MARCH 2015 | icma.org/pm

PM
PUBLIC MANAGEMENT

INSIDE

2 CELEBRATE ETHICAL CONDUCT

18 COLLECTING DISASTER RECOVERY COSTS

24 GEARING UP FOR FIRSTNET

32 TOP 10 OR MORE

CYBERCRIME @ CITY HALL

Plan the Prevention and Response

ADVANCING PROFESSIONAL LOCAL GOVERNMENT MANAGEMENT WORLDWIDE

ICMA

MARCH 2015 | icma.org/pm

PM
PUBLIC MANAGEMENT

INSIDE

2 CELEBRATE ETHICAL CONDUCT

18 COLLECTING DISASTER RECOVERY COSTS

24 GEARING UP FOR FIRSTNET

32 TOP 10 OR MORE

CYBERCRIME @ CITY HALL

Plan the Prevention and Response

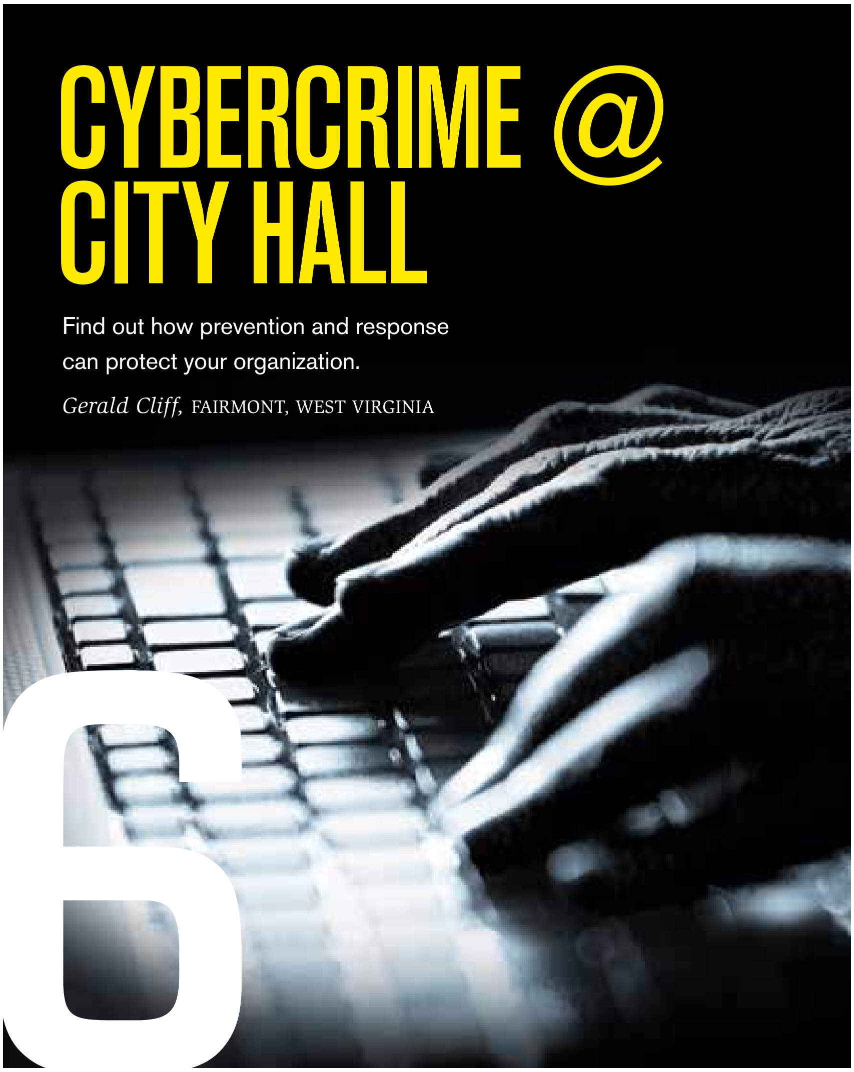
ADVANCING PROFESSIONAL LOCAL GOVERNMENT MANAGEMENT WORLDWIDE

ICMA

contents

March 2015 | Vol. 97 No. 2

cover story



6

CYBERCRIME @ CITY HALL

Find out how prevention and response can protect your organization.

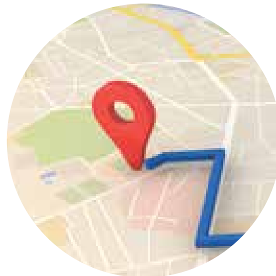
Gerald Cliff, FAIRMONT, WEST VIRGINIA

features

12 CITIZEN DISENGAGEMENT: THE MINORITY OPINION
A new take on resident involvement that might seem odd.
Kevin Desouza, PHOENIX, ARIZONA

18 GETTING DISASTER RECOVERY COSTS MOVING
How to navigate FEMA's rules to collect disaster recovery costs.
Hilary Cairnie, Maria Coor, AND *Bill DeVinney,* WASHINGTON, D.C.

5
Mapping Department



departments

2 Ethics Matter!
Celebrate Ethical Conduct

4 On Point
Are You Reading a Book That You Would Recommend to Your Colleagues?

5 @icma.org

22 Council Relations
Before In Transition

23 Balancing Act
How You Sleep Is How You Work

24 Management Minute
Gearing Up for FirstNet

25 Calendar of Events

26 International Ties
Reinvigorated In Romania

28 Tech Touch
The First 24 Hours

29 Professional Services Directory

32 Top 10 or More
Leading Change

icma.org/pm

This issue of PM is available online and mobile at icma.org/pm February 27, 2015.

BY MARTHA PEREGO

CELEBRATE ETHICAL CONDUCT

Do it with positive stories

Why is it that in our efforts to inspire everyone to do the right thing, we rely on examples of people who did the wrong thing? This hardly seems like the approach designed to produce the best outcome.

Think about all the learning opportunities we face in life. What inspired you to learn to swim? Was it stories of people drowning or the fact that your older sibling succeeded?

So why do we rely so heavily on the bad stories? Is it the scarcity of ethical people in the profession? Is the profession now so ethical that doing the right thing is the uninteresting norm? Or is it just a reluctance to tell our story?

The lack of positive stories about local government professionals reflects the persona of the profession and the challenge of blowing the whistle. We choose to stay out of the limelight. Often the story of what we did right doesn't get shared out of loyalty to the organization we served. Talking about what you did right requires exposing details about those who didn't.

Credible third-party reviews might accelerate sharing positive stories.

Cal-ICMA Ethical Hero Award

The Cal-ICMA Ethical Hero award exists to recognize ICMA members in California who serve the profession with dignity, honor, and integrity.

This year's recipient is Magda Gonzalez. Magda joined the city of East Palo Alto as city manager in 2012. In nominating Magda, a colleague said that she "provided the mayor and city council with her best professional advice.

"Her advice and leadership for the organization was thwarted by certain councilmembers, and they questioned the role of a city manager. Rather than being concerned about her own professional future with the organization, she moved forward with evaluating the effectiveness of programs and looking for efficiencies.

"Her continued focus on finding the best course of action for the city and bringing that information to the council's attention was often met by

PM
PUBLIC MANAGEMENT

Public Management (PM) aims to inspire innovation, inform decision making, connect leading-edge thinking to everyday challenges, and serve ICMA members and local governments worldwide in the pursuit of excellence in local governance.

ICMA EXECUTIVE DIRECTOR
Robert O'Neill, Jr.

DIRECTOR OF PUBLISHING
Ann Mahoney

EDITOR
Beth Payne

DESIGN
Thor Design Studio
www.thor-studio.com

Public Management (PM) (USPS: 449-300) is published monthly except February by ICMA (the International City/County Management Association) at 777 North Capitol Street. N.E., Washington, D.C. 20002-4201. Periodicals postage paid at Washington, D.C., and at additional mailing offices. The opinions expressed in the magazine are those of the authors and do not necessarily reflect the views of ICMA.

REPRINTS: Apply to the editor for permission to reprint any part of the magazine.

SUBSCRIPTIONS: U.S. subscription rate, $46 per year; other countries subscription rate, $155 per year: single copies, $10. Printed in the United States.
Contact: 202/289-4262; subscriptions@icma.org.

POSTMASTER: Send address changes to *Public Management*, ICMA, 777 N. Capitol Street, N.E., Suite 500, Washington, D.C. 20002-4201.

ARTICLE PROPOSALS: Visit icma.org/pm to see "Editorial Guidelines" for contributors.

EDITORIAL INFORMATION
202/962-3619
bpayne@icma.org

ADVERTISING SALES
Ben Harmon
The Townsend Group, Inc.
Tel: 301/215-6710 x106
Fax: 301/215-7704
bharmon@townsend-group.com

PRINTING
Westland Printers
Laurel, Maryland

ICMA
icma.org | icma.org/pm

the council's lack of support without stating legitimate reasons. She also was publicly criticized for performing what professional city managers view as their role in a council-manager form of government. The council decided not to renew her contract."

Magda is currently city manager for Half Moon Bay, California. To read about her and past winners, visit the Cal-ICMA website at http://icma.org/en/ca/home.

Another Ethical Hero

Greg Smith served as manager for Moon Township, Pennsylvania, for 24 years when he encountered the biggest ethical challenge of his career. Dr. Craig Wheeland, political science professor at Villanova University, explored his saga in an article published in the American Society of Public Administration's journal *Public Integrity* (Summer 2013 edition; www.aspanet.org).

As chronicled, an election brought a new majority to the board of supervisors who "broke with the tradition of nonpartisanship, respect for professional management, and ethical practices long established in Moon's political culture."

