's solution, which is usually expensive.

Agencies should also consider using a content delivery network as an entry point to its services because it can mask network connections from attackers. Such services are beneficial but also expensive, so agencies must consider the cost-to-benefit ratio.

Another step agencies can take is establishing a relationship with a managed services partner that can provide built-in protections from DDoS attacks. The partner can distribute the services through different data centers, thereby reducing the exposure and impact of DDoS attacks. •

— Rodney Caudle is director of information security at NIC.

INDUSTRY INSIGHT

BY BILL TOLSON

5 best practices for reducing risk in communication archives

WITH FORMER Secretary of State Hillary Clinton's email practices under scrutiny, email archiving is once again moving to the forefront of the discussion as the FBI determines the risks and impacts of mishandling government-related communications.

It's worth remembering, however, that email is just one piece of a much larger puzzle.

Thanks to new technologies, email now represents less than 50 percent of communications. However, few government IT managers are aware that, along with email, they must archive instant messages, text messages, agency blogs and comments, and agency LinkedIn and Facebook communications. That makes once clear retention rules murky and difficult to apply.

Before IT managers can set and implement data-archiving protocols, they must be aware of and follow five best practices:

1. Know where the servers are located. It is the IT manager's responsibility to be aware of all technology investments and assets so that IT departments can access and keep track of information when regulators, Congress or the courts request it. From there, agencies can create and reinforce more effective policies.

That knowledge also helps IT departments identify whether communications are being sent and received from private versus government servers.

2. Remember that it's not the platform, it's the content. Contrary to popular belief, the issues government agencies face surrounding data archiving have little to do with the communication channel. Whether government data is sent via email or instant message is irrelevant as long as the method of communication adheres to government regulations.

Still, agencies need to have policies and rules in place to capture messages across all communication channels. That can be difficult or impossible when offices are using messaging technologies that range from DOS prompts to Skype.

3. Upgrade legacy archiving technologies. In many cases, government agencies lack the latest (or any) technology to be able to quickly retrieve communication exchanges. Automation can help agencies archive messages quickly, efficiently and securely. However, the ability to search not only keywords but context is essential. It gives users a more accurate way to find specific content and provides more context around conversations.

Those tools can save days or weeks spent determining whether the data was captured and managed correctly or piecing together conversation threads across different communication channels in response to a Freedom of Information Act request.

4. Understand the distinction between personal and government data. An email message might start out with "Free for golf this weekend?" But 15 replies later, it might turn into a discussion about a current government project. Understanding the distinction between personal and agency information is necessary to prevent legal repercussions later. Context takes a primary role here because automated tools can capture and sort information.

Government agencies must remove the gray area regarding archiving of all communications and clearly educate their employees about regulations. Agencies should also have a retention policy in place that is reviewed annually and that clearly articulates archiving responsibilities and practices.

5. Implement an archiving system with security. Lastly, an archiving system's security is crucial to safeguard government data. Protecting sensitive agency information with established and accepted levels of technology provides additional layers of security to limit unauthorized access to information and protect classified data.

Without implementing and enforcing archiving policies at government agencies, it is almost impossible for the IT department to locate and piece together relevant information from communication exchanges. Having the right systems in place and distinguishing among the types of communications are some of the important first steps agencies can take to prevent future mishaps. •

— Bill Tolson is director of product marketing at Actiance.

In many cases, government agencies lack the latest (or any) technology to be able to quickly retrieve communication exchanges.

NASCIO

Representing Chief Information Officers of the States

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 **#NASCIO15**

NEW TOOLS AHEAD FOR DOD'S GLOBAL GRID

DISA is working on multiple initiatives for the Global Information Grid that will substantially boost network situational awareness and increase protection against relentless cyberattacks

BY WILLIAM E. WELSH

The Defense Information Systems Agency will launch a new configuration management tool for the Global Information Grid on Sept. 28 that will give users better visibility into network assets.

A top DISA official told GCN the configuration management tool is just one of a number of near-term enhancements planned for the Defense Department's worldwide data information network, which enables 4.5 million users to share classified and unclassified information. The enhancements are being made by the project team for the three-year-old Global Information Grid Services Management-Operation (GSM-O) program.

Ready For The Next Big Thing For Government

SAMSUNG
BUSINESS™

In today's global economy, technology offers the potential for unparalleled innovation. To realize that potential, you need a partner with the knowledge, innovation and capabilities to empower and strengthen your government agency in a timely manner.

As a trusted provider of secure technology solutions to the U.S. government, Samsung Business™ has put its spirit of innovation and collaboration into delivering products that will help your agency stay ahead of the curve while lowering costs, increasing efficiency and maintaining security.

Nobody Can Predict the Future, But We Can Help You Be Ready for It

Unforeseen conditions and rapid changes are inevitable in the technology arena. We can help you adjust quickly to – and successfully route – such changes through our enterprise-grade products that seamlessly integrate with your agency's infrastructure, keep your data safe with comprehensive solutions and provide employees with beneficial features they truly enjoy using.

Mobile Products

Communicate and collaborate with colleagues more easily and securely than ever with our selection of innovative mobile products and defense-grade Samsung KNOX™ mobile security platform.

Samsung Galaxy Note5 and Samsung Galaxy Note edge

Optimize productivity with the multitasking and innovative note-taking capabilities of Samsung Galaxy Note5 and Samsung Galaxy Note edge. Enjoy familiar, mouse-like editing with the S Pen on a brilliant large-format screen. And have the peace of mind from the moment you turn on the device thanks to embedded KNOX security.

Samsung Galaxy S6 and Samsung Galaxy S6 edge

Get our best display, fastest mobile processor and powerful productivity features wrapped in a sleek metal and glass design you and your employees will want to use.

Samsung Galaxy S6 edge+

The Samsung Galaxy S6 edge+ offers remarkable performance in a large-format, dual-edge design. Enhance productivity with quick access to notifications and contacts on the edge screen. Simplify multitasking with Multi Window capabilities and leading business applications on the 5.7" Super AMOLED display.

Samsung Galaxy S5 Active (AT&T Only) and Samsung Galaxy S5

The stunning, powerful, water-resistant** Samsung Galaxy S5 delivers a brilliant display, fast camera and integrated S Health™ technology to enhance every day. The Samsung Galaxy S5 Active is IP67- and MIL-STD-810G-certified for salt, dust, water and thermal shock-resistance, engineered for use in the field.

***Device has been tested and received an IP (Ingress Protection) rating of IP67, which means that it is protected against dust intrusion and capable of withstanding water immersion between 15cm and 1 meter for 30 minutes.*

Samsung Gear S

See who is calling without reaching for your phone. Reply to emails while you're at a trade show. Send texts right from your wrist. Keep in touch without keeping your phone on you every moment with Samsung's first network-connected* wearable.

**3G coverage not available everywhere and requires a qualifying wireless plan. Consult your carrier for details.*

Mobile Products (cont.)

Samsung KNOX

Defense-grade Samsung KNOX security is a highly resilient mobile platform that brings unprecedented device security to government and enterprises. KNOX allows individuals to combine a single device for work and personal use without compromising security. It also provides greater protection for your sensitive data and cooperation with your IT department's policy requirements by easily integrating with your agency's existing security solution.

Common Criteria and FIPS-Certified Devices

Along with Samsung KNOX security, numerous Samsung mobile devices have Common Criteria certification – which evaluates a mobile device to see that it provides adequate security for its intended purpose. These devices are also FIPS 140-certified, which validates that a mobile device uses and implements encryption algorithms correctly.

