Cyber Risk Remains a Serious Threat Facing Public Entities

By: *Mark Greisiger, NetDiligence®*
Theodore J. Kobus III, Esquire, Baker & Hostetler LLP

Given the large amount of personal information in its possession regarding its citizens, a public entity is a perfect target for a cyber event–any event that allows for the release of confidential and/or sensitive personal information. Public entities commonly store personally identifiable information, including Social Security numbers, addresses and driver's license numbers. A public entity may also store confidential and sensitive personal medical and health information of its citizens and employees. Data breaches affecting public entities are not inconsequential. Not only do these incidents have a financial impact, but they can also lead to public relations nightmares for the public entity. Consider two recent cyber events affecting Utah in March of 2012 and Texas in April of 2011.

Utah

On March 30, 2012, hackers believed to be operating out of Eastern Europe broke into the Medicaid server at the Utah Department of Health. The hackers exploited a default password on the user authentication layer of the system, allowing the hackers to bypass multiple network, perimeter and application level security controls. While 99% of the state's data is behind two firewalls, the affected data on the Medicaid server was not encrypted and did not have hardened passwords. The state's investigation revealed that the Medicaid server appeared to have been rolled out without following the state's own information security protocols. State officials have reported that there has been no known misuse of the data disclosed.

While 99% of the state's data is behind two firewalls, the affected data on the Medicaid server was not encrypted and did not have hardened passwords.

Initially, state officials believed that about 24,000 health claims records containing patient names, Social Security numbers, birth dates, addresses, tax identification numbers and treatment codes were exposed. Less than a week later, state officials reported that 500,000 (18%) of the state's 2.8 million residents, including children, had their health data compromised. In addition, another 280,000 residents (10%) had their Social Security numbers breached. Immediately after the incident, affected Utah citizens were notified and those with exposed Social Security numbers were offered free credit monitoring and identity theft insurance of up to $1 million. Since the incident, the executive director of Utah's Department of Technology Services has resigned, Utah has launched IRIS: Identity Theft Reporting Information System, and a new state position–Data Security Ombudsman–has been created to help any Utah citizen affected by the data breach.

Texas

In April of 2011, the Texas comptroller's office notified Texas citizens regarding a breach exposing 3.5 million records. In this incident, personal data was posted to a public server where it was available, in some cases, for over a year. Of the breached records, 1.2 million, posted in January of 2010, belonged to education employees and retirees from the Teacher Retirement System of Texas. Also, 2 million records from the Texas Workforce Commission, which provides unemployment benefits, were posted in April of 2010. The remaining 281,000 records were from the Employees Retirement System of Texas, belonging to state employees and retirees, which were posted in May 2010. The data was supposed to be transferred per statute by the agencies and used internally at the comptroller's office as part of the unclaimed property verification system. The information affected included names, mailing addresses, Social Security numbers, and in some cases, dates of birth and driver's license numbers. The state's investigation revealed that the data was not encrypted, even though Texas administrative rules require encryption of data files containing sensitive information. State officials also reported that there has been no known misuse of the data disclosed.

The state's investigation revealed that the data was not encrypted, even though Texas administrative rules require encryption of data files containing sensitive information.

As soon as the disclosure was discovered, the state sealed off public access and the data was moved to a secure location. In response to the incident, the Texas attorney general and the FBI launched a criminal investigation.

What can a public entity learn from past cyber events?

As personal data grows in value, the risk of a cyber event to any organization–private or public–grows in value as well. The news covers security breaches affecting entities on a daily basis. Privacy is a front-line consumer rights issue for private and public entities alike. Here are a few things a public entity can do to improve its security and privacy posture, thereby reducing its risk overall.

1. Know the rules.

Numerous privacy regulations and guidelines (e.g., FACTA, state data protection laws, HITECH, the Payment Card Industry Data Security Standard, Red Flag Rules, Safeguard Rules) require the protection of personally identifiable information regardless of where it resides. This includes data that is at rest, in transit, on a network, on a standalone system, on a remote device such as a laptop or thumb drive, and on paper. Identify the applicable laws and guidelines and determine how and where they may impact your entity. Being legally compliant will minimize the risk to your entity in the event of a cyber event.

