



Item 3: Committee Education on Directors and Officers Insurance and Cyber Insurance

Leslie Wiley
Treasurer

Finance & Audit Committee Meeting

ERCOT Public
June 13, 2016

Committee Education

- Agenda
 - Cyber Insurance
 - Directors and Officers (D&O) Insurance

Cyber Insurance

Insurance Types - Difference



Aetb | iStock | Getty Images

Cyber



Social Engineering



Crime

Cyber Liability Risk Factors

- All companies, regardless of industry have an exposure to cyber risk, as we live and work in a digital world.
- Cyber risk can occur via a computer network or a third party customer or vendor's network.
- Breakdown of types of Cyber risks:
 - **Theft or loss of data** – employee data, corporate / financial data
Data may be used for competitive/financial gain or destroyed/scrambled for ideological, extortion, etc.
 - **Communication disruption** – website or network disruption, social media takeover
 - **Operational or physical destruction** or disruption of industrial control systems, machinery, or facilities operated through an electronic matter
 - **Regulatory risk** – HIPAA, FTC, FCC, SEC, NERC, FERC, and more
 - **Reputational risk**
- Threats include internal, external, malicious or accidental threats.
- Technology, media and data (print or electronic) present risk.

Cyber Liability – Types of Data

- **Personally Identifiable Information (“PII”)**
 - Any information that can be used on its own or with other information to identify, contact or locate a single person. Examples include: home addresses, social security numbers, driver's license numbers, bank account information, credit card information, online accounts username and passwords, date of birth, medical / health information, email addresses and passwords (in CA, FL, and PR), etc.
 - Corporate Confidential Information, Bank Account information of Vendors or Business Partners, Trader emails, etc.
- **Payment Card Industry Information (“PCI”)**
 - Credit card information. The Payment Card Industry Data Security Standard is a set of requirements designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment.
- **Protected Health Information (“PHI”)**
 - Includes any information related to the past, present or future physical or mental health or condition of an individual, including the provision of health care or payment of health care that can be linked to a specific individual. This includes medical records and payment history.

