



# Cyber Risk

## A Serious Threat Facing Public Entities

by

Mark Greisiger, NetDiligence

John Mullen, Nelson, Levine, deLuca & Horst

Joseph DePaepe, McGriff, Seibels & Williams, Inc.

## Cyber Risk—A Serious Threat Facing Public Entities

*by Mark Greisiger, NetDiligence, John Mullen, Nelson, Levine, deLuca & Horst, and Joseph DePaepe, McGriff, Seibels & Williams, Inc.*

Are you ready for a data breach incident to be publicized to the world? Whether attributed to a malicious attack or a leak due to a staff mistake, it's no exaggeration to say that a data breach within your organization is not a matter of if, but when. A recent Identity Theft Resource Center (ITRC) study reported a 47% increase in data breaches for 2008, and 2009 is shaping up to be just as bad.

The media illuminates this risk constantly. A few examples include:

- **U.S. Veteran Affairs Department settles data breach case:** Under the terms of the settlement, the VA will pay \$20 million.
- **Chicago Board of Elections:** About 100 computer discs with 1.3 million Chicago voters' Social Security numbers were distributed to aldermen and ward committeemen. A class action lawsuit alleges the board violated the Illinois Personal Information Protection Act.
- **Hamilton County (OH) Clerk of Courts:** Identity thieves used a Hamilton County website to steal the Social Security numbers and other personal data of hundreds of Ohio residents, federal authorities said. Over 1.3 million records such as tax documents, medical records and bank account numbers were automatically posted on the Web site if they were part of a criminal or civil case, land dispute, tax lien or traffic ticket.
- **City of Coral Springs, FL:** Their data services provider was compromised. A notice will be sent out nationwide to affected individuals. The data services provider had names, SSNs, driver's license numbers and dates of birth in its database. Data indicates that 12,120 consumers were affected.
- **Downingtown High School West (PA):** A 15 year old student broke into an office and downloaded files on teachers and thousands of district taxpayers. The information included W-2's with SSNs and SSNs on school district taxpayers. The student shared the information with several other students. According to The Daily Local, 16,595 residents were named in the file, which police say contained more than 41,000 adult taxpayers' names and personal information including Social Security numbers, and more than 15,000 students' names and personal information.
- **Greenville County (NC) School District:** They sold computers that contained Social Security numbers and birthdates for roughly 100,000 students and at least 1,000 employees, according to a district official and the buyers' attorney.

Are there really more information security (privacy) breaches today than a decade ago? Or are data breaches simply being reported today whereas a decade ago they were not disclosed? The answers, like the problems, are not simple. Indeed, there probably are more security breaches today than a decade ago – if for no other reason than the growth of information technology, which provides the ability to capture and use more personal information than ever before. As a result, personal data is growing in value. As the value of data grows, the risks increase as well. Threats from hackers, thieves, third-party contractors and employees make it imperative for public entities to implement safeguards. Privacy is now a front-line consumer rights issue.

Because identity theft is one of the fastest growing crimes, various privacy regulations (FACTA, State Notice Laws and the new ARRA or HITECH Act) require that you protect sensitive data ***no matter where it resides***: on the network; on standalone systems such as tax collection, billing, medical, and marketing databases; on remote devices such as laptops; and on paper.

Moreover, there are now industry standards, such as Payment Card Industry Data Security Standard (PCI DSS) that impose harsh penalties for non-compliance. These are being used by plaintiffs' attorneys as standards of due care for security practices.

Unfortunately, even the most compliance- and security-focused organization can be victimized by a data breach. Bigger often means more complex, with more moving parts and more inter-dependencies. The media underscores this point on a weekly basis, with large, well-managed and well-operated public entities reporting breach events. When a breach occurs, systems may need to be shut down, operations interrupted, and public relations campaigns launched. Computer forensic investigators and lawyers often need to be hired. Information assets may need to be restored. If the breach involved credit card information, cardholders, issuing banks, and credit bureaus may need to be notified. Residents and taxpayers may demand credit monitoring services, and more.

Failure to take the necessary measures to secure information, and to mitigate potential loss if measures taken should fail, may result in significant financial costs. When a cyber risk event occurs, the consequences can be financially crippling with the emergence of class-action lawsuits, huge forensic and mitigation costs, possible identity theft damage litigation, and the loss of your public reputation and the trust of your constituents. Although there may be limitations to private rights of action in some, but not all, of the state notification laws and federal data breach laws, there is no general public entity immunity written into FACTA, HIPAA or breach notice laws. State attorneys general, federal attorneys and various federal agencies have authority to mount investigations and seek the enforcement of these laws. Plaintiffs' attorneys are also out there waiting to pounce.

So, what can you do to ensure that your daily municipal/public entity operations are using prudent and reasonable practices to comply with privacy and security policies as well as applicable laws and regulations? Here are six things you can do immediately to improve your security and privacy posture and reduce your overall risk.

**(1) Know your data.**

The first step in protecting personal data is to determine what data exists and whether or not the information is necessary to accomplish the business or government purposes for which it is being collected. Too often, public entities collect and retain personal information – Social Security numbers, birth dates, credit card numbers – even though they are not necessary to accomplish the core service being provided. Your first step should be to ask if particular information is necessary. If it isn't, don't collect it. If the data is necessary, you should document why it is necessary, how you intend to reasonably protect it (and/or mask it), and how long it is needed. Once the information is no longer required for the identified purpose, it should be systematically destroyed.