From Day One, the conduct of the new majority raised red flags. They excluded staff and minority board members from their discussions. At the reorganization meeting, they appointed a new township solicitor and engineer. While the move was their prerogative, it lacked a competitive process and staff input. The solicitor was a neighbor of a new councilmember; the engineering firm was an unknown entity.

Soon thereafter, the solicitor and the engineering firm billed the township for work that was not authorized by the board and was a surprise to staff. When presented with the facts and the bill, the board approved payment.

The engineering firm established a trend of submitting unreasonable invoices and also failed to provide the substantiating work product. Yet, it had the support of the board majority.

As detailed in the article, each month presented a new ethical concern. Greg and his assistants attempted to address and correct these issues internally. Framing the issues around acceptable practices, they were determined to convince the majority of the board to change their practices. When that approach failed, they documented the questionable items in detailed memos. Correspondence was broadly shared internally. All to no avail.

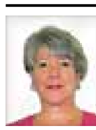
Ultimately, Greg and his assistants arrived at that ethical crossroad. Do you continue to challenge the conduct of the board even when the "bright light of illegality is lacking (although suspected)"? Or do you leave?

Greg shared with colleagues that his obligation to the community, organization, and his personal and professional standards required him to try to resolve the ethical dilemmas created by the board. He said that "What we know scares us, but what we did not know scares us even more."

Greg and his two assistants ultimately chose to resign. Greg was reserved in his public statement noting that "he and the board had very different approaches as to how local government should operate." He was more direct in individually addressed letters to the board. One board member made the letter public. The next month the board selected a new engineering firm.

In the end, Dr. Wheeland noted "resigning appeared to be the best remaining professional practice to call the public's attention to the board's questionable actions." Greg and the two assistant managers continued their careers in local government. Greg passed away earlier this year.

We celebrate these colleagues for doing what was right to uphold the public's trust. Now what steps do we need to take to tell more positive stories? PM



MARTHA PEREGO
Ethics Director, ICMA
Washington, D.C.
mperego@icma.org

ARE YOU READING A BOOK THAT YOU WOULD RECOMMEND TO YOUR COLLEAGUES?

MARCIA RAINES, ICMA-CM
City Manager
Millbrae, California
mraines@ci.millbrae.ca.us

I found the book *For the Love of Cities* by Peter Kageyama (2011) an inspiring read in which the author takes an interesting approach to the passion of building healthy cities. In my opinion, the subtitle "The love affair between people and their places" says it all. While we each spend a significant portion of our professional lives dealing with day-to-day efforts to keep a community on the correct path, I'm not sure how much time and effort we spend on the larger picture.

As Kageyama points out, if we step back and look at the sum of our efforts we can see that cities of today compete to be the best places to live and where the best talent wants to be located. This book looks at residents as those with an emotional connection to the community where they live and what actually makes the difference between one city and another.

The author provides examples that inspire real placemaking. These examples look at what makes one city more appealing than another. It's realizing a connection to the place that residents call a city. The author helps us understand that it's not the transit system or the utilities that we connect with; rather, it's the places and the feel of the community we enjoy or don't enjoy.

As leaders, local government managers should all be inspired to pick up this book and read it before the next council meeting or the next staff meeting. Better yet, give a copy to both the councilmembers and the executive staff team members and challenge them to read it.

We can make our communities more livable for everyone by taking these views to heart. PM

1

CHECKLIST FOR CRISIS COMMUNICATION PLANNING

Tips from ICMA's *InFocus* report can guide a local government's preparations for crisis communication.

▸ icma.org/crisis_communications

2

RICHFIELD KNOWS IT CAN BE INNOVATIVE

Richfield, Minnesota, learned that a culture of innovation is not created overnight. Its Ambassador Team is focusing efforts on spreading the word and providing a greater variety of opportunities for employee participation and engagement.

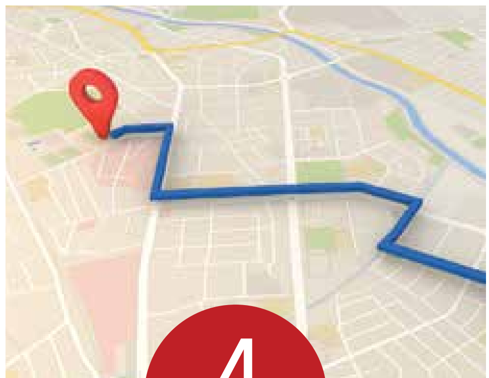
▸ icma.org/innovativerichfieldmn

3

SUPPORTING SMALL BUSINESSES IN JORDAN

Employing city-to-city partnerships and local economic development training, ICMA is helping Jordanian municipalities strengthen their ability to attract investment and facilitate growth through the USAID-funded Local Enterprise Support (LENS) project.

▸ icma.org/lens



4

ITS VERY OWN GIS MAPPING DEPARTMENT

During 2014, Pitkin County, Colorado, created its own GIS mapping department that provides online maps, photographs, and 3D products to the public.

▸ icma.org/pitkincountyGISdept

CYBERCRIME

@ CITY HALL

Discussions of prevention and response can protect your community

By Gerald Cliff

TAKEAWAYS

› Learn about the impacts of data breaches.

› Learn steps to take that will reduce the likelihood of a data breach occurring as well as reduce the severity of an incident if it happens.

As local governments embrace technology and use such financial instruments as credit and debit cards and digital currencies to accept payment for taxes, utility fees, traffic fines, parking fees, and more, the likely result will be increased exposure to personally identifiable information (PII) being compromised, which is part of the reason that identity theft is the nation's fastest growing category of crime.

Local governments of all population sizes maintain records containing names, addresses, ages, and Social Security numbers of employees, taxpayers, contractors, and volunteers. It is a rare entity that does not maintain these records in an electronic format.

It might seem illogical to the local government manager of a small community to envision that the Chinese military, a Russian cybercrime gang, or the Syrian Electronic Army would target his or her community's computers when they could be trying—and in many cases succeeding—to hack into the U.S. State Department, the White House, or the CIA.

While a local database of taxpayers may not yield the millions of records that hacking Target stores, Chase Bank, or some other national chain will, hitting several such smaller and softer targets can yield results that can still bring significant return to identity thieves. Unfortunately for the owner of those records, it can also bring tremendous cost in dealing with the incident.

Major corporations typically have a large reserve with which to address data breaches. Local governments, however, might be bound to a more narrowly constructed budget and perhaps do not have the luxury of a financial reserve with which to prevent—or effectively respond to—a data breach.

Believing that your locality's IT system is too insignificant a target for a hacker tends to ignore some of the reasons, other than identity theft, that hackers will break into your system. Remember, data breach is not limited to someone hacking into your IT system.

A data breach can be the result of lost or stolen paper documents, an insider abusing his or her employment-related access to the system, a lost or stolen laptop or portable electronic storage media, or improper disposal of such electronic devices as copiers and computers capable of retaining information on their internal memory.Then there is the activist hacker who simply wants to disrupt the business of the government entity that somehow offended or disadvantaged him or her, or the political activist who wants to make a statement in support of a favorite agenda.

Citing a report by the National Association of State Chief Information Officers (NASCIO), *Governing* magazine noted in 2011 that 50 percent of states NASCIO surveyed reported spending less than 3 percent of their IT budgets on security. The private sector by comparison spends 5 percent or more, often of a substantially larger pool of resources. Local governments that have not been victimized tend to ignore the potential threat and may be less likely to allocate sufficient funding to a problem that hasn't happened.

Threats Abound

Recent events in a number of communities, including Ferguson, Missouri, provide ample illustration of the damage "hactivism" can do to a city's computer system. Hactivism refers to the use of computer technology to promote political goals (e.g., free speech, human rights). *Government Technology* magazine reported in August 2014 that following the high-profile incidents in Ferguson, the city's IT system was compromised, the Internet crashed, the city's website went down, and phones ceased working at city hall.

The hacker group Anonymous claimed responsibility and left warnings like this: "If you abuse, harass, or harm the protesters in Ferguson, we will take every Web-based asset of your departments and federal agencies off-line." Since that time PII of the chief of police and photos of his home, his wife, and daughter have been released on the Internet.

In March 2014, the Albuquerque, New Mexico, police department was bracing for a potential cyberattack by an Internet hacktivist group in response to the March 16 fatal police shooting of James M. Boyd; however, a brief interruption in website availability was all that was reported. In November 2014, Anonymous did shut down the Cleveland, Ohio, website in response to a police shooting of a juvenile armed with a replica handgun.

An additional threat is the disgruntled employee who has just been disciplined or terminated and decides to take revenge on the employer. In July 2008, *ABC News* reported on a disgruntled IT employee of the city of San Francisco, who took measures that gave him access to areas of the network that he was not authorized to access. The employee created a secret password that gave him exclusive access to most of the city's data, enabling him to prevent other authorized users from gaining access to the system.

Costs of a data breach can be devastating to an already tight local budget. The Ponemon Institute produces an annual survey on the cost of data breaches. The Institute found in its "2014 Cost of Data Breach: Global Analysis," that "the average cost paid for each lost or stolen record containing sensitive and confidential information increased more than 9 percent from $136 in 2013 to $145 in 2014."

Intrusion Costs

The true cost of cyber intrusion is difficult to estimate. There is no one repository for reported incidents of cyber intrusions. The Privacy Rights Clearinghouse (https://www.privacyrights.org) maintains a database that is updated frequently and houses reported incidents dating back to 2005. The Identity Theft Resource Center (http://www.idtheftcenter.org) began generating a yearly breach report for 2013 and continues into 2014. The Breach Level Index (http://breachlevelindex.com) is a third source that provides reports for tracking data breaches.

The National White Collar Crime Center (NW3C; www.nw3c.org) recently examined a total of some 5,000 reported data breach reports obtained from the above three sources. The incidents were categorized into several broad categories, including business, retail, education, governmental, and nonprofit organizations.

