Agenda

- Threats
- Managing the Risk
- Cyber Insurance
- What’s Next?
Sampling of Costs

- 42% of small businesses surveyed have been the victim of a cyber-attack within the past 5 years (NSBA 2015 Year-End Economic Report)
- 91% of data breaches occurred to small merchants
- 60% of small businesses go out of business within six months of a data breach (National Cyber Security Alliance)

Range of Expected Losses by Number of Records
(Adapted from Verizon 2015 Data Breach Investigations Report, pg. 30)

<table>
<thead>
<tr>
<th>Records Lost</th>
<th>Prediction (Lower)</th>
<th>Average (Lower)</th>
<th>Expected</th>
<th>Average (Higher)</th>
<th>Prediction (Upper)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>$1,170</td>
<td>$18,120</td>
<td>$25,450</td>
<td>$35,730</td>
<td>$555,660</td>
</tr>
<tr>
<td>1,000</td>
<td>$3,110</td>
<td>$52,260</td>
<td>$67,480</td>
<td>$87,140</td>
<td>$1,461,730</td>
</tr>
<tr>
<td>10,000</td>
<td>$8,280</td>
<td>$143,360</td>
<td>178,960</td>
<td>$223,400</td>
<td>$3,866,400</td>
</tr>
</tbody>
</table>
Data Breach Costs

- Cost of revelation and investigation
- Cost to verify information
- Legal costs
- Cost of repair
- Fines and penalties
- Notification costs

- Cost of lost availability
- Cost of lost work
- Loss of confidence / reputation damage
- Cost of lost partnerships/vendors
- Public relations costs
- And more
Types of Data at Stake

• **PHI – Protected Health Information**
  - Information created or received by a covered entity or business associate relating to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of health care to an individual, that identifies or can be used to identify individual

• **PII – Personally Identifiable Information**
  - Social security number, driver’s license number, bank account information, credit card information, online/financial account username and password, medical information, health insurance information, and email address and password in CA, FL and PR

• **PCI – Payment Card Industry Information**
  - Cardholder data
Cyber Threats

- **Malicious attack**
  - Ransomware
  - Hackers in network, malware and viruses, phishing scams, physical theft of hardware and paper, denial of service
  - Rogue employees
  - **UNSOPHISTICATED ACTORS**

- **Employees**
  - Negligence related to use and storage of data, failure to follow or learn **POLICIES AND PROCEDURES**, loss of portable devices, mis-mailing of paper, unencrypted emails to the wrong recipients, web use violation, **UNAPPROVED DEVICES**, abuse of access

- **Vendor**
  - Any of the above can occur to a business associates with whom data is shared/system access granted
Regulatory Enforcement (Current Examples)

- **HHS/OCR**
  - Cancer Care Group ($750,000 settlement, August 31, 2015)
    - OCR found widespread non-compliance, and lack of policies, after laptop bag with unencrypted media exposed records of **55,000** patients
  - State-Run Community Mental Health Facility ($150,000 settlement, Dec. 2014)
    - Organization failed to patch systems and continued to run outdated, unsupported software resulting in exposure of **2,743** medical records

- **FCC**
  - $25 million fine against ATT for unauthorized disclosure of information (April 2015 - 280,000 records)

- **State**
  - Indiana – Assurance of Voluntary Compliance (AVC) (multiple fines ranging from $4,000 to $20,000)
  - TD Bank – 260,000 affected ($850,000 nine state fine plus $650,000 Mass. fine in December 2014)
MANAGING THE RISK
Anatomy of a Breach Response

Internal Insured Issues
- Internal reporting
- Broker involvement
- SIR management

Experts
- Breach coach
- Forensic
- Public relations

Investigation
- How did it happen?
- When did it happen?
- Is it still happening?
- Who did it happen to?
- What was and was not accessed or acquired?
- Was information encrypted/protected?

Notice Obligations
- State
- Federal
- Other (e.g. PCI)

Notice Methods
- Written
- Electronic
- Substitute
- Media

Deadlines
- Can be from 48 hours to “without unreasonable delay”

Inquiries
- State regulators
- Federal regulators
- Federal agencies
- Consumer reporting agencies
- Plaintiffs
What Can Be Done?

• Proactive Risk Manager Steps
  • **Empowered Senior Executive**
  • Talk to your IT Security folks; gain an appreciation of the many challenges
  • Not many firms can say: how many records they have; what type of data is being collected, stored, shared, protected; where does all this data reside; when is it purged?
  • **Assess** and test your own staff and operations
  • Incident response plan
  • Document your due care measures (training and enforcement)
  • **Insurance**
  • Red flags, data security and breach response plans – affirmative duties
  • Service level agreements
  • Repeat
Affordable Steps to Take

• Employee training
  • For two years, more than two-thirds of incidents that compromise the cyber-espionage pattern have featured phishing (Verizon 2015 Data Breach Investigations Report)

• Access permissions
  • Limit access of private data to need-to-know employees only

• Password policies
• Regularly scheduled software patches and up-to-date anti-virus
• Incident Response Plan
Cyber Liability: What can be Covered?

- Privacy/security liability (online and offline)
- Privacy regulatory proceeding defense and penalties
- Website content
- Privacy breach response costs
  - Attorney services – no retention
  - Forensic services
  - Notification costs – voluntary included
  - Public relations, crisis management, call center services
- Network extortion costs
- Data restoration costs
- Business interruption and extra expense – by endorsement
- PCI fines and costs – by endorsement
Cyber Insurance Landscape: Where is it going?

-$1.5B going on $6B(?) market
-Broader Coverage
-Concern over ‘aggregate’ risks
QUESTIONS