GCN

TECHNOLOGY, TOOLS AND TACTICS FOR PUBLIC SECTOR IT

AUGUST 2015 • VOLUME 34, ISSUE 8

FEATURE:
Defending against drones
Page 22

HOW TO:
Where to start with CX
Page 30

TOO OLD TO DIE

Deciding what to do about legacy systems

PAGE 13, 14 & 16

STAND
SIT

INSIDE

FEATURES

CASE STUDIES

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

HOW TO

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

Editor-In-Chief Troy K. Schneider
Executive Editor Susan Miller
Print Managing Editor Terri J. Huck
Senior Editor Paul McCloskey
Reporter/Producers Derek Major, Amanda Ziadeh
Contributing Writers Kathleen Hickey, Stephanie Kanowitz, Will Kelly, Suzette Lohmeyer, Carolyn Duffy Marsan, Patrick Marshall, Brian Robinson
Editorial Fellow Mark Pomerleau

Vice President, Art and Brand Design
Scott Shultz
Creative Director Jeff Langkau
Assistant Art Director Dragutin Cvijanovic
Senior Web Designer Martin Peace
Director, Print Production David Seymour
Print Production Coordinator Lee Alexander
Chief Revenue Officer Dan LaBianca

PUBLIC SECTOR MEDIA GROUP

Chief Operating Officer and Public Sector Media Group President
Henry Allain

Co-President and Chief Content Officer
Anne A. Armstrong

Chief Revenue Officer
Dan LaBianca

Chief Marketing Officer
Carmel McDonagh

Advertising and Sales
Chief Revenue Officer **Dan LaBianca**
Senior Sales Director, Events **Stacy Money**
Director of Sales **David Tucker**
Senior Sales Account Executive **Jean Dellarobba**
Media Consultants **Ted Chase, Bill Cooper, Matt Lally, Mary Martin, Mary Keenan**
Event Sponsorships **Alyce Morrison, Kharry Wolinsky**

Art Staff
Vice President, Art and Brand Design **Scott Shultz**
Creative Director **Jeffrey Langkau**
Associate Creative Director **Scott Rovin**
Senior Art Director **Deirdre Hoffman**
Art Director **Joshua Gould**
Art Director **Michele Singh**
Assistant Art Director **Dragutin Cvijanovic**
Senior Graphic Designer **Alan Tao**
Graphic Designer **Erin Horlacher**
Senior Web Designer **Martin Peace**

Print Production Staff
Director, Print Production **David Seymour**
Print Production Coordinator **Lee Alexander**

Online/Digital Media (Technical)
Vice President, Digital Strategy **Becky Nagel**
Senior Site Administrator **Shane Lee**
Site Administrator **Biswarup Bhattacharjee**
Senior Front-End Developer **Rodrigo Munoz**
Junior Front-End Developer **Anya Smolinski**
Executive Producer, New Media **Michael Domingo**
Site Associate **James Bowling**

Lead Services
Vice President, Lead Services **Michele Imgrund**
Senior Director, Audience Development & Data Procurement **Annette Levee**
Director, Custom Assets & Client Services **Mallory Bundy**
Editorial Director **Ed Zintel**
Project Manager, Client Services **Michele Long**
Project Coordinator, Client Services **Olivia Urizar**
Manager, Lead Generation Marketing **Andrew Spangler**
Coordinators, Lead Generation Marketing **Naija Bryant, Jason Pickup, Amber Stephens**

Marketing
Chief Marketing Officer **Carmel McDonagh**
Vice President, Marketing **Emily Jacobs**
Director, Custom Events **Nicole Szabo**
Audience Development Manager **Becky Fenton**
Senior Director, Audience Development & Data Procurement **Annette Levee**
Custom Editorial Director **John Monroe**
Senior Manager, Marketing **Christopher Morales**
Marketing Coordinator **Alicia Chew**
Manager, Audience Development **Tracy Kerley**
Senior Coordinator **Casey Stankus**

FederalSoup and Washington Technology
General Manager **Kristi Dougherty**

OTHER PSMG BRANDS

FCW
Editor-in-Chief **Troy K. Schneider**
Executive Editor **John Bicknell**
Managing Editor **Terri J. Huck**
Senior Staff Writer **Adam Mazmanian**
Staff Writers **Sean Lyngaas, Zach Noble, Mark Rockwell**
Editorial Fellows **Eli Gorski, Jonathan Lutton, Bianca Spinosa**

Defense Systems
Editor-in-Chief **Kevin McCaney**

Washington Technology
Editor-in-Chief **Nick Wakeman**
Senior Staff Writer **Mark Hoover**

Federal Soup
Managing Editors **Phil Piemonte, Sherkiya Wedgeworth**

THE Journal
Editor-in-Chief **Christopher Piehler**

Campus Technology
Executive Editor **Rhea Kelly**

1105MEDIA INC

Chief Executive Officer
Rajeev Kapur

Chief Operating Officer
Henry Allain

Senior Vice President & Chief Financial Officer
Richard Vitale

Executive Vice President
Michael J. Valenti

Vice President, Information Technology & Application Development
Erik A. Lindgren

Chairman of the Board
Jeffrey S. Klein

NSA-grade mobile encryption on its way

BY STEPHANIE KANOWITZ

Given the government's current focus on protecting information, USMobile officials hope to find a ready market for an app that lets employees use their personal smartphones for top-secret communications.

Scrambl3 creates a secure virtual private network that uses end-to-end encryption to send messages from personal devices to an agency server. The company developed the technology when it worked with the National Security Agency to create Fishbowl, a secure phone network available only to Defense Department users.

"We've implemented Fishbowl in the form of a software-defined network, so all of those typical hardware components that you'd find in a mobile network — routers, VPNs, gateways, firewalls, proxy servers — all of those components are expressed or implemented in our system in the form of software," said Jon Hanour, USMobile's president and CEO.

"We've made an affordable version of Fishbowl," he added.

Scrambl3 uses a layered, defense-in-depth approach. Encrypted voice-over-IP calls travel through a VPN connection. When a user logs into the app on a smartphone, it creates a VPN that connects to the agency's server.

With Scrambl3 Enterprise, administrators can set up lists of contacts with whom each user can communicate via the VPN.

Once connected, users can see who among their contacts is also logged in, and then choose whether to communicate with them via email, voice call or text.

"Once you establish this powerful VPN, you can run anything through it," Hanour said. "Anything that you can put on a server, you can use Scrambl3 to communicate with."

Calls are highly encrypted until they reach the recipient, where the app decrypts them. That communication happens at a top-secret grade level as specified by NSA.

Despite that encryption/decryption process, latency is unnoticeable, Hanour said.

For additional protection, nothing is recorded — users can't even leave voicemail — unless the agency specifies otherwise.

The law enforcement community is a prime customer for Scrambl3 because public cell phone networks don't meet heightened police security standards, and photographic evidence requires a secure uploading process.

"The advantage of this architecture is that the communication that the mobile device management software would typically have with the device...can now run inside the VPN, so it makes that even more secure," Hanour said.

"It creates value for the mobile device management system as well because you can protect it inside the VPN," he added.

The solution is scheduled to be commercially available in October, and it will work with Android and Apple iOS devices. •

Obama seeks exascale computing

BY TROY K. SCHNEIDER

President Barack Obama wants an exascale computer, and he is creating a "whole-of-government" initiative to drive the development of supercomputers that far outpace current models.

In a July 29 executive order, Obama established the National Strategic Computing Initiative "to create a cohesive, multi-agency strategic vision and federal investment strategy, executed in collaboration with industry and academia, to maximize the benefits of [high-performance computing] for the United States."

NSCI will be driven largely by the National Science Foundation and the departments of Defense and Energy.

In addition, NASA, the FBI, the Department of Homeland Security, the National Institutes of Health and the Commerce Department's National Oceanic and Atmospheric Administration are designated as the five "deployment agencies" that will put the planned computers to use and take part in planning and development efforts.

The fastest supercomputer in the world today is China's Tianhe-2, which runs at 33.86 petaflops. In April, DOE announced a $200 million investment in a supercomputer that is expected to produce a peak performance of 180 petaflops when it is delivered in 2018.

Exascale computing, which is the stated goal for NSCI, means 1,000 petaflops or higher. •

Boston PD uses new records system to solve cases faster

BY DEREK MAJOR

The Boston Police Department had been using the same records management system for 20 years, and Deputy Superintendent John Daley had a number of reasons for wanting to replace it.

"It was built on an aging architecture, and our requirements had outgrown its feature set," he said.

To replace that system, the department contracted with Intergraph for its inPURSUIT system, which is designed to help solve cases more quickly.

"The Intergraph system...ultimately will enhance the safety of the community and of our officers," Daley said. "Officers and investigators will have access to information in the new system that, previously, they may have had to seek in a dozen legacy systems, if it existed at all."