From that information, a total of 629 incidents of data breaches at the state, county, and municipal levels accounted for the exposure of more than 54.5 million records of individuals' PII since 2005. For the financial implications of this, recall the previously mentioned average of $145 cost per lost record noted above.

Compromised Personal Information

It is important to remember that confidential PII can be compromised in a number of ways that do not involve hacking. The analysis by NW3C, indicated in Figure 1, found that unintended *disclosure* was the most frequent cause of data breach encountered by governmental entities, accounting for 23.8 percent of the total.

A good example of such an incident was noted when one local government mistakenly used the wrong-sized window envelopes to send out income tax forms to its employees, unintentionally exposing Social Security numbers along with their names and addresses.

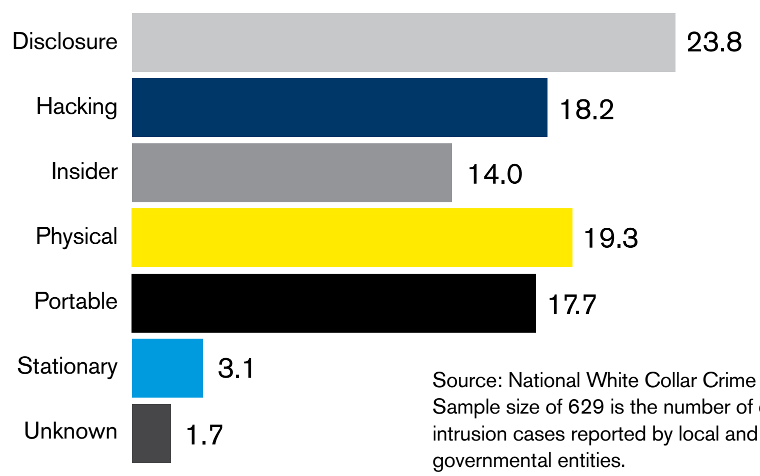
Physical loss or stolen non-electronic physical records represented the second highest category of data breach, accounting for 19.3 percent of the total. This category could include documents containing PII that were left in vehicles and in briefcases or other carrying devices that were reported as either lost or stolen.

Hacking came in third, accounting for 18.2 percent, indicating that as a security threat, it still ranks quite high as an issue that needs to be taken seriously.

Lost or stolen *portable* electronic devices, including laptops, CDs, and such portable electronic media stor-

HAVING AN EFFECTIVE RESPONSE PLAN IN PLACE COULD HELP MITIGATE CIVIL CLAIMS OF NEGLIGENCE AS WELL AS THE INEVITABLE POLITICAL FALLOUT FROM SUCH AN EVENT.

FIGURE 1. Percentage of Total Local Government Data Breaches since 2005.



Source: National White Collar Crime Center. Sample size of 629 is the number of cyber intrusion cases reported by local and state governmental entities.

WHILE A LOCAL DATABASE OF TAXPAYERS MAY NOT YIELD THE MILLIONS OF RECORDS THAT HACKING TARGET STORES, CHASE BANK, OR SOME OTHER NATIONAL CHAIN WILL, HITTING SEVERAL SUCH SMALLER AND SOFTER TARGETS CAN YIELD RESULTS THAT CAN STILL BRING SIGNIFICANT RETURN TO IDENTITY THIEVES.

age devices as external hard drives, USB flash drives, and secure digital (SD) memory cards accounted for 17.7 percent of the sample.

Malicious *insider* activity accounted for 14 percent of the total. When compared with the overall sample of almost 4,500 entities surveyed in which insiders accounted for 12.4 percent, it appears that the insider threat in governmental entities is only slightly higher than in the overall sample covering multiple types of businesses and the education sector.

The potential ramifications of a malicious insider activity where such confidential law-enforcement-only information as investigative case files, witness names, or other information is accessed could significantly magnify the overall impact of this type of data breach.

Of the remaining causes of data breaches, lost or stolen *stationary* devices and *unknown* taken together only accounted for less than 5 percent of the total. Lost or stolen stationary devices consisted of desktop computers, copiers, and fax machines that contained digital memories. It may be that rather than being lost or stolen, these devices are being improperly disposed of without having their memories properly cleared of confidential information.

The marginally good news appears to be that data breaches due to malicious outside intrusion into government IT systems, excluding federal, accounts for only 18.2 percent of the 629 number of incidents analyzed. The rest of the loss of confidential information causes could potentially be addressed by policy through:

- Rigorous employee education.
- More stringent rules regarding access and use of confidential records.
- A rigorously followed policy regarding proper disposal of used or leased equipment.
- A strong policy of investigation and corrective action to dissuade carelessness and unauthorized access of confidential governmental records.

The civil liability attached to a data breach is also a concern when discussing the potential cost of an incident. When the question is asked—"Can a governmental entity be sued for damage resulting from a data breach?"—the answer is: You can be sued for anything. The likelihood that the plaintiff will succeed may be a different matter.

To shed some light on this issue, NW3C's research attorney is assembling an in-depth analysis on this issue, and a white paper will become available this spring at the research section of www.nw3c.org. If local government managers need more information, the NW3C research attorney can provide complimentary consultation on the legal analysis.

Reducing the Impact

In short, the NW3C's conclusion was that in most cases, maintaining an accurate, reliable criminal information system stocked with legal and complete information carries no greater exposure to civil or criminal liability than other government-related activities.

Absent a handful of (presumably) uncommon fact patterns discussed in the above-referenced white paper, the only real danger to the governmental entity is negligence, which is hardly a new area of risk. For government administrators interested in minimizing costs or a data breach, however, reading the white paper is recommended.

The obvious question that remains is: How does an organization mitigate the threat and reduce any potential financial impact of a data breach?

A review of the available literature by NW3C on the issue of data breaches revealed that several sources agree on the course of action to take that should at least reduce the likelihood of a data breach and potentially reduce the cost of recovery, when and if one occurs. The list was further reviewed by NW3C's Computer Crimes Section so as to ensure the most complete list of procedures possible.

Here is a synopsis of those recommendations:

- **Strictly enforce password policies**. Maintain a policy that requires users to regularly select and change satisfactorily strong passwords. Also maintain clearly written, understandable policies regarding access and use of the IT system; educate users; monitor adherence to policies; and most of all, enforce violations of those policies. Policies are of little use if they are not enforced with appropriate corrective action when violations are identified.
- **Restrict remote access**. Closely monitor remote access by employees who may use portable computers during work-related travel. Also limit

and closely monitor any remote access into your system by outside vendors, contractors, and service providers.

Where it is necessary for a third-party vendor or service provider to have access to a government's IT system, be sure that the process is carefully vetted and appropriate safeguards are in place on the third party's IT system. Also engage in periodic monitoring.

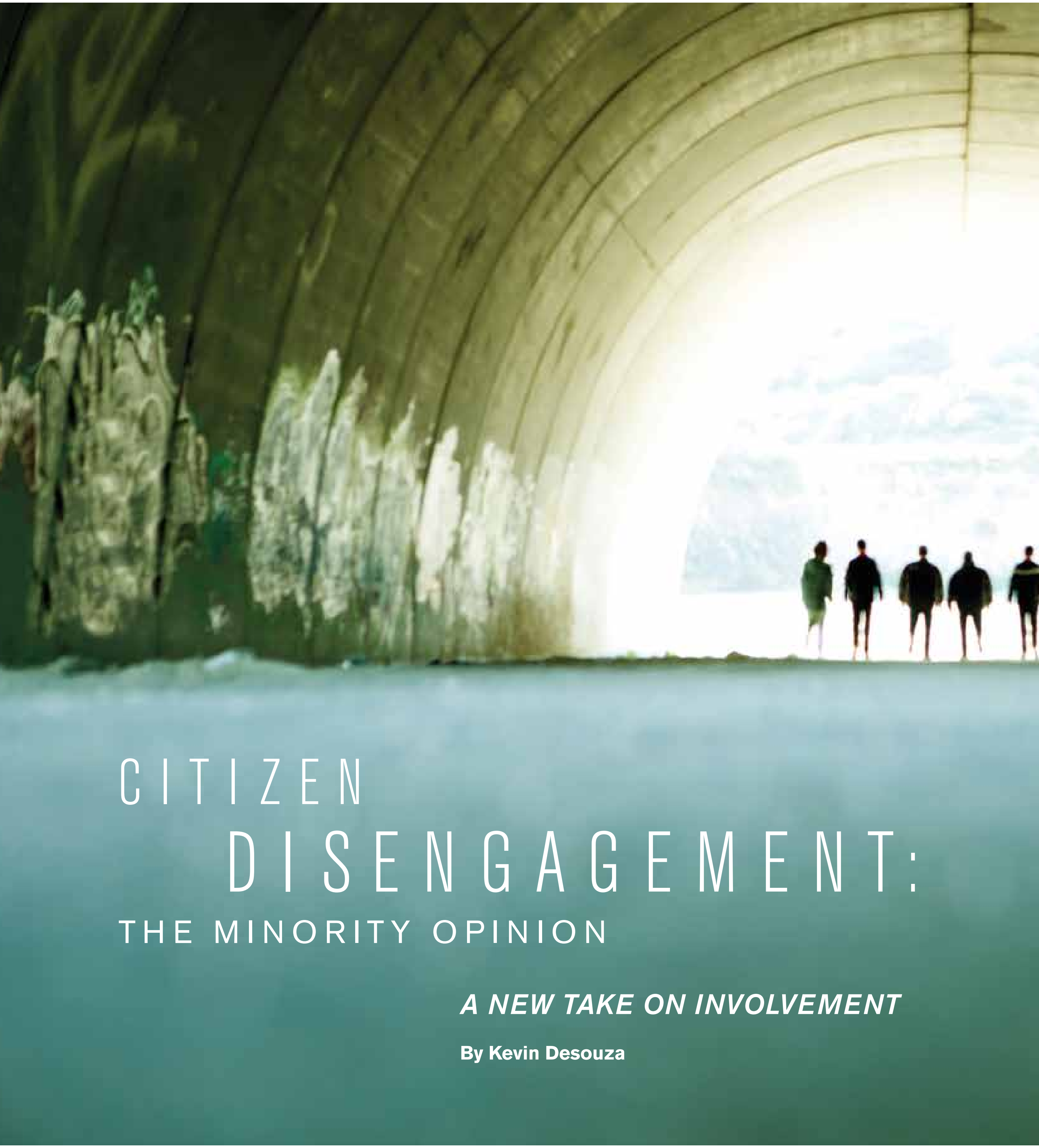
- **Deploy effective antivirus software**. Make sure IT professionals have knowledge of and adhere to current industry standards on antivirus software and anti-intrusion measures. Also be sure that IT professionals in charge of systems are regularly staying on top of the latest developments in malware and intrusion methodologies as they evolve.
- **Look for suspicious activity on the network**. Daily use of any system will typically yield some form of identifiable standard or pattern. Knowing what is normal will make it easier to identify and deal with any anomalies. Periodic audits of activity and looking for anomalies that stand out from otherwise normalized traffic patterns can help avoid a data breach before it happens.
- **Restrict IT system use to business only.** Prohibit surfing the Internet, social media, or anything that is not work related on worksite computers. Depending on the position of the employee, there may need to be limited exceptions, but to the greatest extent possible, restrictions should be established and enforced.
- **Have an effective incident response plan in place before the data breach.** The plan should require periodic assessment and modification as technology and system intrusion methodology evolves. Complete support of top management is necessary to maintain an effective defense against data breach so management needs to be continually briefed on the status of the plan, its required modifications, the results of periodic reviews, and newly emerging threats.
- **Conduct "fire drills."** Stage simulated data breach events to rehearse and evaluate response to a data breach incident.
- **Maintain a plan for effective customer notification and remedial action if a breach occurs**. When PII is compromised, it is essential to have a plan to notify those affected by the breach. If possible, provide identity theft prevention instruction and counseling and identity theft monitoring services by a recognized provider.

