White paper

Public entities: There’s no immunity from network security and privacy risk

Technology, Privacy, and Network Risk Practice
September 2014
Network security and data breaches happen every day to organizations of all types, and public entities are no exception. Government agencies, utility districts, community service agencies, school districts, and municipalities, among others, collect and maintain information for citizens, businesses, organizations, and their own employees. The sheer volume of sensitive information makes the public sector an attractive target for data privacy crimes. Additionally, reliance on technology and computer systems for daily operations can lead to a host of other network security exposures, including denial of service attacks, infection by malicious code, and system interruptions.

To many, data and network security risk seems insignificant compared to other threats such as theft and workplace violence. Yet breaches occur at a much higher frequency and can cause significant financial harm to an agency’s budget. Incidents can result from inadvertent errors, intentional misconduct, or outside criminal activity. Breaches also expose multitudes of residents and employees each year to the risk of identity theft. Reputational harm stemming from a poorly managed breach can be catastrophic.

According to the Privacy Rights Clearinghouse, 227 government organizations disclosed privacy breaches between 2011 and 2013, and the risk is growing. These entities are targets; identity theft is a lucrative business where data brokers profit by selling sensitive personal information. Moreover, ideological, political, or personal motivations may inspire criminals, hackers, or terrorists to infiltrate and try to disrupt a public utility’s networks or systems. These attacks not only threaten a utility’s reliability and resiliency, but could create operational losses.

Consider these recent examples of breaches at public entities:

**South Carolina Department of Revenue.** A cyber attack in the fall of 2012 exposed 3.9 million tax returns, including Social Security numbers (SSNs), and 387,000 credit and debit card numbers. The breach occurred after a Department of Revenue (DOR) employee opened a phishing email, which gave hackers access to the information by infecting DOR servers with a virus that stole access credentials. The state paid $1.3 million to notify taxpayers, $12 million for credit monitoring, and $5.6 million to improve encryption. The state’s budget board ultimately approved a $20.1 million loan to cover the costs associated with the breach and the DOR’s director resigned after a report showed that officials could have done more to protect the information.

**City of Detroit.** In early 2014, a phishing email released malware onto a computer in city hall that froze access to numerous files, which included names, dates of birth (DOBs), and SSNs for 1,700 current and former employees. Although it did not appear that the information was actually accessed, the city still notified the affected individuals and offered them free credit report monitoring and identity theft insurance. The city is now looking into increasing training for city workers on computer security.

**New York utilities.** In January 2012, the SSNs, DOBs, and, in some cases, financial account numbers of approximately 1.8 million customers of New York State Electric & Gas and Rochester Gas and Electric (together, “NYSEG”) were accessed when a third-party service provider improperly shared log-in credentials with an unauthorized subcontractor. In response to the incident, the Public Service Commission issued an enforcement order requiring NYSEG to implement changes to better protect sensitive information. The Commission found deficiencies in personally identifiable information handling policies, as well as technical and physical safeguards with contractors and subcontractors. The NYSEG was also precluded from recovering its breach response costs from customers.

**State of Colorado.** In November 2013, the names, SSNs, and some mailing addresses of 18,800 current and former Colorado state employees may have been compromised when a state employee lost a USB drive while transporting

---


it between work locations. Although the state has a strict policy regarding encryption, the drive that was misplaced was not encrypted. There was no indication that the information was misused or stolen, but affected individuals were still notified.⁵

Primary exposures

- Unauthorized access to or use of computer systems, including by contractors
- Unsecured wireless networks
- Outdated computer equipment
- Loss, theft, or wrongful disclosure of sensitive information
- Data or network sabotage
- Corruption or destruction of digital assets
- Theft or loss of portable media devices (smartphones, tablets, backup tapes, thumb drives)
- Identity theft
- Cyber extortion

Public agencies warehouse an abundance of sensitive information including SSNs, tax records, billing information, health information, and legal records — both for residents and employees. Even with a record retention policy, this data can be kept for many years. Moreover, security failures may affect an agency’s ability to conduct its own business, which could extend to third parties who are reliant on those services to conduct their own business. The resulting loss of income could be staggering.

