TECHNOLOGY'S DARK SIDE:

YES, A DATA BREACH COULD HAPPEN TO YOUR COMMUNITY

By Kirstin Simonson

Technology offers amazing benefits to public entities struggling to find highly effective, cost-efficient ways to provide service to constituents. The dark side, however, is the potential financial impact public entities face when the use of technology backfires.

Consider a system glitch resulting in personal information of public assistance applicants being sent to random addresses in the department systems. Or the local government employee who fails to recognize an email as a phishing attempt and enters information on the fraudulent website that allows an unauthorized third party to gain access to information within the local government's network.

These types of incidents can place public entities at risk, not only facing the potential of a lawsuit for failing to protect information but also additional costs associated with fixing the breach.

At a time when many public entities already face budget constraints, the goal should be to add technology to their bag of tools without increasing the risk that they will be on the losing end of a lawsuit. By carefully assessing the weaknesses of their technology processes, putting adequate precautions in place, creating a response plan in advance, and identifying effective insurance coverage to address claims, public entities can mitigate risk and capture the benefits of technology.

COUNT ON DATA THEFT HAPPENING

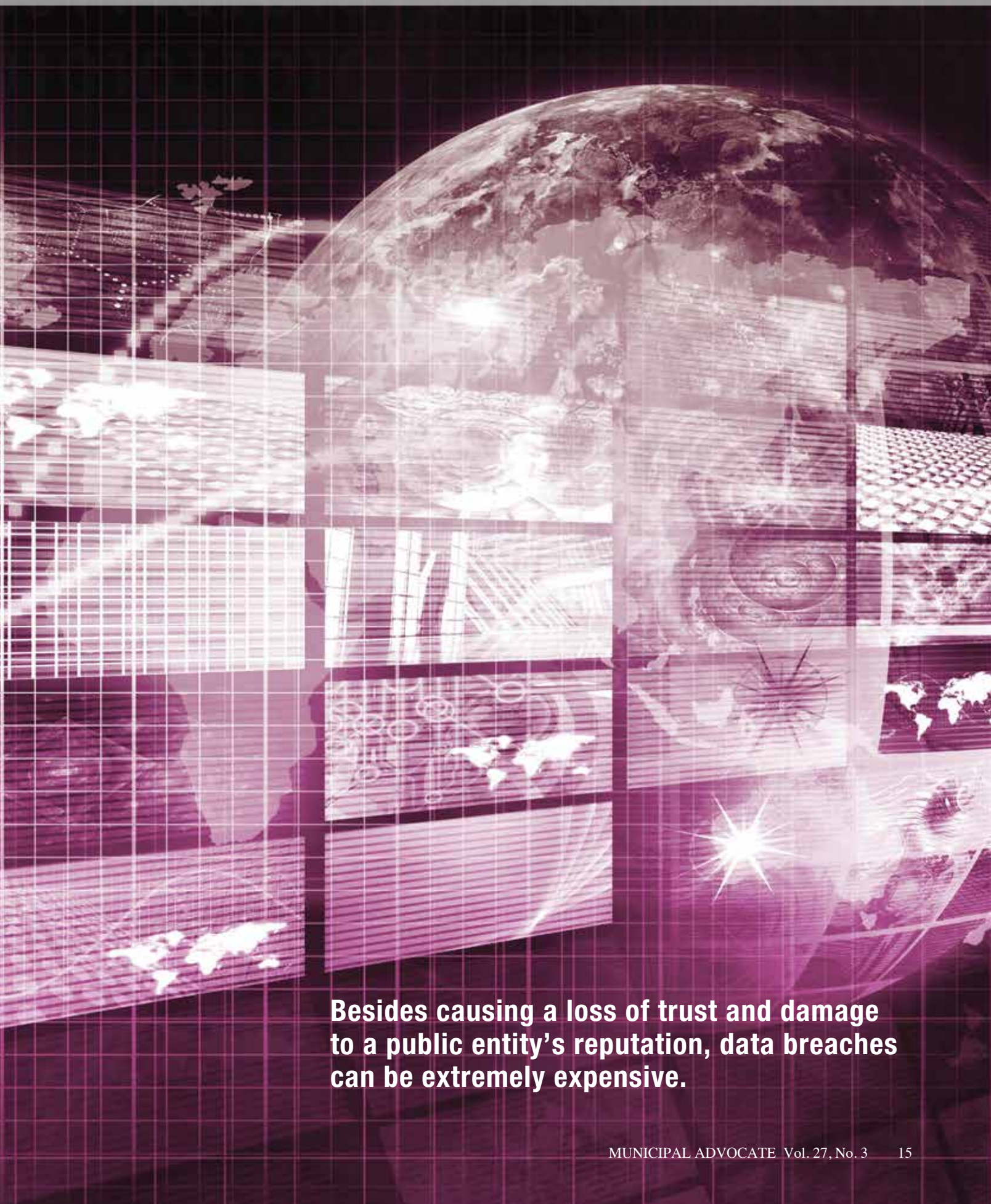
Sometimes it is easier to think that data theft only happens to huge companies that hackers target because they think they will find valuable information.

