

SOLAR STORMS THREATEN DATA CENTERS 3 | TWO WORDS THAT DESTROY IT'S CREDIBILITY 6

# COMPUTERWORLD®

THE VOICE OF BUSINESS TECHNOLOGY

computerworld.com

October 2014

**12** How techies can bring data mishandling and abuses to light *without jeopardizing their career opportunities.*

## Blowing *the* WHISTLE

[ WITHOUT BLOWING YOUR CAREER ]





# COMPUTERWORLD

P.O. Box 9171, 492 Old Connecticut Path, Framingham, MA 01701-9171 | (508) 879-0700

## » EDITORIAL

### Editor in Chief

Scot Finnie

### Executive Editors

Ellen Fanning (features and design)

### Managing Editors

Johanna Ambrosio (technologies)

Sharon Machlis (online)

Ken Mingis (news)

Bob Rawson (production)

### Assistant Managing Editor

Valerie Potter (features)

### Art Director

April Montgomery

### Senior Reviews Editor

Barbara Krasnoff

### Features Editor

Tracy Mayor

### News Editors

Mike Bucken, Marian Prokop

### Reporters

Sharon Gaudin, Matt Hamblen,

Gregg Keizer, Lucas Mearian,

Patrick Thibodeau

### Editorial Project Manager

Mari Keefe

### Senior Associate Editor

Rebecca Linke

### Office Manager

Linda Gorgone

### Contributing Editors

Jamie Eckle, Preston Gralla, JR Raphael

## » CONTACTS

Phone numbers, email addresses and reporters' beats are available online at [Computerworld.com](http://Computerworld.com) (see the [Contacts](#) link at the bottom of the home page).

### Letters to the Editor

Send to [letters@computerworld.com](mailto:letters@computerworld.com). Include an address and phone number for immediate verification. Letters will be edited for brevity and clarity.

### News tips

[newstips@computerworld.com](mailto:newstips@computerworld.com)

### Tech newsletters

Sign up now for breaking news and more at: [www.computerworld.com/newsletters/signup.html](http://www.computerworld.com/newsletters/signup.html).

Copyright © 2014 Computerworld Inc. All rights reserved. Reproduction in whole or in part in any form or medium without express written permission of Computerworld Inc. is prohibited. Computerworld and Computerworld.com and the respective logos are trademarks of International Data Group Inc.



## Table of Contents

### Blowing the Whistle – Without Blowing Your Career

**12** How techies can bring data mishandling and abuses to light without putting their careers in jeopardy. ➤

### 8 Big Trends in Big Data Analytics

**21** Big data technologies and practices are moving quickly. **Here's what you need to know.** ➤

### 5 Techniques for Securing Enterprise Data

**27** Retake control of your data with sandboxing, cloud security gateways and more. ➤

**NEWS ANALYSIS 3** Data centers aren't ready for **electromagnetic pulses.** | **OPINIONS 6** Paul Glen warns IT not to say "It's fixed." | **38** Thornton May asks where modern IT is headed. | **DEPARTMENTS 8** The Grill | **34** Career Watch | **36** Shark Tank



**MORE ON COMPUTERWORLD.COM**

**Security Manager's Journal:** [The security function needs SMART metrics.](#)





# Data Centers Vulnerable to Solar Storms, Nuclear Blasts

IT execs and government officials are aware of the **threats posed by electromagnetic pulses**, but few are doing anything about it.

**BY PATRICK THIBODEAU**

**N BOYERS, PA.**, EMP Grid Services recently opened a 2,000-sq.-ft. data center designed to withstand an electromagnetic pulse (EMP) generated either by a solar storm or a nuclear event.

The recently formed company isn't disclosing exactly how the data center was built or what materials were used. But broadly, it did say that the structure has an inner skin and an outer skin that use combinations of thicknesses and metals to provide EMP protection.

There are other data centers that protect against electromagnetic pulses, which can be generated by solar storms or high-altitude nuclear blasts. Some vendors offer containers and cabinets that they say can shield IT equipment from EMPs, which can fry circuits.

Despite some early moves, there's been little discussion overall about whether EMP protection should become a standard data center risk-mitigation feature.

Talk of the problem picks up periodically, especially when a flare is projected to hit the Earth, as happened in mid-



September this year. The first hit on Sept. 11, and the second a day later. The flares caused few disruptions but did create several beautiful auroras.

### Playing the Odds

More than anything, the latest solar bursts are a reminder of a risk that's real enough to inspire visions of apocalyptic scenarios among Washington policymakers but isn't immediate enough to spur people to do much about it.

History shows that betting against an EMP event is a gamble. On July 23, 2012, a solar super storm released a coro-

nal mass ejection (CME) that passed through the Earth's orbit but missed the Earth itself. It is believed to have been as powerful as the 1859 Carrington Event, a solar storm that disrupted and knocked out the most advanced electronic communications medium of the day — the telegraph.

The perfect solar storm would require a big sun spot cluster and a very rapid CME, and the magnetic field inside the solar storm would have to couple perfectly with the Earth's magnetic field. If that happened, the consequences could be significant, said William Murtagh, program coordinator at the U.S. Space Weather Prediction Center.

"We're concerned that can happen," he said. The 2012 solar storm "was very powerful, and some have suggested it would have been on par with a Carrington-level event." But

that storm wasn't directed at Earth, he noted.

EMP protection can be built into a data center at very little additional cost, said Kris Domich, president of Cyber Innovation Labs — Professional Services (CIL). The company is the founding member of EMP Grid Services. CIL provides infrastructure services.

Domich said the idea for the EMP-resistant data center came from a customer, an insurer, that wanted to protect its data from electromagnetic pulses.

### Low Priority

Lee Kirby, CTO of the Uptime Institute, a data center advisory and research group, said that EMP risks are not high on the list of things that data center managers worry about today.

"When you look at it from a business justification viewpoint, [EMP protection] gets pushed way down the line,

**When you look at it from a business justification viewpoint, [EMP protection] gets pushed way down the line, just from a probability point of view.**

LEE KIRBY, CTO, UPTIME INSTITUTE

just from a probability point of view,” Kirby said.

Nonetheless, he said, the threat of electromagnetic pulses could soon become a topic of much discussion among data center professionals.

There’s increased concern, particularly due to growing military capabilities of North Korea and Iran, that an EMP could be generated by a terrorist-sponsored nuclear blast.

## Widespread Impact

A nuclear blast 60 miles up in the atmosphere could expose about 1.5 million square miles of territory to EMP impacts that could, among other things, knock out SCADA systems that help run the infrastructure of electric and water utilities and oil and gas pipelines.

The loss of electric power over a substantial period of time is “likely to be catastrophic, and many people may ultimately die

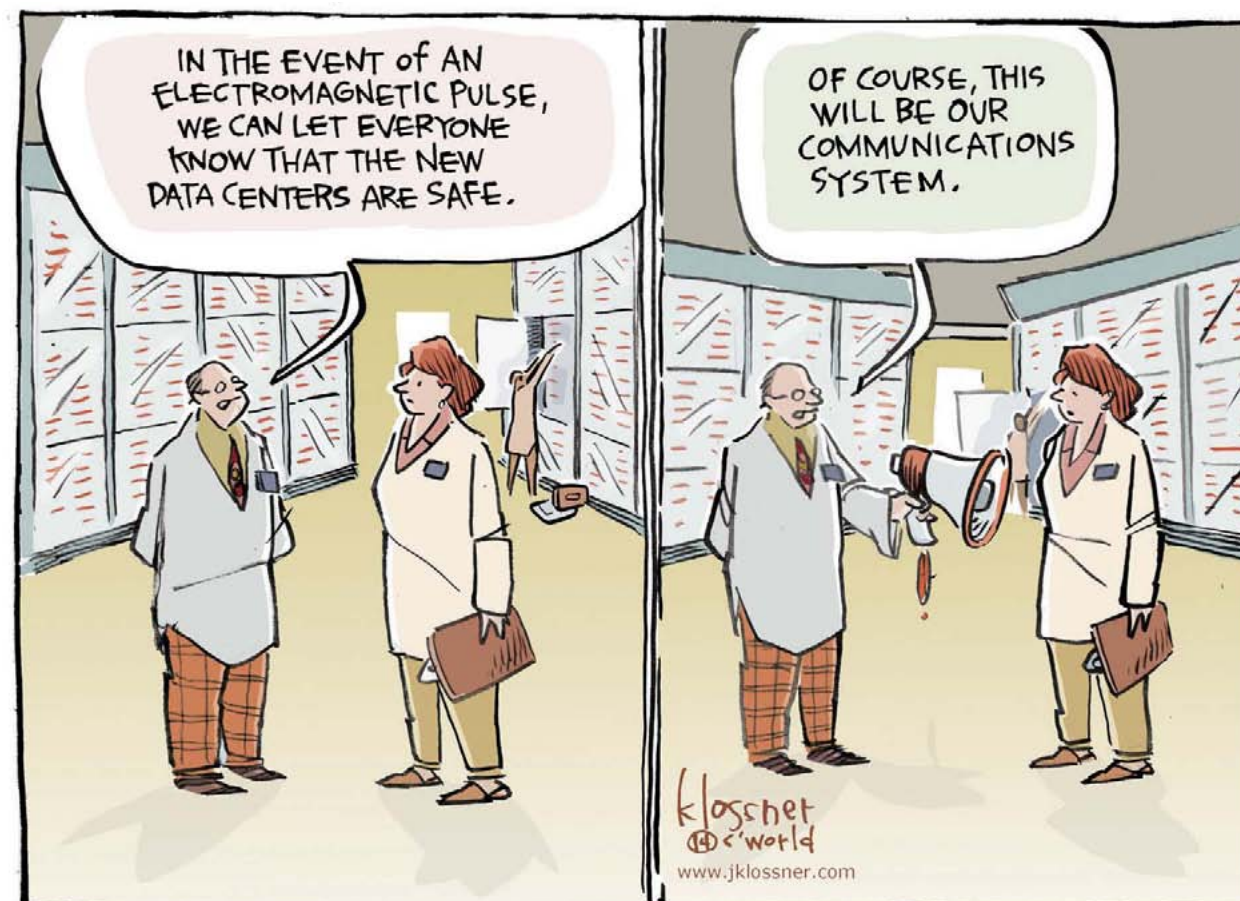
for lack of the basic elements necessary to sustain life in dense urban and suburban communities,” according to a 2008 U.S. government report that examined the effects of an EMP.

