Hearing Memo

Getting it Right on Data Breach and Notification Legislation in the 114th Congress

Senate Commerce Committee, Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

Thursday, February 5, 2015

Witnesses

Ms. Cheri F. McGuire
Vice President, Global Government Affairs & Cybersecurity Policy
Symantec Corporation

Mr. Mallory Duncan
Senior Vice President and General Counsel
National Retail Federation

Dr. Ravi Pendse
Chief Information Officer
Brown University

Ms. Yael Weinman
Vice President for Global Privacy and General Counsel
Information Technology Industry Council

Mr. Doug Johnson
Senior Vice President and Senior Advisor for Risk Management Policy
American Bankers Association

The Honorable Lisa Madigan
Attorney General
State of Illinois

Witness Testimony

McGuire

Last year, nearly 60% of data breaches were caused by network intrusions by unauthorized users. There is a lack of basic cyber hygiene. Basic hygiene is the most cost-effective first step.

In addition to the NIST framework, there is also the Online Trust Alliance Data Protection & Readiness Guidelines.

3 principles that should be applied to data breach notification:

1. The scope of any legislation should apply equally to all entities that collect and maintain records containing sensitive information
2. Implementing pre-breach security measures should be central to any legislation
3. Encryption or other security measures that render data unreadable/unusable at rest or in transit should be a key element to establish a risk-based threshold for notification

Duncan

3 principles for data breach legislation:

1. Uniform notice
2. Express preemption – must be real preemption, otherwise federal law just becomes the 52nd law
3. Strong consensus law – notice should be the same for all entities

Pendse

A single national breach notification law is very important. A hard time limit may be unattainable, but a tiered approach based on size and complexity of the organization may be more attainable.

Johnson

1. We need a national data breach standard. Consumers of banking products are not confined by state borders. Should preempt state laws.
2. A new federal law must recognize existing federal breach notification laws.
3. There must be a strong national data protection requirement. The cost should be borne by the entity that sustains the breach.

Madigan

Any definition of Personally Protected Information must be broad and should be updated by the FTC in response to new threats. Entities too often fail to take basic security measures. A federal breach notification law should establish threshold security requirements. An entity that sustains a breach should not be allowed to undergo a self-serving "harm analysis" to determine whether consumers are notified of the breach. Congress should designate a federal entity to investigate large breaches. She opposes legislation that limits states' abilities to protect consumers.

Weinman

ITI supports 3 principles:

1. Federal breach notification that preempts the state.
2. Timing that is flexible, not prescribed. Pre-mature notification could subject organizations to further attack, might interfere with law enforcement efforts to identify intruders, and yield inaccurate/incomplete information to consumers.
3. Notification should be made to consumers if they're at significant risk of identity theft or financial harm. Theft of unreadable information, for example, does not warrant notification.

<u>Senators' Q&A</u>

Senator Jerry Moran (R-KS) asked if there is a way to pre-empt state law but have states involved in the enforcement of national data breach laws. He noted that AG Madigan is in the minority on the panel in her view of state preemption.

Madigan: Yes. This happens with many different laws, even criminal investigations. I appreciate the concern with the multiple breach laws, but it is somewhat over-blown.

Have any state laws been able to discourage or prevent data breaches? Have any encouraged or incentivized greater security?

Duncan, Johnson: No

Is there developing insurance coverage for data breach?

Johnson: Yes. It's maturing. We have a captive that offers those coverages. We're working with Treasury and trying to figure out how to improve the market and use that has a private incentive.

Senator Richard Blumenthal (D-CT) asked AG Madigan if the experience with narrow federal preemption has been horrible?

Madigan: the concern is that states want to retain the right to respond and protect their citizens.

Senator Blumenthal is troubled that some major retailers have moved to block new, more secure technologies. He's also surprised that the NRF supports preemption of common law, which seems very extreme…more broad than this committee should consider.

Duncan: They are taking it very seriously even at the board level. Some new technologies are unproven, or extraordinarily expensive. But retailers are taking this seriously.

