Local Government Snapshot

NEW YORK STATE OFFICE OF THE STATE COMPTROLLER

Thomas P. DiNapoli • State Comptroller

August 2011

Local Government Information Security:
The Cost of Inadequate Protections

- New technologies are transforming the way we handle information. Web-based applications for completing day-to-day transactions, telecommuting of municipal staff, online banking, and increased reliance on personal communication devices all represent activities that are now considered “business as usual” in governmental operations. Along with these advances comes the responsibility to protect confidential information adequately so that it cannot be accessed by unauthorized individuals. Failure to do so can come at a considerable financial cost. The Duanesburg School District is one of several entities in recent years that have experienced the financial impact of a cyber attack, after hackers successfully transferred $3 million of school district funds into overseas bank accounts.[1]

- Unfortunately, during periods of fiscal austerity, investment in information technology (IT) security by local governments may be diminished as scarce resources are used to support services that are more highly visible to taxpayers. However, the decision to delay or forgo an investment in adequate security protections can carry its own price tag. When the risks of an IT security breach–which can damage government credibility, harm private citizens, and require substantial resources to repair and rectify–are fully understood, adequately protecting information can be recognized as a cost-effective preventive measure.

- When sensitive data is accessed by unauthorized individuals, not only is the public trust compromised, but local governments may face additional expenses related to notifying affected parties, undertaking data recovery efforts, conducting forensic investigations, and defending themselves against any resultant legal claims. Fortunately, there are some simple steps that a local government can take to reduce the chances of becoming a target. Notably, many of these steps involve measures that would not be overly burdensome for a local government to implement.

- The Ponemon Institute estimates an average breach cost of $81 per record for public sector entities.[2] If we apply that cost estimate to the number of individuals (over age 18) who live in New York counties, it is possible to get a sense of the potential dollars at risk under a worst case scenario: a data breach involving a single piece of sensitive information for every adult resident in the county. As shown in the accompanying table, the financial exposure could range from $2.8 million in the average small county to over $67 million in some of the State’s largest counties.[3]

County Characteristics (adult population, 2010 Census)	**Potential Dollars At Risk** ($ millions)
Fewer than 50,000 (average small county)	**$2.8**
50,000-100,000 (average medium county)	**$5.7**
101,000-500,000 (average large county)	**$15.2**
Over 500,000 (largest counties)	**$67.3**

[1] Most of the school district’s money ($2.5 million) has since been recovered.

[2] Ponemon Institute, *2010 Annual Study: U.S. Cost of a Data Breach,* March 2011.

[3] This estimated impact is for illustrative purposes only and represents a worst case scenario on a county wide level, involving all adult residents.

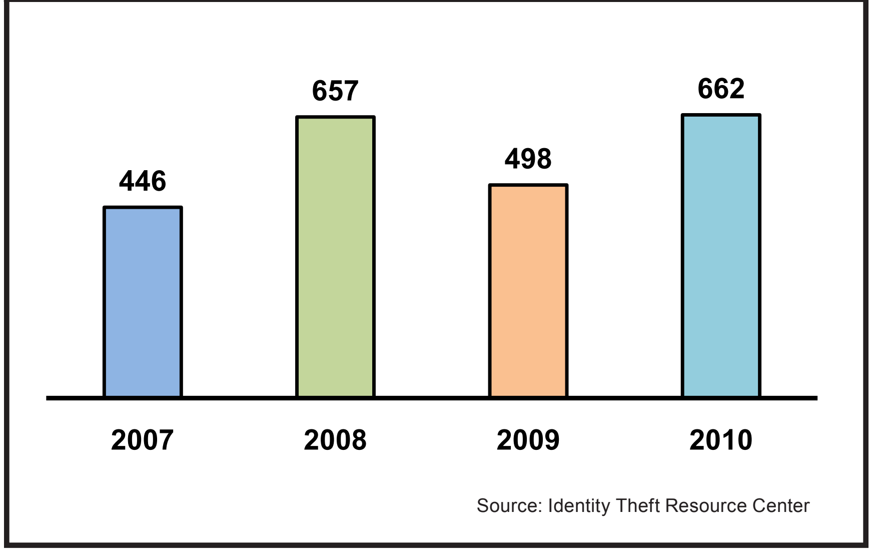
Security Breaches[4] on the Rise

- New York State Technology Law Section 208(8) requires counties, cities, towns, villages, and other local agencies to adopt a breach notification policy. And, in December 2005, a law went into effect requiring municipalities to notify the Office of Cyber Security (OCS), The New York State Attorney General's Office and the State Consumer Protection Board when a breach occurs. As of May 2011, there have been 20 reported incidents related to a local government, BOCES or school district since the law went into effect.

- Nationwide, there has been a 48 percent increase in breach incidents since 2007.[5] Records by Identity Theft Resource Center (ITRC) indicate that there were 662 data breaches in 2010, 104 of which (15.7 percent) were classified as government or military breaches. According to the ITRC, breach incidents are underreported and lack transparency.