Cyber Liability – Causes of a Breach

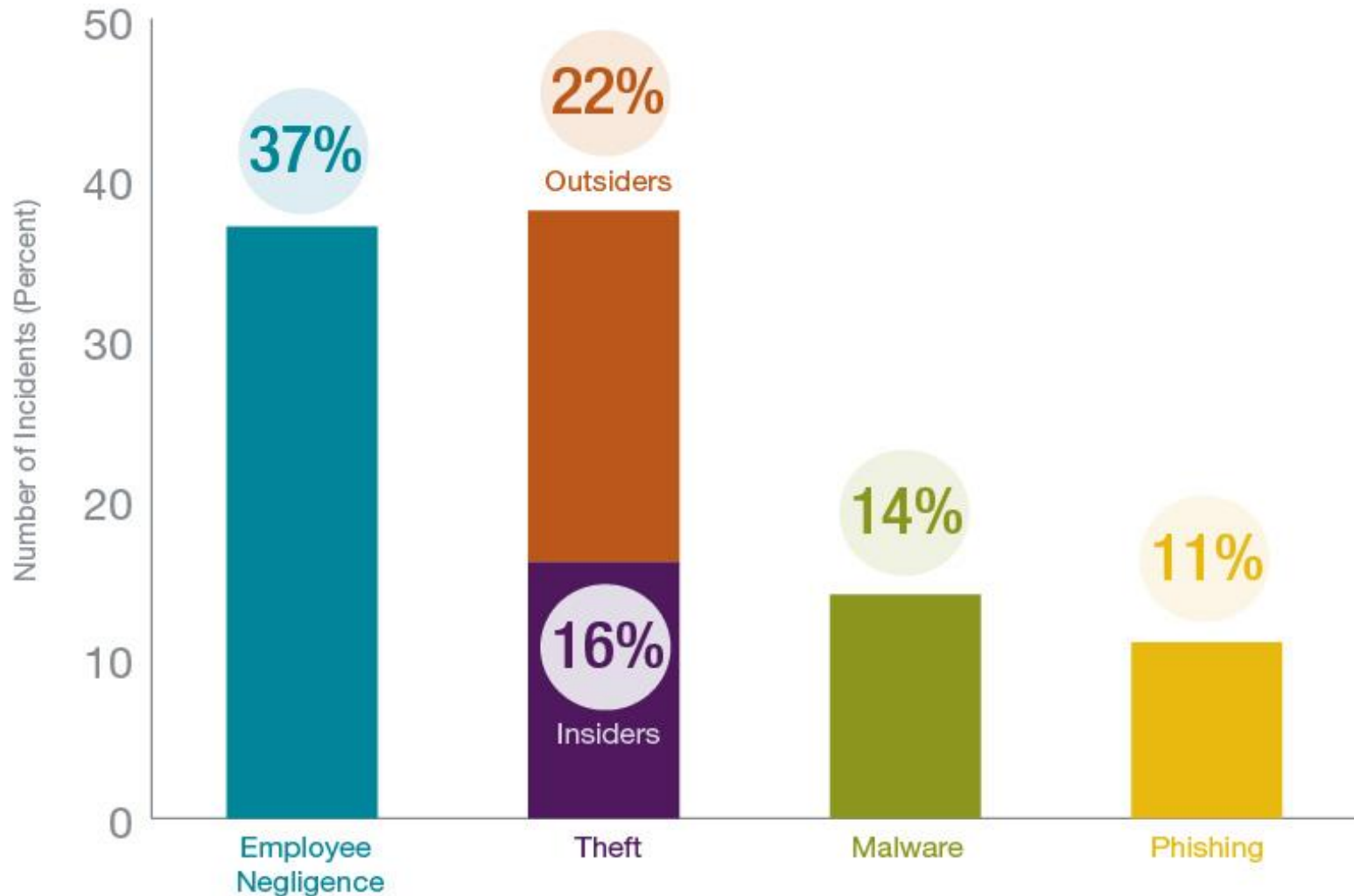
- **Bad Actors**

- Hackers invade network
- Malware and viruses (i.e. hostile or intrusive software, trojan horses, ransomware, spyware, etc.)
- Phishing scams (i.e. fraud where criminals pose as a legitimate company)
- Physical theft of hardware or paper documents
- Deceptive employees

- **Human Error**

- Loss of portable devices (i.e. iPhone, Droid, Blackberry)
- Unintentionally sending email to the wrong recipient
- Bad practices related to document storage or failure to follow procedures

BakerHostetler – Data Security Incident Response Report 2015



Anatomy of a Breach

BREACH DISCOVERY

EXPERTS

- Breach coach
- Forensics
- Public relations

INVESTIGATION—internal/forensic/criminal

- How did it happen
- When did it happen
- Is it still happening
- Who did it happen to
- What was accessed/acquired (What wasn't)
- Encrypted/protected

NOTICE OBLIGATIONS

- State
- Federal
- Other (i.e. PCI)

NOTICE METHODS

- Written
- Electronic
- Substitute
- Media

DEADLINES

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

INQUIRIES

- State regulators (i.e. AG, PD)
- Federal regulators (i.e. OCR)
- Federal agencies (i.e. SEC, FTC)
- Consumer reporting agencies
- Plaintiffs

LITIGATION

- Government Entities
- Class action
- Indemnification
- Subrogation

CNA and Lewis Brisbois Bisgaard & Smith LLP

Cyber Liability Insurance – The Policy

- **First Party Coverage**

- Notification Expense / Credit Monitoring
- Cyber Extortion
- Network / Business Interruption
- Data Asset Restoration
- Crisis Management

- **Third Party Liability Coverage**

- Privacy & Network Security Liability
- Regulatory Claims
- Media Liability
- Other “add-ons” such as Reputational Harm, Cyber Terrorism, Computer Fraud cover may exist, depending on the carrier
- Certain fines & penalties are typically covered