Repairing the power grid could take four to 10 years, at costs exceeding \$2 trillion.

EMPs send out a pulse of energy that can short-circuit electronics in everything from cellphones and automobile computers to enterprise networks. And EMP-generating devices can be built with over-the-counter parts.

Congress has held repeated hearings over the years, particularly since the 9/11 attacks in 2001, and a number of government reports have described the threats posed by EMPs. But there’s no action plan, and the need for EMP protection sits lower on the list of public-sector priorities than projects like repairing or replacing aging

## BETWEEN THE LINES | JOHN KLOSSNER



bridges, roads and water lines.

The problem may be that EMPs are not seen as an immediate threat — the government estimates that a crippling solar geomagnetic storm is unlikely to occur more than once in 100 years. ♦

PAUL GLEN is the co-author of *The Geek Leader's Handbook* and a principal of *Leading Geeks*, an education and consulting firm devoted to clarifying the murky world of human emotion for people who gravitate toward concrete thinking. You can contact him at [info@leadinggeeks.com](mailto:info@leadinggeeks.com).



# Two Little Words That Destroy Your Credibility

**Probably the most common unforced error in IT comes in the form of a simple two-word phrase: 'It's fixed.'**

**WE TECHIES HAVE A HARD TIME** building and maintaining credibility with our stakeholders. High expectations are hard to manage. Bugs happen. And we get blamed unfairly for all sorts of things that are out of our control.

But we also have a habit of making things worse, undermining our credibility inadvertently and unnecessarily. Probably the most common of these unforced errors comes in the form of a simple two-word phrase:

"It's fixed."

Stakeholders have a variety of emotional responses to hearing us utter these words, none of them productive.

Some respond with excitement and gratitude. "Thank goodness! I'm saved!" If you're dealing with issues that have no explicit definitions of "fixed"—like performance problems—their imaginations run wild. They conjure fantasies of systems that work as they wish they would, faster, easier and more reliably than they really do. But these raised expecta-

tions rarely survive contact with reality, and when stakeholders' dreams are crushed, we lose credibility. It wasn't really "fixed" after all. They feel foolish for having had optimism and blame us for making them feel bad. Even if the problem is clear-cut, like an error message, sometimes "fixed" isn't really "fixed." They still get the error message, or a new one. And they feel disappointed.

Others roll their eyes in skeptical disdain. "Yeah, I've heard that a million times



**It's their job to declare something fixed, not yours. If they declared that something was broken, then it's their job to declare that it is no longer so. Your job is to invite them to decide.**

before.” Having been let down too many times, they protect themselves from the pain of disappointment by crushing any hints of optimism. And they judge us as responsible for their negative reactions.

It doesn't help that we usually tell them “It's fixed!” with infectious enthusiasm and pride. We're problem-solvers by nature and love the feeling of having solved a puzzle. We feel that we're helping our stakeholders. We feel competent and powerful. And our excitement intensifies their reactions, raising their expectations or trig-

gering suspicion and cynicism.

To avoid triggering these negative responses, you just have to remember one simple principle:

*It's their job to declare something fixed, not yours.*

If they declared that something was broken, then it's their job to declare that it is no longer so. Your job is to invite them to decide. You may have to influence the criteria they use to decide, helping set their expectations about what is possible, and how “fixed” something can be. But you don't get to make that call. They do.

Instead of declaring something fixed, do three things:

**1 Tell them what you did in language that they can understand.** “We found two places where we tried to speed up database queries.” “We changed one of the system configuration variables.”

**2 Describe your observations.** “It seems much faster now.” “We don't get the error in the test environment.”

**3 Ask them to try it out.** “Can you test it and see if it looks better to you?”

By asking them to decide, you avoid all the emotional damage wrought by that seemingly innocuous statement. It's hard enough to build credibility with stakeholders. You don't need to make it any harder. ♦

# THE Grill

## Simon Szykman

This government CIO is pushing for efficiency and effectiveness in a federated IT model.



**WHEN SIMON SZYKMAN** became CIO of the U.S. Department of Commerce in May 2010, he inherited a federated IT organization that needed to improve its efficiency and effectiveness on multiple fronts. So Szykman applied his strategic vision and consensus-building skills to make progress in both areas. Now he's looking for new challenges; he announced early this year that, after serving four years as Commerce CIO, he will leave the public sector to work in private industry.

**What was your biggest achievement during your tenure at the Commerce Department?** Commerce is

a federated agency with a number of independent decision-making organizations with regard to IT spending and spending in general. Since I've been here, there have been dramatic changes in how IT is managed departmentwide and a realization that the decentralized approach wasn't going to be the most efficient or effective in terms of cost or quality of services.

**What prompted the move away from the decentralized approach?** It was a growing recognition of best practices coupled with a belt-tightening fiscal

- **Fun fact about you:** I'm an adventure seeker. I like to get outside my comfort zone.
- **Past adventures:** Scuba diving, climbing Mount

- Kilimanjaro and wing-walking on a vintage airplane.
- **Music playlist:** My music is pretty diverse, from pop to classic rock to classical.

- **What do you do in your spare time?** Get out and enjoy the fresh air and nature.
- **Hometown:** Great Neck, N.Y.



environment. The inefficiencies that were in place prior to my tenure were becoming less and less tolerable in the fiscal climate we were dealing with.

**What was most challenging about moving to a more centralized model?** The culture of a federated agency and the need for change management across a very large organization. The approach to dealing with that is really working with large numbers of different stakeholders from the internal CIO council — at Commerce that includes representative CIOs from all our large bureaus and organizations — and CFOs and senior career officials and in some cases political [stakeholders] as well. We focused on building consensus for the types of changes we wanted to put in place.

**How did you overcome the challenges?** Obviously communication is a key part of that. Another important part was trying to work with objec-

tive, data-based business cases rather than just appealing to emotional arguments. We worked with data and identified opportunities for improving our services or identified in advance what savings we could expect, and laid out an analytical business case for what we were trying to implement. There was also the need to deal with concerns that the agencies had, concerns that they would be able to maintain service levels once they consolidated infrastructure or services. There were perceptions of risk that had to be effectively managed. It's a complex undertaking.

**What was the biggest lesson you learned in that process?** [The importance] of shared ownership and joint accountability for success, because these types of large change management initiatives aren't going to be successful by the efforts of one individual. Ownership has to cut across organizations. One thing that helped me was I had been the CIO of Commerce's National Institute of Standards and Technology prior to this position, so I was able to appreciate the bureau-level perspectives, and that helped in communications.

**How do you build consensus without burdening initiatives with unreasonable demands from others?** People who have their own requirements don't

**These types of large change management initiatives aren't going to be successful by the efforts of one individual. Ownership has to cut across organizations.**



**Once we reach the goals we want to achieve, we pick up a new one and keep moving forward.**

perceive them to be unreasonable. So it's being able to appreciate different perspectives and strike the right balance. Having a shared commitment to reach the desired objective is part of it. Everyone has to buy in.

**You've called CIO empowerment an issue in government. What do you mean?** At Commerce, I have direct management and budget authority over less than 2% of the department IT spending. Things don't happen merely because I say they must happen. A big challenge is getting everything done in a coordinated, well-managed fashion. We are moving forward in working collectively in a coordinated way. But it remains a federated environment.

**You've blogged about your efforts to cut waste. How do you approach this challenging task?** It was done in a very collaborative fashion and an analytical, data-based fashion. We looked at where we were spending money and on what types of technology. We then looked at opportunities — the types of savings we might achieve by improving how we were buying certain types of technology. Then we looked for where we could make improvements without a tremendous amount of effort or time. So we did prioritization and built consensus for those that were most impactful and easiest to implement.

**How long has this been on your agenda?** It is still ongoing. We did our first departmentwide strategic sourcing contract over two years ago to purchase PCs, replacing over 100 contracts. The most recent strategic sourcing initiative we just completed was a departmentwide contract for networking equipment. Once we reach the goals we want to achieve, we pick up a new one and keep moving forward.

**Can efficiency efforts be institutionalized? Can they become routine?** I think they can. But efficiency isn't the only goal. That implies the primary objective is just to cut costs. Sometimes you're looking at improvement of services through consolidations or freeing up resources to deploy new services. But it can be institutionalized once people start to think about departmentwide initiatives in a new way. Once that happens, over a period of time the default approach to purchasing or deploying new services in the IT world can really shift.