Senator Blumenthal was surprised the NRF is recommending preemption of not only state statutory law, but also common law. This seems extraordinary and unprecedented and broader than this committee should consider.

Senator Deb Fischer (R-NE) asked about foreign governments that require companies to turn over their intellectual property, including source code. How prevalent is that?

McGuire: Symantec is concerned about having to share their IP with anyone. There is a growth in these types of requests.

Senator Fischer asked if it would be better for consumers and businesses if we applied a more uniform regime so that enforcement is based on the sensitivity of information that is being collected.

McGuire: Symantec supports a risk-based application and threshold for what type of data is breached.

Senator Fischer asked about sector-specific requirements.

Weinman: they could be helpful – that it might be easier for Congress to complete breach notification legislation if entities that are already subject to data breach notifications had their requirements remain intact.

Duncan: that would be anathema to the complete protection we need.

Senator Brian Schatz (D-HI) asked who determines when there is need for notification? Where are the standards held?

Weinman: the standards should be codified, but the breached entity makes the determination.

Madigan: there is no over-notification going on at this point.

Senator Schatz asked what state laws would be a strong enough standard to justify preemption.

Madigan: California is a high mark. Texas, Florida, Indiana have some of the most progressive notification laws in the country.

Johnson: Gramm Leach Bliley

Senator Roy Blunt (R-MO) asked about the timeline for notification. He tends to be of the mind that there shouldn't be an arbitrary deadline. He has concerns that "reasonable" could lead to time in court trying to figure out what is reasonable.

Weinman: a number of states do not have a hard deadline and that would be most appropriate. We often hear the phrase "without unreasonable delay." You would look at what the company did leading up to the notification – if they dotted all their I's, listened to law enforcement, etc.

McGuire: depends on the type of breach and the type/size of the organization. If the data is encrypted and unusable, it should haven't to be reported.

Madigan: that is how Illinois' law is currently structured.

Senator John Thune (R-SD) asked why a single federal law is preferable for both consumers and companies?

Weinman: the vast differences among the state laws.

Senator Thune asked Mr. Duncan if the NRF could support any security requirement, like the FTC has, since their members are already subject to those from the FTC.

Duncan: Yes, if it's comparable to the standard the FTC is already enforcing, which is reasonable security standards, and if it's coupled with robust notice requirements.

Senator Amy Klobuchar (D-MN) asked if the Anthem breach would be covered by HIPAA? How do the states coordinate with HHS and other federal agencies?

Madigan: since Anthem claims medical information was not breached, it will probably fall under the various state laws to see if PII was breached. States coordinate with FTC, but haven't had as much interaction with other agencies responsible for health information. Coordination helps everyone especially when we have limited resources.

Senator Klobuchar talked about chip-n-pin technology and noted that after the Home Depot breach, Canadian cards with chip and pin technology were less valuable on the black market.

Duncan: only 25% of the industry is there right now. A significant percentage of the industry will take it up by October, but it doesn't work if the banks only move to pin and signature cards, because the signatures don't provide security.

Johnson: debit cards already have pins. In the credit card environment, consumers prefer to use the signature – otherwise, they'd use their debit card. What really needs to happen is that we need to move away from static numbers, ie: tokenization.

Senator Steve Daines (R-MT) asked what is an appropriate notification time period? When he worked in customer service, they notified customers of a problem as soon as it was discovered. He was disappointed to find that we're considering 30 days. He had an amendment to a House bill last year that required notification within 2 days.

Madigan: flexible is good, but it shouldn't be months. Illinois has seen their "reasonable" requirement abused.

Duncan: you have to make sure law enforcement has time to act, catch the bad guys, companies have time to patch the holes, that they have accurate information (don't notify people and then find their information actually wasn't stolen), etc.

Chairman Moran asked panelists to provide more information on how small businesses are affected and any additional thoughts on how Gramm Leach Bliley and/or HIPAA could provide common ground and be models for new legislation.

Duncan: pointed out that Gramm Leach Bliley provides *guidance* ("should", not "shall") and the states have *mandates* and requirements. A federal law should be a mandate and a requirement.