  Establish a hotline for dealing with reported identity theft incidents that may be the result of the breach. Having an effective response plan in place could help mitigate civil claims of negligence as well as the inevitable political fallout from such an event.
- **Investigate cyber intrusion insurance**. Insurance policies are available to cover data breaches; evaluate your needs to see which might make sense for your community.
- **Always report incidents**. Make sure that all data breaches are reported as required to the appropriate law enforcement authority. PM

ALSO IN THIS ISSUE

For information on guidelines to follow in the first 24 hours after a suspected data breach, see the Tech Touch article in this issue on page 28.

GERALD CLIFF, Ph.D., is research director, National White Collar Crime Center, Fairmont, West Virginia (gcliff@nw3c.org).



CITIZEN DISENGAGEMENT: THE MINORITY OPINION

A NEW TAKE ON INVOLVEMENT

By Kevin Desouza

TAKEAWAYS

› Be cautious about overdoing citizen engagement.

› Citizens are disengaging for a variety of intrinsic and extrinsic reasons.

› The level of citizen engagement is strongly associated with income, education, gender, and personality.

› Five suggestions for well-thought-out citizen engagement.

Citizen engagement is all the rage today. We have been told that governments at all levels must find effective avenues to engage with the public. The legitimacy and effectiveness of public agencies depends on how well residents are engaged in policy deliberation and design.

Given the advancements of information and communication technologies, today's online platforms are seen as the new vehicle to connect with residents. It would not be a stretch to claim that almost every major local government has an online citizen engagement platform. What is even more interesting is the rise of online platforms created by residents for peer-to-peer collaboration and co-creation of solutions to tackle local problems.

Entities as far reaching as the White House have extolled the necessity of citizen engagement for strong communities. Such efforts as the Open Government Partnership (http://www.opengovpartnership.org)—an international platform of 64 participating countries that use resident participation to improve government policies—and the Rebuild by Design contest are now used to develop the most innovative designs after Hurricane Katrina. Hosted by the U.S. Department of Housing and Urban Development (HUD), Rebuild by Design (http://www.rebuildbydesign.org) reflects a desire by the White House to include residents in decision-making processes. This heightened desire is driven by the notion that for national and community success, residents should be involved in solving societies' most pressing challenges.

This concept, however, is not new. The notion that civic participation is the cornerstone of democracy has held true for centuries. One can easily trace its origin to the United States' founding principles. It would be nearly impossible to keep a representative democracy afloat without adequate citizen engagement.

Recently, especially in the U.S. and for most of Europe, a resurgence of interest in citizen engagement can be attributed to the fact that many governments have extremely low approval ratings, are disconnected with issues that need to be contended with on main street, and have lost the trust of the public.[1,2] Through a focused effort to re-engage residents, governments hope to recapture some of the lost trust, engage them in the co-creation of solutions, and foster innovation.

Unfortunately, citizen engagement is not as easy as one might imagine. Despite significant investments on the part of governments, it seldom results in fruitful outcomes.[3] Participation is abysmally low and has been for some time. In 2014, the National Research Center conducted a survey on resident activity and found that only 19 percent of Americans contacted their local elected officials over a 12-month period, and about 25 percent attended a public meeting.[4]

As one city manager remarked to me, "I wish I had never engaged. Engaging made matters worse and only created a coalition that was not going to rest until the program was abandoned."

Such sentiments as this are not rare. It is difficult for me to find a manager who can point to specific outcomes that they have realized with investment in citizen engagement. Yet, most managers are told to invest more in it and increase the intensity at which they connect with residents.

Given that I am never one to shy away from controversy (or create one), I am going to argue that we need to tone down the hype around citizen engagement. Like most things, it can be good in moderation.

IN 2014, THE NATIONAL RESEARCH CENTER CONDUCTED A SURVEY ON RESIDENT ACTIVITY AND FOUND THAT ONLY 19 PERCENT OF AMERICANS CONTACTED THEIR LOCAL ELECTED OFFICIALS OVER A 12-MONTH PERIOD, AND ABOUT 25 PERCENT ATTENDED A PUBLIC MEETING.

Reasons for Disengagement

Several valid reasons exist for why residents disengage, or never engage, regardless of how much effort local government might make to get their attention.

First, people are busy. Back in 2007, the United Nations noted that a quarter of the world's population—more than 600 million people—work excessively long hours (48 hours a week or more).[5] In the United States, 85.8 percent of males and 66.5 percent of females work more than 40 hours a week.[6] In addition to work, they are managing children's social calendars, familial responsibilities, and personal upkeep. Residents with busy lives often do not view engagement with government as a high priority.

Second, people are preoccupied with things more important than your cause, problem, opportunity, or policy. Consider Maslow's Hierarchy of Needs of Human Motivation that outlines the layers of needs to be met for individuals before they can spend time doing more abstract/long-term rewarding activities.

Maslow asserts that we need such basic fulfillments as shelter, food, and interpersonal connection before we can engage in other activities like citizen engagement. This theory has direct implications concerning which residents are engaged and, consequently, whose voices are heard.

Engagement is largely predicated on the notion that community members' voices are being heard to create better outcomes. The main demographic characteristics that are strongly associated with engagement are income, education, gender, and personality. Largely, individuals who are highly educated and more affluent tend to participate more.[7]

There is, however, a large segment of the population who do not regularly participate: the poor and disenfranchised. The bottom 30 percent of American families, for example, earns less than $35,000 a year. These families receive few employer benefits and hold jobs with inconsistent or unpredictable schedules which doesn't allow for much consistent citizen engagement.[8]

Generational differences also play a significant role in engagement. Digital natives, for example, are individuals who have grown up with access to information and communication technologies all of their lives. These are people traditionally born in the early to mid-1990s on to the present. This generation has a different view of engagement. For digital natives, the motivation to participate originates from peer relationships and a quest for self-actualization.

This means that this generation is looking to engage to fulfill an intrinsic need; not to fulfill the traditional notion of citizen engagement as a civic duty. The National Research Center survey further suggests that younger residents are not inclined to speak up. In fact, individuals under the age of 35 who have attended public meetings and contact elected officials are far lower than those over 35.

Third, people suffer from attention deficit disorder. Okay, not literally, but there are multiple things clamoring for their attention when it comes to local engagement in the community, and the ever-expanding digital world also consumes an increasing amount of our attention.

Fourth, citizen engagement can be viewed as a chore and not worth the effort when present conditions are unclear or questionable. Local governments sometimes deal with a scandal or residents' view that governance is failing. News cycles and social media can perpetuate negative perceptions with ongoing news stories or the circulation of rumor and innuendo.

Finally, citizens have seldom seen results and outcomes from the handful of times they have engaged.[9] This seems rather bizarre since we live in a world of real-time or near real-time feedback.

This can happen because people seldom see the outcomes of their efforts due to the long time horizons and the democratic process playing out. The lack of visible outcomes does not validate citizens' efforts; instead, it demeans the time and effort they dedicated to the cause.

Additional Factors to Weigh

Communities are unique places that have their own culture and history, which have both played a role in their citizen engagement or disengagement. Either way, engagement or disengagement came about due to certain conditions, which should be evaluated when weighing future action.

Participation may not be representative of the larger population. Mark Funkhouser, former mayor of Kansas City, notes that at most public meetings, the usual suspects show up—the self-appointed activist, the lobbyist, and regular folks who have gotten angry enough or scared enough to join the dialogue.