Think again. It is true that when it comes to data theft, the headlines often involve major organizations familiar to general consumers. But data theft happens every day to businesses, nonprofits and public entities. The experts who track these kinds of incidents have warned that a data breach is close to inevitable, sooner or later, for any organization that collects and stores digital information.

The challenges of protecting information are not lessening. The Privacy Rights Clearinghouse, which provides an online chronology of reported data breaches (www.privacyrights.org/data-breach), found that the number of incidents declined in 2011: 557 incidents compared to 604 in 2010.

The number of records exposed, however, was far greater in 2011: 30.68 million compared to 12.34 million in 2010. These numbers reflect only records that contain sensitive personal information, such as Social Security numbers and driver license information. Since 2005, the clearinghouse has recorded more than 3,200 breaches potentially exposing more than 563 million records.

Kirstin Simonson is underwriting director for Travelers Global Technology of St. Paul, Minnesota (ksimonso@travelers.com). Travelers is an ICMA Strategic Partner.



Besides causing a loss of trust and damage to a public entity's reputation, data breaches can be extremely expensive.

While the clearinghouse listing offers plenty of big names, including various departments of the federal and state governments, it also has many examples of small public entities that have had data exposed by hackers, employee carelessness and insiders-turned-criminals. Here are just four examples:

- In May 2012, a county in South Carolina discovered that hackers had accessed a database with private information on 17,000 job applicants and vendors.
- In April 2012, a park district in Minnesota found that hackers had harvested user names and passwords for everyone who had ever made an online park reservation or registered for a recreation program—a total of 82,000 people.
- A county tax department inadvertently posted information for 1,000 people who paid tax garnishments. The data, which included names, bank account numbers, and Social Security numbers and addresses, was online and accessible by the public from December 2010 to September 2011.
- In October 2011, a police officer was accused of taking information from a driver- and vehicle-information database and giving it to co-conspirators. The information was used to open bank accounts where fraudulent tax return checks could be cashed.

Besides causing a loss of trust and damage to a public entity's reputation, data breaches can be extremely expensive. Forty-six states now have laws requiring notification of people whose private information has been exposed. Some state laws require payment for credit monitoring services, and some may allow credit card issuers to recoup the cost of replacing compromised cards (estimated to be $3 to $5 per card).

The 2011 Cost of Data Breach Study by the Ponemon Institute found that the average data breach for U.S. companies exposed more than 28,000 records. The cost to take care of the problem averaged almost $200 per record. Direct costs, which include such expenses as notifying people about the exposure of their data, ran almost $60 per record.

Also included within these direct costs are defense costs associated with resulting litigation; costs to indemnify victims from resulting identity theft; internal costs associated with the forensic investigations; legal consultants and other costs to comply with various laws and regulations; and damage to computer networks and costs associated with repair and upgrades. While a business may be able to absorb the millions of dollars these costs add up to, public entities may have great difficulty finding the necessary funds in their tight budgets.

SOCIAL MEDIA MISSTEPS

Data breaches can cause major headaches for public entities, but social media mishaps can also have an unintended impact, and may make them the laughingstock of anyone with an Internet connection. Employees can be caught on video doing something irresponsible or harmful. Once the video is posted on a site like YouTube, an agency can quickly find itself on the defensive.