**Early in your tenure, a review found that the Commerce Department didn't have adequate cybersecurity. What was your strategy for improving it?** We had to improve cybersecurity from a number of angles to obtain measurable improvements. We looked at how we were managing risk for our systems, and we've started looking at operations, rather than



have this just be a security compliance exercise. We looked at existing policies and where there were gaps, and developed new policies where we needed them. We put in more automation and continuous monitoring so we can get more real-time visibility into the state of our systems. And we established metrics and measured how we were doing and reported those metrics up to senior levels, so we were creating high-level visibility.

**What's on the Commerce Department's agenda regarding big data?** Just a few months ago, the Commerce secretary unveiled a new strategic plan, and one pillar is data and how we can make Commerce data available to citizens, businesses [and] the private sector to create new businesses and foster economic growth. Ultimately the goal is to make that data discoverable. You have to develop formats that describe the data so others can discover it. You have to create platforms for that data to be disseminated. This really is in the early formative stages, but we already have examples of how organizations are starting to think about this.


**How are you using data to drive decisions?** Over the next few years, we'll do a modernization of our financial systems that will provide us with more effective, consolidated information about our

finances, and that will support better decision-making from the budget stages to actual acquisitions. The other area is the use of data to improve performance management. We're looking at what metrics are going to be the key for performance priorities and using those metrics to track our own performance.

**What's next for you?** I'm still exploring opportunities, but my next career step will definitely involve IT. I have three main goals. The first is to have fun. The second is to learn — and there's a lot I can learn from the private sector. The third is to help the company I work for prosper. ♦

---

— Interview by Computerworld contributing writer  
**Mary K. Pratt** ([marykpratt@verizon.net](mailto:marykpratt@verizon.net))



**Over the next few years, we'll do a modernization of our financial systems that will provide us with more effective, consolidated information about our finances, and that will support better decision-making from the budget stages to actual acquisitions.**

# Blowing *the* WHISTLE

[ WITHOUT BLOWING YOUR CAREER ]

How techies can bring data mishandling and abuses to light **without putting their careers in jeopardy.**

*By Cindy Waxer*





**T**ECHNOLOGY PROFESSIONALS are among today's most infamous whistleblowers. The list of those who have made headlines for exposing corporate or government skulduggery includes Shawn Carpenter, a network security analyst who blew the lid off a Chinese cyberespionage ring; Bradley (now Chelsea) Manning, who shared more than 250,000 classified State Department cables with WikiLeaks; and Edward Snowden, who leaked top-secret information about NSA surveillance activities.

But for every high-profile case, there are plenty of tales of IT professionals who have accused their employers of wrongdoing without making national headlines or feeling the need to seek asylum in foreign countries.

Take Nell Walton, for example. A former database administrator at Nova Information Systems (now Elavon), Walton filed a whistleblower complaint with the Occupational Safety

and Health Administration in 2005 against the credit card processor for security violations on databases that contained billions of transaction records.

According to Walton, she repeatedly asked the company to bolster its database security—a request that she claims prompted retaliation from Nova's "chain of command." Walton's complaint was dismissed by OSHA. She appealed the decision with the U.S.

**It's like that saying from my childhood: Nobody likes a squealer.**

You can be noble and a whistleblower, but don't expect it to be an easy life.

**JAMES LEWIS,**  
DIRECTOR AND SENIOR  
FELLOW, CENTER  
FOR STRATEGIC AND  
INTERNATIONAL STUDIES



Department of Labor but eventually lost her case against Nova in a federal court. (Elavon didn't respond to an interview request.)

The case, which lasted nearly three years, cost Walton her job, physical health and nearly \$50,000 in legal fees. "It totally pretty much wrecked my life for three years," she says. "Even after the case was over and we lost, it was just awful."

Such is the difficult and often stressful path for IT professionals who dare to expose what they perceive to be misconduct or negligence on the part of their employers. "It's like that saying from my childhood: Nobody likes a squealer," says James Lewis, director and senior fellow of the Strategic Technologies Program at the Center for Strategic and International Studies, a Washington-based think tank. "You can be noble and a whistleblower, but don't expect it to be an easy life."

Yet the potential for techies

to become high-profile whistleblowers is growing, whether they like it or not. For starters, today's data deluge—bits and bytes of information being generated by everything from assembly-line sensors to point-of-sale devices—is fueling a demand for unprecedented data transparency. Suddenly, the public is requesting greater openness from IT departments regarding what data is being collected, how it's being used, how it's being secured and who's accessing it.

At the same time, the stakes have never been higher for organizations to keep their systems secure. According to Ponemon Institute's "[2014 Cost of Data Breach Study: Global Analysis](#)," a report sponsored by IBM, the average cost of a data breach to a company was \$3.5 million, up 15% from the average reported by companies participating in last year's study. The 314 companies from 10 countries that

took part in this year's study estimate they will be dealing with an average of 17 malicious codes and 12 sustained probes each month. IT teams must keep confidential data safe from these mounting threats or face the wrath of angry shareholders, fine-wielding regulatory bodies and disgruntled customers.

All of that puts technology professionals between a rock

and a hard place. On one hand, they're saddled with the awesome responsibility of ensuring data openness and seeing to it that data management practices meet the highest ethical standards. On the other hand, IT professionals who detect—and then report—shoddy security measures or misuse of data are sitting on "a potential powder keg," warns Larry Ponemon,

founder of Ponemon Institute, a privacy and data protection think tank in Traverse City, Mich. It's no surprise that many IT leaders "take the attitude that [reporting malfeasance is] someone else's problem," he says, "or convince themselves that even though it's a data breach, it won't really be harmful to people."

Fortunately, a number of new developments are helping IT leaders more readily embrace their emerging role as corporate watchdogs. Greater legal protections, innovative whistleblowing platforms, new reporting processes, cultural shifts—they all promise to help technology professionals prepare for a new era of high-tech whistleblowing, even under the threat of employer retaliation, lengthy legal battles and foreign exile.

## Legal Matters

For four years now, the Dodd-Frank Wall Street Reform and

# CHECKLIST

*What to do if you suspect corporate misconduct:*

**1 Gather all the supporting documentation you can** to back up your claim and determine which law specifically you believe is being broken.

**2 Use a whistleblowing hotline, if available,** to report a breach or any type of misconduct.

**3 Know your rights.** Find out how state and federal laws can protect you on each step of your whistleblowing journey.

**4 Weigh the risks:** Possibilities include wrongful dismissal, the loss of valuable friendships and exorbitant legal fees.

**5 Weigh the rewards:** Possibilities include financial compensation, protecting the public's interests and good karma.



Consumer Protection Act has received mixed reviews on its ability to fulfill its mandate to reward and protect people who report governmental or corporate misconduct. The legislation works by granting whistleblowers monetary awards ranging from

the SEC has fielded more than 6,000 whistleblower reports.

In addition to offering financial rewards, the Dodd-Frank Act aims to protect whistleblowers from employer retaliation by allowing them to maintain anonymity.

**Companies are grappling with the fact that reports can be made directly to the SEC.** Most are uncomfortable with the notion that they don't know what's being reported about them and that the first time they find out is from a regulator.

**MOHAMMED AHMED**, SENIOR MANAGER,  
DELOITTE FINANCIAL ADVISORY SERVICES



10% to 30% of the money collected in an enforcement action. In fact, in the first seven weeks after the Dodd-Frank Act took effect in August 2011, the Securities and Exchange Commission received 334 tips from informers seeking rewards. Since then,

However, as financial experts continue to debate the impact of Dodd-Frank, many organizations are taking matters into their own hands. "The Dodd-Frank rules around whistleblowing were a good wake-up call, but I'm seeing a lot of organizations stepping

back and asking, 'How can we take this to the next level? What's the Version 2.0?'" says Mohammed Ahmed, a senior manager at Deloitte Financial Advisory Services and co-author of the Deloitte report "Whistleblowing and the New Race to Report."

### How Not to Air Dirty Laundry

For many organizations, the answer is to establish an internal whistleblowing program, complete with a 24/7 hotline and financial rewards for employees who expose bad behavior and faulty systems. Whistleblower hotlines, for example, allow IT workers to anonymously report any misconduct they witness within their organization either by phone or via a Web portal. Although IT professionals are most likely to notice something like the mishandling of

data, other causes for concern include fraud, corruption and illegal activity of any kind, of course, as well as safety violations and health hazards.

Walton says she wishes whistleblower hotlines were available back in 2005 when she decided to tell her employer about her concerns about data security. "I honestly think that a [whistleblowing] channel would have opened [the case] up to people that were more interested in protecting the data rather than protecting their own jobs," she says.

Even so, while more and more organizations are providing internal communication platforms and incentives for whistleblowing, the real motive behind many of these initiatives is to ensure corporate missteps are handled in-house and not brought to the attention of authorities.

The rationale behind many of these internal programs "is to motivate whistleblowers to

report internally first before going to the SEC,” says Ahmed. “Companies are grappling with the fact that reports can be made directly to the SEC. Most are uncomfortable with the notion that they don’t know what’s being reported about them and that the first time they find out is from a regulator.”