Today, online platforms like websites, social media, and apps are often used for citizen engagement. These platforms offer local governments the ability to efficiently engage with citizens and allow for more accessibility. Online civic engagement platforms, however, are no panacea. A lot of hype surrounds the use of these networks; however, we must remember that not everyone uses these platforms,

The Pew Research Internet Project, for example, found that in the U.S., adults of higher incomes use Internet and smartphone technologies to near saturation levels.[10] Almost by default, these tools might target a particular segment of the population.

Also, through online platforms, especially with social networks that include Facebook and Twitter among others, information or sentiments can be easily manipulated to create the illusion of widespread support or disagreement. In 2012, someone tweeted that Syrian President Bashar al-Assad was dead and it was then rebroadcast by a journalist. Within an hour, the news of Assad's supposed death caused oil prices to climb a dollar.[11]

Another factor that comes into play is that citizens often have a limited view of a problem. They are often not in tune with the realities of the local government, including budgetary and technological constraints, political issues, and planning agendas. They also don't always consider the greater good, just their long-term needs. This makes their solutions to problems ineffectual.

Citizen engagement is also expensive and time consuming. Local governments are resource strapped and do not have unlimited resources to divert to this focus. As a result, any resources invested in engagement means that resources are being diverted from other critical issues.

For example, an app called Aloha was developed in Kenya for residents to submit local problems with which they needed help. After a year, there were 400 to 500 points of data on the app; however, only two have been responded to due to staffing issues.[12]

Responsible Engagement

Citizen engagement, like most things, is not free and incurs opportunity costs. Citizen engagement is currently, in my opinion, overdone and not carefully considered.

When citizen engagement isn't done well, community perception can suffer and invite negative scrutiny.

Consider a seemingly small and fun citizen engagement activity by the New York Police Department (NYPD). In 2014, the NYPD tweeted to the residents of New York to post pictures of themselves with NYPD officers using the hashtag #myNYPD. They overwhelming did just that and posted largely negative pictures and comments that focused on the NYPD's alleged penchant for misconduct and resident

FREE RESOURCES

THIS ARTICLE WAS PRODUCED by the enhanced research partnership of ICMA, Arizona State University, and the Alliance for Innovation. This partnership has worked to develop engagement resources and services that focus on the unique ways in which any given jurisdiction can use engagement to achieve its goals and avoid pitfalls that can derail effective engagement.

For more information, visit the ICMA Center for Management Strategies websites listed here, where you will find a variety of resources, free organizational assessment tools, and vetted leading practitioners who can assist in your efforts to do engagement "right."

– www.icma.org/strategies http://icma.org/en/results/management_strategies/leading_practices/civic_engagement
– http://icma.org/en/results/management_strategies/resources/documents_articles

THE STRONG TEMPTATION TO ENGAGE PEOPLE MORE BECAUSE IT'S POPULAR CAN BE DETRIMENTAL TO A LOCAL GOVERNMENT. WHILE I WOULD NEVER GO AS FAR AS TO SAY STOP SEEKING CITIZEN ENGAGEMENT, I WOULD IMPLORE THAT YOU FIND THE RIGHT BALANCE OF ENGAGEMENT.

brutality (see picture posted at: http://www.usatoday.com/story/news/nation-now/2014/04/23/nypd-twitter-mynypd-new-york/8042209).

Given that citizen participation is a cornerstone of a democratic society, here are five suggestions to ensure your local government's effort to engage residents are well-thought out and encourage meaningful collaboration.

Don't cry wolf. Do not conduct citizen engagement casually. Don't ask for feedback you don't need or won't use. If you keep screaming for engagement, eventually it will be part of the noise and get lost and lose its credibility. Choose carefully when and where you want to engage and toward what end.

Be thoughtful. Approach engagement like you would anything else: thoughtfully and carefully. There is a level of unpredictability that is innate in citizen engagement so local governments must consider all possibilities. Research by Professor and author John Alford (see http://mbs.edu/facultyresearch/faculty-directory/Pages/JohnAlford.aspx) as one example, argues that residents should be engaged in simple tasks as it will heighten the level of assistance citizens can offer.[13] Information like this should be used in your engagement strategy to create the best possible outcomes.

Provide residents with clear incentives to engage. The success of crowdfunding platforms has taught us that individuals will engage and collaborate toward solving challenges and innovation if there is incentive alignment. Incentives to contribute should be tailored to attract the most effective collaborators and achieve alignment of motive among collaborators.

Get creative about ways to incentivize like the New York City Big Apps Challenge. To encourage development of tech business, this challenge opted to let participants retain the intellectual property rights of the apps they created.

Provide feedback to participants. One of the most common complaints that people have from spending time engaging is that their feedback goes into a black hole, never to be heard of again. Engaged participation needs to be validated, not placated. If you ask citizens for feedback on something, honor that feedback by showing that it was considered and if it couldn't be used, why.

It is important to dialogue with the community instead of only gathering information. This allows participants to have a realistic view of what can and cannot happen in their community. A simple and polite, "Here is our budget. How do you suggest we fund that?" can go a long way.

Set realistic expectations. Think of what would be considered a good citizen engagement program. Take lessons from the past and lessons from others to conceptualize what engagement should look like for your community. This includes setting expectations and measures and getting feedback, and taking this gathered intelligence into account as you consider future engagement. Citizen engagement shouldn't be approached haphazardly just because it seems like the right thing to do.

Today, local governments are asking residents to engage in everything from participatory budgeting to voting for the best colors for city benches. The strong temptation to engage them more because it's popular can be detrimental to a local government. While I would never go as far as to say stop seeking resident engagement, I would implore that you find the right balance of engagement. PM

ENDNOTES AND RESOURCES

1 http://www.usatoday.com/story/news/world/2014/01/20/distrust-in-government-growing/4655111.

2 http://www.people-press.org/2013/10/18/trust-in-government-nears-record-low-but-most-federal-agencies-are-viewed-favorably.

3 http://www.governing.com/topics/politics/gov-national-survey-shows-citizens-most-vocal-active-in-local-government.html.

4 http://www.un.org/apps/news/story.asp?NewsID=22819&Cr=labour&Cr1=#.U-EyYfldXvZ.

5 http://visualeconomics.creditloan.com/the-state-of-the-40-hour-workweek.

6 http://spectrum.ieee.org/telecom/internet/computer-scientist-warns-of-social-media-manipulation-in-us-election.

7 Homero Gil de Zúñiga and Sebastián Valenzuela. The Mediating Path to a Stronger Citizenship: Online and Offline Networks, Weak Ties, and Civic Engagement. Communication Research. 2011;38:397–421.

8 http://cdn.americanprogress.org/wp-content/uploads/issues/2010/01/pdf/threefaces_exec_sum.pdf.

9 http://www.soulofthecommunity.org.

10 http://www.pewinternet.org/2014/02/27/the-web-at-25-in-the-u-s.

11 http://spectrum.ieee.org/telecom/internet/computer-scientist-warns-of-social-media-manipulation-in-us-election.

12 http://www.wired.co.uk/news/archive/2012-11/13/technology-helps-citizen-engagement.

13 Alford, John. 2009. "Engaging public sector clients: From service delivery to co-production." London: Palgrave Macmillan.

KEVIN DESOUZA is associate dean for research, College of Public Programs; professor, School of Public Affairs; and interim director, Decision Theater, Office of Knowledge Enterprise Development, Arizona State University, Phoenix, Arizona (kev.desouza@gmail.com; web at http://www.kevindesouza.net).

GETTING DISASTER RECOVERY COSTS MOVING

How to navigate FEMA procedures to collect recovery costs

By Hilary Cairnie, Maria Coor, and Bill DeVinney

Communities hit by such natural disasters as hurricanes, earthquakes, fires, floods, tornadoes, and landslides are often faced with large-scale and costly recovery efforts. The Federal Emergency Management Agency (FEMA) is the federal agency whose primary mission is to provide monetary assistance to those communities devastated by disasters, but communities' cleanup efforts might need to be performed before FEMA's financial assistance can begin.

Recovery efforts invariably begin immediately and end with debris removal operations that involve, among other things, removing downed and damaged trees and hauling those materials away. Even a small event is capable of generating tens of thousands of cubic yards of debris and large-scale events can result in millions of cubic yards of debris. Within the first 100 days following Hurricane Sandy, for example, more than 8 million cubic yards of debris were removed from the streets and public areas of affected communities.

Debris removal and the associated costs incurred in performing debris removal may be eligible for federal assistance under the Robert T. Stafford Disaster Relief and Emergency Assistance Act ("Stafford Act"), 42 U.S.C. §§ 5121--5208, under which FEMA is authorized to provide public assistance grants to communities recovering from a natural disaster.

TAKEAWAYS

› FEMA's rules setting out the requirements for public assistance eligibility, particularly with debris removal, can be vague or confusing and difficult to navigate for public officials not familiar with these rules.

› FEMA wields great discretion in interpreting and applying rules that can result in inconsistent application and leave a community unexpectedly burdened with crippling costs.

› A manager can take precautionary measures to protect a community from arbitrary treatment from FEMA.

Debris Removal Funding

The Stafford Act provides relatively vague guidance regarding eligibility of debris removal operations and gives the U.S. President broad discretion to grant funding under the act. The President, in turn, has delegated his authority to FEMA.

FEMA determines whether a community is entitled to receive post-event assistance and if so, the amount. FEMA has implemented rules and developed grant-making criteria to govern the process to be followed when a community seeks assistance.

Broadly speaking, in order to be eligible for assistance, the debris—be it a leaning tree, a fallen or dangling branch, or vegetation clogging a waterway—must be the direct result of an event that is a presidentially declared disaster. If the debris was there before the event occurred, then its removal would not be eligible for public assistance.

