Analyzing Cyber Risk Coverage

Presented by INSURICA

- Analyzing Cyber Risk Coverage –

2400 N. Glenville Drive, Suite B125
Richardson, TX 75082

James Roskopf
James.Roskopf@INSURICA.com
469-443-3489

INSURICA was founded in 1959 and has grown to become one of the 50 largest insurance brokerage firms in the US. With 500+ employees and revenue over $100 million, INSURICA has industry leading resources and top notch professionals. As a member of Assurex Global, we are able to manage risk for our clients on a worldwide basis.

Today’s State of Cyber Security

“As counterintuitive as it sounds, cybersecurity is a human problem, it's a leadership problem, it's not a technical problem.”

What's the Agenda?

- The world is changing and old policies aren't keeping up.
- What are hackers looking for?
- Typical causes of loss.
- Chronology of a data breach.
- New laws can leave your firm exposed.
- What to look for in a good policy.

What just happened?

- New style of claims outrun General Liability and Crime policy coverage.
- Existing policies did not anticipate hacking and email-based liabilities.
- Data theft and Ransomware are commonplace.
- Increasing intellectual property liability claims.
- Increasing business interruption claims.

Brief History of Cyber Insurance

- **Early 2000s** – 1st party coverage added as well as Business Interruption, Extortion, and Forensic coverages
- **July 1, 2003** – California requires businesses to notify clients of data breach. Leads to many states adding similar laws. 1st Party Coverages added including PR, Credit Monitoring, and Notification Expense. New 3rd Party Coverages include Regulatory Fines and Penalties.
- **Mid 2000s** – Breaches become common place in both retail and healthcare
- **2018** – California and New York introduce stronger cyber laws that look like GDPR
- **Current State of the Market** – Leading carriers have better understanding of coverage risks. Pricing is still volatile. Movement towards more Risk Management Services included in policy form.

How big a deal is this?

Exposure not limited to Fortune 500 companies

- Every business has some level of risk
- Exposure is driven by the amount and type of sensitive information held by the company

Breaches are significant

- Forensic and Breach response expenses
- Business interruption Losses
- Cyber extortion
- Regulatory fines and penalties

Ask for help!

- Non-standard forms and process
- Find a broker who knows and can explain this complicated coverage
- Devil is in the details – definitions, exclusions

What are the hackers looking for?

- Medical Records – PHI and PII
- Credit Cards
- Trademarks and Trade Secrets
- DOB, SSN, Drivers License Info
- Banking Details
- Copyright s
- Intellectual property
- Personal Insurance Information

How do they get your stuff?

- Social Engineering
- Business Email Compromise
- Theft of data including Intellectual Property
- Cyber Extortion
- Ransomware
- Credit Card Theft

Just what exactly is a data breach?

Release of information that should be private. Actual release or disclosure of information to an unauthorized individual/entity that relates to a person and that:

May cause the **person** financial or reputational harm

- Personally Identifiable Information (PII)
- Protected Healthcare Information (PHI)

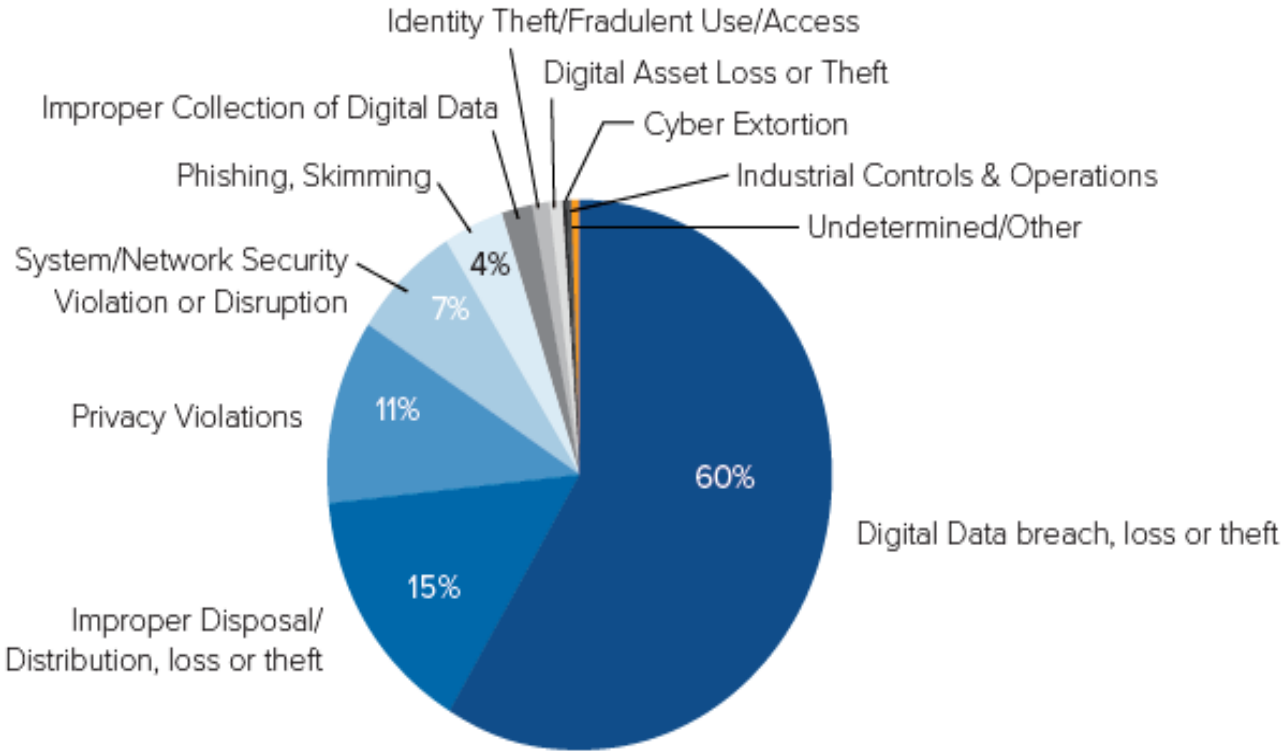
May cause your company financial or reputational harm

