Local Governments in Cyber World

Recognizing and Managing the Risks

Robert A. Spolzino, Esq.

ICMA Conference Presenter

ICMA
99TH ANNUAL CONFERENCE
BOSTON
NEW ENGLAND
September 22-25, 2013

Who am I?

- Why Am I Here?
- What will I accomplish?
- What can you glean from listening to me?

Context and Scale

- Facebook has 600 million users
- 30 billion items are posted on Facebook each month
- 906 million hours are spent each month on social media in US

Cyber Risk Overview

- Three core cyber liability risks
  - Technology errors and omissions
  - Social media/e-publishing liability
  - Data breaches of sensitive information
- Why are municipalities data breach targets?
- Why are municipalities vulnerable to serious damage to ongoing operations from a breach?
- Solutions for managing cyber risks

Technology Errors and Omissions:

- Local governments manage a lot of data
  - Employee records, property records, licensing records, police, fire and ambulance records, credit card data
- Software and hardware sometimes do not function properly
  - Information mailed to wrong recipient
  - Data corruption
- There can be errors in network architecture
  - Public facing web application without a firewall
  - Glitch in segregation permits unauthorized access

Technology Errors and Omissions: Source and Responsibility

- Most are software/hardware design mistakes
- Often involve technologists working as a team
- When internal and vendor IT work together, it may be difficult to determine which entity is at fault—particularly where the Municipality's IT person "authorizes" whatever the vendor does
- Legally and practically, municipality bears responsibility

Technology Errors and Omissions:

- Losses tend to be severe
- May include assertions that technology failure caused:
  - Significant business interruption
  - Failure of business
  - Loss of key contract
  - Damage to customer's business partners
- Technology failure may be used by new management or management under financial strain to excuse poor performance of company

Technology Errors and Omissions: Containment and Risk Management

- Understand interrelationship of companies working on technology project:
  - Which company is responsible for what?
  - What happens if one company's error causes error in another's work?
  - What happens if one company's delay results in delay that impacts another company's work?
  - Which company is responsible for work done by the customer?
  - How does the insurance work? Who is an additional named insured and who controls allocation?

Technology Errors and Omissions: Minimizing Risk

- Avoid providing technology solutions to others – you're not a vendor
- Make technology solution providers contractually responsible if their mistake causes violation of HIPAA or state statutes, or a significant loss
- Be certain that technology solution providers carry adequate and appropriate insurance coverage to respond if they create a significant loss
- Specify how/when publishing is permitted

Social Media/E-Publishing Liability:

- E-publisher has same duty/liability as news outlet
  - Web page /Facebook/Linkedin/blog/twitter/email
  - If you provide the content, you're responsible for it
    - Defamatory comment = defamation
    - Misleading comment = deceptive trade practice
    - Violation of privacy rights in "friend" posting
- Evaluate liability for employees and other "connections"/ "friends"

Social Media/E-Publishing Liability: Frequency

- Frequency is increasing
- Tracking residents/customers/website/blog visitors
  - Cookies
  - Profiles
  - Reverse engineering
- Social media gray area:
  - What belongs to municipality?
  - What belongs solely to employee?

Social Media/E-Publishing Liability: Severity

- Class actions:
  - Settlement value $300,000 - $750,000 (early)
  - Frequently filed in plaintiff-friendly jurisdictions
    - Law of state of plaintiff's residence applies
  - Need reasonable explanation for conduct
  - Upward pressure on settlement values
- Individual plaintiffs:
  - Disclosure of STD testing or HIV status
  - Release of information on public assistance
  - Relative learns of serious injury from employee's Facebook page

Social Media/E-Publishing Liability: Volatility

- Depends on content
- Is plaintiff on a crusade, or willing to resolve early?
- Is plaintiff's counsel trying to "ring the bell"?

Social Media/E-Publishing Liability: Unique Issues for Local Government

- First Amendment
- Fourth Amendment
- Public Employee Rights
- Freedom of Information
- Open Meetings

Social Media/E-Publishing Liability: First Amendment Issues

- Employee Speech
  - Speech related to public duties not protected
  - Speech as member of public is protected
- Public Forum
  - A public forum, even in cyberspace, is probably still a public forum
  - No content-based discrimination
  - Time, place and manner restrictions?