Tablets, Laptops and Zero Client Displays

Put the power of Samsung's mobile computing products to work for you and keep your agency at the cutting edge of innovation while also keeping secure communication a priority.

Samsung Galaxy Tab S2

The thin, lightweight Samsung Galaxy Tab S2 displays presentations and documents crystal clear on the Super AMOLED display. Review, edit and send files quickly with the 1.9GHz octa-core processor. And enjoy superior, customizable desktop interoperability that securely connects your mobile ecosystem.

**A single Microsoft® app is preloaded on the tablet; when the device is connected to the internet and when the app is pressed, the suite of Microsoft Office for Android™ apps is downloaded.*

8.0 INCH (32GB) Wi-Fi® | Black: SM-T710NZKEXAR | White: SM-T710NZWEXAR
9.7 INCH (32GB) Wi-Fi | Black: SM-T810NZKEXAR | White: SM-T810NZWEXAR
9.7 INCH (32GB) LTE | AT&T: SM-T817AZKAATT | Sprint: SM-T817PZKASPR | T-Mobile®: SM-T817TZKATMB | Verizon: SM-T817VZWAVZW

Samsung Galaxy Tab A

The Samsung Galaxy Tab A improves productivity and transforms workflow efficiencies with powerful multitasking features, Microsoft® Office for Android™ apps preloaded* and defense-grade Samsung KNOX security, so your team can work from virtually anywhere.

**A single Microsoft app is preloaded on the tablet; when the device is connected to the internet and when the app is pressed, the suite of Microsoft Office for Android apps is downloaded.*

8.0 INCH Wi-Fi | Smokey Titanium: SM-T350NZAAXAR | White: SM-T350NZWAXAR
9.7 INCH Wi-Fi | Smokey Titanium: SM-T550NZAAXAR | White: SM-T550NZWAXAR
9.7 INCH Wi-Fi with S Pen | Smokey Titanium: SM-T350NZAAXAR

SAMSUNG BUSINESS

Samsung Galaxy Tab Active (Wi-Fi Only)

Ruggedized, enterprise-ready and solutions-ready, the Samsung Galaxy Tab Active is IP67-certified for water and dust resistance and is field-/outdoor-ready thanks to its bundled protective case and 8" daylight-readable display. Don't worry about drops or impacts in active business environments. With its included cover, the Galaxy Tab Active is designed to handle drops of up to 1.2 meters (3.9 feet)*** In addition, it also incorporates NFC, a user-replaceable battery and a 3-year warranty. Finally, defense-grade Samsung KNOX security allows your team to work from virtually anywhere.

****Drop test results meet MIL STD 810G standard.*

SM-T360NNGAXAR

Zero Client Desktops and Displays

The NX-N2-T Zero Client Desktop features built-in PCoIP® technology, which connects users to the corporate cloud while simplifying and securing the endpoint device. NC Series Zero Client Cloud Displays integrate enterprise-grade monitor designs with the latest in VDI zero client technology in an elegant all-in-one package. Samsung zero clients are purpose-built for VDI access, making them the ideal products for a truly centralized IT infrastructure.

21.5 INCH: NC221-S | 24 INCH: NC241-TS | Stand-Alone: NX-N2-T

Samsung ATIV Book 9 and Samsung ATIV Book 9 Plus

Bring clarity to your work on the impressively thin, lightweight ATIV Book 9. SideSync™ capability lets you automatically sync files with select Samsung smartphones, or use the device as a second display. A long-lasting 10-hour battery ensures all-day productivity. Step up to the ATIV Book 9 Plus for full touch-screen capability.

ATIV BOOK 9 | NP900X3K-S01US | NP900X3K-S02US
ATIV BOOK 9 PLUS | NP940X3K-S01US | NP940X3K-S02US | NP940X3K-K02US

Solid State Drives

Handle workloads from high-end computing on client PCs to heavy data center use with our new generation of solid state drives. From our portable T1 SSDs to our 850 EVO and 850 PRO series SSDs, you'll have speed optimized for business use, AES 256-bit encryption to protect sensitive data and high endurance for long-lasting performance.

850 EVO SSD | 1.0TB: MZ-75E1T0B/AM | 500GB: MZ-75E500B/AM | 250GB: MZ-75E250B/AM | 120GB: MZ-75E120B/AM
850 PRO SSD | 1.0TB: MZ-7KE1T0 | 512GB: MZ-7KE512 | 256GB: MZ-7KE256 | 128GB: MZ-7KE128

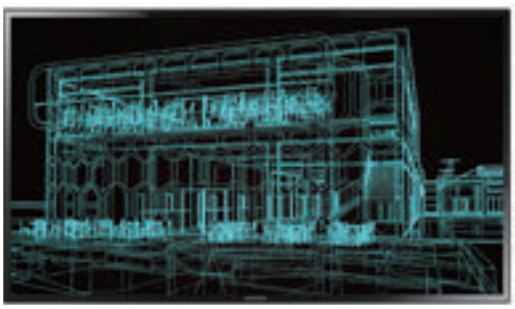
Digital Displays

From conference rooms to lobby signage to fully customized video walls, Samsung SMART Signage Displays allow you to deliver dynamic content and messaging while creating new communication opportunities and experiences at your agency.

ED-D Series LED Display (32"–75")

Get excellent Full HD quality at a smart price with these energy-efficient LED displays that are perfect for boardrooms, conference rooms and general signage in and around your agency.

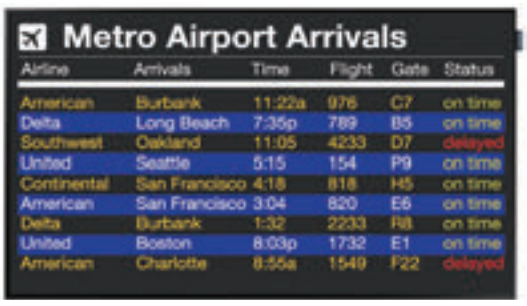
32 INCH: ED32D | 40 INCH: ED40D | 46 INCH: ED46D
55 INCH: ED55D | 65 INCH: ED65D | 75 INCH: ED75D



DM-D Series LED Display (32"–82")

Built for reliable, continuous 24/7 operation, these stunning Full HD displays feature an upgraded Samsung SMART Signage Platform and full range of connectivity options like embedded Wi-Fi® so you can customize your content.

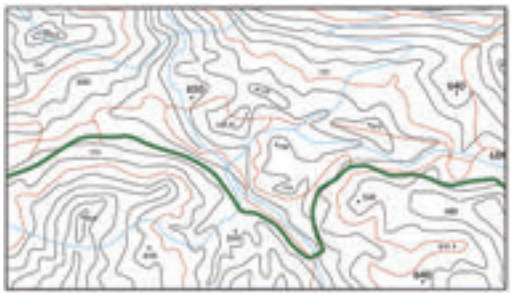
32 INCH: DM32D | 40 INCH: DM40D | 48 INCH: DM48D | 55 INCH: DM55D
65 INCH: DM65D | 75 INCH: DM75D | 82 INCH: DM82D



UD-D Series LED Display (46" and 55")

Create a seamless, premium video wall solution with Full HD displays that have near-seamless 3.5mm bezel-to-bezel specs, ColorExpert Calibration to ensure vibrant, accurate, consistent colors and an embedded SMART Signage Platform.

46 INCH: UD46C | 55 INCH: UD55D



Printers

Samsung's high-performance and resource-efficient printers offer reliable, cost-competitive document-handling solutions while keeping security at top of mind. All printers listed are TAA-compliant for United States government use.

ProXpress M4530ND/TAA

Take business performance to a new level with this monochrome single-function printer. Work fast with a 47 ppm engine and intuitive, easy to use controls. Extra-high-yield toner and drum life lower total cost of ownership and save space in the stockroom.

ProXpress M4020ND/TAA

Enjoy fast 42 ppm performance, professional quality and lower operating costs from this monochrome laser printer. ReCP (Rendering Engine for Clean Page) technology delivers solid printouts with sharp, clear text, while the compact footprint allows this printer to fit in even the most cramped work spaces.

CLP-680ND/TAA

Fast and flexible with true color, this 25 ppm color laser printer for small work groups produces vibrant, high-quality printouts. A simple operating panel, compact design and high-yield toner make it the perfect color printer for any environment.

CLP-775ND/TAA

Optimize the quality of your printouts and reduce operational costs with this 35 ppm color laser printer. It has the speed and easy connectivity to meet your agency's workflow demands, the power to handle print jobs of all sizes and vibrant color to produce brilliant printouts on every page. High-yield toner and up to 3 optional paper trays allow users to print massive reports with minimal intervention.

Desktop Displays

Improve efficiency and productivity with a broad lineup of reliable, cutting-edge Samsung Business™ desktop displays. These commercial-grade monitors have all the power, performance and versatility to handle your agency's needs.

450 Series Monitors

These reliable, cost-effective monitors are perfect for everyday agency use. Energy-efficient improved ergonomics with adjustable stand, a narrow-bezel design and wider connectivity options make the 450 Series versatile enough to meet your agency's needs.

19 INCH: S19E450BR | 21.5 INCH: S22E450B | 21.5 INCH: S22E450D
23.6 INCH: S24E450DL | 23.6 INCH: S24E450D | 27 INCH: S27E450D

UHD 850 and 970 Series Monitors

Make your users more productive with higher-resolution monitors. Our QHD and UHD monitors offer higher resolution than standard 1080p monitors so users can see more details on the screen. Perfect for engineers, programmers, designers, command and control, and anyone wanting more accurate and detailed images that are critical to performing their tasks efficiently and accurately.

23.5 INCH: U24E850R | 28 INCH: U28E850R | 31.5 INCH: U32E850R

Curved Monitors

Enjoy a truly immersive viewing experience that lets you enjoy big, bold and stunning panoramic views while you work. With a design inspired by the curve of the human eye and flicker-free technology, Samsung's energy-efficient, eco-friendly curved monitors deliver a more comfortable, more enjoyable viewing experience.

23.5 INCH: S24E650C | 27 INCH: S27E650C

Samsung Business' extensive portfolio of government contracts includes governmentwide acquisition contracts (GWAC), multiple award schedules (MAS), multiagency contracts (MAC) and blanket purchase agreements (BPA). Below are a sample of some of the contract options available for Samsung products. Products displayed in this catalog are not necessarily available through all of the referenced contracting options.

GSA Schedule | ARMY CHESS COMPUTER HARDWARE, ENTERPRISE SOFTWARE AND SOLUTIONS | CIOCS | AFWay | SEWP V | NGEN

1200 New Hampshire Avenue NW, 6th Floor, Washington, D.C. 20036
For more information call: 1-866-SAM4BIZ

For complete product information and accessories, visit samsung.com/government or samsung.com/business
Follow us: youtube.com/samsungbizusa @SamsungBizUSA

SAMSUNG BUSINESS™

The Defense Department's Joint Information Environment depends on the connectivity provided by the Global Information Grid.

"On the immediate horizon, what we are planning to do is implement a series of technology insertions centered on global IT service ordering," said Jessie Showers, director of DISA's Infrastructure Directorate. The technology insertions are "a series of cyber defense and operational improvements that we are going to do to enhance network configuration management."

In fiscal 2016, the GSM-O project team will automate circuit provisioning to enhance network performance, create tools and dashboards to resolve network outages, and introduce software-defined networking, Showers said.

In a broader strategic sense, DISA and prime contractor Lockheed Martin will keep the Global Information Grid in lock step with the overarching Joint Information Environment by implementing the Joint Regional Security Stacks, Showers said. That work is already underway.

In addition, DISA plans to offer a few coalition partners the opportunity to have their networks supported under GSM-O. Beginning in fiscal 2016, "we will do it on a small scale, and then we will expand it to other coalition partners so they kind of have the same kind of operational support that we furnish to our customers in the DOD," he said.

GLOBAL STOREFRONT FOR SERVICES

The initiatives signal that the GSM-O program has crossed a major threshold by completing the consolidation of disparate tasks under previous contracts. The program is now moving at full speed to enhance and optimize the Global Information Grid on many fronts.

In addition to ensuring that the grid has the latest commercial technology, the GSM-O project team helps DISA guarantee that the grid is secure enough to defeat the millions of cyberattacks against it each day. That requires robust situational awareness to identify and defeat threats.

In the past three years, DISA and contractor employees have consolidated requirements from roughly 20 task orders covering more than 400 work elements under a previous time-and-materials contract and realigned them with the seven-year, performance-based GSM-O contract, Showers said.

That massive transition took place while a number of high-profile missions were continuing, including U.S. military operations in Iraq, Afghanistan and other global hot spots. "We didn't drop a single mission, and no circuit degradation occurred," he said.

The first year of the contract (fiscal 2013) was devoted primarily to contract consolidation to streamline processes and improve program efficiency, said Chris Kearns, vice president of enterprise IT solutions at

LOCKHEED MARTIN

Lockheed Martin. The second year of the contract was marked by a push for operational convergence, whereby personnel support from overseas network centers were brought stateside and consolidated into a single, virtual network operations center supported by staff in Illinois and Hawaii, he said.

In the second year, the project team also launched a portal known as the DISA Direct Storefront, through which DOD Common Access Card users from the military services, combatant commands, and defense and intelligence agencies can buy network connections, mobile devices and unified communications services.

Previously, each military branch acquired network services through its own entity. Kearns said the Direct Storefront offers uniform and precise information regarding cost and the time required to implement a service.

GOAL OF A COMMON STACK

The Joint Regional Security Stacks initiative being carried out through GSM-O will significantly improve situational awareness by giving the military services and DISA a common view of various aspects of network security, officials said.

JRSS is the middle layer, so to speak, of the global data communications network. It handles the network transmissions between the Internet access points and end-user devices. Until now, each military service had its own security stack.

The initiative is being undertaken as part of the Joint Information Environment, a holistic plan designed to give DOD and the military services secure computing capabilities across the breadth of their vast operations.

Centralizing the locally distributed architectures at each base, post, camp and station so that the U.S. military has a common stack across the globe requires two major steps, Kearns said. The first part is a move to Multiprotocol Label Switching to give DOD the requisite bandwidth capability to match the latest technology for managing the flow of network traffic. The second part is the installation of new sets of equipment for the sensitive unclassified area and the secret classified area.

The first U.S. facility to install JRSS was Joint Base San Antonio.

The first stack of JRSS is already operational at Joint Base San Antonio, Kearns said. Twenty-four Unclassified but Sensitive IP Router Network and 25 Secret IP Router Network stacks are at various stages of installation and configuration worldwide.

