DO SMALL BUSINESSES NEED CYBER INSURANCE?

CYBER SECURITY SUMMIT 2016

PRESENTED BY:
JAKE OMANN, CIC, CPCU
“There are only two types of companies: those that have been hacked, and those that will be.”

“There are only two types of companies: those that have been hacked, and those that will be.”

“Even that is merging into one category: those that have been hacked and will be again.” FBI Director Robert Mueller (retired)
AGENDA

- Legal and Threat Landscape
- Cyber Breach Analysis
- Cyber Insurance Overview
- Risk Management Tips
- Q&A
CYBER RISKS AND INDUSTRY TRENDS
Public outcry from these risks has resulted in various federal (and state) laws:

- Health Insurance Portability Accountability Act (HIPAA) (HITECH breach notification rules)
- Fair & Accurate Credit Transactions Act (Red Flag Rules) under FTC
- State Breach Notification Rules
- Gramm Leach-Bliley Rules
- Federal Breach Laws
Information maintained in data systems often represents highly confidential and “sensitive” information:

- Financial
- Medical
- Social Security Numbers (DOB, maiden name)
- Credit information
- Immigration documentation
- Intellectual property (patents, trademarks and copyrights)
- Customer proprietary information
BREACH COSTS BREAKDOWN

Source: Netdiligence 2015 Cyber Report
COMPANY SIZE BREAKDOWN

Source: Netdiligence 2015 Cyber Report
# CYBER LIABILITY COVERAGE – 1\textsuperscript{ST} PARTY

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business income/dependent business income loss</strong></td>
<td>• Reimbursement of loss of income due to a suspension of computer systems (time frame deductible). Reimbursing loss of income due to a data breach to a dependent business partner during the policy period.</td>
</tr>
<tr>
<td><strong>Notification and credit monitoring/crisis management</strong></td>
<td>• The cost of notifying the individuals whose data has been compromised and the offering of services to monitor suspicious credit activity.</td>
</tr>
<tr>
<td><strong>Data asset restoration/forensics/legal/compliance</strong></td>
<td>• Reimbursement of costs to recover, reinstate and recreate intangible assets destroyed during a cyber attack. Forensics obtained to determine what and whose information was stolen. Legal/compliance to determine regulatory and statutory requirements.</td>
</tr>
<tr>
<td><strong>Cyber extortion threat</strong></td>
<td>• Reimbursing investigation expenses and ransom payments resulting from malicious threats to your organization’s computer system.</td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Privacy liability/employee liability</td>
<td>• Class actions and suits brought (including employees) which result in a monetary payment due to the disclosure of a person’s private and confidential information.</td>
</tr>
<tr>
<td>Regulatory defense and civil penalties</td>
<td>• Investigation, fines and penalties that you are legally required to pay</td>
</tr>
<tr>
<td>Media liability</td>
<td>• Legal liability arising from media content transmitted on any computer system. Harm suffered by others due to an infringement of an intellectual property right. Defamation and slander.</td>
</tr>
</tbody>
</table>
STEPS FOR REDUCING CYBER RISKS

1. Identify the legal and regulatory requirements applicable to your industry

2. Audit and upgrade your systems, policies and procedures accordingly
   • Identify and implement appropriate training and vetting practices for respective personnel

3. Evaluate current contracts with third parties and perform due diligence

4. Evaluate your risk management strategy
QUESTIONS?