PUBLIC RISK

Published by the Public Risk Management Association ▸ www.primacentral.org

FEBRUARY 2011

Digital Dilemma

DIGITAL DILEMMA

TAKING ADVANTAGE OF TECHNOLOGY WITHOUT TRIPPING OVER CYBER PITFALLS

By Robin Leal

The days when a government agency accepted a paper check at the front counter, meticulously recorded the amount on a paper ledger and then carefully stored it in a cabinet stuffed with paper files are long behind us. Today, public entities interact with their constituents online, store their information electronically in large databases and accept payment through credit cards and electronic fund transfers.

As public entities know, the digital age makes many aspects of providing information and services much easier. But it also brings with it a surprising degree of liability risk. To manage the risk, public entities must first understand the broad range of potential exposures and then design procedures to thoughtfully address the areas of concern. With insight and planning, potentially costly exposure risks can be substantially mitigated.

CYBER PITFALLS

There are many current examples where public entities are being sued for alleged missteps relating to problems in the electronic space. What follows are just a few of the cyber pitfalls that can arise.

Breach of Privacy

Allowing personal information to fall into the wrong hands not only exposes citizens to potential fraud, but also puts the public agency at risk for damages, penalties and costs. Almost all states have laws requiring the protection of private information and many states have specific mandates for mitigation when a breach of privacy occurs.

Despite heightened awareness about the issue and widespread news coverage when breaches occur, there has been no slowdown in the public sector. According to

Allowing personal information to fall into the wrong hands not only exposes citizens to potential fraud, but also puts the public agency at risk for damages, penalties and costs. Almost all states have laws requiring the protection of private information and many states have specific mandates for mitigation when a breach of privacy occurs.

statistics captured by the Privacy Rights Clearinghouse, which keeps a national registry of breaches of privacy, public entities (government and military) were on track for an 88 percent increase in frequency of privacy breaches for 2010.

Among the types of breaches to be aware of are internal theft by employees, stolen laptops, lost portable storage devices, mailings with Social Security numbers exposed, inadvertent online access to information and much more.

Transmission of Malware

An email is opened with an attachment that looks like it comes from an acquaintance. The virus it contains infects the entity's computer system—and then inadvertently is transmitted to third parties through email. When the third parties can document repair costs and financial losses from their systems shutting down, the entity can face liability claims as well as incur defense costs.

The possibility of a malware attack—viruses, Trojan horses and worms—has multiplied over the years. In 1990, experts estimated there were between 200 and 500 viruses. By 2008, virus-fighter Symantec noted that its anti-virus programs could detect more than 1.1 million viruses.

Social Media Issues

There are several areas of potential liability when a public entity or its employees use social media—Facebook, YouTube, Twitter—to communicate with others. These include liability for defamation or harassment; damages from leaking of private information; and misuse of information found through Internet searches.

A human resources or hiring manager that uses social networking sites to screen applicants or conduct background investigations could inadvertently invite a claim of discrimination if, by reviewing social media, a candidate from a legally protected class is eliminated from consideration. In another example, a clinic employee gossiped about private medical information on a social networking site, exposing the employer to a lawsuit for invasion of privacy.

Infringement of Copyright

Someone else's property can be inadvertently taken without permission—and sometimes without that person even being aware of it. For instance, New York City has long been known as the Big Apple—but that didn't stop Apple Inc. from raising a fuss when the city used an apple logo for an environmental initiative. The company argued the logo was an infringement of its own famous bitten-apple symbol.

Another example is an employee who downloads a copyrighted picture, diagram or narrative from a Web site and uses it in a public entity brochure. While these kinds of exposures existed in the past, they are much more common today because the Internet makes it simple to download materials in a digital form that can be incorporated into documents.

Plagiarism

Similar to copyright infringement, plagiarism can be committed when material is not attributed to its original source. For example, someone might admire the way a vendor presents materials during an information seminar—but to borrow that material to produce their own presentation would be plagiarism.

TAKING PROACTIVE STEPS

The best defense against cyber-liability is to have procedures and processes in place that encourage the careful handling of information and data. Steps to take include:

1. **Create and implement an effective data management plan.** The foundation of a good data management plan is an understanding of the types of information it will contain. Private information may be protected by law; other information may be subject to open-records requests; still other data may be important for running operations but have little impact if it is exposed to the public. Once the different types of information are identified, a plan can include differing levels of security and protection.