More than 400 global sites will complete migration to JRSS through 2019, he said.

"The security stacks being deployed under GSM-O will provide an enterprise-level security boundary and allow us to operationalize our security capabilities and our abilities to make this network look more secure," Showers said. "You can't make it completely secure, but we will make it a lot more secure than it is today."

"This initiative is a major DOD priority," he added. "DISA is using GSM-O as a key pillar to ensure that this effort is successful."

BETTER RESPONSE TO NETWORK EVENTS

Another initiative is the implementation of software-defined networking. "That's the next-generational focus we are taking as well," Kearns said. "It has huge benefits for security, operations and cost efficiencies."

Software-defined networking will make the designated network connections "smart" through the use of software rule sets that will react almost instantly to unforeseen events that cause disruptions. To prepare the Global Information Grid for software-defined networking will require tailoring some data center connections so that they can use advanced architecture, Kearns said.

"Event management is one of the big areas that [software-defined networking] has a benefit to," he added. When events occur and traffic must be rerouted, the pre-established rule sets take over. "If a certain network path becomes unavailable, the network has intelligence coded into it that allows it to reconfigure itself in real time." •

U.S. ARMY

The Federal IT Acquisition Summit

October 20, 2015 | Washington Hilton, Washington, DC

Participating Agencies

SEWP V

NITAAC
CMB Authorized GWACs for IT Acquisition

Featured Speakers From

ARMY CHESS
COMPUTER HARDWARE, ENTERPRISE SOFTWARE AND SOLUTIONS

This second event in the Federal IT Acquisition Summit series provides government IT decision makers with even more contract-specific training opportunities. A must-attend for the acquisition and government IT buying community!

TRAINING OPPORTUNITIES :

- ARMY CHESS: ITES-3 & ADMC-3
- GSA: DPA
- DHS
- NIH-NITAAC: CIO-CS
- NASA SEWP V

FEATURED PANEL SESSIONS:

- FITARA
- Cybersecurity: CDM & Beyond
- GSA: Alliant (incl. Alliant 2 update)
- Cloud: Cloud Changes Everything

Free for Government & Military Attendees

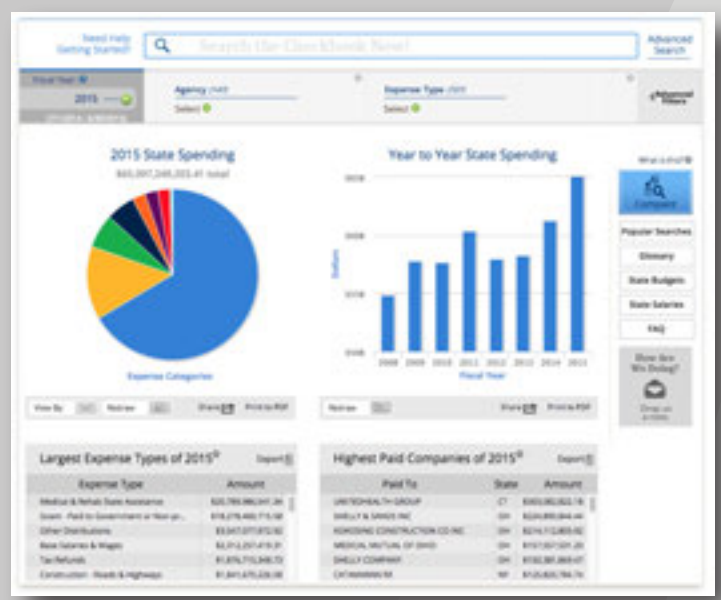
FCW GCN Washington Technology DEFENSESYSTEMS FederalSOUP

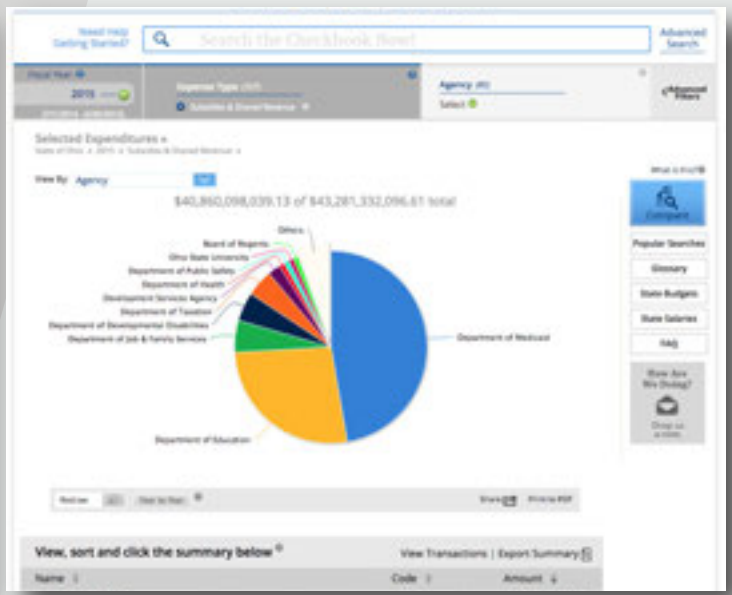
For Sponsorship Opportunities Contact – Stacy Money: smoney@1105media.com

http://FCW.com/FIAS

Shining a light on state spending

Sites that share spending data with the public can save time and money while satisfying the demand for transparency, but many states still have a long way to go





BY JENNI BERGAL

Ohio Treasurer Josh Mandel was mortified last year when a consumer watchdog group gave his state a D-minus for transparency in providing online access to information on government spending. And he decided to do something about it.

In December, Mandel's office launched a user-friendly, cutting-edge financial transparency website that this year earned Ohio the only A-plus in a national review of state websites that tell the public how state government spends taxpayer money.

Every state now runs some kind of public accountability — or "checkbook" — site with the goal of increasing transparency and accountability. But although many states have been ramping up their efforts to make their sites accessible and comprehensive, some still have a long way to go. Eighteen states' sites received grades of C, D or F in an annual evaluation this year by the U.S. Public Interest Research Group.

State checkbook websites vary considerably. Some are easy to use and provide lots of information with one click, making it easy for users to unearth information. Others are difficult to navigate or don't contain as much information.

"If you were to compare Ohio with Alaska or Idaho, you'd see huge differences in how user-friendly [the site] is," said Phineas Baxandall, a senior analyst at U.S. PIRG.

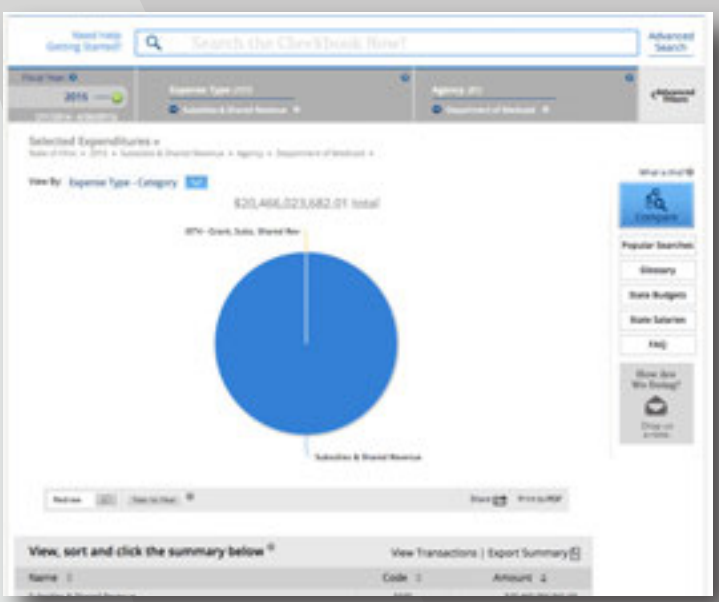
Every year, states spend hundreds of billions of dollars on contracts with vendors and nonprofit organizations; subsidies, such as tax credits, for companies to spur development; and other expenditures. States created checkbook websites to share information about that spending with the public so that taxpayers could know who is getting the money and for what purpose.

"It's extremely important because you have a new set of eyes on this information, not just those of someone in government," said LaVita Tuff, a policy analyst at the Sunlight Foundation, a nonprofit organization that promotes open government.

State financial officials say checkbook websites can help save money by identifying inefficiencies and reducing the amount of time employees spend fulfilling information requests. Also, posting contract information on the websites can result in more competition and lower bids. Interested vendors might see that they could win a contract by offering a lower price, and state agencies might see that they could consolidate contracts to get a better deal.

For instance, Massachusetts saved $3 million by eliminating paper, postage and printing expenses related to information requests by state agencies and paperwork from vendors, according to U.S. PIRG. Texas was able to renegotiate its copier machine lease and save $33 million over three years. And in South Dakota, a reporter used the website to launch an investigation into subsidies that led to the state saving about $19 million by eliminating redundancies.

"I think these websites are very important," said Kinney Poynter, executive director of the National Associa-



OhioCheckbook.com

OhioCheckbook.com features interactive charts and uses a Google-style search engine that's easy to navigate. It lists every state government expenditure, the official responsible for each contract and his or her contact information. Users can search, compare, share and download information on more than $473 billion in spending from the past eight fiscal years.

tion of State Auditors, Comptrollers and Treasurers. "More transparency provides better information for all of those involved, whether they be citizens, contractors or legislative bodies."

GRADING STATES

Now in its sixth year, the U.S. PIRG report evaluates and grades states on their online transparency initiatives and how well they provide access to spending data. It examines whether checkbook sites offer comprehensive, one-stop, one-click access to users and whether it makes large sets of data easy to download.

A growing number of states are doing a better job. Fourteen got an A this year, up from eight last year. Louisiana and Illinois were among those that improved their grades.

Other states that have made progress include Colorado, which got a B-plus after it overhauled its portal to make it easier to use, and Kansas, which vaulted from a D-minus to a B by revamping its site to make information more accessible and easier to download.

Connecticut, which got an A for the first time this year, recently launched OpenCheckbook, an easy-to-use, comprehensive site that allows users to search real-time information about payments to vendors, nonprofit groups and others.

"You not only have direct access to micro and macro information about the operation of state government, but you can search it, compare it, trend it and download big datasets," said state Comptroller Kevin Lembo. "I'd like to think that we're pushing the envelope in this area."

He added that because government officials tend to want to keep information close, checkbook websites are especially important for transparency.

"We don't like other people telling us we're doing things wrong," he said. "The result of pulling information in and holding it tight is that public confidence continues to erode."

Lembo said he was so pleased with OpenCheckbook, which was paid for with existing funds, that last month he launched OpenBudget, a new feature that will let users compare what was budgeted to what was actually spent.

"It's extremely important because you have a new set of eyes on this information, not just those of someone in government."

LAVITA TUFF, SUNLIGHT FOUNDATION

But not all states have improved their websites enough, according to U.S. PIRG.

Fifteen got a C or a D. And California, Alaska and Idaho received an F in 2014 and again in 2015. Two of those three do not have a central database for searching or viewing details on spending, the report states, and not one of them provides information on economic development subsidies.

"These three are not user-friendly," said Baxandall, who co-authored the report. "It's like finding a needle in a haystack."

OHIO OUT IN FRONT

After last year's embarrassment for Ohio, Mandel said he embarked on a mission to create an online tool that would empower taxpayers to hold state government accountable. The result was a website that Baxandall calls state of the art.

OhioCheckbook.com features interactive charts and uses a Google-style search engine that's easy to navigate. It lists every state government expenditure, the official responsible for each contract and his or her contact information. Users can search, compare, share and download information on more than $473 billion in spending from the past eight fiscal years.

"This site is not built with the MIT computer science major in mind," Mandel said. "It's built with the most basic computer user in mind."

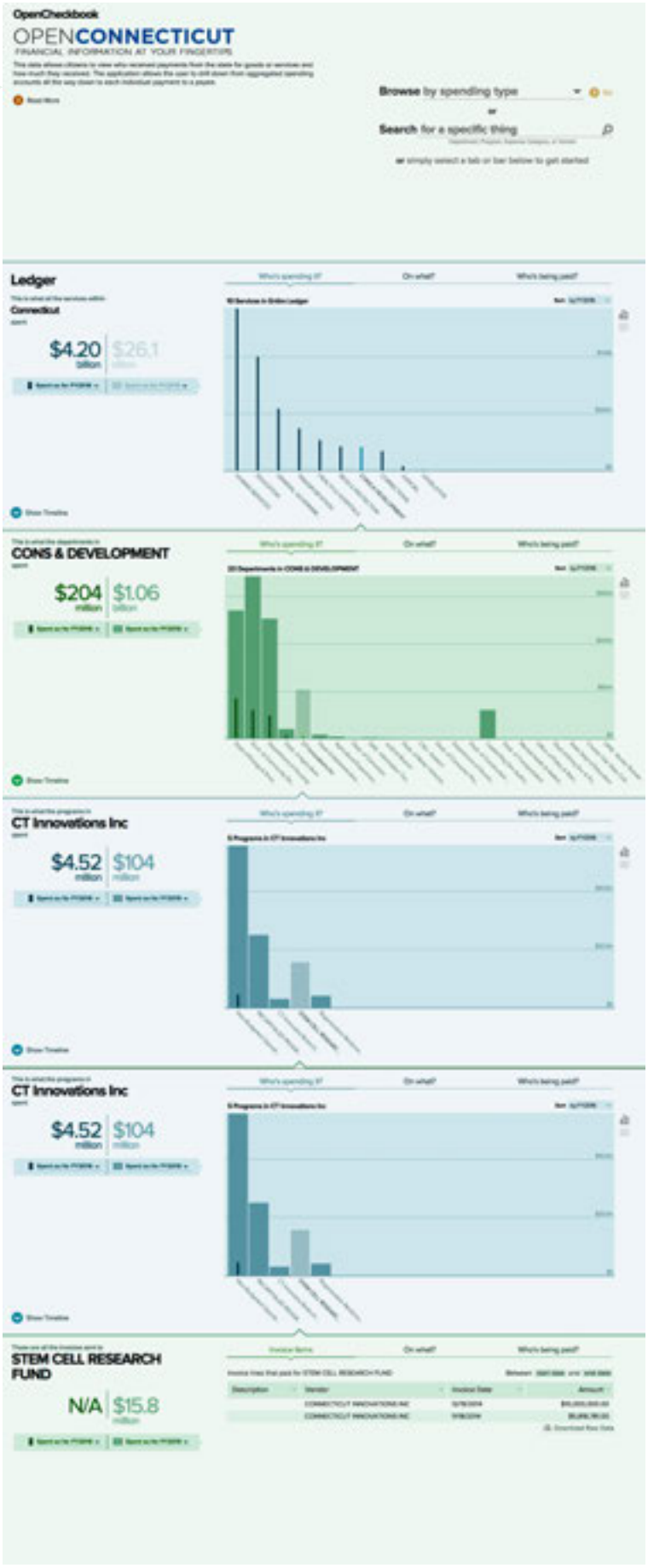
He added that 284,000 searches have been conducted on the site since its launch in December.