The debris also must in some way encumber a public right of way or public property (parks, recreation areas, roads, sidewalks, etc.) in such a way that it threatens public health and safety, or improved property, like roads, pathways, and power lines.

The applicant for public assistance for emergency debris removal, which usually is a state or local government, must present evidence demonstrating the eligibility for identifying, removing, and disposing of that debris. The applicant must also demonstrate that the costs incurred to identify and remove eligible debris were reasonable.

An applicant's public assistance request can be denied as the grants to remove disaster debris are by definition discretionary, and FEMA's decisions under the Stafford Act are not subject to judicial review. A community cannot challenge FEMA's decision in court; the court, be it federal or state, has no jurisdiction to consider such a matter.

Administrative Review Process

In lieu of judicial review, FEMA has implemented an administrative process for reviewing the decisions of its officials and representatives. The administrative review process consists of two levels of appellate review within FEMA.

The first appeal may be lodged with FEMA's regional office ("first-level appeal"), that being the FEMA region tasked initially with deciding the application for relief. Sometimes these appeals are denied in whole or in part, and sometimes the appeals are settled by FEMA and the applicant. If an appeal is settled or decided favorably for the applicant, there would be no need to file a subsequent appeal.

If the first-level appeal is denied in whole or in part, the applicant may file a second appeal with FEMA headquarters (the "second-level appeal"). Sometimes these second-level appeals are denied in whole or in part, and sometimes they are settled by the parties. The process for both appeals is similar, but the deciding officials are not the same. FEMA maintains a public database of appellate decisions.[1]

In the aftermath of Hurricane Katrina and through Section 601 of the 2009 stimulus act, Congress allowed aggrieved communities to seek independent review of FEMA decisions through a special arbitration process.

For disputes arising out of certain disasters occurring before 2012, arbitrations against FEMA could be filed before a panel of three judges sitting on the Civilian Board of Contract Appeals (CBCA). The CBCA arbitration panel reviewed the application for public assistance de novo. In other words, the panel reviewed the same evidence presented to FEMA and decided anew, as though for the first time, whether the applicant qualified for assistance.

> The last thing that community leaders struggling with a natural disaster should have to contend with is an unwarranted denial by FEMA of public assistance.

A Shift in Procedure

For disasters declared on or after October 30, 2012, the arbitration procedure has shifted from CBCA to the U.S. Coast Guard's Office of Administrative Law Judges. The shift to a new forum also entails the application of a narrower standard of review, under which FEMA's decision will stand so long as it has a reasonable and rational basis and is not found to be arbitrary or capricious.

Preparedness Is Key

In order to better prepare for the possible paperwork associated with public assistance proceedings, community leaders should develop emergency preparedness plans because these plans identify the necessary first steps in responding to a natural disaster, identify the individuals responsible for accomplishing those tasks, and identify the community's available resources for those critical tasks, including capability and capacity of nearby hospitals or medical centers, vehicles and heavy equipment available for emergency evacuation, and personnel and contractors available for emergency repairs.

Thus, when disaster strikes community officials already know what tasks must be done, who will perform those tasks, and which resources are available to complete them.[2] With that information readily available, community leaders will later be better prepared to justify the resources expended when requesting public assistance from FEMA.

Communities will pull together in time of disaster to help one another and to achieve the greater good for the benefit of all. That same esprit de corps can be mustered long before a disaster is forecasted.

Local community leaders from area businesses, churches, government, schools, and volunteer organizations can organize to provide human capital to form and implement preparedness plans—plans that, however informal, could make the difference between a favorable and unfavorable FEMA determination. Millions of dollars are at stake for any given disaster.

Whether or not a disaster preparation plan has been developed, once a disaster hits, communities can act with C.A.R.E.:

Communicate with FEMA. During the recovery process, applicants and their contractors should work as closely as possible with FEMA personnel to try to avoid instances in which the applicant's interpretation of FEMA eligibility criteria differs from FEMA's eligibility determinations.

Always document communications with FEMA. Applicants and their contractors can and should maintain contact with FEMA representatives through electronic correspondence or some other written communication. Follow-up after meetings or teleconferences with FEMA personnel should be done through e-mail to enhance clarity and mutual understanding of recovery work and the public assistance process.

Recognize your rights. If FEMA denies part or all of an applicant's request for public assistance funding, the applicant has the right to appeal that denial and may have the right to seek arbitration.

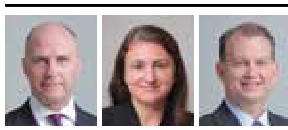
Evaluate FEMA precedent. Applicants should use FEMA's second-level appeal decisions to develop the strongest case for recovery should FEMA decide along the way that the applicant is not entitled to complete relief. According to FEMA's Public Assistance Appeals Database, 152 appeals decisions fall under the category of "debris removal."[3] Understanding the nuances of these cases might help applicants as they proceed through possible appeals and arbitration in the future. PM

ENDNOTES

1 The database of FEMA appellate decisions can be found at https://www.fema.gov/appeals.

2 A template for a community disaster plan can be found at http://www.state.in.us/isdh/files/PREPARE_Disaster_Plan_Template_IN_8_08.pdf.

3 See https://www.fema.gov/appeals.



HILARY CAIRNIE and **MARIA COOR** are partners, and **BILL DEVINNEY** is counsel, BakerHostetler, LLP, Washington, D.C. (hcairnie@bakerlaw.com, mcoor@bakerlaw.com, wdevinney@bakerlaw.com).

BY MIKE CONDUFF, ICMA-CM

BEFORE IN TRANSITION

Stay calm, communicate, and reach out

The local government management profession is grounded on the concept that managers serve at the pleasure of the governing body and that they, to the best of their ability, reflect the elected officials' desired outcomes for the communities in their managerial and organizational direction.

We hold it to be truth that if the governing body changes, and it, in turn, wants a managerial change and is willing to abide by the terms of an agreement regarding separation and severance, then we hold up our heads, load up our families, and go on to the next challenge.

We even have an idiom associated with this occurrence: "In transition."

On paper, this principle and this phrase sound noble, even laudable. In life though, it hurts. Anger, fear, and frustration are felt. Hard conversations with family and friends are held.

Self-doubt creeps in. What should I have done differently? Why did I not see this coming? How could I have prevented this?

A manager might commit a decade or more of his or her life to a community. Sacrifices of family and personal time—and sometimes even health and relationships—are dutifully given and through careful stewardship, progress is made.

In time the electorate gets perhaps a bit complacent and before long, the council changes. For no other reason than, "You have been here too long" or "Nothing personal, we just want our own person," the manager is looking at uprooting kids from school and a partner from a job or a career. This might also include putting a cherished home on the market—perhaps at a financial loss—and moving on.

Giving Each Other a Chance

In my current governance-related role, I often see the precursor to the in-transition phase. Either the elected officials or the manager senses that relationships are amiss and a job is at risk, and I am asked to provide education on good governance in the hope that by understanding roles, the relationships can be mended.

When I discover this is the case, I try to shift the emphasis of the training from roles to communication or from good governance to just giving each other a chance. The fact is that too many times I see good elected officials and good managers get crossways over matters that should never rise to the level of moving on.

In this age of total online capture, almost anything that gets said, texted, or tweeted is preserved and scrutinized and used as fodder for one position or another. He said/she said is now online for all, and often it hurts on many levels.

I do dearly believe that a good governance system provides the framework for elected and appointed officials to work together for the betterment of a community. Just as any team needs a roster, a position process, and a playbook, so too does local leadership need to understand who does what, when, and why.

Not many of us received group process training in graduate school, and in many cases, just understanding group dynamics and getting groups to agree on how they can correct member misbehavior can be incredibly healing.

Reach Out

It takes courage and valor for a manager—or an elected official for that matter—to risk an intervention, but the reward in terms of role satisfaction can be huge. If it appears that the conclusion is foregone, then the effort, even if not successful, can be viewed as skill building for the next time.

If you find yourself worried about the latest election or turnover of elected officials, I encourage you to reach out immediately and repeatedly to the new members. Yes, they may have preconceived notions about you, and they may have said hurtful things, but closing them off or avoiding them only validates their misunderstandings.

Demonstrate up close and one-on-one that you are a person of integrity with the same love of the community they hold. If they rebuff you—and they likely will at least once—find another approach, including a friend in common or a person of stature in the community to host a meeting. If it takes hiring a professional trainer, that is a small investment compared to the cost of a managerial change.

I also encourage managers to reach out to their professional network. It is okay, even a manifest sign of maturity, to share with a trusted colleague that you are nervous or fearful about the relationship with the governing body. We have all felt that way, and in my experience many of us are feeling that way now.

Simply having a safe environment to share the emotion can lessen it dramatically. Your colleagues can help you see the image in the mirror more clearly than you can on your own.

At the end of the day, if indeed you are involuntarily moving on, at least you have the satisfaction of knowing that you did all you could reasonably do, and you will have gained valuable skills in the process. PM

MIKE CONDUFF, ICMA-CM
Former City Manager
President and CEO
The Elim Group
Denton, Texas
mike.conduff@theelimgroup.com

BY JEFF DAVIDSON

HOW YOU SLEEP IS HOW YOU WORK

Don't shortchange yourself

Years back, the director of Stanford University's sleep center concluded most adults "no longer know what it feels like to be fully alert." The National Sleep Foundation found that almost 68 percent of adults are getting too little sleep, and 58 percent suffer from some type of insomnia at least once a week.[1] These people are not simply a little groggy or sluggish, but completely and undeniably walking around as if in a stupor.

As a highly productive professional, you've probably already discovered that when you shortchange your sleep too often, your mind and body simply don't respond anywhere near optimal capability. What you do the night before significantly affects your ability to get things done.