Social Media/E-Publishing Liability: Fourth Amendment Issues

- Prohibits unreasonable searches and seizures
- Accessing e-mails ,texts, etc.?
- Issue is expectation of privacy
  - Where employee routinely exceeded text allotment and knew that policy allowed municipal employer to access texts, municipal employer did not violate Fourth Amendment by searching texts to determine what was work-related. *City of Ontario v. Quon* (2010)

Social Media/E-Publishing Liability: Public Employee Rights

- Right to engage in concerted activities regarding terms and conditions of employment
  - NLRB – Facebook postings critical of management are protected
    - No different than conversations at water cooler
  - PERB – Public employer may enforce policy prohibiting use of e-mail for personal purposes, including union activities
    - But watch out for past practices

Social Media/E-Publishing Liability: Public Employee Rights

- Employee use of personal social media
  - Employee can be disciplined for union website posting comparing supervisors to Nazis. *Curran v. Cousins* (1st Cir. 2007)
  - Police officer can be disciplined for posting sexually explicit materials on personal website. *Dible v. City of Chandler* (9th Cir. 2008)
  - Municipality liable to employee who was fired after expressing anger in Facebook posting over firing of co-workers who had supported boss' opponent in election. No qualified immunity. *Mattingly v. Milligan* (E.D. Ark.,11/1/11)

Social Media/E-Publishing Liability: Public Employee Rights

- Employee use of personal social media (cont.)
  - Sheriff was not liable for firing employee who “liked” his opponent in election. “Liking” not sufficiently substantive to have First Amendment protection. *Bland v. Roberts* (E.D.Va., 4/24/12)
  - Police officer denied promotion due to Facebook comments about favorable treatment for superior officer’s nephew was not entitled to First Amendment protection because comment endangered discipline in department. *Gresham v. City of Atlanta* (N.D.Ga. 5/7/12)

Social Media/E-Publishing Liability: Freedom of Information Issues

- Identities of persons to whom publicly-owned computer have been issued and records of websites visited on must be disclosed
- Content of e-mails may be exempt, depending on its substance
  - Usual rules for exemptions apply

Social Media/E-Publishing Liability: Open Meetings Issues

- Blogs or chats involving quorum of public body?
  - “Communications on the city's Facebook page regarding city business by city commissioners may be subject to Florida's Government in the Sunshine Law, section 286.011, Florida Statutes. Thus, members of a city board or commission must not engage on the city's Facebook page in an exchange or discussion of matters that foreseeably will come before the board or commission for official action.” Fla. Att'y Gen. Op. 2009-19 (2009)

Social Media/E-Publishing Liability: Containment and Risk Management

- Awareness of e-publishing
- Social media policy
  - Conflict with individual free speech rights?
  - Clarity about who “owns” content
  - Consider realistic enforcement
- Training

Steps to Minimize Social Media/E-Publishing Risks

- Develop and implement a social media policy
- Explain impact on of posting and emailing
- Specify how/when publishing is permitted
- Balance publication policy with free speech rights

Social Media/E-Publishing Liability: Local Government Policies

- Examples
  - http://www.seattle.gov/pan/SocialMediaPolicy.htm
  - http://www.mrsc.org/policyprocedures/m58vasocmed.pdf
  - http://www.fairfaxcounty.gov/opa/getfairfax/facebook-comments-policy.htm
  - http://www.nyc.gov/html/misc/html/social_media_policy.html
  - http://cams.ocgov.com/Web_Publisher/Agenda05_18_2010_files/images/O00610-000108A.PDF

(These policies are provided as examples only and are not endorsed by Wilson Elser.)

Breaches of Sensitive Information

- HIPAA HITECH Act = obliged to protect Protected Health Information ("PHI")
- Laws of 46 States = obliged to protect Personally Identifiable Information ("PII")
- Consumer protection/deceptive trade practices
- Breach of contract
- Negligence/fraud

What is the leading cause of data breaches?