Similarly, an employee who posts damaging remarks on Facebook or who ruffles feathers with an insensitive tweet on a public Twitter account can raise questions about the employer's responsibility and potential liability.

There are examples of businesses being exposed to ridicule or anger after videos were posted online and went viral, reaching millions of people: a delivery man throwing a box that contained a computer monitor over a home's fence, a pizza employee adulterating food orders, and a musician singing a parody about an airline destroying his guitar and refusing to pay for it.

While there are fewer widely known examples, public entities have not escaped this kind of uncontrollable digital criticism. One notable video is of a federal General Services Administration employee rapping about being able to freely waste taxpayer money and buy anything he wants. The video apparently was shared humorously at a 2010 GSA conference in Las Vegas, a conference that the federal inspector general later revealed cost $822,000. The investigation resulted in the firing of several top administrators.

DEFENDING YOUR ORGANIZATION

The time to start thinking about how to handle the dark side of technology isn't after a data breach or social media disaster occurs. Preparing in advance is critical to successfully limiting the damage and positioning your agency to respond appropriately.

Of course, an effective firewall can protect your data, and a solid training program can keep your employees on the right side of social media. But being prepared for the worst is even more important because it is almost impossible to completely eliminate the risk that comes from data breaches and social media mishaps.

Here are steps that address both proactive and reactive measures:

Assessment: Understand the risks your public entity may potentially face. The key to addressing your exposure is to first understand just what that exposure involves. Public entities have the potential to collect staggering amounts of private and confidential information during the normal course of business. The use of social media as a communication and collaboration tool is becoming more common. And, whether you actively engage in online commerce or use social media tools, your constituents, your employees, and all those around you are—all of which can put you in harm's way. A comprehensive assessment of computer systems and safeguards already in place is a good starting point to determine where the gaps may be and what additional efforts are needed to close them.

Protection: The fact that some of the most technologically sophisticated organizations have suffered data breaches should be an indicator that no one is immune. It is important to continually manage the information security practices you have put in place to ensure compliance and that updates are happening.

The security of the network is important, but it is also important to remember that in many instances the data breach event or social media hiccup was the result of employee behavior. Installing new hardware/software and network security measures are important pieces in protecting the organization. But employee education coupled with strong employee management tactics are equally important.

Response Plan: When the worst-case scenario happens, it is important to be able to respond quickly and efficiently to lessen the impact of the event. Create a plan for handling a negative event, including identifying an incident response team. If a data breach occurs or a social media crisis is building, what steps will you take first? Who will notify authorities, who will handle media, and who will be the liaison to constituents?

The time to start thinking about how to handle the dark side of technology isn't after a data breach or social media disaster occurs.

The plan should assign responsibilities and provide a framework for action so that key decisions are already in place and do not have to be made when everyone is under pressure and the situation is changing rapidly.

Risk Transfer: Public entities already carry insurance to transfer risk for a wide range of potential liabilities, and they often believe their commercial general liability policy or other traditional policies will respond. These policies, however, are often not designed to cover the exposures created by managing their online reputation or managing their exposure to data privacy risk.

It is important to have an in-depth discussion with your insurance agent to discuss where the insurance gaps may be and consider a cyber insurance policy specifically designed to provide insurance protection for data breaches and other evolving exposures not covered by the traditional property or general liability insurance.

Cyber insurance policies can offer defense and indemnification associated with the liability for failing to prevent unauthorized access to information or the liability associated with misuse of content. These policies are also designed to provide additional coverage for many of the first-party expenses associated with managing a data breach, including compliance with the notification requirements of various laws. Expenses can also involve managing the public relations expenses associated with negative publicity.

Risk managers for public entities may feel that their organizations are not a target for hackers or angry customers. But in a digital age, almost any organization can end up on the wrong end of a data breach or social media transmission. By taking steps in advance, public entities can defend themselves against the dark side of technology while still enjoying the benefits it brings.

Reprinted with permission from the December 2012 issue of Public Management, *published by the International City/County Management Association.*