### Solutions Hidden in Plain Sight

If today’s internal whistleblowing tools fail to instill confidence in IT leaders, there’s a growing crop of third-party sites and submission systems to choose from.

Tor (previously known as The Onion Router), for example, is an anonymizing program that routes traffic through a network of multiple nodes — or virtual tunnels — to anonymize the identities of its users.

According to the Tor website, the technology bounces communications around a distrib-

uted network of relays operated by volunteers around the world. Tor prevents websites from tracking users, be they CIOs or political dissidents, so those individuals can remain undetected if they want to, say, communicate sensitive information to journalists, connect with authorities or browse whistleblowing sites.

Another option is GlobaLeaks, an open-source whistleblowing framework that’s designed to help IT professionals report wrongdoing without having to rely on in-house tools or technologies. “Whistleblowing is risky,” says Marco Calamari, a member of the Hermes Center for Transparency and Digital Human Rights in Milan, Italy, which developed the innovative technology. “GlobaLeaks is a highly configurable software built on the foundation of Tor, which allows for anonymous browsing of the Inter-



**Whistleblowing is risky.**

MARCO CALAMARI, MEMBER, HERMES CENTER FOR TRANSPARENCY AND DIGITAL HUMAN RIGHTS





**We cannot guarantee the security of any submissions** and we do not have the organization to handle whatever would be submitted to us.

**VOLKER ROTH**, PROFESSOR, FREIE UNIVERSITÄT

net.” The upside of GlobaLeaks, which boasts 5,000 voluntary servers and 1 million users, is its ease of use, which allows even nontechnical people to set up their own anonymous whistleblowing sites.

One of today’s more innovative submission systems is an on-line advertising network called AdLeaks. Unlike tools such as Tor, which rely on SSL connections over an anonymizing network to mask a user’s identity, AdLeaks works by embedding AdLeaks ads onto a website.

These ads contain code that encrypts a whistleblower’s messages, which are then delivered back to AdLeaks as small packets of encrypted information. By letting a whistleblower’s browser substitute messages with encrypted parts of a disclosure, AdLeaks ensures the sender is completely unobservable and that eavesdroppers can’t distinguish between a regular brows-

er’s transmissions and those of a whistleblower’s browser.

But even AdLeaks isn’t a fool-proof solution. For one thing, because it leaks only a small piece of information each time, the process may take weeks to complete. And because AdLeaks is a research project, the system is still considered part of an experimental research product line. Professor Volker Roth of Freie Universität (Free University) in Berlin, who is spearheading the project, says, “We cannot guarantee the security of any submissions, and we do not have the organization to handle whatever would be submitted to us.”

### Joining the Executive Ranks

As whistleblowing technologies continue to multiply and mature, Ponemon says there’s an attitudinal change afoot in IT departments that could spur greater openness among

technology professionals. “People who work in the security trenches or in IT who are not supervisory level or above often feel as if no one is going to listen to them even if they do see a problem,” he says.

It’s a difficulty that Walton says she faced when she was a database administrator. “Between the business and the IT department, there was just a real kind of disconnect on the severity of the [data security] issue,” she recalls. “That can happen a lot in business. . . . A CIO has to be very good at explaining the technical side and the risks. That’s what was missing all those years ago.”

But that’s changing as the role of a technology professional is slowly being redefined in the face of growing responsibility. For example, “more chief security officers are being elevated to a higher level,” says Ponemon. “Companies want a person not to just be a technician but to be

part of the governance solution. They want people to own the responsibility and accountability, which basically gives the CSO more power.”

### Greater Purpose, More Processes

With greater power comes the need for more formal processes that identify the steps IT professionals should take when they detect misconduct. Consider, for example, the recent controversy surrounding the U.S. Department of Veterans Affairs. Whistleblowers have stepped forward accusing the department of tweaking computer systems to make it appear that veterans waiting weeks for medical appointments had no wait time at all.

“The issue for IT folks is what do they do?” says Lewis. “Do they go and tell their boss that the software is under-reporting waits? Absolutely—that would

**People who work in the security trenches or in IT who are not supervisory level or above** often feel as if no one is going to listen to them even if they do see a problem.

LARRY PONEMON, FOUNDER,  
PONEMON INSTITUTE



be a responsible thing to do. But what if their boss says, ‘Don’t tell me about it, I don’t want to know.’ What do they do then? That’s where you have to make one of these decisions about how much stress you want in your life. It might work out really well but you are taking a risk.”

To minimize such risks, Ahmed says more IT professionals need to step up and participate in efforts to establish whistleblowing policies. “Oftentimes the whistleblower program is considered a legal general counsel area,” he says. But that’s a mistake. “A technology group can play a very important role in helping design a whistleblower program and in analyzing the type of reports that are coming in, particularly as they relate to topics of information security.”

For instance, Ahmed says that when deploying an in-house whistleblower hotline, a technology professional can act



“as either an adviser or a partner in setting up these types of programs and influencing the kinds of reports that would be of use to IT as they try to protect the organization.”

### Know Thyself

Education can also go a long way toward helping IT professionals better handle the sensitive issues that can arise from having unfettered access to confidential data and sophisticated computer systems. What access to confidential information does IT have? Do IT staffers understand their roles and responsibilities? Can they differentiate between data that is and is not sensitive? What are their responsibilities for reporting misconduct? What whistleblowing mechanisms are in place? How will they be protected if they choose to speak up? What proof is required to substantiate a breach or misconduct?

## TECHIES WHO TALKED

### WHISTLEBLOWER: Karen Silkwood

- **Disclosure:** The American chemical technician and labor union activist spoke out about the poor corporate practices that compromised the health and safety of workers in a Kerr-McGee nuclear plant.
- **Resolution:** Silkwood died in a car crash under mysterious circumstances. Years later, Kerr-McGee settled with the Silkwood estate out of court for \$1.38 million.

### WHISTLEBLOWER: Alan Parkinson

- **Disclosure:** The Australian mechanical and nuclear engineer helped expose the unsatisfactory cleanup of the British atomic bomb test site at Maralinga in South Australia.
- **Resolution:** Parkinson was eventually removed from the project and wrote a book about his ordeal entitled *Maralinga: Australia's Nuclear Waste Cover-up*.

### WHISTLEBLOWER: Shawn Carpenter

- **Disclosure:** A former network security analyst at Sandia National Laboratories, Carpenter discovered that a sophisticated group of hackers was infiltrating hundreds of computer networks and accessing

sensitive data at major U.S. defense contractors, military installations and government agencies.

- **Resolution:** Carpenter's employment was terminated when he informed the U.S. Army and the FBI about the security breaches. Today, Carpenter continues to work in the national security field.

### WHISTLEBLOWER: Edward Snowden

- **Disclosure:** The former National Security Agency contractor and IT infrastructure analyst gave reporters top-secret documents suggesting that the NSA is collecting phone records on millions of Americans.
- **Resolution:** To avoid facing charges related to the leaks, Snowden fled to Russia, where he recently received a three-year residence permit.

### WHISTLEBLOWER: Bradley (now Chelsea) Manning

- **Disclosure:** The U.S. Army intelligence analyst was convicted in July 2013 of violations of the Espionage Act for downloading and releasing more than 250,000 classified State Department cables and sending them to WikiLeaks.
- **Resolution:** Manning was sentenced to 35 years' confinement at the maximum-security U.S. Disciplinary Barracks at Fort Leavenworth in Kansas and was dishonorably discharged from the Army.

— CINDY WAXER

Only by making IT professionals distinctly aware of their roles — and of the way whistleblowing will impact them both personally and professionally — can companies successfully enlist IT in efforts to achieve greater accountability.

### Proceed at Your Own Risk

The enormous burden of whistleblowing, however, should never fall squarely on the shoulders of a single IT professional. Rather, Roth says, “it’s extremely important that corporations send a signal that they assure whistleblowers that they will protect their identity and protect them from harm.”

But there are no guarantees that an IT professional who lifts the veil on corporate misconduct will emerge from the experience personally and professionally unscathed. “If you work at a company and you release damaging information about them, how will that company regard you in the future?” Lewis asks. “Frankly, there will be a diminution of trust. You can add more legal protections [for whistleblowers], but there still will be social penalties that are going to be hard to avoid.”

Just ask a whistleblower. “It’s not for the faint of heart,” says Walton. “I’ll put it that way.” ♦

---

**WAXER** is a Toronto-based freelance journalist. She has written articles for various publications and news sites, including The Economist, MIT Technology Review and CNNMoney.com.

---

# Discussion Underway



## (want in?)

The Computerworld LinkedIn Forum is a community for all things IT: news, analysis and discussion about topics within IT, including careers, management and hot topics. If you are an enterprise IT practitioner at any level we’d love to have you join.

Apply for membership today at  
[www.computerworld.com/linkedin](http://www.computerworld.com/linkedin)

**COMPUTERWORLD**  
on **LinkedIn**





**Big data technologies and practices are moving quickly.** Here's what you need to know to stay ahead of the game.

**BY ROBERT L. MITCHELL**

**B**ILL LOCONZOLO, vice president of data engineering at Intuit, jumped into a data lake with both feet. Dean Abbott, chief data scientist at Smarter Remarketer, made a beeline for the cloud. The leading edge of big data and analytics, which includes data lakes for holding vast stores of data in its native format and, of course, cloud computing, is a moving target, both say. And while the technology options are far from mature, waiting simply isn't an option.