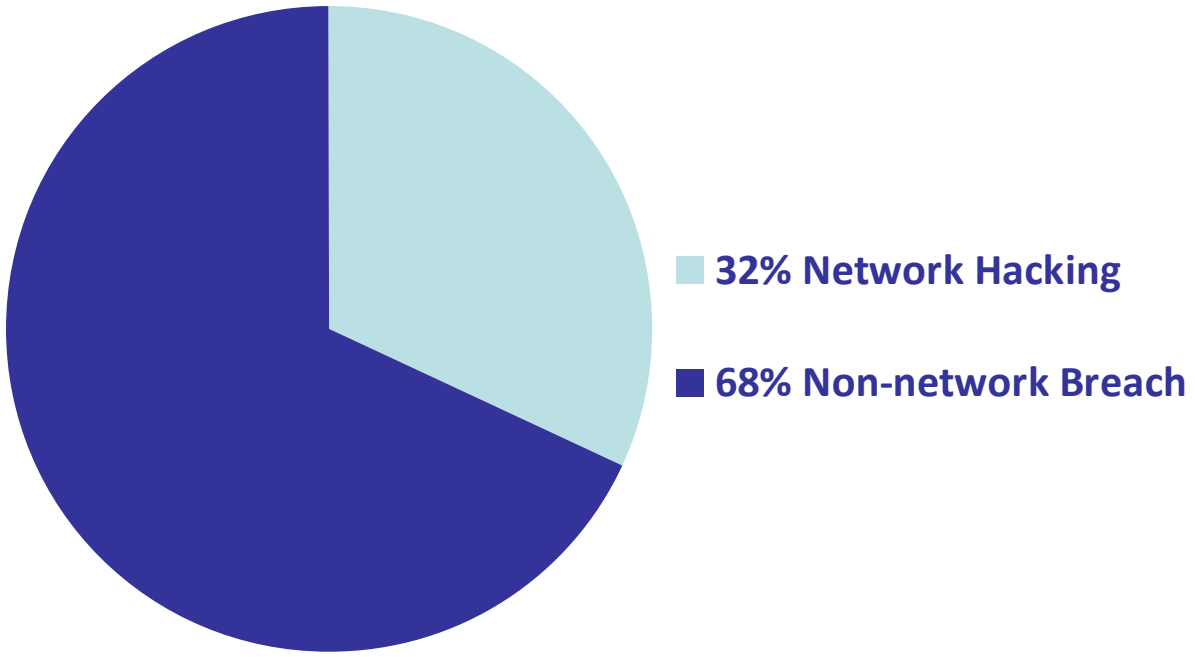
- **Network hacking**

  OR

- **Non-network breach**

What is the leading cause of data breaches?

- **68% of breaches DO NOT INVOLVE NETWORK BREACH**



Data Breaches: Frequency

- Question isn't IF, but WHEN
- Office break in
- Laptop/iPad/mobile device lost or stolen
- Paper document lost/inappropriate disposal
- Mailing error

Data Breaches: Severity

- Key is number of impacted individuals
- SQL (programming language) injection attacks
- Botnets
- Social engineering
- Peer-to-Peer networks
- Employee/former employee/vendor

Liability for a Vendor's Breach

- 30- 40% of all breaches are caused by a vendor for which another entity is vicariously liable.
- Who has access to sensitive information?
  - Off-site storage facility
  - Disaster recovery back up tapes/archives
  - Mail room/courier/photocopy/shredding/service
  - Cleaning service
  - Payroll/benefits provider

How Much Does a Breach Response Cost?

- **Tangible Costs**
  - Legal Fees $$$
  - Public Notification $$$
  - Public Relations $$$
  - Credit Monitoring $$$
  - Customer Reimbursement $$$
  - Forensic Investigation $$$
  - **Total** **$$$$$$$**

How Much Does a Breach Response Cost?