- Customer Data, Applicant Data, Current/Former Employee Data
- Corporate Information/Intellectual Property

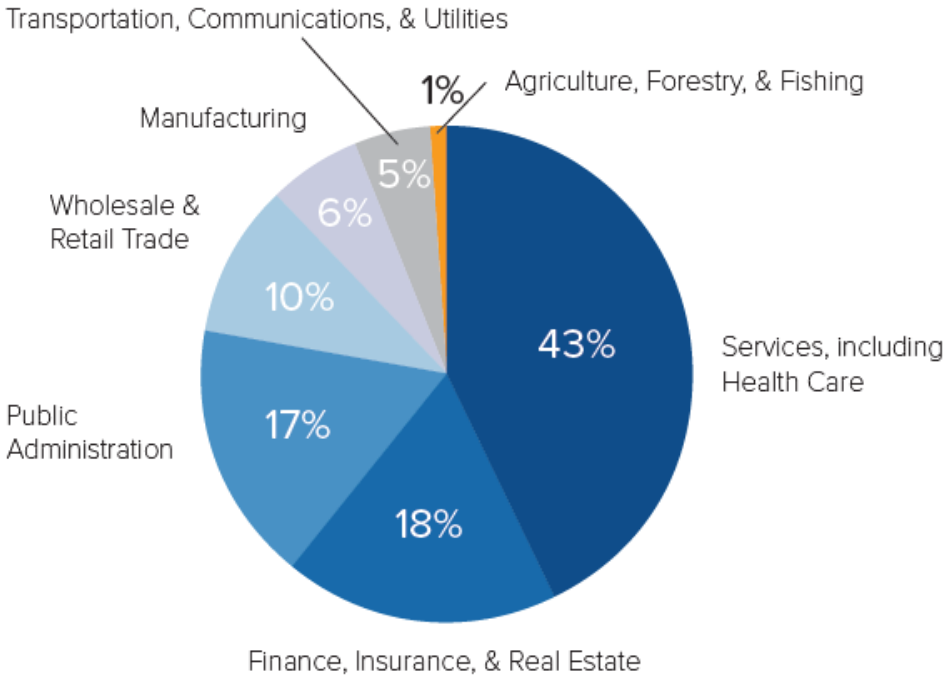
Most breaches are not caused by hacking!

- Improper Disposal of Paper Documents
  - Un-shredded Documents
  - File cabinets without checking for contents
  - X-Ray Images
- Lost/Missing/Stolen Electronic Assets
  - Computers, smart phones, backup tapes, hard drives, servers, copiers, fax machines, scanners, printers
- Mishaps due to Broken Business Practices – MISTAKES!
- Rogue Employees
- Phishing/Spear Phishing Attacks
- Network Intrusions/Hacks/Malware Viruses
- **Human Error and Accidents!**

Causes of Loss



Losses by Industry



Data breaches keep happening. So why don't you do something?

Despite the headlines, the likeliest cause of a data breach is employee mistakes – Lost files and devices are a far greater day-to-day threat than hackers.