"The reality is that the tools are still emerging, and the promise of the [Hadoop] platform is not at the level it needs to be for business to rely on it," says Loconzolo. But the disciplines of big data and analytics are evolving so quickly that businesses need to wade in or risk

# 8 BIG TRENDS

## *in* Big Data Analytics

being left behind. “In the past, emerging technologies might have taken years to mature,” he says. “Now people iterate and drive solutions in a matter of months—or weeks.”

So what are the top emerging technologies and trends that should be on your watch list—or in your test lab? *Computerworld* asked IT leaders, consultants and industry analysts to weigh in. Here’s their list.

## 1 **Big Data Analytics in the Cloud**

Hadoop, a framework and set of tools for processing very large data sets, was originally designed to work on clusters of physical machines. That has changed. “Now an increasing number of technologies are available for processing data in the cloud,” says Brian Hopkins, an analyst at Forrester Research. Examples include Amazon’s Redshift hosted BI data warehouse, Google’s BigQuery data analytics service, IBM’s Bluemix cloud platform and Amazon’s Kinesis data processing service. “The future state of big data will be a hybrid of on-premises and cloud,” he says.

Smarter Remarketer, a provider of SaaS-based retail analytics, segmentation and

**In the past,  
emerging technologies  
might have taken  
years to mature.  
Now people iterate  
and drive solutions  
in a matter of months  
— or weeks.**

**BILL LOCONZOLO**, VICE PRESIDENT  
OF DATA ENGINEERING, INTUIT

marketing services, recently moved from an in-house Hadoop and MongoDB database infrastructure to the Amazon Redshift cloud-based data warehouse. The Indianapolis-based company collects online and brick-and-mortar retail sales and customer demographic data, as well as real-time behavioral data and then analyzes that information to help retailers create targeted messaging to elicit a desired response on the part of shoppers, in some cases in real time.

Redshift was more cost-effective for Smart Remarketer’s data needs, Abbott says, especially since it has extensive reporting capabilities for structured data. And as a

hosted offering, it’s both scalable and relatively easy to use. “It’s cheaper to expand on virtual machines than buy physical machines to manage ourselves,” he says.

For its part, Mountain View, Calif.-based Intuit has moved cautiously toward cloud analytics because it needs a secure, stable and auditable environment. For now, the financial software company is keeping everything within its private Intuit Analytics Cloud. “We’re partnering with Amazon and Cloudera on how to have a public-private, highly available and secure analytic cloud that can span both worlds, but no one has solved this yet,” says Loconzolo. However, a move to the cloud is inevitable for a company like Intuit that sells products that run in the cloud. “It will get to a point where it will be cost-prohibitive to move all of that data to a private cloud,” he says.

## 2 **Hadoop: The New Enterprise Data Operating System**

Distributed analytic frameworks, such as MapReduce, are evolving into distributed resource managers that are gradually turning Hadoop into a general-purpose data operating system, says Hopkins.



With these systems, he says, “you can perform many different data manipulations and analytics operations by plugging them into Hadoop as the distributed file storage system.”

What does this mean for the enterprise? As SQL, MapReduce, in-memory, stream processing, graph analytics and other types of workloads are able to run on Hadoop with adequate performance, more businesses will use Hadoop as an enterprise data hub. “The ability to run many different kinds of [queries and data operations] against data in Hadoop will make it a low-cost, general-purpose place to put data that you want to be able to analyze,” Hopkins says.

Intuit is already building on its Hadoop foundation. “Our strategy is to leverage the Hadoop Distributed File System, which works closely with MapReduce and Hadoop, as a long-term strategy to enable all types of interactions with people and products,” says Loconzolo.

### 3 **Big Data Lakes**

Traditional database theory dictates that you design the data set before entering any data. A data lake, also called an enterprise data



**People build the views into the data as they go along. It's a very incremental, organic model for building a large-scale database.**

**CHRIS CURRAN**, PRINCIPAL  
AND CHIEF TECHNOLOGIST, PWC'S  
U.S. ADVISORY PRACTICE

lake or enterprise data hub, turns that model on its head, says Chris Curran, principal and chief technologist in Pricewaterhouse-Coopers' U.S. advisory practice. “It says we'll take these data sources and dump them all into a big Hadoop repository, and we won't try to design a data model beforehand,” he says. Instead, it provides tools for people to analyze the data, along with a high-level definition of what data exists in the lake. “People build the views into the data as they go along. It's a very incremental, organic model for building a large-scale database,” Curran says. On the downside, the people who use it must be highly skilled.

As part of its Intuit Analytics Cloud, Intuit has a data lake that includes clickstream user data and enterprise and third-party data, says Loconzolo, but the focus is on “democratizing” the tools surrounding it to enable business people to use it effectively. Loconzolo says one of his concerns with building a data lake in Hadoop is that the platform isn't really enterprise-ready. “We want the capabilities that traditional enterprise databases have had for decades — monitoring access control, encryption, securing the data and tracing the lineage of data from source to destination,” he says.

## 4 More Predictive Analytics

With big data, analysts have not only more data to work with, but also the processing power to handle large numbers of records with many attributes, Hopkins says. Traditional machine learning uses statistical analysis based on a sample of a total data set. “You now have the ability to do very large numbers of records and very large numbers of attributes per record” and that increases predictability, he says.

The combination of big data and compute power also lets analysts explore new behavioral data throughout the day, such as websites visited or location. Hopkins calls that “sparse data,” because to find something of interest you must wade through a lot of data that doesn’t matter. “Trying to use traditional machine-learning algorithms against this type of data was computationally impossible. Now we can bring cheap computational power to the problem,” he says.

“You formulate problems completely differently when speed and memory cease being critical issues,” Abbott says. “Now you can find which variables are best analytically

by thrusting huge computing resources at the problem. It really is a game changer.”

“To enable real-time analysis and predictive modeling out of the same Hadoop core, that’s where the interest is for us,” says Loconzolo. The problem has been speed, with Hadoop taking up to 20 times longer to get questions answered than did more established technologies. So Intuit is testing Apache Spark, a large-scale data processing engine, and its associated SQL query tool, Spark SQL. “Spark has this fast interactive query as well as graph services and streaming capabilities. It is keeping the data within Hadoop, but giving enough performance to close the gap for us,” Loconzolo says.

## 5 SQL on Hadoop: Faster, Better

If you’re a smart coder and mathematician, you can drop data in and do an analysis on anything in Hadoop. That’s the promise — and the problem, says Mark Beyer, an analyst at Gartner. “I need someone to put it into a format and language structure that I’m familiar with,” he says. That’s where SQL for Hadoop products come in, although any familiar lan-

guage could work, says Beyer.

Tools that support SQL-like querying let business users who already understand SQL apply similar techniques to that data. SQL on Hadoop “opens the door to Hadoop in the enterprise,” Hopkins says, because businesses don’t need to make an investment in high-end data scientists and business analysts who can write scripts using Java, JavaScript and Python — something Hadoop users have traditionally needed to do.

These tools are nothing new. Apache Hive, for example, has offered a structured, SQL-like query language for Hadoop for some time. But commercial alternatives from Cloudera, Pivotal Software, IBM and other vendors not only offer much higher performance, but also are getting faster all the time. That makes the technology a good fit for “iterative analytics,” where an analyst asks one question, receives an answer, and then asks another one. That type of work has traditionally required building a data warehouse. SQL on Hadoop isn’t going to replace data warehouses, at least not anytime soon, says Hopkins, “but it does offer alternatives to more costly software and appliances for certain types of analytics.”



**6** **More, Better NoSQL**  
 Alternatives to traditional SQL-based relational databases, called NoSQL (short for “Not Only SQL”) databases, are rapidly gaining popularity as tools for use in specific kinds of analytic applications, and that momentum will continue to grow, says Curran. He estimates that there are 15 to 20 open-source NoSQL databases out there, each with its own specialization. For example, a NoSQL product with graph database capability, such as ArangoDB, offers a faster, more direct way to analyze the network of relationships between customers or salespeople than does a relational database. “These databases have been around for a while, but they’re picking up steam because of the kinds of analyses

people need,” he says.

One PwC client in an emerging market has placed sensors on store shelving to monitor what products are there, how long customers handle them and how long shoppers stand in front of particular shelves. “These sensors are spewing off streams of data that will grow exponentially,” Curran says. “A NoSQL key-value pair database [such as Redis] is the place to go for this because it’s special-purpose, high-performance and lightweight.”

**7** **Deep Learning**  
 Deep learning, a set of machine-learning techniques based on neural networking, is still evolving but shows great potential for solving business problems, says Hopkins. “Deep learning ... enables computers to rec-

ognize items of interest in large quantities of unstructured and binary data, and to deduce relationships without needing specific models or programming instructions,” he says.

In one example, a deep learning algorithm that examined data from Wikipedia learned on its own that California and Texas are both states in the U.S. “It doesn’t have to be modeled to understand the concept of a state and country, and that’s a big difference between older machine learning and emerging deep learning methods,” Hopkins says.

“Big data will do things with lots of diverse and unstructured text using advanced analytic techniques like deep learning to help in ways that we only now are beginning to understand,” Hopkins says. For example, it could be used to recognize many different kinds of data, such as the shapes, colors and

**Big data will do things with lots of diverse and unstructured text using advanced analytic techniques like deep learning to help in ways that we only now are beginning to understand.**

**BRIAN HOPKINS**, ANALYST, FORRESTER RESEARCH

objects in a video — or even the presence of a cat within images, as a neural network built by Google famously did in 2012.