The inPURSUIT system's master indices link individuals to multiple types of information, such as cases, vehicles and addresses, and that approach gives police more complete information for criminal investigations.

The entire department was trained to use the new system, but there were challenges. "Any time change is introduced into someone's routine, there will be a period of adjustment, and the new system is much more comprehensive in the types of information it can collect," Daley said. "In some cases, it requires more effort from officers in the field." •

READ ME

What: "Transform Government from the Outside In," a report by Forrester Research.

Why: Seven of the 10 worst organizations in Forrester's U.S. Customer Experience Index are federal agencies, and only a third of Americans say their experience with the government meets expectations.

Findings: Forrester said governments must embrace mobile, turn big data into actionable insights, improve the customer experience and accelerate digital government.

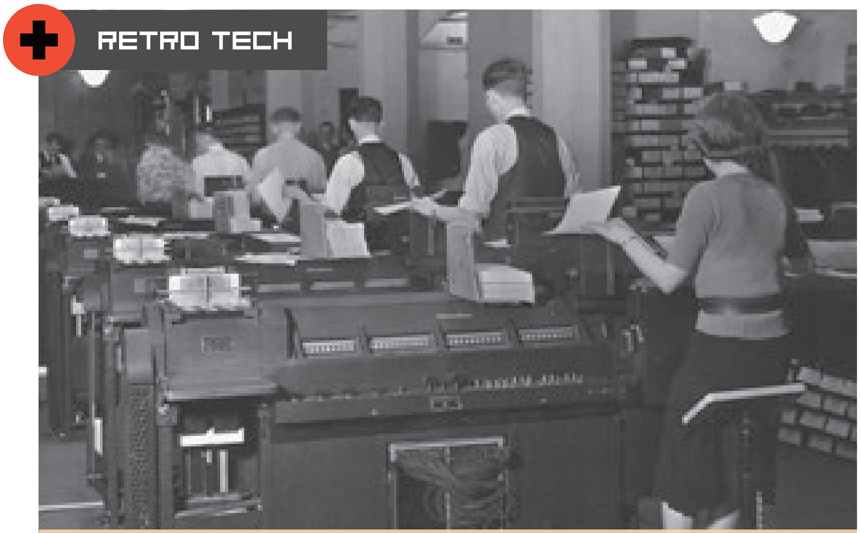
Agencies must start by making mobile the primary platform for connecting with citizens.

Government agencies must also find ways to integrate, share and use the large amounts of data they collect. By aggregating data, governments can increase responsiveness and make better short-term decisions and long-term plans.

Better customer experience can improve the efficacy of legislation, compliance, engagement and the effectiveness of government offices. That means making processes easier and available via user-friendly websites.

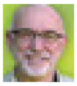
Takeaway: Improving the government customer experience requires accelerating the pace toward digital government through integrated mobile and analytics technologies and practices.

RETRO TECH



GCN has covered government IT since 1982, and the technology itself started earlier still. In this 1940 photo, for example, Social Security Administration clerks use massive tabulating machines to manage the records of millions of Americans.

EVERETT HISTORICAL/SHUTTERSTOCK



CYBEREYE
BY BRIAN ROBINSON

Windows XP: The operating system that just won't die

IT'S BEEN ONE of the longest retirement parties in the IT world, but we should finally be able to say that Windows XP is gone.

Except that it isn't, and what that means for the security of a large slab of government users is an open question.

Microsoft officially ended its support for XP in April 2014, meaning it would not provide any more versions of the venerable operating system that was introduced way back in 2001.

Last year, it also stopped providing security patches for XP, though it continued to deliver anti-malware signature updates for a time.

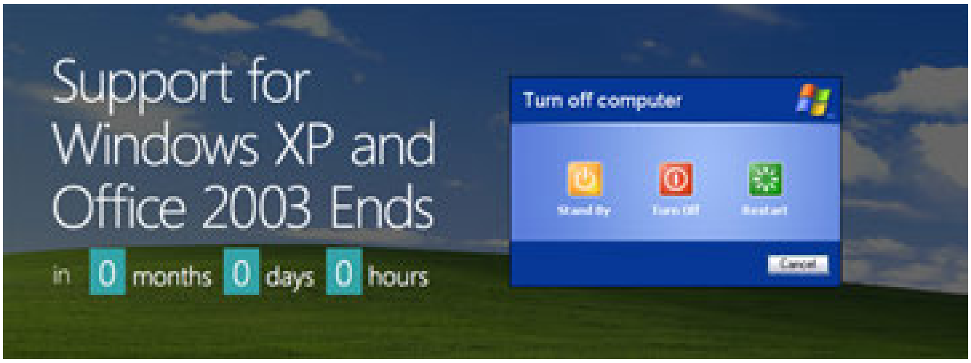
That last grace period finally came to an end on July 14 when Microsoft finished with XP signature updates and the use of its Malicious Software Removal Tool for XP. If your XP machine gets infected with malware from now on, that's just too bad.

OK, you say, every agency must have figured this out a long time ago and ditched XP in favor of another operating system that is regularly updated.

If only that were so. Unfortunately, there still seem to be plenty of these old systems around. Earlier this year, market analyst Net Applications said XP makes up nearly 17 percent of the total worldwide desktop operating system market.

Other analysts have cited a lower percentage, but they still say more than 10 percent of desktop users work with XP.

There are no overall figures for government use, but occasional revelations indicate that the number is not insubstantial. The Labor Department's CIO was quoted earlier this year as saying there were still some 10,000 XP users at her agency, while the two-year, $9.1 million contract the Navy recently signed with Microsoft for direct support of 100,000 mission-critical systems included thousands of XP computers.



Labor and the Navy are trying to transition away from those kinds of legacy systems, and so must the other agencies still running the aged operating system.

However, no one knows how vulnerable the machines are.

In the wake of the recently announced breaches at the Office of Personnel Management, OPM executives admitted the attacks on their systems could have been going on for at least a year, which means there's a good chance that some XP systems have been successfully penetrated. And attackers need only one infected machine to access other systems in the enterprise.

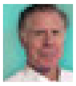
So, you say, at the very least agencies must be targeting those old XP systems as a priority for replacement. Again, that's hard to say. And some recent reports and surveys indicate that it's hard to unite desire and reality in government IT.

In a recent survey, the Professional Services Council reported that cybersecurity remains the top priority for government CIOs, but modernizing the IT environment in a way that could aid their cybersecurity efforts remains a challenge for many because the predominant portion of their IT budgets goes to maintaining legacy systems. The Defense Department, for example, said only 20 percent of its budget is available for investing in next-generation solutions.

The situation is no better at the state and local level. In a study of state IT investment management strategies, a National Association of State CIOs report states that nearly half of its members spend 80 cents of every IT dollar on maintaining existing systems.

What all this suggests is that old Windows XP systems could be a problem for cybersecurity for some years yet, particularly if replacing them gets lost in the intense competition among IT priorities.

According to Microsoft, Windows XP is now dead, dead, dead. Except when it's not. •



EMERGING TECH

BY PATRICK MARSHALL

Oakland builds real-time crime apps for residents and police

WHEN THE OAKLAND, CALIF., Police Department asked Ahsan Baig's team for a way to publish its 911 call data, his initial idea was to build a Web-based app that residents could use to check on incidents in their neighborhoods.

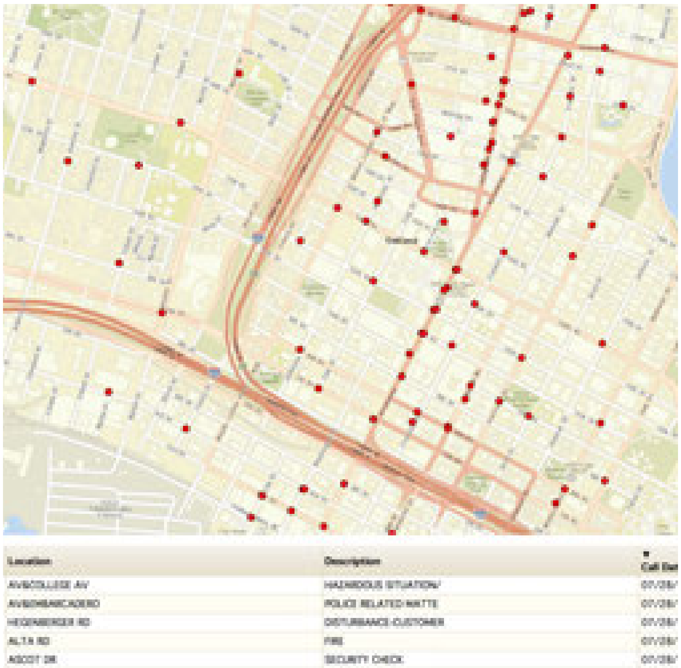
Police officials wanted to provide the data as a spreadsheet, said Baig, the city's division manager of public safety services and business applications. As it happened, however, Baig's team was in the middle of a major GIS platform upgrade.