Breach Fatigue – Don't reuse passwords, rely on two-factor verification, install software only from trusted sources, question any alert that pops up on your screen and get a password manager.

Chronology of a Data Breach

- Discovery – often by a client or the government
- Despair
- Forensic evaluation and Legal Review
- More Despair
- Short Term Crisis – Notification, Credit Monitoring, and Public Relations issues
- Despair continues
- Long Term Consequences – Class action lawsuits, Regulatory fines and penalties, Income Loss, and Reputational Damage
- With a well-planned defense, life is good again.

What does GDPR got to do with it?

- The EU initiated the expansive General Data Protection Regulation (GDPR) privacy law in 2018 that applies to any company doing business in the EU. A data breach that violates the tenets of the law can lead to oppressive financial penalties.
- The New York Department of Financial Services (NYDFS) has promulgated rules quite similar to GDPR.
- The California Consumer Privacy Act of 2018 is even more sweeping in terms of individual privacy rights.
- Expect other states to begin following suit.

Cyber Liability Insurance – what to look for.

- **Don't depend on endorsements to existing policies.**
- **Read the exclusions!**
- **Key components of a great policy:**
  - Pay on Behalf of policy form is important
  - Is credit restoration offered, not just credit monitoring?
  - Is a risk management program included?
  - Are paper files covered?
  - Is the coverage trigger an "incident" or lawsuit?
  - Are the acts of rogue employees included?
  - Is business interruption included?
  - Is cyber extortion included?

Insurance Coverage – 1st and 3rd Are you safe?

1st Party:

Damage to digital assets

Business Interruption

Extortion

Crisis Management

Forensic Expense

Notification Expense

Credit Monitoring Expense

3rd Party:

Legal Liability

Defense Costs

Regulatory Liability

Contractual Liability

Cyber Insurance Outlook

- Five insurance markets write vast majority of coverage: Coalition, Beazley, Hiscox, AIG, and Travelers.
- Market immaturity and lack of coverage standardization are two reasons that make underwriting cyber products tricky at best.
- Cyber Security firms may include insurance as part of their risk mitigation package.
- Cyber Risk Aggregation may lead to a new version of terrorism coverage.

Solutions –
Markets with the best offerings

Coalition – offers many risk management tools including: Credential monitoring, patch management, threat monitoring, and ransomware prevention.

Beazley – Pre-Breach Response tools including resources for incident response planning, employee training, compliance, and security best practices.

Key Takeaways

- Data breaches are the new normal.
- Current insurance policies don’t contemplate the risk.
- The devil is in the detail.
- Work with a broker specializes in the coverage.
- Understand what to look for in a good policy.
- Be proactive, don’t wait until something has happened.

Analyzing Cyber Risk Coverage

Questions and (some) Answers

New Solutions from

Claim Examples

A 2016 data breach insurance claims study done by Net Diligence found that the average breach cost was $665,000 and with the average cost of a settlement was nearly $900,000

Your subcontractors can wreak havoc on your firm. Are they compliant? Do they have Cyber insurance?

A communications company sues for lost revenue and expenses to recover billing files for wireless customers that were deleted by their software vendor who was updating the system.

Indemnity Paid: $750,000

Defense Costs Paid: $150,000

More Examples

- Kaiser Permanente was fined $200,000 for publicly posting 150 patient names, addresses and medical records on their website

- A retailer experienced a DDoS attack on its website. During the attack, which lasted several days, the retailer experienced a significant decrease in online sales, though it received no extortion demand. No personally identifiable information (PII) was involved. Insurance company paid $300,000 in Business Interruption loss.

- After a DDoS attack that forced an online retailer to take down its website, the retailer received a demand from the hacker for several thousand dollars in Bitcoin, threatening a larger DDoS attack if the retailer did not pay. Rather than pay the monetary demand, the retailer purchased upgraded DDoS protection services in response to the threat. Insurance company paid $60,000 in cyber extortion loss.

Even More Examples

- An international software company suffered a significant malware attack across its systems. The company incurred significant amounts in external forensic costs for investigation and data recovery and restoration. Insurance company reimbursed the company over $800,000 in data protection loss and privacy breach costs.
- A public entity suffered a security breach that took down all systems. The organization incurred substantial costs in response to the downtime and suffered significant data loss. Insurance company paid over $190,000 in Business Interruption and data protection losses.
- A healthcare organization's offices in Phoenix, Chicago, and Nashville were affected by the Pink Slip virus. Forensic investigators determined that protected health information and personally identifiable information were not compromised by the incident. Insurance company paid over $120,000 in data protection loss.