“This notion of cognitive engagement, advanced analytics and the things it implies ... are an important future trend,” Hopkins says.

## 8 In-memory Analytics

The use of in-memory databases to speed up analytic processing is increasingly popular and highly beneficial in the right setting, says Beyer. In fact, many businesses are already leveraging hybrid transaction/analytical processing (HTAP) — allowing transactions and analytic processing to reside in the same in-memory database.

But there’s a lot of hype around HTAP, and businesses have been overusing it, Beyer says. For systems where the user needs to see the same data in the same way many times during the day — and there’s no significant change in the data — in-memory is a waste of money.

And while you can perform analytics faster with HTAP, all of the transactions must reside within the same database. The problem, says Beyer, is that most analytics efforts

**IT managers and implementers cannot use lack of maturity as an excuse to halt experimentation.**

MARK BEYER, ANALSYT, GARTNER

today are about putting transactions from many different systems together. “Just putting it all on one database goes back to this disproven belief that if you want to use HTAP for all of your analytics, it requires all of your transactions to be in one place,” he says. “You still have to integrate diverse data.”

Moreover, bringing in an in-memory database means there’s another product to manage, secure, and figure out how to integrate and scale.

For Intuit, the use of Spark has taken away some of the urge to embrace in-memory databases. “If we can solve 70% of our

use cases with Spark infrastructure and an in-memory system could solve 100%, we’ll go with the 70% in our analytic cloud,” Lo-conzolo says. “So we will prototype, see if it’s ready and pause on in-memory systems internally right now.”

## Staying One Step Ahead

With so many emerging trends around big data and analytics, IT organizations need to create conditions that will allow analysts and data scientists to experiment. “You need a way to evaluate, prototype and eventually integrate some of these technologies into the business,” says Curran.

“IT managers and implementers cannot use lack of maturity as an excuse to halt experimentation,” says Beyer. Initially, only a few people — the most skilled analysts and data scientists — need to experiment. Then those advanced users and IT should jointly determine when to deliver new resources to the rest of the organization. And IT shouldn’t necessarily rein in analysts who want to move ahead full-throttle. Rather, Beyer says, IT needs to work with analysts to “put a variable-speed throttle on these new high-powered tools.” ♦





# 5 Techniques *for* Securing Enterprise Data

Retake control of your data with sandboxing, cloud security gateways and more. **BY STACY COLLETT**

**W**HEN IT COMES to securing enterprise data, picture an IT leader with one foot on a dock and the other on a boat. Now watch the boat slowly drift away. Mobile, cloud and big data technologies are dragging businesses into uncharted waters, and data endpoints are moving

further and further from the IT department's control.

Meanwhile infrastructure is barely able to handle existing threats — let alone new ones. IT departments are obviously stretched, often without the manpower or skills to handle growing security needs.

A string of enterprise security breaches shows the obvious strain. In 2013, Verizon reported

more than 63,000 security incidents and 1,367 confirmed data breaches worldwide in its annual security breach investigations report. In the first half of this year, some 395 data breaches were reported to regulators in the U.S., according to the Identity Theft Resource Center.

“We’ve shattered the perimeters of our businesses,” says Chris Gray, vice president of enterprise security and risk at Accuvant, a Denver-based provider of IT security products and services. “We’re outsourcing, we’re shoving everything to the cloud, we’re enabling mobility and [allowing] alternative

means of access at levels that we’ve never done before.” As a result, he adds, “we’ve opened up holes . . . and spread everything out. Instead of watching one spot, we’re now watching 50 — which makes the problem we’re facing all the greater.”

It’s not all gloom and doom. More than 90% of those breaches analyzed by Verizon fit into just nine distinct security patterns. Security experts say there are ways to balance security risks with the opportunities that new technologies provide.

Here are five data security technologies worth considering this year.

## 1 Endpoint Detection and Response Solutions

To regain control, businesses are looking to automated tools that detect, correct and even predict security breaches, says Mike Lloyd, CTO at Red-Seal Networks, a Sunnyvale, Calif.-based security vendor. “The need for automation is clear if they’re short-staffed or can’t get the talent,” or if the number of access points to cover is just too great, he says.

Endpoint threat detection and response tools can satisfy the need for continuous protection from advanced threats at endpoints like tablets, phones and laptops. These tools monitor endpoints and networks, and store data in a centralized database. Analytics tools are then used to continually search the database to identify tasks that can improve the security state to deflect common at-

**We’ve shattered the perimeters of our businesses. We’re outsourcing, we’re shoving everything to the cloud, we’re enabling mobility and [allowing] alternative means of access at levels that we’ve never done before.**

**CHRIS GRAY**, VICE PRESIDENT OF ENTERPRISE SECURITY AND RISK, ACCUVANT



**We can build in zones of where we do business. If a device goes outside of a zone, it will alert us and we can take a proactive approach.**

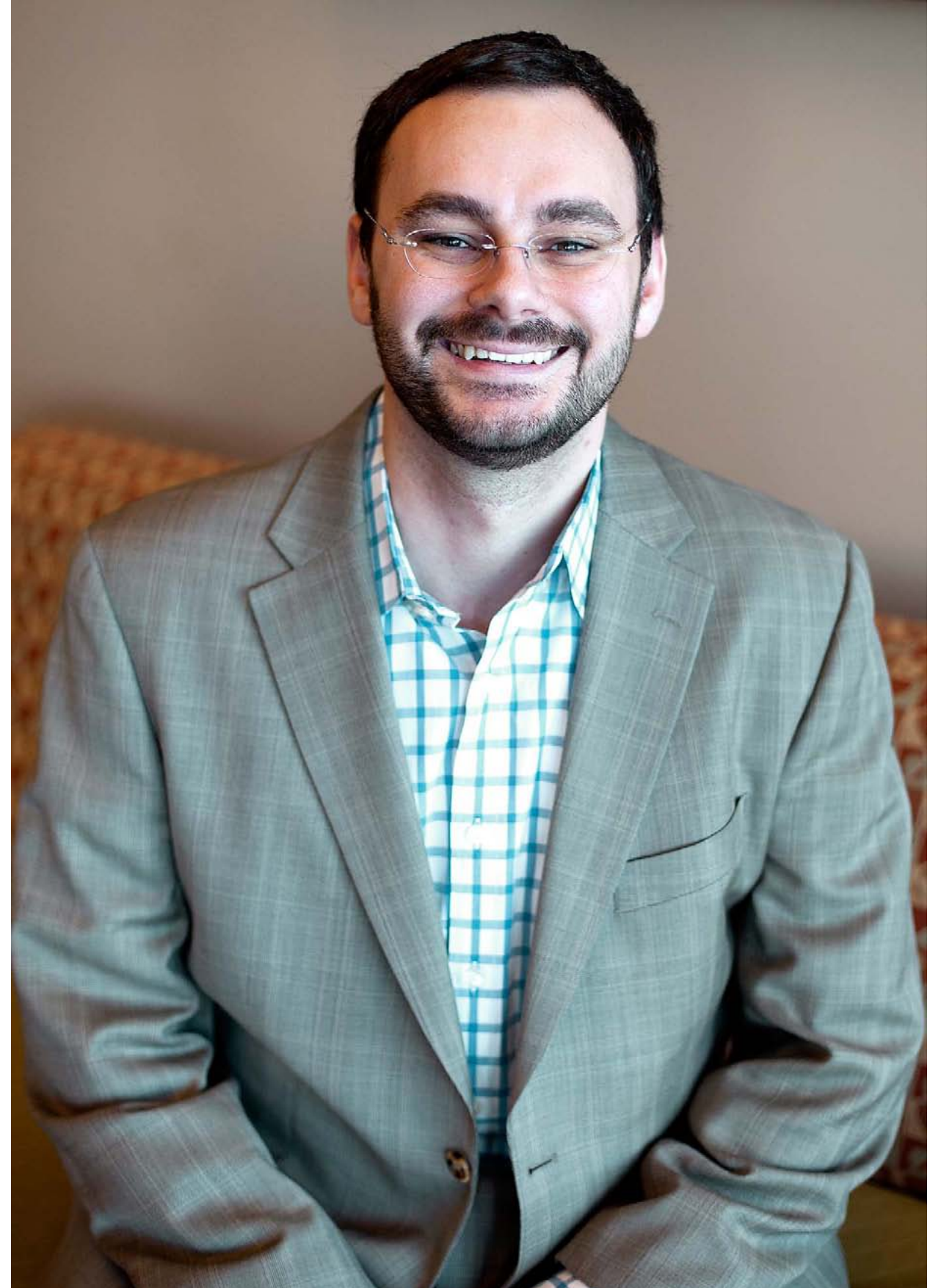
**ANTHONY MANNARINO** (RIGHT), IT DIRECTOR,  
SECURITY AND COMPLIANCE, CIGNA-HEALTHSPRING

tacks, provide early identification of ongoing attacks (including insider threats) and rapidly respond to those attacks, according to a report presented at the Gartner Security & Risk Management Summit in June. These tools can then help IT security staffers to quickly investigate the scope of attacks and stop them.