“We looked at the request and said, ‘You know, there's a better way of doing this. We could put together an application that would provide you with more of the information that you're looking for,'” he said.

Baig turned to his primary GIS software provider — Esri — for help in building the app, which was developed using the company's ArcGIS platform.

Three months later, in June 2015, the Oakland Police Department's Calls for Service app was launched. The Web-based app allows residents to view incident reports in near-real time, either as point data on the map of Oakland or in tabular form.

For now, the information provided is succinct and includes only the date and time of the incident, a very brief (one- to four-word) description of the incident, the police beat, council district and incident number. The app does not include information on some categories of crimes — rape, terrorist threats, suspected child abuse — that might involve ongoing security issues or violate victims' rights.



Location	Description	Call Dat
AV&COLLEGE AV	HAZARDOUS SITUATION/	07/28/
AV&EMBARCADERO	POLICE RELATED MATTE	07/28/
HEGENBERGER RD	DISTURBANCE-CUSTOMER	07/28/
ALTA RD	FIRE	07/28/
ASCOT DR	SECURITY CHECK	07/28/

The Oakland, Calif., Calls for Service app allows residents to view police incident reports in near-real time.

CITY OF OAKLAND

One pleasant surprise for the police was that when Baig's team built the public app, they also built internal dashboards for the officers.

Not surprisingly, the internal app offers access to much more detailed data. Each area commander has a custom dashboard that focuses on data for that area and includes additional details about the incidents and real-time information such as which officers are responding, their level of experience and skill sets.

The response to the internal dashboards has been enthusiastic. “Our command staff was really amazed,” Baig said. As a result, “we're using that internal application as a launching pad. We're going to have more layers of real-time information, including vehicle locations.”

While the public Calls for Service app has not been available long enough to provide a meaningful measure of its impact, Baig said the site gets a good number of hits.

“So far, we have very positive feedback,” Baig said. “People are liking it.”

He added that residents have started asking for the information to be sent via an RSS or XML feed, a feature that the city expects to add in the near future.

Baig is also looking into the possibility of adding one-click way for residents to provide information about incidents.

“Maybe when you open up an incident, we can have a resident quick form where they can provide additional information,” he said, similar to the way people can currently contribute information about potholes or broken streetlights.

Oakland's approach to public and internal crime dashboards has generated inquiries from police departments in other cities, including Chicago, Berkeley and several towns in Southern California. •

13TH ANNUAL

ENTERPRISE ARCHITECTURE

EA TODAY: MAKING THE MISSION POSSIBLE

EVENT BEGINS IN 1 MONTH!

EA TODAY: MAKING THE MISSION POSSIBLE

How? Find Out at the Enterprise Architecture Conference!

WORKSHOPS: OCTOBER 5
CONFERENCE: OCTOBER 6–7
WASHINGTON, DC
WALTER E. WASHINGTON CONVENTION CENTER

THE 13TH ANNUAL ENTERPRISE ARCHITECTURE EVENT IS THE PREMIER educational forum for enterprise architects and project managers to convene and learn from expert practitioners in EA on the latest methods, frameworks and policies impacting the EA community.

EDUCATION TRACKS INCLUDE:

- Achieve Mission Outcomes
- Strengthen Enterprise Management

SESSION TOPICS WILL INCLUDE:

- Agile
- Security and Privacy
- Business Analytics
- Big Data
- Role of the Chief Data Officer

… just to name a few!

Attendees will receive an official certificate of attendance and CEUs for participating at this highly anticipated event.

Reserve Your Seat Today —
Space is Limitied!

GovEAconference.com

USE PRIORITY CODE: EAE15

PRESENTING SPONSORS

FEAC Institute

ZACHMAN INTERNATIONAL ENTERPRISE ARCHITECTURE

EVENT SPONSORS

In2itive

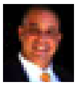
software AG Government Solutions

PARTNERING MEDIA

OMG WE SET THE STANDARD

PRODUCED BY

PUBLIC SECTOR EVENTS GROUP



INDUSTRY INSIGHT

BY JOHN ZAROUR

How to avoid becoming the next OPM

AS WE LEARN MORE about the Office of Personnel Management data breaches, federal leaders are left wondering how such incidents can occur and whether other agencies are vulnerable to similar attacks. The incident prompted Federal CIO Tony Scott to initiate a 30-day cybersecurity "sprint" that called on agencies to evaluate their security practices and address vulnerabilities.

But federal agencies aren't the only ones that should be re-evaluating their approach to security.

State and local governments are also undoubtedly on the radar of today's advanced cyberthreat actors. States collect valuable data, and many agencies store citizens' personally identifiable information just as the feds do. So while attention is focused on solving cybersecurity in D.C., states should also be watching closely and investing in their own cyber defense efforts.

To effectively address today's security needs, state and local IT leaders must embrace new ideas and innovative technologies.

One of the biggest opportunities for improving security is through data analytics. Government organizations at every level — from the biggest federal agencies down to local government — are producing, collecting and storing more data from more sources than ever before. Managing and using that information are daunting tasks for state and local governments, which have limited resources and budgets.

The biggest reason agencies aren't making the most of their data is that they don't have the right tools in place to do so. That's not to say analysis isn't happening. There are many state agencies that are successfully analyzing data and finding value in the information. In most cases, however, the analysis is happening in silos using multiple technologies for different datasets, which provides a limited view of the intelligence.

States that wish to improve security practices and achieve operational, single-pane visibility should make sure they adopt analytics solutions that have:

- The ability to pull in machine data from disparate sources for analysis and the scalability to accept new data sources as they emerge.
- The flexibility to correlate the data from multiple sources (logs, clouds, applications, sensors, networks, etc.) and visualize it via dashboards.
- The speed to perform analysis quickly and support real-time responses to security breaches.

Another emerging capability that is becoming increasingly relevant for government is behavioral analytics. Most recent government breaches, including the ones at OPM, were perpetrated by actors with legitimate credentials, and the same tactic has been used to infiltrate state and local government systems. Therefore, one of the keys to preventing a serious security incident is focusing on detecting the threats that are already on the network, whether they are insiders or external attackers who have illegally obtained valid credentials.

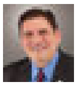
Technologies that tap into machine-learning and data-driven behavioral analytics are better equipped to defend against breaches than traditional security information and event management solutions. The right approach can enable security systems to identify anomalous behaviors by users and automatically tag them for further investigation.

Comprehensive analytics capabilities are important to the security and modernization of state and local government. Security operations and policy changes are driven by intelligent decision-making, but gathering data and converting it into actionable intelligence are difficult without the right technologies to support the process. Platform analytics enable both proactive detection and defensive threat mitigation, and the information can be shared across agency departments and deliver value more quickly.

While attention is focused on solving cybersecurity in D.C., states should also be investing in their own cyber defense efforts.

State and local agencies would be wise to keep all this in mind as they re-evaluate their security posture and explore investing in solutions to help prevent their own OPM-like breaches. •

— *John Zarour is director of state and local government and K-12 at Splunk.*



INDUSTRY INSIGHT

BY TONY ENCINIAS

Mainframe as a service: Big iron without big headaches

ALTHOUGH THEY ARE CONSIDERED very old technology, mainframe environments are still widely used to manage large-scale batch and transaction processing jobs.

Without mainframes, most state governments could not operate their departments of health and human services, tax departments or departments of motor vehicles, or run the numerous other baseline governance activities on which taxpayers depend.

The technicians who know how to manage those environments are aging as well. It is estimated that 35 percent to 40 percent of the workforce trained on mainframes could retire tomorrow.

Most CIOs would probably elect to replace their mainframes with more advanced cloud computing and storage solutions. However, governments often have enough funds to run their mainframes but not the funds (or the appetite for new taxes) to replace them. That leaves CIOs with the choice of managing existing mainframe environments with the staff available today or choosing mainframe as a service (MaaS), which provides computing and storage capabilities as a cloud service.

Government institutions will be dependent on mainframes for years to come, even with the advances in cloud computing. But the talent constraints combined with the cost of replacing mainframes argue for outsourcing the infrastructure and support to capable third parties.

The key benefit of MaaS is that the provider pays for the maintenance and upgrades to IT infrastructure, which can mean dramatic cost and risk avoidance for government CIOs.

> Talent constraints combined with the cost of replacing mainframes argue for outsourcing the infrastructure and support.

The MaaS user pays only for the computing, storage and batch time consumed in the course of normal operations. That approach frees government employees to focus on their business functions rather than on the IT infrastructure.