A breach exposes an agency to regulatory scrutiny, reputational damage, and potential litigation. While state agencies may be entitled to sovereign or governmental immunity, it is unclear whether counties, municipalities, and local agencies are shielded. Lawsuits arising from a network security or privacy event can come from multiple sources, including the victims of a breach. But even when there is no lawsuit, the cost of responding to a breach is staggering and can create financial instability.

The responsibility to protect private data

While some public agencies may be exempt from the disclosure requirements of a state privacy breach notification law, that trend is changing. Starting in 2014, California extended the application of its breach notification law from state agencies to all public agencies. Public agencies may also be required to comply with the following:

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH)
- Payment Card Industry (PCI) security standards
- Fair and Accurate Credit Transactions Act (FACTA)
- Red Flags Rule

Five myths you can’t afford to believe:

1. **Network security and data privacy is only a problem for large agencies.** Network security and data privacy risk is a concern for all organizations and incidents happen to agencies of all sizes. Rogue employees, data thieves, and unscrupulous contractors are looking for opportunities to take advantage of even the slightest weakness or mistake. Will it happen to you?

2. **We can afford to self-insure the risk.** With greater demands on limited budgets, many agencies knowingly go without coverage. They wrongly believe that, if something happens, they can afford to cover the costs. According to a 2014 Ponemon Institute study, the average U.S. cost of data breach is $201 per record.⁶ Even a small breach event of 1,000 records could easily exceed $200,000 — a sum that many public entities cannot easily absorb.

3. **Coverage is expensive and hard to get.** This may have been true 10 years ago, but today there are many carriers offering network security and privacy liability coverage. The insurance is more affordable and accessible than ever.

4. **Our general liability policy will cover us.** General liability insurance typically covers bodily injury and property damage. Courts have consistently ruled that data is not property and is considered intangible. If you don’t carry specialized coverage for financial injury arising from a failure of network security or a failure to protect confidential information, you’re probably exposed.

---


5. **We have vendors who handle our billing transactions and payroll. If they have a breach, it’s their problem, not ours.** This is generally not true. The data owner (the person or entity collecting the data) is ultimately responsible for what happens to that data. Therefore, a breach at a trusted contractor still triggers your notification obligations; this risk can’t be transferred to that vendor partner.

**Questions to consider**

There are many reasons why public agencies are vulnerable and targeted. For one, proactive, preventative measures prior to a breach event are generally lacking. It is essential for organizations to be prepared, including adopting strict policies and procedures surrounding data privacy and security, along with a concrete, comprehensive plan for incident response. Consider these questions:

- Have you adequately educated your employees about their responsibility to protect private information?
- Have you implemented standard procedures for the access to and use of private data? Is access to data limited to a “need to know” basis?
- Do you restrict and/or encrypt data that is stored on mobile devices including backup tapes?
- Do you have procedures for managing your contracts with contractors and vendors including indemnification, insurance, and significant limitations of liability as respects data breaches?
- Do you follow encryption standards?
- Do you have a written policy regarding the dissemination of personal information on public and social media sites?
- Do you have a breach incident response plan? Have you tested it?
- How often do you monitor networks, websites, and databases to detect potential issues?
- What will you do if a potential issue is identified?

- Do you have adequate reserves or insurance protection to manage the financial impact of a breach?

Readiness is the most important step. Public entities can’t afford to figure things out after a breach occurs. It’s critical to have a ready-to-use incident response plan, an on-call forensics expert, and a privacy attorney on retainer. Then, when a potential issue is identified, the agency is ready to mitigate the effects of the breach and deter any potential litigation.

**Solutions**

Wells Fargo Insurance has the experience, knowledge, and market relationships to help your organization implement a comprehensive strategy for managing technology, network security, and privacy liability. Working with the industry’s leading insurance markets, we provide access to cost-effective products that cover costs associated with:

- Unauthorized access or use of computer systems
- Theft, loss, or wrongful disclosure of proprietary information
- Identity theft
- Data or network sabotage
- Corruption or destruction of digital assets
- Loss or theft of portable devices
- Errors and omissions related to technology and the internet
- Cyber extortion and cyber terrorism
- Network business interruption
- Regulatory defense, fines, and penalties
- Crisis management

**How can we help?**

For more information on this topic, contact your local Wells Fargo Insurance sales executive, or visit us at wfis.wellsfargo.com.