Cybersecurity: Emerging Exposures for Technology Companies

October 7, 2010
Your panelists

David Allred, Head of the Technology Segment for North America Commercial at Zurich

 Liesyl Franz, Vice President for Information Security and Global Public Policy at TechAmerica
Overview of Today’s Discussion

- Current laws and regulations: U.S. and international
- Emerging legislation and its potential impact
- Exposures to technology companies
- Risk management techniques to mitigate those exposures
- What to look for in choosing the right insurance coverage
“Take action against the vendor”

Attorney Susan Lessack

“Hacked! Limiting employer liability for breached of employee data.,” Business Management Daily (businessmanagementdaily.com, Sept. 29, 2009)
A Complex And More Demanding Regulatory Environment

Industry-specific legislation
- 1996 – Health Insurance Portability and Accountability Act (HIPAA) – Health care providers
- 1999 – Gramm-Leach-Bliley Act (GLBA) – financial records/reporting

State legislation – breach reporting
- 2003 – California Senate Bill 1386 (CA SB 1386)
- Subsequent state legislation (currently 44 states)

Federal Trade Commission
- Red flag rule – August 1, 2009 – anyone who “grants” credit

American Recovery and Reinvestment Act (ARRA)
- Includes Health Information Technology for Economic and Clinical Health Act (HITECH Act) - 2009
  - Broadens scope of HIPAA compliance to include more ‘business associates”
  - Subtitle D addresses privacy and security concerns associated with the electronic transmission of information

Doing Business Outside U.S.
Stringent privacy and data security laws

- Personal information cannot be collected without consumer permission, and consumers have the right to review the data and correct inaccuracies
- Companies that process data must register their activities with the government
- Employers cannot read workers’ private email
- Personal information cannot be shared by companies or across borders without the express permission from the subject of the data
Go Forward View: Emerging Laws and Regulations
Congress

National Cybersecurity

- S. 3480 – The Protecting Cyberspace as a National Asset Act (Sens. Lieberman/Collins/Carper)
- S. 773 – The Cybersecurity Act (Sens. Rockefeller/Snowe)

Regulatory Framework

- Designation of “Covered Critical Infrastructure” (and downstream implications for IT, Comms, and other providers)
- Identification and evaluation of cyber vulnerabilities to CCI – and promulgation of regulations by DHS regarding security measures
- Direction and/or approval of emergency measures by DHS upon Presidential declaration of cyber emergency (with some liability protection)
- Annual certification of compliance
- Information sharing
- Study on global supply chain security with impact on Federal Acquisition Requirements
Security and Data Breach

- S. 3742 – Data Security and Breach Notification Act (Sen. Pryor)

Regulatory framework:
- Conditions for notification of data breach by all organizations
- Pre-empts state laws
- Enforcement by Federal Trade Commission for unfair or deceptive acts; enforcement by State Attorneys General for harm to citizens
- Safe harbor from notification requirements for preventative security measures that render data unreadable, unusable, and indecipherable
Administration Activities

- National Strategy for Trusted Identities in Cyber Space (NSTIC)
- Global Supply Chain Security
- Department of Commerce – Internet Task Force
  - Privacy
  - Cybersecurity
  - Intellectual Property Protection
- National Institute for Standards and Technology
  - FISMA compliance
  - Risk management
  - Smart Grid
- Department of Health and Human Services
Liabilities for Tech Companies
The Cybersecurity Landscape

- **Who will be a target for lawsuits:** software developers, system integrators, system outsourcing firms, data storage and retrieval companies, systems security developers, system security consultants and auditors

- **Security and privacy risks go beyond data breaches:** Industrial attacks, sabotage, corruption of a system or network

- **Cloud computing** is growing
  - lower infrastructure costs
  - real-time scalability for users
  - results greater security risks

Purchasers of technology products and services are increasingly seeking ways to contractually limit their liabilities and define technology vendors’ responsibilities for data breaches
Two Root Causes Of Breaches

Technical
- Failure of firewalls
- Improper system setup and maintenance
- Password authentication protocol failure
- Hacking
- Lack of encryption
- Loss of paper files

Human (social engineering)
- Poor passwords
- Failure to protect passwords
- Physical security of premises and equipment
- Failure to secure paper records
- Improper disposal of records
- Intentional acts
Potential Loss Scenarios Caused By Failure Of Your Product/Service

Theft/misuse of customer personal information

Transmission of malicious code
- Cost to remediate security vulnerability
- Cost to investigate event
- Liability to customers and other third parties

Sabotage, defacement and vandalism
- Cost to remediate website and other content
- Hourly income while offline
- Liability to third parties for inappropriate content

Denial of service attacks
- Lost income due to a network interruption
- Extra expense to restore the network
- Cost to remediate website and other content

Online extortion
- Cost to remediate security vulnerability
- Cost to investigate event
- Extortion demand
Potential Indirect Loss Potential Of Breaches

- Reputational damage
- Crisis management costs to restore reputation
- Costs of notification
- Legal liability and breach mitigation costs
“Take action against the vendor”

Attorney Susan Lessack

Litigation: Real And Potential

- Lawsuit: Crawfish Town USA, et al v Computer World and Radiant Systems -- filed March 2009 in Lafayette, La
- Lawsuit: June, 2005, CardSystems Solutions - $16 million

Other examples of vendors implicated in customer data breaches:

- Health Insurer, WellPoint claimed that a failed security update performed by a third-party vendor was responsible for a data breach
- Enterprise software solutions vendor HummingBird Ltd lost a piece of equipment belonging to Texas Guaranteed Student Loan Corp, containing unencrypted personal information
- An undisclosed number of Chase customers were sent notification letters after a vendor lost a tape containing sensitive information
- Hackers disabled an e-mail notification service, enabling them to transfer $465,000 from a business bank account.
Risk Management and Insurance
Risk Management: Looking Beyond Insurance

- Enterprise Risk Management (ERM) – competitive, legal, financial, reputation

- C-suite support
  - Brand protection
  - Hiring practices
  - Product/service implementation
Risk Management: Looking Beyond Insurance

- **Security**
  - Designed into the product, not “add-on”
  - Clear responsibility for security portion of product
  - Formal product development process followed, including QA/QC documentation

- **Contractual controls**
  - Clearly delineate responsibilities between developer, implementer and user
  - Define checks on process with documentation

- **Implementation**
  - Who does it vendor or client
  - Clear instructions on implementation – integration with other systems
  - Configuration
  - Migration of data from old system
Risk Management – Looking Beyond Insurance

If SAAS, Host, Cloud…

- Network controls
  - Storage and transmission of data
  - Application and operating system backups
  - Separation of data for customers – virtual as well as physical

- Human controls
  - Background checks (criminal, finance)
  - Drug testing
  - Social engineering training
  - Use of passwords, storage practices, mobile

- Physical security
  - Facility
  - Data

- Data retention strategy
Insurance: What To Look For In Cyber Liability Coverage

- Does coverage respond to “failure of your product/service” as well as "loss of your data"?
- Is a data breach event clearly defined?
- Does it cover loss of business information as well as personal information?
- Will it respond to a regulatory action as well as litigation by customers?
- Will it protect the company if the breach is caused by a “rogue” employee?
- Will it respond to an employee suit against the company (HR information)?
- How does it work in conjunction with your E & O and GL policies?
Questions and Answers

David Allred
david.allred@zurichna.com
www.techinsurance.zurichna.com

 Liesyl Franz
liesyl.franz@techamerica.org
www.techamerica.org
Contact Information

David Allred
david.allred@zurichna.com
www.techinsurance.zurichna.com

 Liesyl Franz
liesyl.franz@techamerica.org
www.techamerica.org
The information in this presentation was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute legal advice and accordingly, you should consult with your own attorneys when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.