The site was built in 18 months and cost $814,000, all of which came from his existing budget.

"We're confident this will save taxpayers money," he said. "Politicians and bureaucrats are thinking more about their expenditures because they know it's going to be posted online."

Mandel said his next move is to convince the state's more

Connecticut's OpenCheckbook allows users to search real-time information about payments to vendors, nonprofit groups and others.



than 3,900 local governments to post their spending information on the site. Earlier this month, a legislative panel gave him permission to use $2.7 million of his agency's funds over the next two years to pay for a program that would expand the website to include local government expenditures.

Mandel said 245 local governments have already committed to the partnership, and more than 300 others have expressed interest.

WHAT'S NEXT?

Even the states with the best checkbook sites can do better, Baxandall said.

No state website, for example, includes spending for all public/private partnerships or quasi-governmental entities, such as those that operate toll roads or special boards.

But Baxandall said some states — including Florida, Massachusetts and Oregon — are starting to post some of that information on their websites.

"Those are areas where transparency is particularly important because they're normally outside the scrutiny of the public or the budget process," he said.

Baxandall added that the state websites should also compare what's being budgeted with what's being spent and that they should follow Ohio's lead in working with local governments to post data on their spending as well.

The next step toward transparency might be for states to put the reams of financial data into context and figure out what was accomplished, he added.

"Are they on target? Have they completed 20 percent of the work? That's a lot of analysis, and it requires a lot of time and effort," he said. "That might be Transparency 2.0. We've got all this data out there, but what does it all mean?"

Poynter agreed that it would be helpful if states attached some meaning to the data they put online.

"There is so much information," he said. "At what point does it become overwhelming and it loses meaning? It's important to put the information in some kind of context."

Lembo said even state websites that, like his, have received an A have room for improvement.

"The technology has evolved so significantly that our work is never going to be ending," he said. "We're always going to be looking for the next best way to open the curtain and engage the public." •

— Jenni Bergal is a staff writer for the Pew Charitable Trusts' Stateline.

Why SDN matters: The case for reducing complexity

To understand the potential of software-defined networking, it is important to know where it came from and what it can do

BY MIKE YOUNKERS

Software-defined networking is a major trend in the IT industry, as big as cloud computing and data analytics. And as with many mega-trends, there exists a fair amount of confusion and rhetoric on the topic, which is dangerous for IT decision-makers inside and outside government.

Nevertheless, SDN is already helping improve operations at government agencies. To understand its potential, it is important to have some context on its origins, its current use and its prospects for the future.

WHAT IS THE PURPOSE OF SDN?

Every new technology product or approach starts with the need to overcome a challenge. The impetus for SDN was the incredible complexity that exists in designing, deploying and maintaining modern-day networks.

Networks do two things: They set up connections based on a set of criteria to identify the shortest, quickest or most secure path (the control plane) and then they move data across those connections (the data plane). The fundamental premise of SDN is to separate the decision-making happening in the control plane from the execution of those decisions in the data plane.

When the network frameworks were originally established, considerable effort was put into building layers into the data plane. Those layers make it simple, fast and efficient to change something in one layer without affecting any other layers in the same plane.

For example, when a faster physical technology comes along — think switching from copper to fiber — an upgrade can be done without affecting the higher layers.

Unfortunately, there is no similar layering within a network's control plane. Instead, numerous protocols determine how to set up connections. Over the years, more and more protocols have been added, creating ever greater complexity. By splitting the control plane from the data plane, the complexity of the control plane can be addressed without disturbing what already works well in the data plane.

Once the split occurs, we can apply good computer science principles in the control plane to solve similar problems once and then reuse that solution to reduce complexity. That's what defines SDN: Its fundamental purpose is to simplify the design, deployment and operation of networks by bringing rigor and structure to the control plane.

WHY DOES SDN MATTER FOR GOVERNMENT?

SDN solutions can help government CIOs address key challenges they are facing today. It can help improve user experience, increase agility, reduce IT complexity and lower operational costs as budgets decline. The new models offer the flexibility and scalability agencies need to innovate and enhance service offerings for citizens.

SDN is not easy. But there is no doubt that it can offer tremendous value for agencies as they seek to simplify and improve network operations.

Those features are attractive for agencies seeking to improve their network operations.

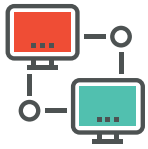
For instance, the Defense Information Systems Agency issued a request for information about SDN earlier this year to gain a better understanding of how experts in the network and cloud industries are innovating and using the new capabilities.

The smartest thing DISA did was openly pose three challenges their IT department faces and ask how industry would solve each with SDN. That is the right approach because it focuses on solving real problems with SDN capa-

How SDN works

We break down how one of the hottest new trends in IT today functions and how it can be used to benefit your network.

1 THE CONTROL PLANE VS. THE DATA PLANE



A network does two things: sets up connections based on a set of criteria to identify the shortest, quickest or most secure path and then moves data across those connections. Connections are set up on the **control plane**, and data is moved on the **data plane**.

2 LAYERING IN THE NETWORK PLANES

Layers are built into the **data plane**, which make it simple, fast and efficient to change something in one layer without affecting any other layers in the same plane.

The **control plane** has no similar layering. Instead, numerous protocols determine how to set up connections. More protocols have been added over the years, creating greater complexity.

3 THE SDN SOLUTION

With the planes split, good computer science principles can be applied to the **control plane** to solve similar problems once, then reuse those solutions to reduce complexity without disturbing anything in the **data plane**.

PROS OF USING SDN

- Helps improve user experience
- Increases agility
- Reduces IT complexity
- Lowers operational costs as budgets decline
- Offers the flexibility/scalability agencies need to innovate/enhance service offerings for citizens

bilities rather than looking at specific technology first.

Security is another reason the Defense Department and other agencies should be considering SDN. Typically, we think of the SDN controller as pushing policy and control messages "down" to the network elements. However, the SDN controller's ability to use two-way communications between controller/application and network elements can play a huge role in security. Agencies can improve threat detection by using the SDN controller to automatically alert the network to suspicious events and direct further investigation.

THE FUTURE OF SDN

The hype around SDN is growing in government and prompting many CIOs and CTOs to educate themselves on the technology's key concepts and benefits. It is important that agencies understand SDN capabilities and the options available to them before diving into the pool headfirst.

By taking advantage of SDN solutions that integrate with existing hardware and open-standard distributed routing protocols, agencies can ease SDN elements into their infrastructure and operations teams.

SDN is not easy. It can leave even the smartest minds in government IT confused and searching for answers. But there is no doubt that it can offer tremendous value for agencies as they seek to simplify and improve network operations. •

— Mike Younkers is senior director of systems engineering for Cisco's U.S. Federal team.