Most experts agree that losing three to four hours of sleep once a week won't cause any long-term problems. You might feel terrible the next day, but you can recover somewhat by going to bed earlier the next evening or napping if that is an option for you. You might have to force yourself to get into bed at 9 p.m. on evenings when you'd rather be up and about, but do it. Your body will thank you.

If you're missing out on more than 10 hours a week, decide to catch up on your sleep now before you further diminish your capabilities. Recovery might take a month or more, but it will be worth it.

The Body's Clock

Heart beats, breathing, speaking, and even hiccupping have their own rhythm. If you sleep too little or for that matter too much, you disrupt your internal cycles that required millions of years to evolve.

Each of your body's functions is reset every 24 hours, which parallels the natural daily light cycle. The essence of your being is subject to this circadian rhythm, which is the daily cycle of activity in living organisms. Altering that rhythm for a prolonged period will prove to be contrary to your own physiology.

Martin Moore-Ede, a former professor at Harvard Medical School and founder of CIRCADIAN,® a research and consulting firm dedicated to improving productivity, health, and safety in round-the-clock operations, observed that certain times of the day are important to sleep through, including between 2 a.m. and 5 a.m., when human physiology is at its lowest level of alertness. Highest alertness, by the way, is between 9 a.m. and noon, and also 4 p.m. to 8 p.m.

If you happen to be short on sleep some particular day, such light exercise as stretching or a brief walk is a good idea. Your energy level may perk up for an hour or two. If you have the opportunity to nap, that would help as well.

All About Napping

Napping increases your alertness for the rest of the day. Some people nap easily; others can't seem to nap at all. You already know into which camp you fall. The best nap time is between 2 p.m. and 3 p.m. Any later and your nap may be too deep, interfering with your nightly sleep.

While naps can be helpful, they are not a good substitute for regularly getting the right amount of sleep. It's best not to use naps to catch up on sleep if you shortchange yourself nightly.

Your quality of sleep will be much higher and the immediate benefits more apparent if you nap in a bed or cot as opposed to a chair. Although everyone feels a little groggy for a few minutes after a nap, this gradually subsides.

Short naps are more productive than long naps. A short nap will leave you refreshed; a long nap could interfere with your sleep that evening. Naps of 20 minutes or less usually help avoid REM sleep, a deep-sleep stage from which you're likely to wake up groggy and stay that way.

To derive the most from your nap time, safeguard the nap area before you nod off by making sure that phones or other gadgets will not disturb you. Post a "Do Not Disturb" sign if that will help.

You might need to readjust your sleeping habits or your pre-bedtime rituals, but getting enough sleep is vital to having enough energy to successfully get through your workday. Most definitely, how you sleep is how you work. PM

ENDNOTE

1 http://sleepfoundation.org/sleep-disorders-problems/insomnia.

JEFF DAVIDSON, MBA, CMC, is principal, Breathing Space® Institute, Raleigh, North Carolina (www.BreathingSpace.com or Jeff@Breathingspace.com). An author and presenter on work-life balance, he holds the world's only registered trademark from the United States Patent and Trademark Office as a "Work-Life Balance Expert."®

BY MARK RYCKMAN, ICMA-CM

GEARING UP FOR FIRSTNET

A nationwide broadband network to ensure public safety

It's been more than 10 years since the 9/11 Commission issued its report that detailed events leading up to the terrorist attacks on September 11, 2001. The report identified several failings of the U.S. intelligence community and deficiencies in first-responder systems.

One of the commission's findings was the lack of interoperable communications capabilities for first responders to share mission-critical information during their response efforts. The commission concluded that "Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public-safety purposes. . . ."

Fulfilment of that recommendation from the 9/11 Commission is now becoming a reality. Media coverage of the Middle Class Tax Relief and Job Creation Act of 2012 focused largely on the extension of unemployment benefits and the temporary Social Security tax reduction.

A little publicized provision of the act, however, was the creation of the First Responder Network Authority (FirstNet). Congress established FirstNet as an independent authority within the National Telecommunications and Information Administration (NTIA).

Building a Nationwide Network for Public Safety

FirstNet is charged with ensuring the development, operation, and maintenance of a nationwide interoperable broadband network for public safety. Prime spectrum for the network's deployment has been allocated, as well as $7 billion in funding.

Congress created a board of directors with representatives of the President's Cabinet, along with telecommunications industry professionals, and public-safety representatives. Congress also mandated the establishment of a Public Safety Advisory Committee (PSAC) to ensure that the development and operation of the network meets the needs of first responders. Thirty-five national professional associations, including ICMA, have appointed representatives to serve on the PSAC.

Improving Situational Awareness

Why do we need a nationwide broadband network for public safety? Public-safety personnel are continually seeking ways to improve situational awareness to more quickly and effectively respond to incidents. In order to raise situational awareness, first responders have an increased need to share such wireless broadband data as surveillance video of large-scale events, floor plans for fighting structure fires, or patient vital signs to emergency rooms from ambulances that are en route.

These applications need a stable platform with the capacity to handle large data transmissions. Current commercial networks often cannot support public-safety needs during major emergencies, as was experienced in the aftermath of Hurricane Katrina.

Public safety also currently cannot prevent non-priority users from accessing such networks when first responders need priority access to increased data transmissions during an incident. FirstNet is being designed to address these needs while keeping monthly subscription fees competitive with what users currently pay.

The Role of Managers

City and county managers are in an important position to help FirstNet build a nationwide network dedicated to public safety. Managers are community leaders, recommending strategic public-safety initiatives, helping set funding priorities, and appointing senior public-safety officials.

As FirstNet becomes a reality, managers need to provide input into the design and operation of the network to ensure it meets local jurisdictions' needs at an affordable cost. Managers also need to ensure their jurisdictions are positioned to take advantage of FirstNet's full capabilities once the network is deployed.

So how should local government managers prepare for the deployment of this new network? First, they should gain an understanding of FirstNet's capabilities and how it will assist public-safety agencies to provide more cost-effective services.

Information is available on FirstNet's website at http://www.firstnet.gov, in such trade publications as *Urgent Communications* and *MissionCritical Communications*, and through state and local outreach events that will be coming to your areas. Managers should share this information and developments with elected officials, public-safety staff, and neighboring jurisdictions.

Second, get to know your state's single point of contact (SPOC) and FirstNet's staff. NTIA has awarded state and local implementation grant program (SLIGP) funds to 54 states and territories. These funds are being used for outreach to the public-safety community to assist in planning the network's development.

As part of these grants, each state has assigned a single point of contact to lead these efforts. You can identify your state's SPOC and contact information on FirstNet's website. FirstNet is also hiring regional outreach personnel well versed in public-safety communications issues. Your SPOC and FirstNet's staff will be able to keep your community apprised of the planning, development, and deployment processes within your state.

Third, begin identifying information sharing needs within your organization for broadband applications that can improve your public-safety services. These could include the need to view police dash cams at your dispatch center, accessing water system storage data during firefighting operations, or viewing the status of arriving public safety units in real time. This process will need to engage members of your management team, public-safety personnel, and information technology departments.

Upgrading communications systems to digital technology, improving interoperability, and expanding coverage take time. Improving basic communication systems now will help you more readily transition to FirstNet's services in the future.

Finally, give FirstNet feedback concerning the types of issues that are important to public safety in your area. These could be local control issues that need to be considered in the network design, barriers to interoperability, affordability of participating in the network, and more.

You can provide feedback through the Public Safety Advisory Committee, your state's SPOC, FirstNet's staff, and any future request for information (RFI) and public notice processes issued by FirstNet. This network needs your input and support to ensure it meets the needs of public safety and gains the acceptance of local elected officials and managers who will authorize the necessary funding for monthly subscription costs and equipment upgrades.

This is an exciting time in public safety. Managers need to be on the leading edge of this effort. The development of a nationwide public safety broadband network has the ability to revolutionize the delivery of public-safety services.

Our public-safety personnel need these advanced technologies to continue to provide the high-level service to which the public has grown accustomed as we manage our communities with ever-tightening budgets. PM

THE DEVELOPMENT OF A NATIONWIDE PUBLIC SAFETY BROADBAND NETWORK HAS THE ABILITY TO REVOLUTIONIZE THE DELIVERY OF PUBLIC-SAFETY SERVICES..

MARK RYCKMAN, ICMA-CM, is city manager and director of public safety, Corning, New York (mryckman@stny.rr.com). He serves as ICMA's representative to FirstNet's Public Safety Advisory Committee.

The Peleș Castle is located in Sinaia, Transylvania, Romania.

PHOTO BY WARREN MASTER

BY DAVID BIGGS, ICMA-CM

REINVIGORATED IN ROMANIA

International exchange recharges professional batteries

Romania may seem like a strange stop while on a journey through a job-transition period, but I spent 10 days there in June 2014 before starting my new position as manager of Hercules, California. I was committed to finding professionally engaging activities while in transition, so I looked at volunteer and pro-bono opportunities, including those in other countries.

Luckily, I was engaged in some fulfilling interim assignments. In early June, when I knew that my Hercules position had been secured, I came across the opportunity to participate in an American Society for Public Administration (ASPA) delegation to Romania. Always interested in experiences that will broaden my professional perspectives, I opted to use part of the two weeks I had between jobs to participate in the 10-day trip.

Exploring the Challenges

The purpose of the trip was to share leading public administration practices and to participate in a four-day conference in Romania, while also embarking on site visits. The visit coincided with the 25th anniversary of the fall of communism in that country.

The international exchange explored challenges with Romanian local government counterparts regarding the continuing decentralization of services across a still-emerging democracy with a strong tradition of central control. The itinerary included meetings with public officials in Bucharest and in a variety of counties and cities in the central and eastern regions of Romania.