Data Breach Calculation Tools

Net Diligence Breach Calculator– Sample Breach – 1,000,000 PII

Data Breach Costs

 CALCULATE

INCIDENT INVESTIGATION

<input type="checkbox"/> FORENSICS INVESTIGATION	<input type="text" value="\$220,000"/>	<input type="radio"/>
<input type="checkbox"/> SECURITY REMEDIATION	<input type="text" value="\$300,000"/>	<input type="radio"/>
<input type="checkbox"/> BREACH COACH @ LEGAL GUIDANCE	<input type="text" value="\$38,000"/>	<input type="radio"/>
SUBTOTAL	<input type="text" value="\$558,000"/>	

CUSTOMER NOTIFICATION / CRISIS MANAGEMENT

<input type="checkbox"/> CUSTOMER NOTIFICATION	<input type="text" value="\$1,000,000"/>	<input type="radio"/>
<input type="checkbox"/> CALL CENTER	<input type="text" value="\$75,000"/>	<input type="radio"/>
<input type="checkbox"/> CREDIT/ID MONITORING	<input type="text" value="\$290,000"/>	<input type="radio"/>
<input type="checkbox"/> PUBLIC RELATIONS	<input type="text" value="\$20,000"/>	<input type="radio"/>
SUBTOTAL	<input type="text" value="\$1,385,000"/>	

CLASS ACTION LAWSUIT

<input type="checkbox"/> DEFENSE	<input type="text" value="\$699,000"/>	<input type="radio"/>
<input type="checkbox"/> eDISCOVERY	<input type="text" value="\$1,100,000"/>	<input type="radio"/>
<input type="checkbox"/> PUBLIC RELATIONS	<input type="text" value="\$559,000"/>	<input type="radio"/>
SUBTOTAL	<input type="text" value="\$2,358,000"/>	

PCI

<input type="checkbox"/> FINES & PENALTIES	<input type="text" value="\$0"/>	<input type="radio"/>
<input type="checkbox"/> FRAUD ASSESSMENTS	<input type="text" value="\$0"/>	<input type="radio"/>
<input type="checkbox"/> CARD REISSUANCE	<input type="text" value="\$0"/>	<input type="radio"/>
SUBTOTAL	<input type="text" value="\$0"/>	

REGULATORY FINES & PENALTIES

<input type="checkbox"/> STATE AG	<input type="text" value="\$508,300"/>	<input type="radio"/>
<input type="checkbox"/> HHS	<input type="text" value="\$0"/>	<input type="radio"/>
<input type="checkbox"/> OTHER (FTC, SEC, ETC.)	<input type="text" value="\$598,750"/>	<input type="radio"/>
SUBTOTAL	<input type="text" value="\$1,107,050"/>	

TOTAL COST

PER RECORD COST

Important Information: The numbers presented in the NetDiligence® Data Breach Cost Calculator are estimates and provided for education and illustration purposes only. Actual expenses and liability exposures due to identity theft or data breach incident may vary based on variables not considered in this calculator. Numerical results presented in the Data Breach Cost Calculator are based on a proprietary formula developed by NetDiligence and its insurance industry partners. This formula takes into account information available in the public domain and information obtained through various websites that track breach statistics. Please note: This calculator is not intended to predict insurable perils or related costs and has no bearing on any insurance policy.

Total Estimated Cost of Breach: \$5,408,050

Total Estimated Cost Per Record: \$5

Data Breach Calculation Tools

Net Diligence Breach Calculator– Sample Breach – 1,000,000 PCI

Data Breach Costs

 **CALCULATE**

INCIDENT INVESTIGATION

<input type="checkbox"/> FORENSICS INVESTIGATION	<input type="text" value="\$154,000"/>	<input type="radio"/>
<input type="checkbox"/> SECURITY REMEDIATION	<input type="text" value="\$210,000"/>	<input type="radio"/>
<input type="checkbox"/> BREACH COACH @ LEGAL GUIDANCE	<input type="text" value="\$38,000"/>	<input type="radio"/>
SUBTOTAL	<input type="text" value="\$402,000"/>	

CUSTOMER NOTIFICATION / CRISIS MANAGEMENT

<input type="checkbox"/> CUSTOMER NOTIFICATION	<input type="text" value="\$1,000,000"/>	<input type="radio"/>
<input type="checkbox"/> CALL CENTER	<input type="text" value="\$75,000"/>	<input type="radio"/>
<input type="checkbox"/> CREDIT/ID MONITORING	<input type="text" value="\$290,000"/>	<input type="radio"/>
<input type="checkbox"/> PUBLIC RELATIONS	<input type="text" value="\$14,000"/>	<input type="radio"/>
SUBTOTAL	<input type="text" value="\$1,379,000"/>	

CLASS ACTION LAWSUIT

<input type="checkbox"/> DEFENSE	<input type="text" value="\$699,000"/>	<input type="radio"/>
<input type="checkbox"/> eDISCOVERY	<input type="text" value="\$770,000"/>	<input type="radio"/>
<input type="checkbox"/> PUBLIC RELATIONS	<input type="text" value="\$559,000"/>	<input type="radio"/>
SUBTOTAL	<input type="text" value="\$2,028,000"/>	

PCI

<input type="checkbox"/> FINES & PENALTIES	<input type="text" value="\$25,000"/>	<input type="radio"/>
<input type="checkbox"/> FRAUD ASSESSMENTS	<input type="text" value="\$12,500,000"/>	<input type="radio"/>
<input type="checkbox"/> CARD REISSUANCE	<input type="text" value="\$2,000,000"/>	<input type="radio"/>
SUBTOTAL	<input type="text" value="\$14,525,000"/>	

REGULATORY FINES & PENALTIES

<input type="checkbox"/> STATE AG	<input type="text" value="\$508,300"/>	<input type="radio"/>
<input type="checkbox"/> HHS	<input type="text" value="\$0"/>	<input type="radio"/>
<input type="checkbox"/> OTHER (FTC, SEC, ETC.)	<input type="text" value="\$0"/>	<input type="radio"/>
SUBTOTAL	<input type="text" value="\$508,300"/>	

TOTAL COST

PER RECORD COST

Important Information: The numbers presented in the NetDiligence® Data Breach Cost Calculator are estimates and provided for education and illustration purposes only. Actual expenses and liability exposures due to identity theft or data breach incident may vary based on variables not considered in this calculator. Numerical results presented in the Data Breach Cost Calculator are based on a proprietary formula developed by NetDiligence and its insurance industry partners. This formula takes into account information available in the public domain and information obtained through various websites that track breach statistics. Please note: This calculator is not intended to predict insurable perils or related costs and has no bearing on any insurance policy.

Total Estimated Cost of Breach: \$18,842,300

Total Estimated Cost Per Record: \$19

Verizon – 2015 Data Breach Investigations Report

The forecast average loss for a breach of 1,000 records is between \$52,000 and \$87,000.

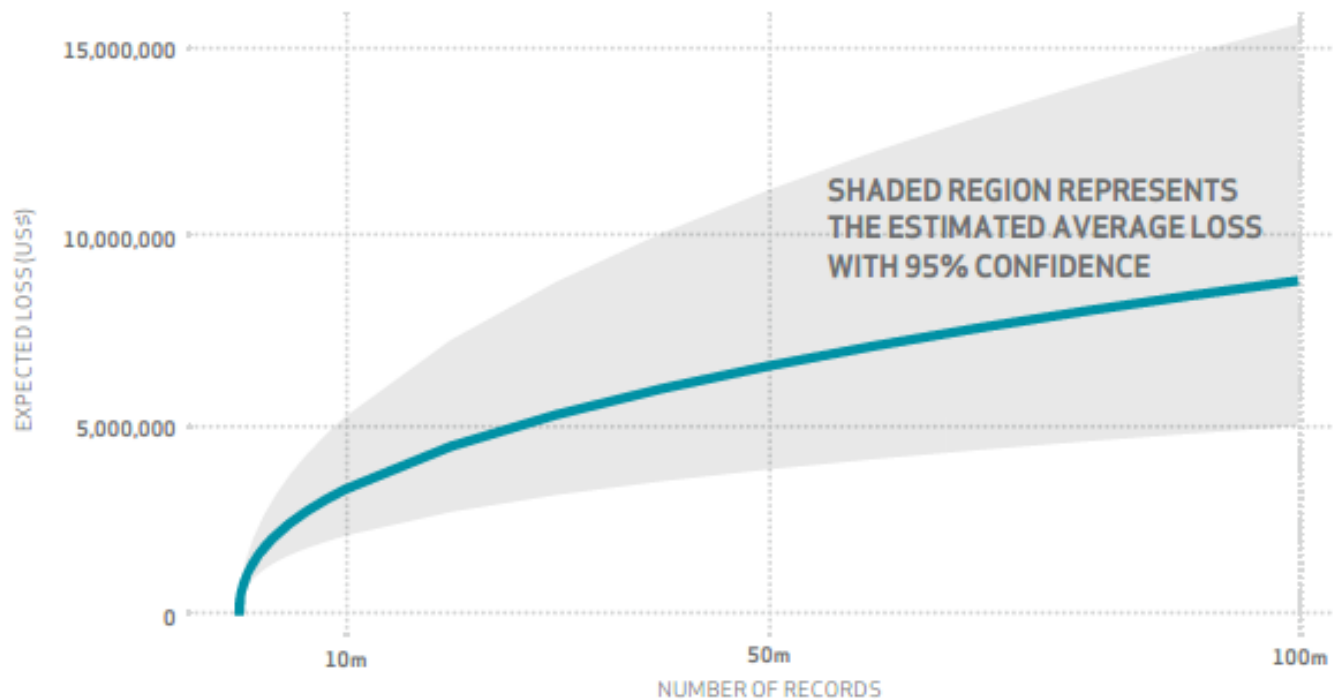
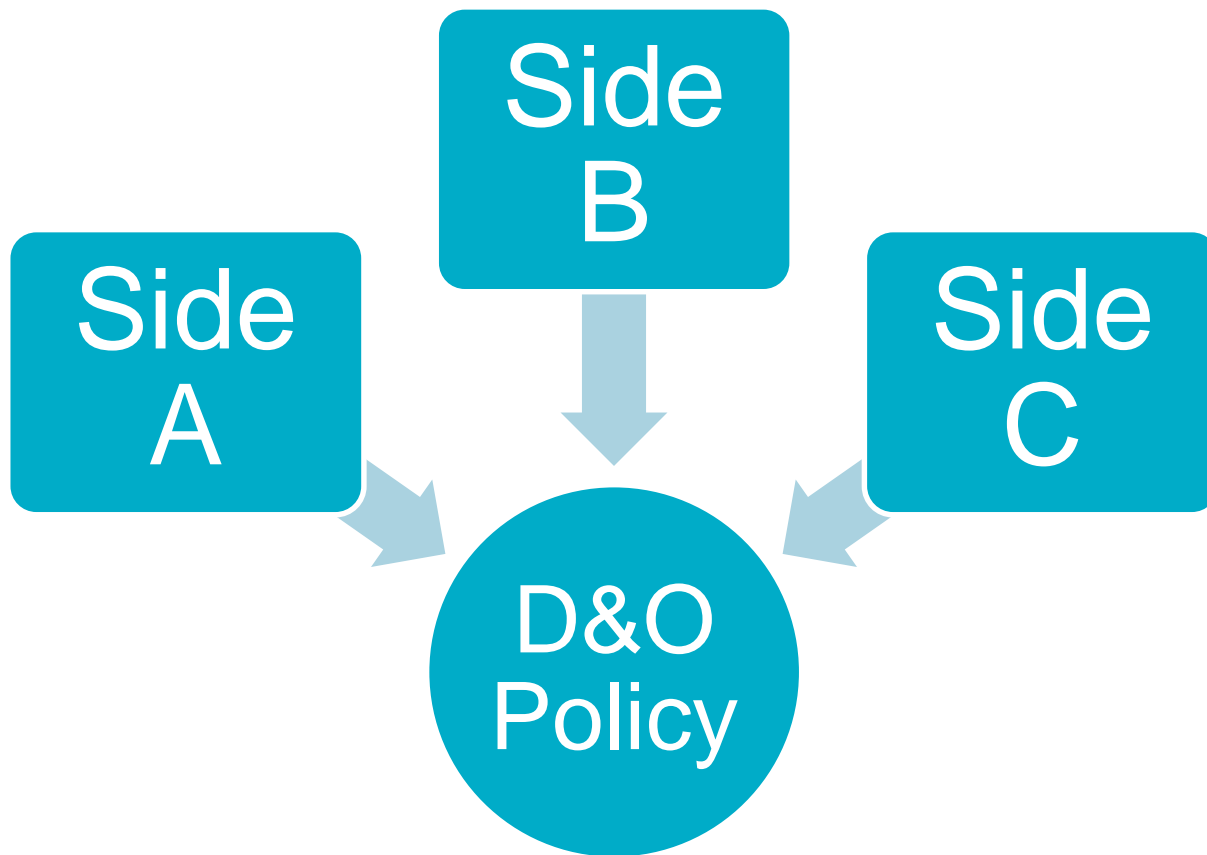


Figure 22.

Expected average loss by records lost

Directors and Officers Insurance

Elements of D&O Insurance



Side A

Non-Indemnifiable Loss is “loss for which no Organization is permitted or required to indemnify, or is permitted or required to indemnify but does not do so by reason of Financial Impairment.”

There are instances when the Organization cannot indemnify a director, officer or other individual against a D&O-related claim, such as when the individual has acted in bad faith, illegally or against the interests of the company. Another situation when indemnification is not available includes bankruptcies.

•**Bankruptcy:** When a organization is financially insolvent, indemnification owed to a director or officer for a “D&O” suit (such as a claim alleging a breach of fiduciary duty) might be considered an unsecured obligation by the court and subordinated to other debts of the organization.

The important aspect of A-side coverage is that it protects directors and officers against loss that they would otherwise pay out-of-pocket.

Side B

Most claims fall under this coverage part.

The organization documents (articles of incorporation, bylaws, company agreements) typically allow the organization to indemnify individual insureds for claims made against them, if such individuals:

- Acted in good faith and in a manner that was in the best interests of the company, and
- With respect to any criminal proceedings, had no reasonable cause to believe their conduct was unlawful.

The distinguishing characteristics of a Side B claim are that 1) the claim is made against individuals, and 2) indemnification by the organization is provided.

Examples of B-side claims include:

- Claims against an employee in his or her capacity as such.
- Administrative or regulatory investigations and proceedings against an individual insured.

The retentions do not stack. If multiple retentions apply to a claim, either because claim involves more than one type of claim or more than one insuring agreement, then the sum of the retentions will not exceed the largest retention.

Side C

Entity coverage is triggered when a claim is made against the organization itself.

The entity coverage in a nonprofit D&O policy is typically broader than it is in a public D&O policy. Nevertheless, there are exclusions in the D&O policy that narrow the scope of what is covered under this coverage section. The most common exclusions that apply to a claim against the entity are:

- Breach of contract
- Professional liability (usually added if the organization provides professional services)
- Intellectual property

As stated above, the retentions do not stack. Only the largest retention applies to each claim.

The D&O Policy

- Employment Practices
- When is the policy triggered
- Who is insured
- Claim definition
- What is considered a loss
- Major exclusions

Claim Examples

- Bankruptcy
- Fraud
- Breach of Fiduciary Duty
- Misrepresentation
- Wasting of Corporate Assets
- Unfair Methods of Competition and Unfair Trade Practices
- Antitrust and False Advertising
- Trade Secrets

Potential Claim Process

\$75 million in total coverage

Second Excess Layer
\$25 Million

First Excess Layer
\$25 Million

Primary Layer
\$25 Million