**(2) Know your public entity.**

Obtain an annual independent, enterprise-wide network security 'e-risk assessment' that evaluates the people, processes and technology underlying your security and privacy posture. An objective, third-party assessment allows you to identify specific vulnerabilities and legal liabilities, so you can focus on hardening security precisely where needed. In other words, it ensures that you spend your security budget on necessities, not luxuries. The assessment should include a third-party penetration test to evaluate whether internet-facing systems are capable of deflecting the known hacker exploits that threaten public entities.

**(3) Know your people.**

Personal information is collected, processed and used throughout many aspects of municipal operations. As such, many people are involved with how consumer information is collected and processed. The same holds true for compliance. There is no one person or position that can achieve full compliance with information security and privacy requirements. Security professionals, IT staff, lawyers, risk managers, township managers, Board members and public relations personnel all have roles and must provide input. Establish cross-disciplinary working groups to address these issues. The members of the group should "translate" their issues and concerns so that others in the group gain an understanding of what needs to be done. Coming at this solely from an IT or legal perspective will not work. It requires leadership from the highest levels in the organization.

**(4) Know your providers.**

You have an obligation to use suppliers and processors that are competent to adequately protect the personally identifiable information of your constituents. This requires that you have a basic knowledge of the capabilities of your providers, how their personnel are trained and what processes

and procedures they have in place to protect your data. Verify, in writing, that the data is either returned or destroyed when it is no longer needed.

Make sure you have attorneys working with security professionals to interpret privacy and security laws and put policies and procedures in place that comply with those laws. Attorneys should also be engaged to address external contractual relationships with service providers, including drafting privacy and security contract terms to establish security controls, incident response, enforcement, monitoring, and transferring risk of loss.

#### **(5) Know the law.**

With the complex patchwork of privacy and security laws that exist in the U.S. (local, state, federal and international law are often at issue), even identifying which laws apply can be difficult. Once applicable laws are identified, they need to be analyzed to see how and where they may impact your public entity. In some cases, it may be possible to find commonalities between privacy and security laws and streamline compliance. Other times, costly remediation may be required to address multiple compliance regimes. While this process can be daunting, it is a prerequisite to achieving a legally compliant entity. It's the classic business challenge: a penny now or a dollar later.

#### **(6) Manage your risks.**

No matter what measures you take or how much you spend on training, network security or physical safeguards, residual risk will always exist. Be aware: your standard general liability insurance coverage does not cover this risk. Consider transferring your remaining risk through network and privacy liability coverage. With this approach, you reduce your overall expense for network security and privacy protection. Remember however, while you may be able to transfer financial risks through the purchase of insurance, you can't transfer the duty to implement and maintain appropriate safeguards and your insurance company will require a baseline of reasonable security.

### **Conclusion**

Public entities that have taken the appropriate measures **before** a breach event occurs will be able to minimize the damage. Only when you implement an ongoing program for data protection can your municipality or agency effectively walk the tightrope between privacy, security and legal risk. A formal **Cyber Risk Assessment** can give you a better understanding of your data security strengths and weaknesses. If the assessment points to residual e-risk exposures (which is normal), you can strengthen your risk posture using traditional risk management practices: eliminate, mitigate, accept or transfer (insure) the risk.

## **About the Authors**

### **Mark Greisiger**

As President of NetDiligence®, a leading cybersecurity assurance-risk assessment services organization, Mark Greisiger is an authority on cybersecurity and network risk for computer-dependent businesses, government agencies and financial institutions. NetDiligence services are engaged by the majority of US & UK insurers in the privacy liability insurance industry. Mark is a member of FBI Infragard (Philadelphia Chapter) and a frequent contributor to various insurance industry magazines. He speaks regularly at industry events, including the 2005 ABA Risk Management Forum, PLUS 2006 & 2007, RIMS 2007 & 2008 and the Advanced Forum on Cyber Risk Insurance. You can contact Mark at [mark.greisiger@netdiligence.com](mailto:mark.greisiger@netdiligence.com).

### **John Mullen**

John F. Mullen leads Nelson, Levine, deLuca & Horst's Complex Litigation Practice Group with a focus on defense of security and privacy data breach events. John practices nationally, currently handling litigation in Pennsylvania, New York, New Jersey, West Virginia, Delaware, Virginia, North and South Carolina, Florida and Georgia. He also speaks and authors articles regarding privacy, data loss and breached security throughout the United States and has been published on cyber/data loss issues in BEST's Review. John's cyber response team includes 8 partners with an average of 18 years of litigation experience in complex class action and MDL matters. You can contact John at [jmullen@nldhlaw.com](mailto:jmullen@nldhlaw.com).

### **Joseph DePaepe**

Joseph DePaepe CPCU, CIC is Senior Vice President at McGriff, Seibels & Williams of Oregon. For the past eighteen years, Joe has been working with public entity risk on a national level, and has involved himself in all lines of coverage through the development and management of Alternative Risk Solutions for public entity clients. You can contact Joe at [JDePaepe@McGriff.com](mailto:JDePaepe@McGriff.com).