2. **Build and maintain a strong technology infrastructure and an institutional culture of data protection.** Besides just using firewalls to keep hackers out, other strong measures need to be in place to control how employees use information. The plan should cover building, maintaining and updating secure networks, implementing strong access control measures, regularly monitoring access to network resources and maintaining an information security training and compliance policy that is applied to all employees.

3. **Control access to data.** Encryption is the gold standard for storing personal data so it does not go astray. In many cases, state laws that include onerous mitigation measures exempt organizations that have lost encrypted data. In addition, the danger of data being breached can be lessened by restricting who can access it, restricting the use of portable drives (including

HOW DOES DATA ESCAPE? LET US COUNT THE WAYS

Many people think hackers are the biggest threat to data security. But public agencies have been embarrassed to lose information in a number of other ways.

1. An inside job—A temp employee for a county has been convicted of ID theft after his assignment in the HR department gave him access to steal personal information for more than 30 employees and commit fraud in their names.

2. Cat burglar—While on vacation, a county employee's work laptop was stolen. More than 35,000 residents had their names and Social Security numbers jeopardized by the theft.

3. Dumpster diving—A woman was sentenced to 34 years in prison for using teacher data to open credit accounts, purchase goods and steal items shipped to homes. She found information for thousands of teachers in a school district Dumpster.

4. Careless handling—Personnel records, law enforcement reports and other documents that were scheduled to be burned were found stored in office furniture being auctioned by a city. When potential buyers called the paperwork to the attention of the city, the documents were retrieved. In another example, a town's cancelled payroll checks, with Social Security numbers and bank account information, were discovered beside a road. The wind had knocked a box off a truck carrying them to a recycling station.

5. Online glitch—An assessor set up an online process for victims of a natural disaster to request property tax relief. The site required canceled checks, tax returns and other data to be uploaded. To make the process easier for applicants, staff removed the password requirement, unaware that the data was then accessible to anyone who clicked on the site.

6. It's on/in the mail—A mailing from one state agency that used an outside vendor had Social Security numbers printed below the addresses when the envelopes went out. In another case, a state official inadvertently sent the names, Social Security numbers and other personal information for 139,000 people to an investment industry publication.

The Ÿst defense against cyŸr-liability is to have procedures and processes in place that encourage the careful handling of information and data.

laptops and thumb drives) and actively monitoring who opens, copies or moves files that need a high level of protection.

4. **Enforce employee technology policies consistently.** Policies should be in place that address how and when employees can use social media and other technology tools on the job. In addition, employees should be educated about the potential for damaging the entity's reputation or exposing it to liability if they make statements in chat rooms or on social networking sites that reflect poorly on the public entity. Once policies are in place, make sure they are consistently enforced so they are taken seriously and become a part of the entity's ingrained culture.

5. **Look beyond digital data.** Although cyber liability emphasizes electronic transmission of information, the fact is that data is often breached when paper records are exposed. Effective paper record retention policies are needed, including guidelines for disposing of information no longer needed by shredding, recycling or some other acceptable method.

6. **Have the right coverage.** Even the best policies and procedures cannot always eliminate human error. After a mistake happens is the wrong time to find out that the entity's general liability coverage excludes cyber risks. Instead, public entities should work with their insurance agent to determine the best cyber liability coverage for the entity's needs. Not all public sector liability insurance policies offer the same level of coverage for cyber risks.

Technology has opened the door for public entities to provide their constituents with faster, more convenient services. At the same time, it has allowed the stockpiling of information that can be damaging if it is diverted to the wrong hands and it has enabled much easier access to copyrighted and trademarked materials. These and other factors have greatly increased the potential for liability. By taking steps to manage these new risks, a public agency can avoid many cyber pitfalls. ■

Robin Leal is the director of professional lines for Travelers Public Sector Services.

Additional Resources

Readers who want more detailed information can check out the following Web sites and white papers:

Potential Vulnerabilities in Municipal Communications Networks, a US-CERT Informational Focus Paper: www.us-cert.gov/control_systems/csarchive.html.

The Web site for TRUSTe, a leading organization promoting privacy, www.truste.org. Resources include a privacy policy white paper, a Forrester Report titled, *Privacy Seals: Opt In or Opt Out?* and security guidelines.

The Web site for SANS Institute, a leading organization in computer security training, www.sans.org. Click on "free resources" for *A Short Primer for Developing Security Policies* and templates for various types of policies.

Protecting Personal Information—A Guide for Business, a white paper available at www.ftc.gov/infosecurity.

Information Compromise and the Risk of Identity Theft: Guidance for Your Business, a white paper available at www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm