



## Cybercrime @ City Hall

**Discussions of prevention and response can protect your community**

*by Gerald Cliff*

**FEBRUARY 27, 2015**

**Learn steps that a local government can take to reduce the likelihood of a data breach occurring as well as to 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.

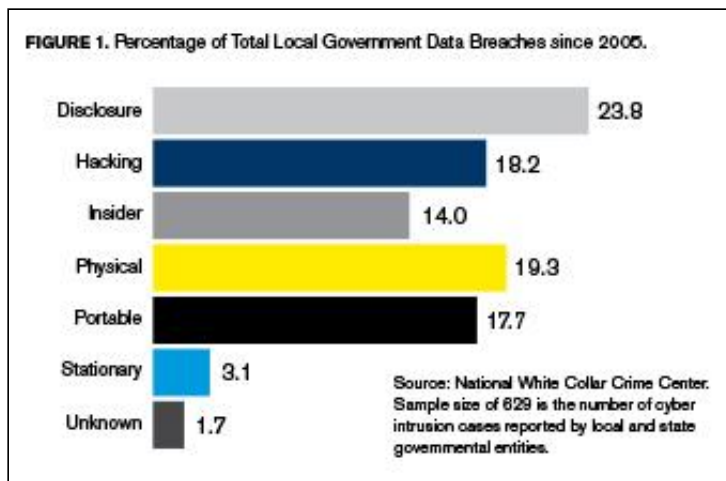
Costs of a data breach can be devastating to an already tight local budget. The Ponemon Institute produces an annual survey on the cost of data breaches. The Institute found in its "2014 Cost of Data Breach: Global Analysis," that "the average cost paid for each lost or stolen record containing sensitive 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](http://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 storage 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 the plaintiff will answer is: You can be sued for anything. The likelihood that

To shed some light on this issue, and a government may provide complimentary analysis.

## Reducing the

In short, the NW3C research attorney assembled an in-depth analysis on the research section of [www.nw3c.org](http://www.nw3c.org). If local information, the NW3C research attorney can provide analysis.

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.

## 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 "The First 24 Hours" in this issue.

Site Menu	
ICMA	
ICMA University	
ICMA Publications	
PM Magazine	
ICMA Program Centers	
ICMA International	
Knowledge Network	
Browse Jobs	
News	
Events	
Contact Us	
Log In	
Create New Account	
CityLinksWMTR	

About the Mobile Site / Feedback

View Full Site