Multistate database cuts duplicate benefits

Hurricane Katrina prompted five states to pool their information to reduce fraud and abuse of disaster and food assistance

BY STEPHANIE KANOWITZ

In the wake of Hurricane Katrina in 2005, massive amounts of aid were pumped into five Gulf Coast states, and officials quickly realized they were facing the potential for abuse and fraud.

In response, Alabama, Florida, Georgia, Louisiana and Mississippi created the National Accuracy Clearinghouse (NAC), which uses identity analytics and advanced linking technology to find duplicate benefit applications in near-real time.

As a result, Mississippi is now saving about $161,000 a month — or $1.9 million a year — in duplicate benefit payments. And the group wants to expand its reach because the more states that participate, the more improper payments will be found, increasing the potential for savings.

"After Hurricane Katrina, there had been so many states involved in issuing food and disaster assistance, or [Disaster Supplemental Nutrition Assistance Program], there was a lot of room for duplicate participation and/or fraud across those states," said Joel Savell, NAC project director. "The states were limited in how they could prevent that and ensure program integrity. It was pretty much a manual process due to the extent of the disaster."

Beyond addressing fraud in disaster assistance, NAC helps the states reduce duplicative payments through the overall Supplemental Nutrition Assistance Program, which they had been doing individually and without much collaboration, Savell added.

The states regularly submit their data to NAC in an agreed-upon format. When people apply for assistance, NAC uses algorithms to find overlaps in identifying information across the

Distributing the massive influx of aid after Hurricane Katrina made state officials realize that they needed a better system to identify duplicate applications.

LORI MARTIN / SHUTTERSTOCK

states, such as names, Social Security numbers and birth dates.

For example, an application for assistance in Florida from someone who is already receiving assistance in Mississippi would be flagged. Florida officials would send a notice to their counterparts in Mississippi saying that the beneficiary had relocated to Florida so that Mississippi would stop sending payments, Savell said.

NAC can also detect duplicate applications and notify the other state. "In Mississippi, we even have that automated for the ones that are a high-confidence match," he said. "The system automatically emails the other state to a centralized email box for NAC."

AN INSTANT SUCCESS

The states tapped Iknow and LexisNexis Risk Solutions to design, implement, host and provide ongoing operational support for NAC. The companies used the Drupal content management system for interfaces that let states create reports, track use and search for dual participation, according to an Iknow project summary. They also tapped open-source high-performance computing cluster technology for its data-handling capabilities.

Information sharing happens in two ways: States can query NAC and get a real-time response, or they can submit requests through a batch or data file process each day and insert that information into their eligibility processes.

The information in NAC is updated automatically through a secure file transfer between the states and LexisNexis Risk Solutions. All the information is stored in the LexisNexis Secure Data Cloud.

The states ran a pilot test of NAC from June 2014 to May 2015. Last summer, the information from all five states was combined, and since then NAC has been applied to each new SNAP and D-SNAP applicant at enrollment.

Alabama and Mississippi saw 74 percent and 71 percent decreases, respectively, in the average number of dual participants per month after implementing NAC, according to the Public Consulting Group, which independently evaluated NAC. The organization also found that 72 percent of claims identified as dual participation were intentional program violations, and 25 percent were because of inadvertent client errors.

> "After Hurricane Katrina, there had been so many states involved in issuing food and disaster assistance...there was a lot of room for duplicate participation and/or fraud across those states."
>
> – JOEL SAVELL, NAC

Following that success, the five states and PCG are finalizing plans to bring other states on board. A report was due to the U.S. Agriculture Department's Food and Nutrition Service, which provided a grant for NAC's development, by the end of August. FNS will write its own report for Congress by the end of November.

A WILLINGNESS TO COLLABORATE

Tim Meeks, NAC's project lead, attributes the system's success not only to detecting and preventing more duplication but also to the states' willingness to collaborate.

"The states came together prior to the pilot...and created a common set of business rules," he said. "All the states were following the same set of rules specifically related to dual participation matches within the NAC process."

The investment in NAC has been minimal for the states, which can use existing automation and secure file transfer and web services to implement it. New states must pay a setup fee, and all participants pay an annual hosting fee that is based on the average household member count for that state.

In Mississippi, the hosting fee is $60,000 per year, but the system is identifying and preventing an average of more than 300 dual beneficiaries each month — for monthly savings of $161,000 after the hosting fee, Savell said.

States stand to earn a return on investment within a month of using NAC, and as additional states sign on, the savings will grow.

"We know we will have the potential for dual participation in just about every state in the nation," Savell said. "So that is a very conservative number as far as savings is concerned because it only focuses on the other four states."

NAC is the product of a public/private collaboration, but all states currently use the Public Assistance Reporting Information System, a federal/state data-matching service that detects potential fraud. But the system's process is labor-intensive and misses warning signs, according to a whitepaper from LexisNexis. As a result, Meeks and Savell said they hope NAC sees wider adoption after Congress reviews their report. •

County first responders get mobile data system

Maryland's Frederick County installed laptops in fire and rescue vehicles to share real-time data and reduce voice radio traffic

BY AMANDA ZIADEH

Maryland's Frederick County has integrated ruggedized Panasonic CF-53 laptops into 172 fire and rescue vehicles to reduce voice radio traffic and enhance public safety.

"As our fire and rescue system gets bigger, voice radio traffic becomes almost a detriment because you begin to have messages about fire and rescue incidents get mingled together and become confusing and in some cases can slow us down," said Tom Owens, director and chief of the county's Division of Fire and Rescue Services.

The laptops for first responders and dispatchers provide a better alternative to voice communications. The computers connect with dispatch centers through wireless cellular networks and are connected to the county's data infrastructure "to provide the best security measures," said Stephani Stockman, a software integrator at Frederick County's Interagency Information Technologies Division. Data shared through the county's private network is encrypted.

The laptops use Intergraph's Mobile for Public Safety 9.1 incident management software to communicate with the computer-aided dispatch software that the county has used since 2005. The new solution is expected to provide a more seamless stream of real-time data and workflow management.

When units are sent to an incident, responders will receive a message through the mobile data terminal that gives them the address and any other pertinent information. Without using radio communications, the dispatch center can track which units and personnel are responding.

While en route, responders can receive information about changing conditions at the scene without generating voice radio traffic. The system uses maps generated by the county's Geographic Information System Department to pinpoint addresses, locate fire hydrants and reveal blind spots in approaching intersections. GPS data lets responders see the locations of all the county's other emergency vehicles as they respond to an incident.

In addition to saving the county money and providing immediate, automated information to responding units, the mobile data terminals are expected to ease the workload for 911 dispatchers.

"Less voice interaction [and] more work with the computers — which they are doing as part of the regular process anyway — really make the communication process with our responding units much more efficient," Owens said.

Initially, cellular network availability was a challenge, and testing with earlier deployments left room for adjustments. "We tested for several months in advance in a training environment as well as [with] selected users in the live environment," Stockman said.

To handle the new equipment, first responders, volunteers and career personnel were offered months of hands-on classroom training that included sample call scenarios, refreshers and helpful reference documents.

The county-funded project cost $975,000, and the new software has been made available to other local government agencies in the area that also rely on mobile data terminals. •

LISSANDRA MELO / SHUTTERSTOCK

10 steps to secure your print processes

Multifunction printers are as vulnerable as computers, so agencies must incorporate them into information security plans

BY CHRIS STRAMMIELLO

The Federal Trade Commission's recent report, "Copier Data Security: A Guide for Businesses," makes a succinct yet powerful statement that is sure to get the attention of any organization: "Digital copiers are computers," and organizations should incorporate those devices into their information security plans.