- The level and type of risk to a local government may vary depending on its size. Large municipalities are more vulnerable because of the sheer volume of information they maintain and collect on a daily basis. Smaller municipalities are also at risk because they might not have the proper IT system or because they lack access to IT professionals who can guide them in proper network management and security. Regardless of how big or small an organization is, municipal employees who keep work-related data on a home computer, or who access work resources remotely from a personal device, present a major risk.

Number of Breaches (Nationwide)



Source: Identity Theft Resource Center

[4] A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an unauthorized individual.

[5] Collins, Hilton, "Stats Suggest Breach Reporting Should be Mandatory", Government Technology Magazine, January 19, 2011.

In the News

- In the Town of LeRoy, the FBI was called in to investigate when the Town began experiencing difficulties with computers dropping off a network that was connected to the statewide criminal justice and motor vehicle systems. Illegal software was found on the computer which was later traced back to The Netherlands. The intruder was a 14-year-old who was using the network for illegal Internet games. Financial information from local businesses was also accessible on the network. It was determined that the Town lacked a firewall for Internet and network connections. The cost of the repairs, upgrades and training totaled $80,000.[6]

- The Town of Pittsford, discovered that someone had logged into their online commercial banking account and wired $139,000 through various places in the United States and internationally. The FBI is investigating the incident and $4,800 has already been recovered.[7] The theft occurred even though firewalls and antivirus software were in place at the time of the incident, both of which may have been bypassed through exploitation of an internal user directly through email or some other social media attack.

- A 16-year-old sophomore at Shenendehowa High School in Clifton Park, was charged with unauthorized use of a computer and third-degree identity theft after he was caught hacking into the school's computer system for the second time in less than a year. He had previously been caught hacking into the system and accessing personal information about school employees.

- Several Fayetteville-Manlius High School students allegedly tampered with the school's computer and changed their grades by using a piece of spyware equipment known as a keylogger. The school's network is the same one used in nearly 50 school districts across Central New York. School officials estimated the cost to the District to be more than $8,000.[8]

- Not all data breaches are the result of malicious intent. The Town Clerk in Eastchester mistakenly included social security numbers in a Freedom of Information Law request made by The Journal News. The newspaper made the request for employee names and payroll as part of story on government and school district salaries.

[6] Presentation by Shelley Stein, Supervisor of the Town of LeRoy, "Now That We Know What We're Supposed to Do, How Are We Going to Do It?", New York State Office of Cyber Security Conference (2007).

[7] Lamothe Jr., Ernst, "Hacker Steals $139,000 from Town of Pittsford Account", Democrat and Chronicle, June 15, 2011.

[8] www.nyssba.org/index.php?src=news&refno=235&category=On%20Board%20Online%20Feb%2025%202008

Resources

- Even in challenging fiscal times, local governments and school districts should do what they can to keep IT security on their priority lists. Approaching security measures from the perspective of cost avoidance is one way for local officials to frame the issue during budget discussions.

- Municipalities, especially smaller municipalities, face a significant hurdle. Limited resources combined with few options for securing outside funding continue to restrict local officials' ability to prioritize IT security in their communities. Out of necessity, some local governments have found developing shared service opportunities to be a promising way to better leverage their resources. Schools districts have been able to avail themselves of the IT services provided through their BOCES.[9]

- OSC assists local governments and school districts through integrated training events and through its audit function. Audits conducted between 2007 and 2010 revealed numerous instances of inadequate IT security protocols in local governments and school districts. Some of the specific recommendations put forward in these audit reports include:

    1. Developing and distributing written IT policies, including breach notification procedures;
    2. Limiting, restricting and periodically updating access rights to systems and equipment;
    3. Developing and testing disaster recovery plans;
    4. Configuring strong access controls on firewalls;
    5. Providing information security awareness training to all personnel;
    6. Regularly tracking/monitoring system activity, including all remote access activity;
    7. Providing for secured off-site storage of back up data;
    8. Maintaining an up-to-date inventory of software and equipment; and
    9. Maintaining up-to-date virus protection.

- There are a variety of other resources available to local officials on the topic of IT security. The New York State Office of Cyber Security (OCS)[10] was created in 2002 to address cyber security and critical infrastructure needs. New York State is also involved with the Multi-State Information Sharing and Analysis Center (MS-ISAC),[11] which facilitates sharing of information on a nationwide basis and is a central resource for gathering information on cyber threats at both state and local levels. Both of these entities offer an array of helpful guidance materials and MS-ISAC materials specifically target non-technical users.

[9] **www.dhses.ny.gov/ocs/local-government/**

[10] **www.dhses.ny.gov/ocs/**

[11] **www.msisac.org/localgov/**

New York State Office of the State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor • Albany, New York 12236

www.osc.state.ny.us August 2011