Best of all, CIOs can ditch the nerve-jangling task of maintaining aging computer equipment.

A deeper examination of MaaS reveals a longer list of benefits, including:

- **Scale.** MaaS allows users to scale up or down according to their changing requirements.
- **Continuity.** MaaS offers assurances of business continuity because vendors can offer redundancy that agencies might find cost-prohibitive. It means markedly reduced downtime in the event of a mainframe failure and assurances of full recovery in the event of a disaster because data is mirrored at a second site.
- **Ease of migration.** The MaaS vendor runs the same IBM z Systems mainframes that governments are running, so migration is smooth.
- **Predictable costs.** Top-tier vendors will offer a service-level agreement that gives accurate predictions of the cost of transportation, installation, de-installation, configuration, initial training, requested levels of managed service and preventive maintenance. Users of MaaS move to a consumption model for mainframe services and pay for them out of operating expenses rather than capital expenses.
- **Support.** The best MaaS vendors offer 24/7/365 support.
- **No deactivation charges.** Top-tier providers will have no minimum charges and no penalty for deactivation of services, which offers great operational flexibility to CIOs or others managing the mainframe environment.

It would probably be to agencies' advantage to replace mainframes over the long term. But budget constraints often force the government to settle for an interim solution that gets the job done. And MaaS allows agencies to get top performance without having to pay outright for top-tier IT infrastructure.

The rising popularity of MaaS is easy to understand once all its benefits are taken into account. Adopting MaaS is just a matter of a new mindset in terms of how mainframe services are consumed, but clearly, it is becoming a top option for mainframe operators looking for prudent solutions to today's pressing personnel and budget constraints. •

— Tony Encinias is vice president of public-sector strategy at ViON and former CIO of the Commonwealth of Pennsylvania.

INDUSTRY INSIGHT

BY CHRIS O'MALLEY

The misunderstood mainframe is ready for another round

WHAT CAN BE REPLACED in favor of newer, more efficient, safer technology? CIOs and CTOs of large organizations constantly ask the legacy question. And not just because the Office of Personnel Management's recent data breaches have raised that inquiry for the mainframe and its Cobol programming language. A deeper examination is warranted, but it's likely the ultra-secure mainframe was not to blame.

Underappreciated in our cloud-fixated era, the mainframe is in fact the most powerful, cost-efficient technology fueling government databases and applications. It has retained that distinction throughout its 63-year history and should prompt us to review our negative perceptions of legacy systems.

How has the mainframe managed that longevity? There are several answers, but one is its ability to constantly modernize, adapt and address new technology needs. Look closely and you'll see that, right now, we are in the early stages of another period of mainframe rejuvenation. Here are the early clues.

Look closely and you'll see that, right now, we are in the early stages of another period of mainframe rejuvenation.

The one bright spot in IBM's recent earnings was the mainframe. Sales of the new z13 — a machine capable of handling 100 Cyber Mondays every day — grew 9 percent, with 24 percent capacity growth. That was particularly impressive given last year's strong quarterly performance; IBM's mainframe business had a difficult revenue comparison to beat.

Another clue is the disconnect between the number of organizations exploring mainframe migrations and the rare few actually executing them. My colleagues and I are hearing this from several industry analysts, and their anecdotal evidence is supported by a recent global survey of CIOs in which 88 percent said the mainframe will continue to be a key business asset in the next decade.

Other notable results from that survey:

- 81 percent said their mainframes are running new or different workloads than they did five years ago and handling greater big-data throughput.
- 78 percent see the mainframe as a key driver of innovation.
- And in a finding particularly relevant to the OPM breach: 70 percent of CIOs said they were surprised by the additional work and money required to ensure new platforms could match the security of the mainframe.

As today's CIOs grapple with the need for real-time performance and unmatched security, they are starting to have a new appreciation for the mainframe and are investing accordingly. But several key challenges remain before an organization can have its mainframe investment support the needs of the future:

- **Agility.** The speed at which applications must evolve or add features is at odds with the slower pace of mainframe development. The mainframe must be more responsive to business needs with more frequent software updates and shorter mainframe development time.
- **Collaboration.** Typically the mainframe was seen as performing set tasks and rarely, if ever, interfacing with other systems. This is out of sync with the sprawling interconnected technologies upon which large organizations now depend. Simplification and standardization in the mainframe ecosystem are coming and will speed that progress.
- **Brain drain.** Many mainframe engineers are retiring, and organizations must enable the next generation to understand the business logic built into their most critical applications. CIOs can accelerate preparations for this generational shift by providing the right tools, processes and culture to fully capitalize on their mainframe knowledge base.

Forward-thinking organizations are already rejuvenating and expanding the return on their mainframe investments by addressing those issues. And that process is simply repeating the historical pattern of the mainframe, which has always managed to keep pace with the times.

So the biggest mainframe challenge might not be about replacing legacy technology but about reversing legacy thinking. •

— Chris O'Malley is CEO of Compuware Corp.

GCN

Technology,
Tools and Tactics
for Public Sector IT

Where you need us most.

Mobile

Tablet

Desktop

Print

COBO
Available Here

TOO OLD TO DIE?

Some legacy systems will likely never move to modern platforms, but agencies must get smarter about what to migrate and how

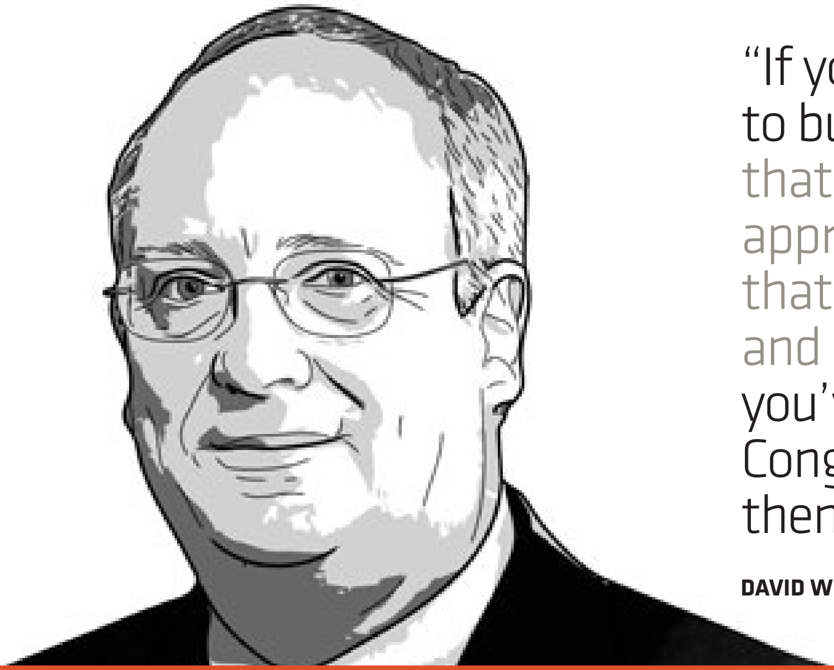
BY BRIAN ROBINSON

This summer's revelations of massive security breaches at the Office of Personnel Management not only set millions of feds on edge. The breaches also highlighted, yet again, agencies' reliance on legacy IT systems, some of which are decades old.

The solution in most cases is to replace or at least upgrade them — but that's much easier said than done.

OPM Director Katherine Archuleta, who has since resigned, told congressional oversight panels in June that a large share of the blame for the breaches belonged with the legacy systems on which her agency depends, and they are proving tough to modernize. OPM CIO Donna Seymour told the same lawmakers that it was impossible to encrypt data in some of those systems.

Some of the systems in question are more than 20 years old and written in Cobol, Seymour said. Getting them to the point at which they could be fully encrypted and accept other security measures, such as two-factor authentication, would require a full and very expensive rewrite of the software.



> "If you decide you want to build a new system, that also requires a different appropriation [from] the one that provides operations and maintenance dollars, so you've then got to go to Congress and convince them of the need."

DAVID WENNERGREN, PROFESSIONAL SERVICES COUNCIL

Beyond such improvements, simply maintaining existing IT systems is an expensive proposition for government agencies. The Professional Services Council's latest survey of federal CIOs and chief information security officers found that, on average, 75 percent of IT budgets go to operations and maintenance (O&M) of existing infrastructure. That number will go down over time, but the CIOs and CISOs said that three years from now they expect to put just over a third of their budgets into development, modernization and enhancement.

Some sectors are even worse off. For example, the Defense Department currently spends 80 percent of its IT budget on existing systems. And the Navy recently awarded a $9.1 million contract to Microsoft to support legacy Windows programs such as XP. The deal could run through 2017 and eventually cost more than $30 million.

David Wennergren, a former DOD technology executive and now senior vice president of technology at the Professional Services Council, said upgrading legacy systems is a complex process for most agencies.