Nashville-based insurance provider Cigna-HealthSpring wants to be proactive in the way it monitors the security of its mobile devices. The number of iPads and iPhones that HealthSpring issues to employees is expected to double in the

next two years as the company adds more online apps and offers more reporting capabilities in the field, says Anthony Mannarino, IT director, security and compliance.

HealthSpring uses Absolute Software's Computrace product to monitor and track employees' mobile devices. The benefits of using the software include "knowing what's on the device [and] being able to remotely wipe it," Mannarino explains. New software capabilities let HealthSpring check on devices in real time. "We can build in zones of where we do business. If a device goes outside of a



**This idea of monitoring the outcomes of activity and looking for malicious stuff on the backside after a program is executed is really becoming crucial to success.**

PETE LINDSTROM, ANALYST, IDC

zone, it will alert us and we can take a proactive approach,” often before the user even realizes it’s missing, he adds.

## 2 Sandboxing

Inevitably, some malware or hacker will make it through the security perimeter. One of the easiest things that enterprises can do to ensure that their data remains safe when that happens is to add sandboxing capabilities that can automatically isolate suspected malware that’s been detected on a network device, says Pete Lindstrom, an

analyst at research firm IDC. Once the malware is isolated and is safely away from active systems, the sandboxing tool will run the application and analyze its potential effect. “This idea of monitoring the outcomes of activity and looking for malicious stuff on the backside after a program is executed is really becoming crucial to success,” he says.

Dedicated sandboxing tools, available from vendors such as FireEye, do the job but can be expensive, Lindstrom says. But other security vendors are adding sandboxing features to existing products. “It’s not uncommon for the antivirus players to have it, and most of the network security players have some sandboxing capabilities,” he says.

Cigna-HealthSpring uses FireEye’s sandboxing application. “They can see a threat and run it in a sandbox environment to see what it does, and

we can stop it,” Mannarino says. “If [the tool] is reporting that it’s trying to connect to some site in China, then we can go into our Web filtering technologies and make sure we put blocks on those URLs.”

For many companies, the tricky part may be understanding and analyzing the results uncovered by the tool, Lindstrom adds, but there are services that help make sense of the results. Companies offering such services include DataHero in San Francisco and ClearStory Data in Menlo Park, Calif.

Lindstrom predicts that sandboxing functionality will become standard fare in security products in the next two or three years.

## 3 Security Analytics

Most security teams have a wealth of data coming from myriad endpoints and security prod-



ucts. “The problem is they lack actionable, decision-making indicators,” Lloyd says.

Analytics is becoming a cornerstone of security capabilities. Going forward, Gartner predicts that all effective security protection platforms will include domain-specific embedded analytics as a core capability. By 2020, 40% of enterprises will have “security data warehouses” for storing and monitoring data to support post-event analysis, according to Gartner. Over time, this data, combined with other intelligence, will create a baseline for normal activity and make any deviations noticeable.

Florida-based Broward Health, the third-largest health-care system in the U.S., deploys an arsenal of security technologies to protect its patient and company data, but Ronaldo Montmann, vice president of

IT, still doesn’t have the big picture. “We have next-generation firewalls, the best intrusion-prevention systems, data loss prevention systems in place, identity management solutions in place — but they operate in silos,” he explains. In addition to a comprehensive system, he wants the ability to predict future vulnerabilities.

“We’re trying to see if we can [take] the big analytics software that we bought for the financial and clinical system and leverage that for infrastructure to look at events and correlate those events in a meaningful way so we can predict or under-

stand how they relate.”

But that also requires a team of senior-level staffers who understand all the nuances of the technology that the hospital system supports and can work collaboratively and proactively to maintain the network.

A protocol algorithm looks at event logs at the server, switch and workstation levels and gathers information “that typically a human being wouldn’t be able to process,” Montmann says. That data is analyzed to correlate issues on the network. “We’re trying to design an environment where we can learn more about what’s going on in

**We’re trying to design an environment where we can learn more about what’s going on in the network and perhaps those different odd behaviors can lead us to understand whether it’s malware [or] a hacker.**

RONALDO MONTMANN, VICE PRESIDENT OF IT, BROWARD HEALTH



**This is really the wave of the future for how IT folks are going to get visibility and control into cloud architectures.**

**PETE LINDSTROM,**  
ANALYST, IDC

the network and perhaps those different odd behaviors can lead us to understand whether it's malware [or] a hacker." Montmann says he expects to have the analytics team in place by the first quarter of 2015.

## 4 Cloud Security Gateways

The state of Wyoming in August announced plans to discontinue most of its data center operations and move its physical equipment to commercial colocation facilities. It will continue to manage its own physical servers at the colocation centers, but this outsourcing step is part of a broader plan to move the state's computing resources to cloud services. No doubt, security will be a top-of-mind issue when it comes to protecting data in the cloud.

Enterprises that use the cloud should consider cloud

security gateways. These on-premises or cloud-based security policy enforcement points are placed between cloud services consumers and cloud services providers to interject enterprise security policies as the cloud-based resources are accessed.

"This is really the wave of the future for how IT folks are going to get visibility and control into cloud architectures," Lindstrom says.

Operating like unified threat managers in the cloud, cloud security gateways provide access security or policy enforcement, but they monitor activity using analytics, handle data loss prevention functionality on the back end, and apply communication encryption, as well as encryption of structured and unstructured data. Cloud security gateways can be deployed entirely in the cloud or as edge-based appliances.

"It's a very useful way to ad-

dress the problems of loss of visibility and control that you typically get in the cloud, and it's not particularly expensive," Lindstrom adds.

## 5 Adaptive Access Control

Despite the need to lock down data, IT departments also need to support business operations by allowing a wide range of mobile devices to access corporate systems. To keep data safe, Gartner suggests using adaptive access control, a form of context-aware access control that acts to balance the level of trust against risk at the moment of access using a combination of trust elevation and other dynamic risk mitigation techniques. Context awareness means that decisions about who is and isn't granted access reflect current conditions, according to Gartner, and dynamic risk



mitigation means that access can be safely allowed where otherwise it would have been blocked. This type of access management architecture allows companies to provide access from any device in any location, and makes it possible to set up different levels of access to a range of corporate systems depending on users' risk profiles.

Gartner recommends other security technologies and techniques, including the use of machine-readable threat intelligence services provided by third parties and adopting containment and isolation as a fundamental security strategy

— an approach in which everything that is unknown is treated as untrusted. Other technologies that the research firm advises security professionals to consider include software-defined security, in which security functionality is embedded in all new applications, and interactive application security testing, which combines static and dynamic testing techniques in a single solution.

### Choosing Security Technologies

Deciding if and when to deploy one of these up-and-coming security technologies depends on the structure of the organiza-

tion and the amount and types of data that are considered to be valuable, says David Brown, director of Accuvant's technology solutions practice. "How is your data used, who needs access to it and what is your budget," not just for the technology but the staff to support it, he says. For instance, "security analytics has some good solutions out there, but it also takes multiple smart people to manage it," says Brown.

At the end of the day, it's all about balancing risks and opportunities to grow the business, security leaders say.

"There's always an acceptable level of risk, so finding and agree-

ing on that line usually takes multiple parties — legal, leadership, human resources and people in the business — to decide what is best," Mannarino says.

Lindstrom agrees that the amount of risk in IT is indeed increasing, "but that's the result of a thriving economy," he says.

"If you take an economics approach to technology risk management, you have trade-offs," he notes. "Most folks are doing it successfully. Embrace the nature of risk, manage it, and don't let it manage you." ♦

---

**COLLETT** is a Computerworld contributing writer. You can contact her at [stcollett@comcast.net](mailto:stcollett@comcast.net).

**There's always an acceptable level of risk, so finding and agreeing on that line usually takes multiple parties — legal, leadership, human resources and people in the business — to decide what is best.**

**ANTHONY MANNARINO**, IT DIRECTOR, SECURITY AND COMPLIANCE, CIGNA-HEALTHSPRING

# Career WATCH



ASK A PREMIER 100 IT LEADER

## Catherine Maras

*The Bexar County, Texas, CIO answers questions on kicking your career off with no experience, the qualities she looks for when promoting into management and the value of writing skills.*

**Soft skills become more and more important as you move up the management ladder.**

CATHERINE MARAS, CIO,  
BEXAR COUNTY, TEXAS

**As a single mom going to school while working full time to support myself and my daughter, I've had one dead-end job after another. Now I'm about to get my degree in computer science, but I was never able to get even the lowest job in IT to gain experience. Do you think I'll be able to break into IT now? I'm 25 and suddenly very worried about this.** First, congratulations on your accomplishment. Based on your journey to secure your degree in computer

science, you possess many valuable qualities that will supersede your lack of IT experience. You have deep experience in life through your juggling of multiple responsibilities. I recommend that you scour the job sites of both government and for-profit entities. You possess both the analytical and soft skills that will benefit any organization.

**When considering who to promote into a management position, what qualities do**

## IT's Big Earners

**The top-paying IT positions,** as ranked by Mondo, an IT recruitment and placement firm. The low end reflects rates paid in locales such as Florida and Dallas, and the high end is what to expect in San Francisco and New York.