One of the first meetings was with a Senate committee composed of five national senators who were charged with shepherding a controversial regionalization and decentralization plan through the legislature. This exchange proved to be extremely insightful as the process was a key concern to local government officials we interacted with during the balance of the trip.

A four-day forum titled Collaborative Public Management: Pathway to Good Governance at the Local Level was the centerpiece of the international public management exchange. This forum was attended by some 100 participants from local governments in Romania. Sessions included presentations by Romanians and included several topics that are also familiar to U.S. managers:

- Community and citizen engagement: managing change, community development, and volunteer involvement.
- Collaborative governance across local jurisdictions and sectors.
- Stronger and safer communities.
- Performance management.
- Curbing corruption: making ethics and justice a priority.
- Energy options for today and tomorrow.
- Global view of centralized and decentralized approaches.

Interesting Insights

The balance of the itinerary was dedicated to visits to local government offices and facilities, as well as historic sites, including touring the environmentally

LEFT: A "Good Governance Forum," was held in Brasov, Transylvania, Romania.

BELOW: A meeting was held with Romanian senators at the Parliament Building in Bucharest, Romania.

PHOTOS BY WARREN MASTER

significant Danube Delta area in order to gain a better appreciation for Romania.

It was interesting to learn that the Romanian participants viewed the United States as having a much more developed local government experience. I found that we face many of the same issues, including engaging residents successfully, especially in such areas as developing the annual budget; delivering services and meeting service demands with diminishing resources; and managing the changing relationship between the central governments (similar to state and federal governments).

One of the most interesting insights was that Romanian local governments generally only undertake what the central government specifically authorizes—unlike local governments in the United States that have a strong tradition of home rule and operate on a more independent basis.

In the July 2014 issue of *Western City*, the monthly magazine of the League of California Cities, League Executive Director Chris McKenzie summarized this home-rule tradition best from the California perspective: ". . .in the absence of a conflict with a general state law, a city council has the same power to enact a city ordinance without state legislative authorization as it does with it. Why would cities fail to use such a fundamental attribute of home rule?"

Perhaps this approach would be key to a successful transition to a more decentralized relationship between the central government and local governments in Romania.

Personal and Professional Benefits

The effort to involve ICMA members in this delegation was designed to ensure local government practitioners were included and could share hands-on experiences. Former ICMA President and retied City Manager Ed Daley, who is still active in local government in Virginia, and I were the two city managers as part of a delegation that included academic and other public-sector representatives.

I can attest to the great personal and professional benefit from participating and being able to share real-life experiences with others and would encourage my colleagues to seek out these opportunities as part of supporting the "I" in ICMA.

I also can highly recommend this type of opportunity to recharge and sharpen skills in preparation for a new position, especially as someone who had been in transition for a substantial period of time. Being a local government manager is a rewarding yet challenging career, and taking time out to connect with colleagues and be of service to others, especially in an international context, is a reinvigorating experience.

Romania is a beautiful country with engaging and talented local government professionals striving to better their communities, and my stop there proved to be time well spent. PM

DAVID BIGGS, ICMA-CM, is city manager, Hercules, California (dbiggs@ci.hercules.ca.us).

BY MARK SHELHART

THE FIRST 24 HOURS

Step-by-step guidance after a suspected data breach

When a high school principal couldn't turn on her computer one morning, she assumed it was a minor technical problem with her machine. She quickly changed her mind, though, when within minutes she received phone calls from staff and students throughout the school about the lack of Internet access and computers that failed to start.

News quickly broke that every school in the district had lost access to the Internet. It was all due to one person. A recently fired IT employee illegally accessed the district's computers using a school administrator's username and password, and then destroyed a significant amount of data, including lesson plans, final papers, and athletic records in an effort to take revenge.

A single individual who has the power to create a massive security breach can affect an incalculable number of people. When the unexpected happens, local governments and any organizations associated with them need to act quickly. The first 24 hours are critical to successfully navigating a suspected security breach.

Here are critical steps local officials should take in this situation:

Look at your watch. The first two hours after learning of a breach are the most important since you must assemble a team and gather as much information as possible about the damage, along with the potential cause of the breach.

Find one clock (you don't want variation in timing) and write down the details of the suspected breach: exactly what time you noticed the breach, who you spoke with after discovering a problem, and any details that can be assembled. This information will come in handy later when you develop the in-depth liability report and relay information to a variety of stakeholders.

Identify your goals. A security breach elicits a strong emotional response, but you need to take a step back and determine your primary objective. Do you want to stop the attack, try to catch the culprit, or prevent future attacks? Aligning your team around the same goal or goals will lead to a greater chance of success and stop emotions from getting in the way of a solution.

Leave the power on. It's tempting to immediately pull the plug on affected machines in an attempt to prevent further damage. The majority of today's attackers, however, leave a trail in the computer's memory as well as on the hard disk. Shutting down a computer and rebooting deletes valuable code saved on the machine and may destroy any evidence of tampering.

Instead, quarantine affected machines by unplugging the network connection and not the power cord. This will preserve valuable information and save other machines from potential threats.

Look before you leap. There's a fine line between transparency and discretion when dealing with a breach. What initially seems like a dire situation may turn out to be reparable after a few hours of investigation. In order to avoid causing panic, you need to properly evaluate the suspected breach before making a public announcement.

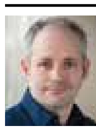
Typically, breach-related announcements occur three to five days after the incident. You don't want to overshare or interfere with the current investigation, but it's important not to hide anything. Stakeholders deserve a high-level snapshot of both the breach and your plan of action.

There are important things to do before going public. Make sure to gather your forensic evidence and address any obvious public-facing vulnerabilities.

YOU DON'T WANT TO OVERSHARE OR INTERFERE WITH THE CURRENT INVESTIGATION, BUT IT'S IMPORTANT NOT TO HIDE ANYTHING.

When you make a public announcement, it will grab the attention of not only investigative reporters, but also the hacking community. You want to make sure your organization is as prepared as possible for the additional scrutiny.

The key to successfully handling a breach is to react quickly and in an organized manner. By following the steps outlined above and making a governmentwide commitment to providing IT security education for all staff members, governments can recover from a breach and move forward with their primary goal of serving their residents for years to come. PM



MARK SHELHART
Senior Manager of Forensics and Incident Response
Sikich LLP
Milwaukee, Wisconsin
mshelhart@sikich.com

BY JERRY NEWFARMER

10 TIPS: LEADING CHANGE

Key steps for positive progress

We know that change in an organization is certain to occur. Leaders and staff members change, issues change, and tools and techniques for providing services change.

But change just for the sake of change is stupid. I once watched a leader taking over as the new city manager from outside the organization with a charge from the council to "shake things up." The councilmembers wanted their government to change. The manager began by announcing to his department heads and all who would listen that he was a "change agent."

To everyone inside the organization this meant he was setting out to change them, which was the effect of his message. It may have made him—and the council, initially—feel good, but you can imagine how it made city staffers feel about themselves.

Here are 10 basics to effectively lead useful change:

1 The starting point is respect. The good leader instinctively knows that his or her starting point, when taking the reins, has to be respect for the people, the organization, and the way work is done. The human beings who manage and operate local governments are there because they were selected and well trained to serve the public, and none of them sets out to perform badly. Everyone wants to be part of a successful, respected enterprise.

2 Good change is continuous. Enterprises that are able to be successful in sustaining quality performance over long periods of time are organizations that recognize and embrace continuous improvement, not one-off steps.

3 The carrot is better than the stick. Set a positive "can do" tone stressing continuous improvement as the change wanted throughout the fabric of the organization.

4 Demonstrate personal leadership. Celebrate successes to establish the expectation that continuous improvement is the goal.

5 Energize your staff training program or create an organizational development program.

6 Take specific personal steps to nurture talent by engaging individual staff members. Move people around and give them assignments "outside the box" that help the broader organization. Actively support participation in professional organizations.

7 Refresh your employee recognition program to celebrate the energy your people put into continuous improvement.

8 Don't let stick-in-the-mud managers come between you and energetic supervisors who want to improve their operations. Reinforce the expectation that everyone in the enterprise can contribute to good change by holding senior managers accountable.

9 Require managers on the staff to prepare and carry out a current improvement plan every year, or every two years if you're on a two-year planning cycle, which is actually the best practice.

10 Refine your performance appraisal program, which probably needs improving anyway, to solicit subordinate feedback about managers' performance.

Change for the sake of change is nonsense. But so is setting static standards that never change. The best organizations are those that value and constantly work at continuous improvement. PM

JERRY NEWFARMER
President and CEO
Management Partners
Cincinnati, Ohio
jnewfarmer@managementpartners.com

MARCH 2015 | icma.org/pm

PM
PUBLIC MANAGEMENT

INSIDE

2 CELEBRATE ETHICAL CONDUCT
18 COLLECTING DISASTER RECOVERY COSTS
24 GEARING UP FOR FIRSTNET
32 TOP 10 OR MORE

CYBERCRIME @ CITY HALL

Plan the Prevention and Response

ADVANCING PROFESSIONAL LOCAL GOVERNMENT MANAGEMENT WORLDWIDE

ICMA

MARCH 2015 | icma.org/pm

PM
PUBLIC MANAGEMENT

INSIDE

2 CELEBRATE ETHICAL CONDUCT

18 COLLECTING DISASTER RECOVERY COSTS

24 GEARING UP FOR FIRSTNET

32 TOP 10 OR MORE

CYBERCRIME @ CITY HALL

Plan the Prevention and Response

ADVANCING PROFESSIONAL LOCAL GOVERNMENT MANAGEMENT WORLDWIDE

ICMA