"You've got to have a strategic decision that it's time to migrate off System A, and then [ask] what's that migration plan going to look like and does everyone agree on that direction," he said. "If you decide you want to build a new system, that also requires a different appropriation [from] the one that provides operations and maintenance dollars, so you've then got to go to Congress and convince them of the need."

Alternatively, Wennergren said, organizations could take advantage of consumption-based models that allow them to use O&M funds, such as the cloud. Rather than build a wholly new system, agencies could hire a provider to deliver the service "and pay them by the drink," he said. That way the onus is on the provider to determine whether a new system is needed to support the outsourcing contract — and if so, the provider pays for it.

It's a question of priorities, he added. A new Web-based front end might be enough to provide users with an efficient and modern experience, even though there's a legacy system chugging away in the background. And out of 100 legacy systems at a given agency, half might be fine just the way they are while the other 50 are woefully out of date, leaving the agency with operating systems that are no longer supported and core functions that "are held together with duct tape," he said.

"So you have systems where you either have a compelling opportunity or a compelling need that you have to deal with first," Wennergren said. "If you can first understand what you have, then you can put together migration plans about how and why to move systems this year."

THE IMPORTANCE OF AN APPLICATION AUDIT

NASA has been one of the strongest proponents of the cloud for those purposes and of hybrid solutions in particular.

Certain physical systems, such as supercomputers, must stay within NASA's infrastructure, said Roopangi Kadakia, the agency's Web services executive, at a recent cloud security conference hosted by GCN sister publication FCW. But by using the hybrid cloud, she added, "I can actually start building applications. I can take advantage of that data [produced by legacy systems] in different ways, in more innovative ways that wouldn't be possible if we had to keep it all within our environment."

Kadakia has also talked about how NASA's flagship portal, NASA.gov — with its 150 applications and some 200,000 pages of content — took just 13 weeks to move. And that included upgrading from the old technology where the site was previously hosted.

To move NASA's more than 64,000 applications to the cloud requires assessing the security risks, she said. The least risky approach is a staggered migration that involves moving some 10 percent of NASA's publicly accessible websites to the cloud each year.

However, Ed Airey, product marketing director at Micro Focus, said migrating systems and applications is not the only way to improve them, and in some cases, it might not be necessary or even possible to do that, particularly when the platforms or the applications running on them are strategic to the organization.

"Platforms in many ways can be considered separate from the applications," he said. "The applications themselves can retain the business rules and logic and the data itself, while being reconfigured to operate and interact with modern technologies such as Java and Microsoft's .NET."

The problem with trying to upgrade cornerstone, decades-old Cobol systems is that an agency has invested years of development effort in the applications based on them, and much of the business and mission success of the organization depends on that. So the first thing an agency must do is get a full appreciation and understanding of how those applications work, Airey said. And that's not always easy.

"In some cases, applications are very well documented, and [agencies] have the staff and resources in place to not only support the application but also to understand how the different business components fit together," he said. "But as people retire or move on, and in some cases as the technology itself changes, that landscape becomes more complex."

Kadakia said conducting an application audit to identify and mitigate critical vulnerabilities, some of which the applications' users were not aware of, was responsible for much of the cost of NASA's migration.

When agencies lack documentation or insight, change becomes risky because administrators don't fully understand the implications of what they are about to do, Airey said. Because of that fear, they sometimes defer the changes and end up with a much bigger problem further down the road.

THE **DEFENSE DEPARTMENT** CURRENTLY **SPENDS 80 PERCENT OF ITS IT BUDGET** ON EXISTING SYSTEMS. AND **THE NAVY RECENTLY AWARDED A $9.1 MILLION CONTRACT** TO MICROSOFT TO SUPPORT LEGACY WINDOWS PROGRAMS SUCH AS XP.

THE DEAL COULD RUN THROUGH 2017 AND EVENTUALLY COST MORE THAN $30 MILLION.

OTHER MIGRATION ROUTES

A problem with many legacy applications is that they were written in a monolithic or vertical way, said Jason Andersen, vice president of business line management at Stratus Technologies. That approach makes it difficult to migrate the applications because they are not compatible with the current service-oriented IT architectures, in which applications tend to be spread across various tiers and services. Therefore, legacy applications — particularly mission-critical ones — often require a wholesale rewrite in order to migrate them.

One solution would be to also rework some of the infrastructure on which those applications depend. Instead of putting most of the reliability and security into the applications themselves, which was the old way of doing things, agencies could put that functionality into the infrastructure. It would cost a bit more, but agencies would save on the iterative testing and requalification that the rewritten and often significantly larger applications would require, Andersen said.

Another approach is to move the application to a more amenable infrastructure, but there are some potential pitfalls, he added. The application might have been written for an operating system that's no longer supported or it might include special hooks or application programming interfaces that must be accommodated.

An evolving approach to upgrading or migrating applications is to only move certain parts of them, Andersen said.

"Essentially, the application gets tweaked by putting the right API set in front of it, then you can move it piece by piece," he added. "So you might move the user interface first, or the transaction or message queue, then save the hardest part for last, the one that could really bite you."

That hardest part will happen only when an agency understands how everything works together and has a stable infrastructure in place. Andersen said that's one of the reasons why there are still so many mainframes in government: Agencies elected to move the parts they could and left behind the pieces they didn't want to mess with, so "they kind of did a hybrid migration, if you will."

A PREFERENCE FOR STARTING FRESH

Stan Tyliszczak, staff vice president for technology integration and chief engineer at General Dynamics IT, said it would be less risky to migrate a legacy application as a whole because the various pieces of the application are working together as an ecosystem.

Database applications, for example, rely on fairly high-speed connectivity between front and back ends, and if an agency were to separate those pieces — perhaps by putting a wide-area network between them, with the kind of latencies that produces — the application might wind up not working at all.

Even so, he admitted to a growing interest in what he called split solutions — "such things as an analytical cloud that gives access to analysis tools that are tied into a data lake that has disparate sources around the world, not just your own, and you can choose the most appropriate tools for the job [and] can create very robust solutions. If you can have that kind of environment, it's a different story, but we are only at the very front edges of deploying that kind of technology today."

Given their druthers — and budgets — most agencies would probably prefer to develop applications from scratch in the cloud rather than migrate legacy applications. That's what DOD IT professionals would do, according to a recent MeriTalk survey. More than half of the respondents said building new is the smarter way to go, versus just 18 percent who chose migration. Some 28 percent anticipated using a mix of both strategies.

Security concerns, the need to maintain data structure and the fact that the legacy applications were custom-built to DOD requirements were the chief reasons respondents gave for choosing migration over building new applications. However, the cost of migrating was a major concern.

Tyliszczak said the study shows that, given the choice, agencies would prefer to build something new so they would not have to deal with all the thorny issues that bubble beneath the surface with a legacy application. Migration is only advantageous when an application was developed recently and when migrating it is fairly easy and does not pose a big risk, he said.

In the end, agencies must make their own decisions about whether and how to migrate applications based on the best way to use scarce resources and constrained budgets. For that reason alone, some legacy applications might remain in dedicated, on-premise hardware or, at best, in virtualized environments with spruced-up, Web-capable front ends.

Wennergren said several things could happen given the tough financial environment that agencies operate in today. Budget pressures could prompt people to lead the charge toward change. But instead people often hunker down and protect what they have "because it's easier to defend the programs of record, and that's often why we tend to hold onto legacy stuff for too long," he added.

That's also a reason why government still spends so much on maintaining legacy systems. Perhaps the OPM breaches will be the final straw that pushes legacy issues ahead of other priorities. "It's clear we've fallen behind on IT modernization," Wennergren said, "and it's clear that it has to be addressed." •

The Federal IT Acquisition Summit

Exploring Strategies, Options & Innovations

October 20, 2015

Washington Hilton, Washington, DC

EDUCATION & TRAINING FOR KEY CONTRACT VEHICLES

This second event in the Federal IT Acquisition Summit series provides government IT decision makers with contract-specific training opportunities as well as insights on key issues that are reshaping the federal acquisition environment. Featured vehicles include GSA Alliant (including an Alliant 2 update), NASA SEWP V, and NIH CIO-CS.

Free for Government & Military Attendees

Supporting Agencies

SEWP V

NITAAC
OMB Authorized GWACs for IT Acquisition

FCW GCN Washington Technology DEFENSESYSTEMS FederalSOUP

For Sponsorship Opportunities Contact

Alyce Morrison: amorrison@1105media.com or Kharry Wolinsky: kwolinsky@1105media.com

For More Information Visit: http://fcw.com/fias

CAN TECH DELIVER A DRONE DEFENSE

DON MCCULLOUGH / WWW.FLICKR.COM

Federal and state agencies are wrestling with laws and regulations governing hobbyist UAVs — and turning to technology for new solutions

BY MARK POMERLEAU

Unmanned aerial vehicles (UAVs) have proven to be a serious headache for airspace regulators. Businesses have pushed the Federal Aviation Administration to more quickly integrate UAVs into the national airspace because of their potential economic impact — estimated in the billions — and hobbyists are also permitted to fly drones, albeit under significant constraints.