2. Know your exposure.

A first step in protecting your data is to determine what data exists and whether or not the data is needed. Superfluous data should not be collected. If the data is necessary, determine how to protect the information. Conduct an internal or external third-party review of your computer system security. Also, determine how long the information is needed. Do you still have data from the 80s? You likely do not need it. Once you have determined your potential exposure, determine how to decrease your risk. The largest breaches typically occur due to forgotten data.

3. Know your employees.

Unfortunately, even the most compliant and security-focused organization can fall victim to a data breach. In fact, the most common cause of a cyber event today is not hacking, but simple human error. Full compliance requires buy-in from every public entity employee. Most data breaches involve confidential information stored outside the network system on laptops, smartphones, thumb drives, etc. Educate your employees regarding your state's statutes protecting personal information. Train your employees on your entity's policies and procedures for safeguarding personal information. **Note that your state's sovereign immunity laws may not deflect liability for a cyber event, including an event caused by an employee within his/her duties.**

4. Know your public entity's network security risk.

Annually, obtain an enterprise-wide network security risk assessment that analyzes the people, processes and technology underlying your security and privacy posture. Allowing a third party to identify specific vulnerabilities and legal liabilities allows your entity to focus on the risks that need to be minimized. Considering the budgetary restraints that affect a public entity, a risk assessment will help you focus funds where they are most needed.

5. Know your business partners.

Not only do you have an obligation to protect your state's data, you also have the obligation to employ business partners that adequately protect the personally identifiable information of your state's citizens. Inquire as to your business partners' policies and procedures for safeguarding of personal information. Ask how their employees are trained regarding data protection. Most importantly, after completion of an engagement, verify with your business partner that data is returned or destroyed.

6. Manage your risks.

Your public entity's general liability insurance usually provides for "bodily injury" and "property damage." Property damage is often defined as physical injury to tangible property, including the loss of use of property. Case law differs by state as to whether electronic data is tangible property. Therefore, be aware that your standard general liability insurance coverage does not typically cover a cyber event. A cyber policy may be a good idea–but remember that transferring your entity's financial risk does not transfer your duty to implement and maintain appropriate safeguards for protecting your citizens' information. Below are a few things to look for in a cyber policy:

Your standard general liability insurance coverage does not typically cover a cyber event.

- Coverage for forensic analysis following a breach;
- Coverage for breach review, analysis and response by a law firm;
- Coverage for credit monitoring for affected individuals, if needed;
- Coverage for expenses for vendors associated with notifying individuals;
- Coverage for call center support.

What can I do now?

Be proactive in protecting your public entity's image, and more importantly, protect your citizens. Know that a cyber event will happen. The only question that remains is when. Public entities that have taken the appropriate measures before a cyber event occurs are better equipped to minimize the damage that may result. Review your policies and procedures for safeguarding personal information; train your employees regarding those policies and procedures. Determine where exposure exists and decrease the associated risks. Your citizens trust you with their personal information. You must ensure that it is protected.

Public entities that have taken the appropriate measures before a cyber event occurs are better equipped to minimize the damage that may result.

NetDiligence®
Cyber Risk Assessment & Data Breach Services

Mark Greisiger is the President of NetDiligence® which provides cyber risk assessment services for Risk Managers to help them better understand if their organization deploys reasonable & prudent security and privacy safeguards in an effort to mitigate data breach loss & liability risk. Since 2001 NetDiligence services have been utilized (and often required) by the majority of insurers in US & UK that offer privacy/cyber liability insurance products, providing loss control & crisis response services for their insured business clients. Prior to starting NetDiligence Mark worked for over a decade in the insurance industry where he developed and was an underwriter for an early 'hacker insurance' product. Mark is a frequent contributor to various insurance & risk management publications on similar topics.

You may contact Mark at
mark.greisiger@netdiligence.com

Baker Hostetler

Ted Kobus is a partner in the New York office of Baker & Hostetler LLP and is National Co-Leader of the Privacy, Security & Social Media Team. Ted advises clients, trade groups and organizations regarding data security and privacy risk management, breaches, response strategies, litigation and regulatory actions affecting businesses and government entities. He has counseled clients involved in significant breaches implicating state and federal laws, international laws and other regulations and requirements. He regularly deals with the Offices of Attorneys General, state insurance departments, Office of Civil Rights (OCR)/Health and Human Services (HHS), Secret Service, FBI and local police and forensics professionals as part of handling of data breaches.

You may contact Ted at
tkobus@bakerlaw.com