- **Intangible Costs**
  - Lost community goodwill/trust
  - Reduced future revenues
  - Drain on employees and operations

HIPAA HITECH Compliance

- Penalties are being assessed
- Most frequent HIPAA privacy compliance issues:
  - Impermissible uses/disclosures of PHI
  - Lack of safeguards of PHI

FTC Consent Orders generally require:

- No future misrepresentations of safeguards
- Maintain comprehensive security program approved by FTC
- Design, implement and regularly test safeguards
- Controls on 3d party custodians—includes contractual provisions
- Continuous future evaluation of exposures and adjustment of controls in response

FTC Consent Order Generally Requires

- For 20 years:
  - Initial and biennial assessments by independent auditors
  - FTC to approve audit firms and audit results
- For 5 years:
  - Obligation to “self incriminate” by providing FTC with documents including internal memos that could indicate potential non-compliance with consent order
- For 3 years:
  - Furnish FTC with full details on assessments
- Upon FTC demand:
  - Provide consent order compliance report

Litigation of Cyber Exposures: Common Causes of Action

- Breach of Contract
  - Failure to maintain confidentiality in accordance with privacy policy
- Negligence
  - Failure to meet the standard of care
  - Caused plaintiff's damage
    - Recovery: Compensatory damages
- Fraud
  - Deceived plaintiff
  - Deception caused plaintiff's damage
    - Recovery: Compensatory damages

Litigation of Cyber Exposures: Common Causes of Action

- Deceptive/Unfair Trade Practice

  Business Practice [e.g. web page] deceived plaintiff

  Deception caused damage to plaintiff

  Recovery: Treble compensatory damages and attorney's fees

- Punitive Damages

  Reprehensible conduct [gross negligence to malice]

  Compensatory damages awarded

  Recovery: Additional amount to punish wrongdoing and deter others

Why are municipalities breach targets?

- Data rich operations
- Municipality is service-focused, not data-focused
- Officials/employees are mobile
- IT outsourced or funding limited
  - “My Cousin Vinny” problem
  - Cloud computing

Why are municipalities data breach targets?

- Botnets make it profitable for cyber criminals to target small operations
- Large numbers of interconnected computers, generally including zombies:
  - Obtain system access
  - Seek marketable data
  - Harvest the data
  - Send payload back to criminals

Why are Municipalities Vulnerable to Serious Damage from a Breach?

- Operational vulnerability:
  - Damage to reputation
  - Distraction from core business
  - Fewer employees must carry the burden of handling the breach
  - Responding to a live breach isn’t a good time to learn about breaches!

Why are Municipalities Vulnerable to Serious Damage from a Breach?

- Financial vulnerability, absent breach response insurance:
  - Unplanned, immediate significant cash flow drain
  - Difficulty funding current obligations
  - Impact on bank loan covenants and financing

Breach: Containment and Risk Management

- Develop a breach avoidance and response plan now
  - Information inventory: What sensitive information do you need to keep, where do you keep it, who has access, how do you protect it? Can you prove this is reasonable?
  - Protect PII and PHI: Put a plan in place to keep as little as possible, protect it well, identify ways of spotting possible unauthorized access.

Breach: Containment and Risk Management

- Develop a breach avoidance and response plan now
  - Training: Make sure that everyone knows what to do right away if they think that sensitive information might have been accessed without authority.
  - Vendor management: Know what to do if a vendor with access to your information exposes it?

Prepare and Test the Breach Response Plan

- Speed and accuracy matter!
- Regulatory compliance: Federal regulations, and state statutes
- Protect reputation by communicating well, and addressing concerns fairly
- Good breach response = enhanced reputation; poor response = disaster

Protecting the Bottom Line: Why Cyber Insurance Matters

- Cyber insurance:
  - Protects cash flow and residents
  - Covers e-publishers' liability
  - Includes access to breach response services
  - Provides access to public relations assistance

Protecting the Bottom Line: Why Breach Insurance Matters

- Cyber insurance:
  - Responds to first party breach response costs
  - Ensures that a vendor's promise is backed by an insurance policy that will cover breach response costs and damages
  - Preserves existing insurance limits for "regular" claims

Questions/Comments?

Additional Information…

Robert A. Spolzino, Esq.
Wilson Elser Moskowitz Edelman & Dicker, LLP
Robert.spolzino@wilsonelser.com

ICMA
99TH ANNUAL CONFERENCE
BOSTON
NEW ENGLAND
September 22-25, 2013

ICMA

99TH ANNUAL CONFERENCE

BOSTON

NEW ENGLAND

September 22-25, 2013