Recent incidents involving the latter group have made national headlines. A drone crashed on the grounds of the White House, a video surfaced of a machine gun firing from a quadcopter, and drone-flying hobbyists have disrupted firefighting efforts in California. Such incidents have prompted government officials to search for stronger detection and even kinetic defensive measures to thwart such nuisances or potential threats.

Government agencies at the federal and state levels are initially attempting to manage the problem through education. The Department of Homeland Security circulated a bulletin on July 31 to several local law enforcement jurisdictions warning of the threat nongovernment drones can pose. The FAA, for its part, has launched a voluntary compliance and information campaign about flying drones, especially into fire zones.

And in California, legislators have gone a step further and proposed legislation that would not only ban all non-sanctioned UAVs over active fires but provide immunity for firefighters who damage or destroy such drones and also permit law enforcement to jam their signals.

It is difficult to detect the devices because of their small size; under FAA regulations, hobbyist drones must weigh less than 55 pounds. Although radio-wave detection tends to be highly accurate for larger aircraft, many drones — like the gyrocopter that famously landed at the U.S. Capitol — evade detection because they are too small and fly too low.

Some drones use geofencing to avoid designated no-fly zones. PrecisionHawk, a private drone company in North Carolina, has developed a solution for monitoring drones that agriculture and oil companies use to get a better view of their assets. The company's system sends an alert to the drone operator's smartwatch when the UAV flies too close to a predetermined no-fly zone.

During a recent demonstration, the operator attempted to fly into that region, but an autopilot feature overrode the commands and took the aircraft away from the no-fly zone.

TRAFFIC LIGHTS, JAMMERS AND HACKERS

In terms of the national airspace, NASA is working with the FAA on a system that would adapt ground traffic rules — such as lanes, stop signs and lights — for low-flying drones. More specifically, the proposal would provide "airspace design, corridors, dynamic geofencing, severe weather and wind avoidance, congestion management, terrain avoidance, route planning and re-routing, separation management, sequencing and spacing and contingency management." NASA held a three-day conference in July focused on safely integrating UAVs into its proposed traffic-management system.

Experts say technology challenges are hindering development of an efficient, accurate and legal method to guard against unwanted and unsafe hobbyist drone activity. So when rogue drones are detected that pose a threat or interfere with government activity, what can be done to neutralize them?

Jammers block the radio waves or GPS signals drones use to navigate and communicate with the operator on the ground, but as PCWorld pointed out, federal law bans signal jammers because they indiscriminately block signals for devices within their sphere of influence.

Hacking is another option. Many off-the-shelf hobby drones are extremely vulnerable to software attacks. They "were constructed to be easy to connect to," said Kathleen Fisher, a program manager at the Defense Advanced Research Projects Agency, during a recent "60 Minutes" story on drone security. "So they weren't constructed with security in mind at all."

Lee Pike, research lead for cyber-physical systems at Galois, told GCN that hackers exploit those vulnerabilities through software bugs that allow them to take full control of the vehicle because they are operating on unsecure networks that lack authentication and encryption. While noting that it is feasible to use hacking as a defense, he stressed that hacking is a nuanced skill.

"The one reaction I have is about safety," Pike said. "You want to make sure that you aren't causing more problems when you hack into a vehicle. For example, causing the quadcopter to crash and a battery...to explode could cause more harm than good."

> Hacking is another option. Many off-the-shelf hobby drones are extremely vulnerable to software attacks.

Nevertheless, once a software flaw is discovered in a hobbyist drone, "it is systemic in every system that has that software," said Pike, whose company conducts research and development related to software security.

THE MILITARY'S APPROACH

For the Defense Department, small hobbyist drones that radar cannot detect have the potential to be used by the nation's adversaries. Thwarting and defending against small UAVs were a key focus at the Black Dart 2015 event, an annual military exercise. This summer's event focused on live-fly, live-fire counter-UAV technology.

"If there is anything that the terrorists have shown, it's that they'll be innovative and use anything that they can at their disposal to do what they're trying to do," Air Force Maj. Scott Gregg, Black Dart project officer, told reporters. "What we're trying to do at Black Dart is make sure that we are staying ahead of the game and that we have a good understanding of their capabilities before those capabilities outpace ours."

Thales SA, a French manufacturer of defense electronics, has tested a system that uses radar to detect a drone, a camera to identify it, and jamming tools to override the system and take control of the device's path, the Wall Street Journal reported. A prototype is expected next year and will include a portable, vehicle-mounted solution.

The Army, meanwhile, has developed a direct and decisive way to deal with unwanted drones. Its C-RAM system has been tested to detect and intercept incoming drones then shoot them out of the sky. The system was designed to counter rockets, artillery and mortars — hence its acronym — but it has been adapted to counter small UAVs.

C-RAM uses a 50mm cannon that can launch command-guided interceptors, a precision tracking radar interferometer as a sensor, a fire control computer, and a radio frequency transmitter and receiver for launching munitions.

That's probably overkill for hobbyist drones that stray off course, but the Army is concerned about defending against UAVs that have been armed and turned into flying improvised explosive devices. •

CASE STUDY OPEN DATA

How 3 cities got public transit apps on the cheap

Chattanooga, Baltimore and Cleveland have opened their transportation data to help people view real-time transit options

BY AMANDA ZIADEH

Three more cities now have real-time public transportation information available to commuters, without having to develop or maintain the mobile apps themselves. All it took was improved open data and some serious collaboration with civic-minded coders.

All three cities — Chattanooga, Tenn.; Baltimore; and Cleveland — are now served by Transit App, which uses open public transportation data to display local travel options and departure times in 99 cities worldwide. Users can view bus schedules, subway maps and bike routes, and they can also request service from Uber.

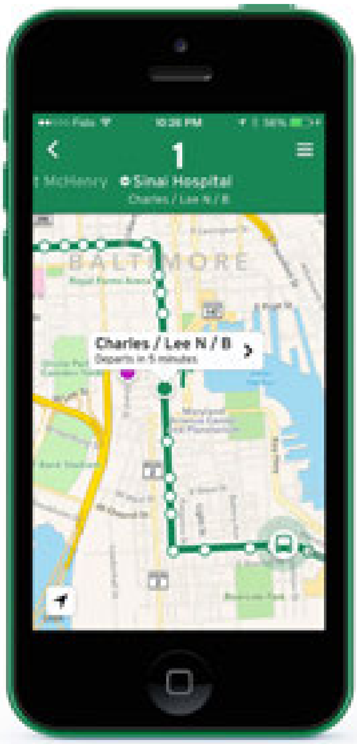
Transit App relies on a city's open-data portals and transportation information from various local agencies, which means cities that have better data are more likely to be added to the service.

According to Transit App, Chattanooga had not offered its information online before it became one of the app's locations. Through a partnership with a Code for America team and the Chattanooga Area Regional Transportation Authority, officials made digital transit schedules available to third-party developers on GitHub.

That effort, combined with some social media campaigning, moved the city to the top of Transit App's wish list.

Soon after, Chattanooga had a Transit app with schedules, a trip planning tool, information on a bike-sharing program and real-time data. According to Transit App, the citywide service was created at no cost to the city.

After Chattanooga's success, the Transit App team was inspired by a Baltimore project led by a Code for America brigade captain, Chris Whong.



Transit App is helping people make better use of public transportation in Baltimore, where most residents don't have cars.

MEDIUM.COM/@TRANSITAPP

He was frustrated by the inefficiency of Maryland's online bus tracker, so he created a real-time bus location map using data from the Maryland Transit Administration's website.

According to Transit App, Baltimore's transit-tracking system had already cost the city $2.7 million, and officials said it would cost another $600,000 to transform that information into a shareable format.

Once Code for America was able to access Baltimore's real-time transit information with Whong's help, the Transit App team incorporated the data into its systems and opened up yet another easy-to-use city service — one that is especially beneficial for a city like Baltimore, where more than half of residents do not have a car.

More recently, Transit App was able to do the same for Cleveland after a request from that city's Code for America brigade. Transit App contacted the city's CIO, who allowed the company to access and use the necessary data from the Greater Cleveland Regional Transit Authority provider.