- 1 CIO/CTO:** \$150,000 - \$230,000
- 2 Chief security officer:** \$135,000 - \$200,000
- 3 Application architect:** \$130,000 - \$170,000
- 4 Vice president, IT:** \$130,000 - \$165,000
- 5 Director, IT:** \$125,000 - \$165,000

- 6 Network architect:** \$125,000 - \$150,000
- 7 VP, engineering:** \$120,000 - \$165,000
- 8 VP, infrastructure:** \$120,000 - \$165,000
- 9 Security manager:** \$120,000 - \$160,000
- 10 MySQL DBA:** \$120,000 - \$130,000

SOURCE: MONDO, BASED ON DATA FROM 4,000 PLACEMENTS THIS YEAR



**you most want to see?** The qualities I look for when promoting into a management position are deep knowledge of the subject matter combined with the soft skills of working with people. And the soft skills become more and more important as you move up the management ladder due to the need to achieve business goals through teams. It is a given that an IT professional possesses the subject matter expertise; however, the ability to lead people

and meet the organization's long-term strategy blends both skills sets.

**In the course of my career, I have written many analyses, case studies and white papers. Are my writing skills of value as I try to move into a larger leadership role?** I was very fortunate to have had a dedicated high school English teacher who stressed

critical thinking and writing. Possessing these skills will separate you from the rest of the management candidates. The ability to articulate and convey an idea in a concise written form is

highly valued, especially when you are able to demonstrate your knowledge of the organization's strategy by writing case studies and white papers that show your thinking to be aligned with the organization's goals. ♦

If you have a question for one of our Premier 100 IT Leaders, send it to [askaleader@computerworld.com](mailto:askaleader@computerworld.com), and watch for this column on Computerworld.com.

## Work Without End

**Americans seem to be finding it harder to take vacations, and when they do go away, they find it difficult to avoid working during their allotted downtime.** According to an

April 2014 Glassdoor online survey, the average employee takes only half of his or her vacation time, and 61% of the respondents said they do some work when they do take time off.

And there's evidence that all of this is intensified for senior people working in IT. Just 30% of senior IT professionals surveyed this year by TEKsystems said their employers did not expect them to be available during vacations. Things are better down the ranks, with three-quarters of entry-level and mid-level IT professionals saying they face no such expectation.

**NO RESTING** | 3 out of 20 U.S. employees have taken no paid time off over the past 12 months.

Percentage of vacation  
or paid time off used

Percentage of  
employees

100%

25%

76% to 99%

10%

51% to 75%

10%

26% to 50%

15%

1% to 25%

25%

0%

15%

**DURING THEIR TIME OFF...**

■ **24% were contacted by co-workers** about a work-related matter.

■ **20% were contacted by their bosses** about a work-related matter.

■ **17% had a hard time not thinking about work.**

■ **9% reported that family members complained** about their working.

# SHARKTANK

TRUE TALES OF IT LIFE AS TOLD TO SHARKY



HAL MAYFORTH

## The Right Tool for the Job

**NON-IT PILOT FISH** is picking up a part on Saturday morning at the air-conditioning equipment distributor where he works when he runs into two IT guys prepping to move racks of servers from the second floor of one building to another – and they figure it will take all weekend. “I said, ‘Why don’t you just wheel the racks to the second-floor ledge, and I can use the forklift to move it from Building 1 to Building 2?’” says fish. “The two of them looked at each other

and thought I was crazy. I had both racks moved in 30 minutes and the system was up and running by 1:30 p.m. We all enjoyed a nice weekend after that.”

### 22-Carat Catch-22

This jewelry store keeps reporting that its employ-

ees can’t connect to the Internet, and this pilot fish keeps getting sent out to fix the problem – every week for three months. The sad thing is, fish knows what the problem is. “The jewelry store was down with a problem several months back,” says fish.



**The guard insisted that there was nothing he could do but told the computer operator she was welcome to lodge a complaint with the sergeant.**

“The fact that the store’s network connection was down was duly logged. The problem was fixed, but no one labeled the store back up. So about once a week, network security notices that people from a down site are logged in. That shouldn’t happen, so the security guys disable those user IDs. And the users can’t get that reversed out on their own because to get help they have to log in first. I come out, get everyone enabled, close the work order and leave. They can’t seem to get the

record fixed, so the security people keep seeing the site as down and the users from that site as breaking into the system, so they keep disabling them.”

### **It’s All in the Game**

It’s the early 1980s, and this junior computer operator at a big university is headed across campus to print payroll checks. “When she was leaving the main campus parking lot for the computer center, the security guard asked if she was done for the day,” recalls a pilot fish in the

know. “She said no, she was going to the remote facility for a while. The guard told her she probably wouldn’t be able to park in the main lot when she returned, since there was a basketball game that afternoon and her spot might be given to a VIP. She asked for the guard’s name and ID. He insisted that there was nothing he could do but said she was welcome to lodge a complaint with the sergeant at the security building. She said, ‘I’m not asking so I can register a complaint.

I’m going to the remote facility to print paychecks. You’ve been very polite, so I want to be certain that yours is not one of the occasional misprints that take a week of work with the accounting department to get replaced.’ The guard assured her that her space would be available upon her return.” ♦

### **SHARKY’S SAVING A SPACE**

*for your true tale of IT life, so send it to me at [sharky@computerworld.com](mailto:sharky@computerworld.com). You’ll snag a snazzy Shark shirt if I use it.*

Futurist **THORNTON A. MAY** is a speaker, educator and adviser and the author of *The New Know: Innovation Powered by Analytics*. You can visit his website at [www.thorntonamay.com](http://www.thorntonamay.com) and contact him at [thornton@thorntonamay.com](mailto:thornton@thorntonamay.com).



# Where Is Modern IT Headed?

**While most groups today make use of the word *modern*, the word has all but disappeared from the IT vocabulary.**

**JERRY GARCIA** of the Grateful Dead was once asked what the band's goal was. His response: "Our goal is to make the music only we can make." Like so many other things, this sound bite got me thinking about IT. What is the value only enterprise IT can make?

In today's world, what is IT's distinctive skill set? What is it that only we can do? Put another way: In the future, what will be IT's superpower? To answer this set of questions, I dusted off my Rolodex (a decidedly non-modern artifact), went to 100

of the smartest businesspeople I know, and asked them a simple question:

Where do you think modern IT is heading?

As it turns out, that is a very difficult question to answer. I'll get to that, but first, let me explain why I asked the question the way I did.

## **What's With the Word *Modern*?**

I included the word *modern* in my question for three reasons. One reason—which derives from an eloquent explanation

that the chief operating officer of a publicly traded financial services firm once gave me—is that IT, now that it touches everything and everybody, everywhere and everywhen, can no longer really be thought of as just one thing. The list of tasks that fall within the genus IT is almost limitless. It includes maintaining a multicontinent ERP system, patching productivity software, establishing machine-to-machine communication between sensors, negotiating data management policies with European governments, embedding



ethics in the code governing unmanned vehicles, designing the user interface for bartending robots on a Royal Caribbean cruise ship, getting the sensors in a mattress to talk to the sensors in the home HVAC system to algorithmically determine and then create the optimal environment for REM sleep, managing the call desk that supports customers enjoying Bose's SoundTouch home audio system, and setting behavioral incentives designed to induce blue-collar workers on the shop floor to input inventory and parts use data. So when we discuss IT in the modern age, we have to be a bit more specific about which IT we're talking about. There are multiple ITs. I want to talk about the future-facing part of our now-fragmented discipline. I want to talk about "modern" IT.

Reason 2 derives from a discovery that really surprised me.

One of the tools anthropologists use to study tribal behavior is word use—that is, how do various groups use, abuse or not use language? I was surprised to learn that while most groups today make frequent use of the word *modern* (modern finance, the modern home, modern literature or modern art), the word has all but disappeared from the IT vocabulary. I have not yet finished my analysis of why this might be. Perhaps we in IT do not use the word *modern* because we're convinced that everything we do is modern and thus we view the word as redundant. I want to reintroduce *modern* into the IT discussion. I want to rebrand IT as modern.

Reason 3 is that outside of IT, what we do inside of IT is not perceived as being particularly modern. Anything but, in fact. Our discipline, more likely than not, is viewed as being the

antonym of modern—behind the times. I want to rebrand IT as being part of the future. The general narrative pulsing on the screens that comprise modern existence today portrays a Manichean world where IT is slow and stupid, speaks in tongues (geek speak) and has no idea about how the business makes money. This portrayal is ludicrous. The CIO is one of the most important members of the executive team, if not the most important. I believe *modern CIOs should be paid more*—much more. (But that's a subject for another article.)

### No Consensus

If you put 100 senior IT executives in a room (as we just did at Ohio State University) and ask them where modern IT is heading, you will not get a consensus answer. Even if the CIOs are from the *same* vertical market,

as were the public-sector CIOs at the FLGISA 2014 Annual Conference and the GMIS 2014 Annual Conference, you will not get a consensus answer.

Responses exist on a spectrum from "IT disappears" to "IT pulls a Putin and takes over." Linglong He, the award-winning, high-energy and spectacularly charismatic CIO at Quicken Loans, told students and faculty at Ohio State that "technology is the driver. Business is the passenger." This is in marked contrast to the CIO at a high-performing utility who raised the question of whether the CIO—essentially the EVP/SVP of information—will face the same career extinction as the now departed and forgotten 19th-century chief electricity officer.

I welcome your thoughts and comments as we move forward in our examination of where modern IT is heading. ♦