Cyber Risks and Insurance: Understanding the Exposure, Knowing the Coverage and Limiting the Risk

Moderator:

Jeffrey J. Vita
Saxe Doernberger & Vita, P.C.

CBA Annual Meeting
June 17, 2013
What Is Information Security?

To ensure protection against unauthorized access to or use of confidential information.

To ensure the accuracy and completeness of information to protect company business processes.

To ensure that information and vital services are accessible for use when required.
Threats to Information Security

- Hacker, Insider, Competition, Lost Device/information
- Natural Disaster, Power Outage, Denial of Service, System Crash, Lost Device
- Hacker, Insider, Competition
Who Is Responsible?

**External Agents (98%)**
- Organized crime
- Nation States
- Political Activists (hacktivists)
- Corporate Spies
- Rogue Hackers

**Insiders (4%)**
- Disgruntled
- Careless
- Accidental
- Money motivated
- Well intentioned

Verizon DBIR 2012
## How Do They Do It?

<table>
<thead>
<tr>
<th>External Agents</th>
<th>Insiders</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Technical Attacks</td>
<td>• Inadvertent (Oops)</td>
</tr>
<tr>
<td>• Malware / Spyware / Scareware</td>
<td>• Insecure communication (Email)</td>
</tr>
<tr>
<td>• Exploitation of vulnerabilities in configurations or code (hacking)</td>
<td>• Lost equipment</td>
</tr>
<tr>
<td>• Botnets</td>
<td>• Laptops</td>
</tr>
<tr>
<td>• Social Engineering</td>
<td>• USB Drives</td>
</tr>
<tr>
<td>• Removable Media</td>
<td>• Paper</td>
</tr>
<tr>
<td>• Email / Phishing</td>
<td>• Tapes</td>
</tr>
<tr>
<td>• Physical Theft or Loss</td>
<td></td>
</tr>
</tbody>
</table>
Why Do They Do It?

- Financial gain
- Political statement
- Lack of awareness
- Circumvent policies
- State-sponsored espionage
- Personal vendetta
- Bragging rights
<table>
<thead>
<tr>
<th>Organizational Size (By # of Employees)</th>
<th>Number of Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 10</td>
<td>42</td>
</tr>
<tr>
<td>11 - 100</td>
<td>570</td>
</tr>
<tr>
<td>101 - 1,000</td>
<td>48</td>
</tr>
<tr>
<td>1,001 - 10,000</td>
<td>27</td>
</tr>
<tr>
<td>10,001 - 100,000</td>
<td>23</td>
</tr>
<tr>
<td>Over 100,000</td>
<td>10</td>
</tr>
<tr>
<td>Unknown</td>
<td>135</td>
</tr>
</tbody>
</table>
How Do You Know?

- Someone will tell you

- Know what is normal or expected
  - Financial Account Activity
  - Data Access
  - Network Activity

- 85% of breaches took weeks or more to discover
- 92% of incidents were discovered by a third part
What Should You Be Doing?

• Implement and update security policies
• Conduct effective security awareness training
• Establish base-level controls
• Get an independent assessment done
• Form an incident response team
• Know where your sensitive data is located
• Insist on senior management active involvement

• 97% of 2012 breaches were avoidable through simple or intermediate controls
Base-Level Technical Controls

1. Strong password policy
2. Account lockout policies
3. Anti-virus protection
4. Comprehensive patch management
5. 2-factor authentication for remote access
6. Encryption for removable media and mobile devices
7. Business-class wireless authentication
Initial Matters

- Response is not a substitute for preparation
- Pre-breach assessment
- Policies and Procedures
- Incident/breach team identified and trained
- Not just about e-data – paper, own IP
- Due diligence on business partners and vendors
What Standards Apply

• Federal Law – HIPAA, HITECH, GLBA, SEC Guidance
• State – wide variance in treatment
• Industry specific – insurance, banking, utilities
• Contracts
• EU
Crisis Management

- Mobilize response team of legal, forensics, broker/insurer, PR
- Seal the breach
- Immediate investigation/interviews
- Coordinate through counsel - privilege
• Required or advisable
  • Government authorities
  • Insurers – work with broker
  • Business partners – contracts, vendor agreements
  • Individuals – 46 states (DC, PR, USVI) have notification statutes - consider a vendor
  • Public at large

• Credit monitoring
Business Interruption

- Restoration – hardware/data
- Loss of Income
- Supply chain or other interruption
- Extra expenses
Regulatory Issues

- Notice
- CT AG
- Fines & Penalties
- Redress Fund
Legal Liability & Reputation

- Private Suits – standing
- Class/Mass Actions
- Customers/Vendors
- Insurer Requirements – notice, cooperation
- Reputational damage
- Is someone else responsible?
- Are you responsible for others’ losses?
Cyberspace Under Siege

Law firms are likely targets for attacks seeking to steal information off computer systems

Andy V. Sabett remembers some years ago when a law firm installed glass-breakage sensors on the windows of its 43rd-floor conference room, where documents often were compiled for big cases. The firm wanted to guard against the possibility that someone would rappel from the skyscraper’s observation deck and break through the windows to steal sensitive information.