Although Cleveland's real-time information is not yet fully open and integrated, the Transit App cited the city's strong advocacy for open data — as evidenced by multiple groups such as Open Cleveland, Hack Cleveland and Neighborhood Progress — as encouraging signs that the city is committed to transparency. •

Data sharing helps NC enforce workers' comp laws

A revamped Web-based system that allows agencies to pool valuable data is already reaping benefits

BY AMANDA ZIADEH

North Carolina is using shared state government data to crack down on businesses that falsify or neglect to carry workers' compensation coverage. The state's Government Data Analytics Center makes that sharing possible, and real revenues are being generated as a result.

GDAC is a statewide project that facilitates data sharing and integration among participating agencies and helps them define and develop their analytical needs. Established in 2007 as a business intelligence program in the Office of the State Controller, GDAC moved into the Office of Information Technology Services in 2014 and has redoubled its efforts to share data and improve government operations.

Before the state partnered with IT vendor SAS to build GDAC, North Carolina did not have the proper tools to access and share information among various agencies to detect coverage fraud.

"We've never really been proactive about going out and trying to make sure folks have coverage before an employee gets injured," said Bryan Strickland, director of compliance and fraud investigations at the Industrial Commission, which ensures compliance with workers' compensation laws in the state.

Often, an injured worker would file a claim only to discover he or she was not insured after the commission ran a background check. The employee would be responsible for the costs associated with the injury, which created a series of problems for the company, the state and the employee.

The commission lacked the neces-

SHUTTERSTOCK

sary preliminary data, and workers and companies were unaware of the penalties associated with coverage fraud.

The solution was GDAC. The Web-based system, which went live in April 2014, enables and encourages agencies to share valuable data in order to tackle statewide problems like the ones related to workers' compensation.

The Industrial Commission refers to its GDAC-based solution as the Noncompliant Employer Tracking System (NETS). The secure Web-based application was built using an SAS Fraud Framework. Authorized users can access data collected from multiple state sources to support the generation of leads for investigation.

Strickland said some 600 employers who lacked workers' compensation coverage before the system was implemented now have that coverage, and the commission has collected nearly $1 million in civil penalties from 101 misdemeanor charges.

Because of GDAC, the commission can use data from the Division of Employment Security, for example, to determine how many employees a company has. Data from the North Carolina Rate Bureau (NCRB) is sent directly into the commission's network and then to SAS for analysis. SAS sends that analyzed data to the commission to show whether or not those employees have coverage.

For example, if an employer is shown to have three employees but NCRB information does not indicate that the company has workers' compensation coverage for them, the system generates an alert for possible noncompliance.

The commission can also tap into the North Carolina secretary of state's information. Because companies are required to submit annual reports to the secretary of state, that office has the most up-to-date information on those companies.

However, officials had some security concerns about NCRB data. For instance, if insurance companies could see what rates their competitors were offering, they might try to steal clients by underbidding.

Given the sensitive information involved, the state chose to keep GDAC on a private network, Strickland said. The system is accessible only by authorized government personnel.

> "We've never really been proactive about going out and trying to make sure folks have coverage before an employee gets injured."
>
> – BRYAN STRICKLAND, INDUSTRIAL COMMISSION

Cleaner data also plays a major role in fraud detection. Although some companies might have the required insurance, for example, their carriers might have poorly updated systems. That causes the commission to waste valuable time and money sending letters of violation to companies that do indeed have coverage.

The Industrial Commission now takes that information to NCRB personnel, who contact carriers to enforce and stress the importance of updated information.

Although the core NETS and GDAC databases are accessible only by authorized government personnel, some information is made public on the Industrial Commission's website. So homeowners, for example, can confirm that their roofing contractor has appropriate insurance coverage.

"Before we even started this system, who knows how reliable that data even was?" Strickland said. "The data that the Rate Bureau is putting out and that the public has access to is actually better data now."

Sharing data likewise opened doors for the contributing agencies. The information the Industrial Commission retrieves from NCRB is also made available to the Division of Employment Security, which allows officials to identify companies that have workers' compensation coverage but are not paying any unemployment benefits, for example. The agency can then contact the employer to resolve the issue.

Furthermore, it is against the law to willfully fail to carry worker's compensation insurance. Certain law enforcement officers who use GDAC can sort data geographically by industry-heavy areas and proactively conduct sweeps and enforcement operations.

That approach has increased awareness and led to the number of criminal charges jumping from 18 last year to 101 for the year ending June 30, according to Strickland.

Before the NETS system, the commission generally closed about 400 cases a year. Since GCAC launched in April 2014, the agency has closed more than 2,300 cases, Strickland said.

The Industrial Commission is now looking into misclassification of employee data to determine whether some employees are actually independent contractors. The agency is also working with the Department of Insurance to incorporate data into NETS and hopes to bring the Department of Revenue into the GDAC system soon. •

National lab trades two MDM services for Citrix

Oak Ridge National Laboratory moved to a central platform and expanded mobile capabilities by choosing a Citrix solution

BY STEPHANIE KANOWITZ

Managers at the Energy Department's Oak Ridge National Laboratory were using two separate systems to manage lab-owned mobile devices and a bring-your-own-device program. Before long, however, that approach became too cumbersome, so they looked for a remedy.

"We had gotten into this model where we had multiple management systems to maintain for our mobile environment," said Tina Snyder, the lab's mobile device team lead.

Officials chose a Citrix solution because it gave them the opportunity to not only move to a central platform but to provide different capabilities for different user groups. "It also allowed us to reduce some costs [and] become more integrated with the other Citrix applications and services that we have," she said.

With Citrix, 1,400 employees and contractors can use their own devices to remotely access lab data, and that is a substantial increase. Suzanne Willoughby, the lab's client computing operations lead, said that in the past, officials had to limit the number of users with mobile access and allow only one device per user. Now Citrix access is automatically enabled for all salaried lab employees.

Other capabilities that Citrix brought to the lab include creating internal applications for specific user groups, delivering virtual apps via Citrix XenApp and implementing a single sign-on with user-based certificates.

"When we set up our BYOD program, we made the decision to use user certificates…[which] are stored in the Citrix bin-level container when an end user enrolls," Snyder said.

Each user creates a personal identification number to access the Citrix environment. That PIN, his or her Active Directory credentials and user certificate provide the credentials for security. The system complies with Federal Information Processing Standard 140-2, which covers security requirements for cryptographic modules.

A third of the 4,400 employees at Oak Ridge National Laboratory's sprawling campus outside Knoxville, Tenn., can now use their own devices to access lab resources.

FLICKR.COM/OAKRIDGELAB

Once workers have access, they open the Citrix Worx Home app, log in with the PIN and start working. If they need an app, they can download it from the lab's Worx Store. "It really is that simple," Snyder said.

Through Active Directory groups, Snyder and her team manage the apps that enable access to email, calendars, contacts, remote desktops and a workflow browser that provides access to internal websites. Other apps designed for the system include:

- TimeTracker, which salaried employees use to log their hours so managers can approve them.
- Finder, which lets users look up people and locations. For instance, a search for a conference room results in a map pinpointing its location.
- RESolution, a research enterprise resource planning system.

The lab has been a Citrix customer since the 1990s. The latest implementation was released in October and works with Apple and Android devices.

So far, there have been no reports of connection problems because of slower home bandwidth rates or computing power.

The initial deployment did have "its ups and downs," Snyder said, but the lab worked with Citrix to address the problems, and "in the last two to three months, things have calmed down quite a bit, and it's pretty stable at this point."

Lab officials expect the improved remote access to help them recruit and retain skilled workers. It makes the lab's mobile environment closer to what's found in private industry.

"As the person who was managing the BlackBerries before, [I believe] the BYOD program has been a great success," Snyder said. "People have really liked it and love being able to use their own devices instead of having to carry two. I think as we go forward and we see more capabilities for the tablets and more applications — especially built for internal access — you'll see a lot of people getting excited about what they can do with it."

She said the next step is upgrading the mobile device management servers to the latest release.

She also plans to take advantage of Citrix's new dynamic containerization capability, which means the lab doesn't have to get an unsigned copy of an app from a vendor to make it available in its Worx Store. Instead, it can apply a management layer to apps available from large resources such as iTunes. •

Where to start with customer-experience design

According to the General Services Administration's CX champion, it all begins with good listening skills and common sense

The General Services Administration's Martha Dorris, who now directs the Office of Strategic Programs, has spent years helping federal agencies improve their citizen services. She recently talked with GCN Editor-in-Chief Troy K. Schneider about the fundamentals of good customer-experience design, particularly when it comes to mobile technology.

This transcript has been edited for length and clarity.

Thinking about the customer experience is very much in vogue right now, but it's a really vague idea. Where do you start?

First off, it's worth noting that the government has had requirements and executive orders and [the Government Performance and Results Act] in place since 1993. So the idea of focusing on your customer is not a new idea, although it's hard. It sounds easy, but it's hard because it impacts every part of an organization.

This year, the administration created a cross agency priority goal on customer service. It's a really exciting time to connect the importance of customer experience to the world of technology and digital services.