Digital copiers, also known as multifunction printers (MFPs), can print, scan, copy and fax. They have hard drives, embedded firmware and the ability to communicate with other systems on the network. They are susceptible to the same security vulnerabilities that a computer is, and without the proper security measures, MFPs pose a significant risk of sensitive information exposure.

Networked MFPs are now common in the workplace, and employees use them daily to print, scan and fax documents over the network. In many instances, those documents contain sensitive information. To prevent damaging data breaches, government organizations must control and protect both the physical and electronic access points on their MFPs.

Here are 10 specific steps that agencies must consider to secure MFPs, based on common scenarios that exist in most environments.

1 Require user authentication

There is no MFP more unsecure than one that allows anonymous use. Such devices are susceptible to various forms of abuse and can make tracing the source of a data breach or leak virtually impossible. Authentication enables the auditing, reporting and tracking of user activity and various other security features.

2 Restrict access based on user authorization

Just because a user has authenticated into the system, that doesn't mean he should have access to every function. At the MFPs, users should only have access to the network resources they normally do.

3 Centrally audit all network activity

Security standards require most organizations to implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports. Centrally building an audit trail of all copy, print, scan, email and fax activity at every networked MFP will bring use of those devices into compliance.

4 Encrypt data to and from MFPs

All data transmitted to and from an MFP should be encrypted. Government agencies must use encryption technology that meets specific security guidelines defined by Federal Information Processing Standard Publication 140-2.

5 Implement pull printing

To avoid exposing sensitive documents, secure printing requires that users authenticate at the device before documents are released. The device must print only those documents that are associated with the authenticated user, and the print job must not be stored on the device prior to printing.

6 Implement rules-based printing

Rules-based printing controls output by analyzing print jobs according to a set of established rules before releasing them. Organizations with established print policies, such as U.S. Army Directive 2013-26 "Armywide Management of Printing and Copying Devices" or the General Services Administration's PrintWise program, can enforce those policies by implementing rules-based printing.

7 Enforce trusted destinations

Once necessary measures have been taken to restrict access to an MFP's network functions through authentication and authorization controls, agencies must ensure that the devices are configured to prevent documents from being scanned or faxed to destinations that might risk the exposure of sensitive information. A common high-risk scenario is a networked MFP that is configured for scan-to-email and outbound analog faxing without controls in place to validate the email address or fax number of the recipient.

8 Monitor and control PII activity

Most government organizations have policies to protect personally identifiable information and other sensitive content. For example, the Department of Homeland Security issued a handbook with mandatory guidelines for all employees to follow to protect PII within and outside the organization. Similarly, the Navy published a guide containing compliance requirements and protective measures to safeguard Navy and Marine Corps information. Agencies should use software to systematically enforce the PII policies they have enacted. Without a solution in place, organizations must rely on employees to follow the protocol, which leaves no room for user error.

9 Standardize and integrate network scanning

One common problem with traditionally configured MFPs is that no two devices in an organization are set up the same way for document scanning. However, standardization would enable administrators to centrally control network folder scanning with a single configuration. Integration support is also important for all major commercial document systems to ensure direct and secure scanning.

10 Control access points

To prevent damaging data breaches, government organizations must control and protect both the physical and electronic access points on their MFPs. The penalties, settlements and costs for failing to safeguard sensitive information are increasing, and there are simply too many touch points that create risk in sharing information. Most of them involve the technologies that organizations are counting on — especially networked MFPs that copy, print, scan, fax and email.

Agencies must act to enable the compliant exchange of sensitive information by adding a layer of security and control to paper-based and electronic processes. They need an approach that transparently applies automated security techniques that cannot be circumvented and that authenticate users, control access to workflows, encrypt data, validate network destinations, monitor and control all documents containing PII, and build and maintain an audit trail of user activity.

By adopting that approach, government organizations can minimize the manual work and decisions that introduce human error, mitigate the risk of non-compliance and avoid the damaging costs of sensitive data exposure. •

— Chris Strammiello is vice president of global alliances and strategic marketing at Nuance Communications.

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

MEDIA CONSULTANTS

Mary Martin
(703) 222-2977
mmartin@1105media.com

Bill Cooper
(650) 961-1760
bcooper@1105media.com

Matt Lally
(973) 600-2749
mlally@1105media.com

Ted Chase
(703) 876-5019
tchase@1105media.com

PRODUCTION COORDINATOR

Lee Alexander
(818) 814-5275
lalexander@1105media.com

PUBLIC SECTOR MEDIA GROUP
CORPORATE HEADQUARTERS
9201 Oakdale Ave., Suite 101
Chatsworth, CA 91311
www.1105media.com

WISHLIST

Tech we hope to see in the p

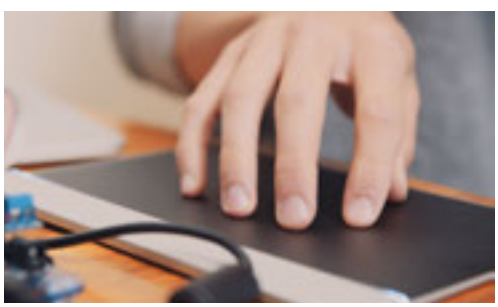
Eora 3D

High-resolution 3D scanning has been challenging, particularly in the field. But Eora 3D is one of several new solutions that turn ordinary smartphones into portable imaging stations. A typical scan can capture 8 million points in less than five minutes. A tripod mount and a Bluetooth-controlled turntable offer additional flexibility for capturing objects large and small.

MultiFab

Additive manufacturing has massive potential – NASA recently tested a 3D-printed rocket fuel pump – but printing with more than one material is still difficult and expensive. Researchers at MIT's Computer Science and Artificial Intelligence Laboratory, however, have developed a device that can print with 10 materials at once and do so at a resolution of 40 microns.

What new technologies do you think GCN readers should learn more about? Tell us on Twitter: **@GCNtech #GCNwishlist**.



Sensel Morph

Is it finally time for a new approach to input? The Sensel Morph looks like an ordinary trackpad, but this multitouch device takes sensitivity to new levels. It has a grid of 20,000 force sensors, allowing even the lightest brushstrokes or fingertip shifts to be detected. The device can detect as many as 16 touches simultaneously and is built to accommodate overlays tailored to specific uses.

ACQUIRE

Acquisition & Management Show

Coming June 2016!

2016

JUNE 8-9

WALTER E. WASHINGTON CONVENTION CENTER

WASHINGTON, DC

Exhibit space is now available!

Contact Stacy Money for pricing & details

smoney@1105media.com 415.444.6933

ACQUIREshow.com

Tracks Include

- ACQUIRE Office Management
- ACQUIRE Professional Services
- ACQUIRE Information Technology
  - FEDERAL IT ACQUISITION SUMMIT
- ACQUIRE Acquisition Management
- ACQUIRE Project Management
- ACQUIRE Industry Days
  - Washington Technology
- ACQUIRE Happy Fed
  - Federal SOUP

IBM Hybrid Cloud:

If you have to choose between freedom and security, don't.

There's a new way to cloud. With the IBM hybrid cloud, more flexibility doesn't mean less control. You're free to mix and match public and private cloud environments to run the services and apps you need while maintaining security across all your systems. Learn more at ibm.com/madewithibm

Smarter clouds are made with IBM.