That kind of security plan might have been sufficient back in the days of Sean Connery’s James Bond, but it’s hardly adequate to protect against the security threats hanging over law firms today.

Those threats come primarily from cyberspace, the network that includes the Internet, computer systems, telecommunications networks, and embedded mechanisms that control many military operations and critical industries like petroleum, airlines and electricity. Cyberspace, in other words, is the digital infrastructure that keeps modernized governments, economies and societies functioning.

The digital infrastructure in the United States and other countries around the world is under siege. Some experts even describe efforts to infiltrate computer networks as the precursor to a new type of warfare in which the front lines are computers sitting on desks in the offices of government officials, corporate employees and even lawyers.
China-based hackers looking to derail the $40 billion acquisition of the world’s largest potash producer by an Australian mining giant zeroed in on offices on Toronto’s Bay Street, home of the Canadian law firms handling the deal.

Over a few months beginning in September 2010, the hackers rifled one secure computer network after the next, eventually hitting seven different law firms as well as Canada’s Finance Ministry and the Treasury Board, according to Daniel Tobok, president of Toronto-based Digital Wyzdom. His cyber security company was hired by the law firms to assist in the probe.
Law360, New York (March 01, 2013, 1:54 PM ET) -- In the growing number of "virtual" law firms, attorneys and clients in far-flung cities gather in digital environments housed in climate-controlled "tier four" server farms, ringed by enough retinal scans, encryption and redundancies to give Jason Bourne a migraine.

It's a high-tech vision at odds with a legal industry where many well-paid professionals guarding clients' valuable secrets still prioritize ease over safety. But it's one direction security experts say the industry is going as it tries to accomplish potentially conflicting goals: Becoming more efficient through technology while combating a growing number of sophisticated cyberattacks.
Law firms that represent healthcare providers and health plans have another level of information safeguards to add to their internal HIPAA compliance assessments. Bloomberg News has reported that approximately 80 law firms had been hacked since 2010 and that the FBI convened a meeting of the top 200 law firms in New York City to advise them that the increasing number of electronic intrusions clearly indicates that law firms are increasingly seen as weak links in information security and, therefore, will be targeted with greater frequency.

While the hackers in the Bloomberg article (available at http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html) have been linked to individuals in China and the law firms involved, to a great extent, were active in merger and acquisition matters, law firms representing healthcare entities should take notice because they have discrete obligations under HIPAA and HITECH to implement safeguards for Protected Health Information.

While any firm can be the victim of a cyber-attack, an attack that results in the unauthorized disclosure of patient-identifiable health information (such as “phishing” attacks or certain “worm” viruses) can subject the firm to investigation by the Office For Civil Rights of the U.S. Department of Health and Human Services. In such an investigation, one of the first questions will be the documentation of information security safeguard policies, and a current security assessment. Both are critical to defensibility of the firm’s information management practices and, to put a fine point on it, the firm’s continuing ability to retain healthcare business.
Ethical Considerations Regarding Safeguarding Client Data:

Competence

Confidentiality

Duty to Protect and Preserve Property
Recent amendment to Rule 1.1—Competence

Maintaining Competence. To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.
Recent amendment to Rule 1.6-Confidentiality

(e) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.
From new commentary to Rule 1.6

The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of subsection (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).
A client may require the lawyer to implement **special security measures not required by this Rule** or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client’s information in order to comply with **other law**, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer’s duties when sharing information with nonlawyers outside the lawyer’s own firm, see Rule 5.3, Official Commentary.
Rule 4.4. Respect for Rights of Third Persons

(b) A lawyer who receives a document or electronically stored information relating to the representation of the lawyer’s client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.
For purposes of this Rule, “document or electronically stored information” includes, in addition to paper documents, email and other forms of electronically stored information, including embedded data (commonly referred to as “metadata”), that is subject to being read or put into readable form. Metadata in electronic documents creates an obligation under this Rule only if the receiving lawyer knows or reasonably should know that the metadata was inadvertently sent to the receiving lawyer.

Some lawyers may choose to return a document or delete electronically stored information unread, for example, when the lawyer learns before receiving it that it was inadvertently sent. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document or delete electronically stored information is a matter of professional judgment ordinarily reserved to the lawyer. See Rules 1.2 and 1.4.
Whether the lawyer is required to take additional steps, such as returning the document or electronically stored information, is a matter of law beyond the scope of these Rules, as is the question of whether the privilege status of a document or electronically stored information has been waived.

Similarly, this Rule does not address the legal duties of a lawyer who receives a document or electronically stored information that the lawyer knows or reasonably should know may have been inappropriately obtained by the sending person.
(b) A lawyer shall hold property of clients or third persons that is in a lawyer’s possession in connection with a representation separate from the lawyer’s own property. Funds shall be kept in a separate account maintained in the state where the lawyer’s office is situated or elsewhere with the consent of the client or third person. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of seven years after termination of the representation.
Cloud computing guidance:

More cloud guidance:

PROTECTING THE POLICY HOLDER: 
Assess Risks and Coverage Options/Possibilities

• **Proactively Identify Risks**
  • Where are the cyber landmines and what creates them?
    • The release of, or access to, confidential or sensitive data stored, managed and/or created via electronic systems
      • - Internally and externally created risks
    • Compliance matters
    • Accidents
    • Crimes
• Typical First Party Losses
  • Equipment
  • Software
  • Business Interruption
  • Notification costs
  • Consultants/FTEs
  • Regulatory Compliance

• Third Party Losses
  • Defense/Attorney’s Fees
  • Experts and Consultants
  • Damages/Settlements
• Possible Coverage Under Traditional Insurance Policies
  1. Commercial and Property
  2. Crime
  3. CGL
  4. D&O
• Insuring Provisions:

• We will pay for direct physical loss or damage to Covered Property
• We will pay for the actual loss of Business Income due to necessary suspension of your operations . . . The suspension must be caused by direct physical loss of damage to property at the premises...
Commercial Property Policy
Business Interruption Policy

• Key Issues:
  • Is the damage “direct”?  
  • Is the damage “physical”?  

• Check Policy Language:
  • Current ISO Form Policies generally exclude or severely limit coverage for “electronic data”  
  • Older policies might not reference “electronic data”
• Insuring provision:

  • Computer Fraud: We will pay for loss or damage to “money”, “securities” and “other property” resulting directly from the use of any computer to fraudulently cause a transfer of that property . . .
Commercial Crime Policy

Key Issues:
- Is the damage “direct”?
- Does the property at issue (e.g. credit card information or personal information) constitute covered “property”?

Check Policy Language:
- Current ISO Form Policy:
  - Excludes loss resulting from unauthorized use or disclosure of confidential information of another person which is held by you
  - “Other property” does not include electronic data
CGL Policy

• Insuring Provisions:
  • Coverage A: “property damage” meaning:
    • Physical injury to tangible property, including all resulting loss of use of that property
    • Loss of use of tangible property that is not physically injured
  • Coverage B: “personal and advertising injury”
    • Oral or written publication, in any manner, of material that violates a person’s right of privacy
CGL Policy

• Key Issues:
  • Property Damage:
    • Is there damage to or loss of use of “tangible property”? 
  • Personal and advertising injury:
    • What constitutes “publication”? 
    • Has there been a “publication”? 
    • Does the publication “violate a person’s right of privacy”? 

Check Policy Language:

Current ISO Form Policy:

"Property damage" excludes electronic data from the definition of "tangible property"

Coverages A and B both exclude coverage for the distribution of material in violation of the Telephone Consumer Protection Act (TCPA), CAN-SPAM Act of 2003, or any other "statute, ordinance or regulation that prohibits or limits the sending, transmitting, communicating or distribution of material or information."
• Coverage under one or more policy may be triggered
• Risks are rapidly evolving
• New products continue to be developed – help clients with negotiations and renewals
Three core cyber liability risks:

• Technology errors and omissions
• Media/e-publishing liability
• Data breaches of sensitive information
Technology Errors and Omissions:

- Software or hardware does not function properly
  Information mailed to wrong recipient
  Data corruption
- Error in network architecture
  Public facing web application without a WAF
  Glitch in segregation permits unauthorized access

Problem most likely vendor’s IT
Steps to minimize technology errors and omissions risks

• Avoid providing technology solutions to others, unless it is a core business

• 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
Steps to minimize media/e-publishing risks

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

Evaluate liability for employees and vendors
What is the leading cause of data breaches?

68% of breaches DO NOT INVOLVE NETWORK BREACH

- 32% Network Hacking
- 68% Non-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
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
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**

<table>
<thead>
<tr>
<th>Cost</th>
<th>$$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Fees</td>
<td>$$$</td>
</tr>
<tr>
<td>Customer Notification</td>
<td>$$$</td>
</tr>
<tr>
<td>Public Relations</td>
<td>$$$</td>
</tr>
<tr>
<td>Credit Monitoring</td>
<td>$$$</td>
</tr>
<tr>
<td>Customer Reimbursement</td>
<td>$$$</td>
</tr>
<tr>
<td>Forensic Investigation</td>
<td>$$$</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>$$$</td>
</tr>
</tbody>
</table>
How much does a breach response cost?

Intangible Costs

- Lost patient and community goodwill/trust
- Reduced future revenues
- Drain on employees and operations
• 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!
Cyber insurance:

• Protects cash flow and patients

• 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 E&O limits for E&O claims
This presentation is a summary of legal principles. Nothing in this presentation constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney. The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.