It's like the customer experience life cycle: Who are your customers? How do they want to get information? What's the experience you want them to have? What drives their experience in terms of both their hardcore satisfaction and their perception?

For example, is your customer the 35 to 40 million students who are interacting with federal student aid? Or is it the 20 plus million veterans who are getting services from the Department of Veterans Affairs?

If you take the veterans example, you can't just say, "My customer is a veteran." You have a veteran of World War II. You have a recent Iraq/Afghanistan veteran. When you break those down even further, you start to see how certain segments of your customers would actually want to interact with you differently.

Doing some third-person research and interviewing customers on how they currently work with you — what are those drivers? — and developing some personas are really a good place to start.

Then you can start mapping the journey of what are their needs and how would they interact with you. You map what those pain points are, what the emotion is when they're going through that process, how many times they're touching your organization. And within that organization, what are those touch points?

Then as you're going through it, you think through from a mobile perspective, where are the mobile moments? Where does it make sense that you provide that service or the ability to conduct that piece of business with that agency in a mobile way?

It's a very discrete function that they're trying to accomplish in a mobile way.

One example is in GSA we have per diems, so if you're traveling then you can go online and you see what is a per diem rate for that area. The IRS mobile app on what's the status of your tax refund — that's the No. 1 question people are asking, so being able to do that in an easy way through an app makes sense.

How do you start to draw that journey map? Is that done with brainstorming and coming up with personas to represent the audience? Or are you using focus groups?

VA went through a process of going across the country and actually interviewing veterans to come up with personas. You take all those interviews, and you come up with behavior-based personas. Then you come up with scenarios for how that specific person might be interacting with your organization.

You should actually have real customers involved in it so you understand the emotions that customers are going through when they're trying to get a benefit, schedule a medical appointment, whatever it is they're trying to do.

Then you take all that and eventually you can draw it all out into a chart, where you can see in one place all the organizations that are touched, what the process is, what the emotions are and where the pain points are. You pull that out and extrapolate — what are some actions we can take that are going to resolve, improve, help that pain point?

ZAID HAMID

I think any time you're measuring, you want to make sure you're measuring what you really want to accomplish. But a key metric for every customer experience would be: Were you able to complete the task that you came to complete?

How do you go about measuring success? Does it depend on each project, or are there key metrics that should always be a starting point?
I think any time you're measuring, you want to make sure you're measuring what you really want to accomplish. But a key metric for every customer experience would be: Were you able to complete the task that you came to complete?

There also are perception measures, things like overall satisfaction and user loyalty — would you recommend that app to somebody else, and would you come back and use that app again?

Then you can go into more key performance indicators. In the beginning, you may want to see how many people are downloading an app, what's the usage of it, and is that growing over time? Then once you have a certain number of people using it, how many people are continuing to use it?

Then there are technical things like how long does it take to load the app, is the system up, and then at the very end, what is the user experience?

And as you're building it, you should be testing it every step of the way to make sure that your design is meeting the users' needs. So you're not getting to the end of it and having to rebuild something that's going to be costly when you could have caught it very early in a design stage.

You mentioned the importance of having real customers in the mix. Who else should be part of this conversation? Who are the other stakeholders?
Within an agency, it would be your technology shop — especially if you

have a digital services team — and the program. The program should own that app, and then they should have the resources around them to help build it.

And then it should all be tested by customers.

Are there hallmarks of a good customer-experience process or effort that you look for when you are brought in for a conversation? Are there clear signals that something is primed for success — or obvious red flags?
I think a red flag would be, "We built this mobile app, and we'd like to go out and let people test it," as opposed to "We have a team that has built it and iterated it and done very short sprints along the way so that we've made sure to test throughout the process."

If people don't have customer input, they're in trouble because mobile apps are expensive to build and to maintain. And people are starting to get more selective about the apps that they want to put on their phones.

You really want to make a meaningful, valuable resource that enables your customer to be able to get the job done.

Are there other points you think are important to mention that I haven't touched on yet — anything that someone who is about to embark on this process should know before they start asking questions?
I think people need to keep it simple and make sure that they really understand who their customers are and what their expectations are because we're all short of resources and we want to make every dollar count.

Is this a situation where you need to bring in a customer experience team or consultant, or is it something mindful project managers and developers could do themselves?
It depends on the agency. Some agencies are creating their own digital services teams, and this is the way they operate — agile, user-centered design, short sprints, all that. When you have a team like that, you're OK.

ZAID HAMID

I think people need to keep it simple and make sure that they really understand who their customers are and what their expectations are because we're all short of resources and we want to make every dollar count.

For me the bigger issue is: Do you need an organization that focuses on the customer in a holistic way? That's the ideal situation.

But it comes down to this: I think if you have the right resources internally and you have adopted those kinds of practices within the agency, then you should be fine. You may need technical skills or mobile app developers. It could be that you can design yourself, but you need a contractor to help you develop it.

We've done some things at GSA to help agencies test mobile apps. When an agency would want to test something on many different mobile platforms, we solicited people from across government and they've loaded an app on their phone and tested it for that agency.

It keeps an agency from having to go out and invest in a lot of different types of technology when you can just pull people from across the government to actually do usability testing, which is a really effective way to test.

There's also Open Opportunities, which is a platform that allows you to do micro tasking, so agencies can actually put a task on the Open Opportunities platform and request that people help them do some of these kinds of things.

And we're in the planning stages of a customer experience summit. So we will have lots more to come. •

ADVERTISER INDEX

Enterprise Architecture East	www.GovEAconference.com	11
Face-to-Face Event Series	www.GCN.com/events	5
Fujitsu America, Inc	www.ez.com/gcns	36
GCN Newsletter	www.GCN.com/subscribe	29
SQL Server Live	www.sqllive360.com	9
The Federal IT Acquisition Summit	http://fcw.com/fias	21
Visual Studio Live - New York	www.vslive.com/newyork	35
VARIDESK	www.varidesk.com	2

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

1105 PUBLIC SECTOR MEDIA GROUP

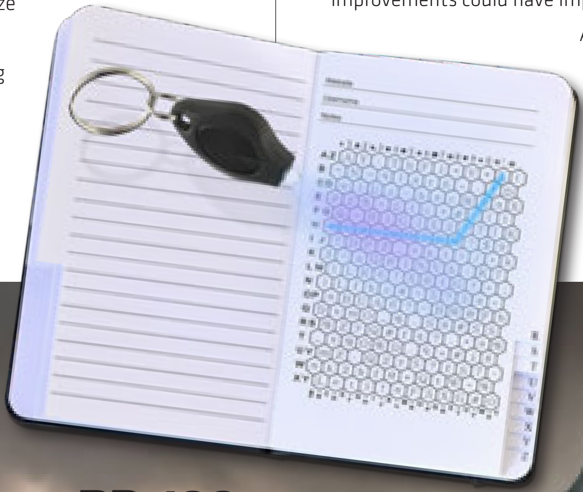
CORPORATE HEADQUARTERS
9201 Oakdale Ave., Suite 101
Chatsworth, CA 91311
www.1105media.com

WISHLIST

Tech we hope to see in the public se

Enigmaze

Two-factor authentication is gaining traction in government, but a good password is still critical. Enigmaze offers an old-school tool for creating highly secure passwords: The notebook comes with dozens of grids that make do-it-yourself algorithms easy. Storing those passwords in the notebook might not be entirely safe (even with the invisible ink pen), but Enigmaze allows for several methods of stumping a would-be password thief.



Wi-Fi reflector chips

As wearables enter the workforce, battery life could be one of the biggest limitations. NASA's Jet Propulsion Laboratory is working on chips that would trim power use by reflecting Wi-Fi signals rather than relying on traditional transmitters and receivers.

Reflection also transmits data three times faster than traditional Wi-Fi, and those improvements could have implications far beyond Apple Watches and Fitbits.

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

Black Hornet PD-100

This lightweight reconnaissance drone provides full-motion video and thermal imaging for up to 25 minutes per flight, with a range of just over a mile. Video is stored on the base unit, which the operator carries along with a handheld controller. The Black Hornet weighs just 0.6 ounces, and the full system is less than 3 pounds.

Army Special Forces have been testing the drones, but other uses include disaster response, law enforcement, and search and rescue.

shaping tomorrow with you

FUJITSU

Processing paperwork at the highest levels

You'll find government compliant Fujitsu scanning solutions in some high places. From the world's fastest high-volume document scanners to versatile, easy-to-use scanners for desktops, Fujitsu has one you should consider. Include the ability to integrate with dozens of leading software providers and you have a strong and reliable solution that lasts. Get started today by visiting **ez.com/gcns**

See the New FUJITSU Document Scanner fi-7160

LEARN MORE AT energystar.gov