Cyberinsurance: Necessary, Expensive and Confusing as Hell

Presenters: Sharon Nelson and Judy Selby
Setting the stage

• 2018 report from PwC – one-third of US businesses have some form of cyberinsurance

• PwC – Police premiums to reach $7.5 billion by 2020

• More than 60 insurance companies offering cyberinsurance

• 22% of solos and small firms reported having suffered a data breach. Over 1/3 of large law firms have been breached – ABA 2017 TECHREPORT

• SEC – Half of small business that are breached go out of business in 6 months
Setting the stage

• Insurance company Beazley – fraudulent instruction incidents quadrupled in 2017 – average loss $352,000
• Top 3 affected sectors – professional services (22%), financial services (21%) and retail (12%)
• Marsh survey 2017 – only 19% highly confident in entity’s response to a cyber incident
• Only 30% had an incident response plan
Necessary

- To manage enormous risk
- Technology is not a silver bullet
- Employees are a major risk
  - Clicking on links/attachments
  - Losing devices/having them stolen
  - And much, much more . . .
  - Training cuts risk, but doesn’t eliminate it
Expensive

• Pricing all over the map
• $10,000 plus is normal for small firms
• 35% growth in cybersecurity industry – 2016
• Allied Market Research – global market will reach $14 billion by 2022
Confusing as hell

• What does your current (non-cyber) policy cover?
• Cyber coverage is all over the map
• 2017 Deloitte report – not enough data for reliable predictive models
Confusing as hell

• No apples to apples comparison
• Referrals from colleagues? Not so much . . .
• Applications are often 20 or more pages
• 2017 RAND Corp. study - only 13% of cyberinsurance policies cover cyberattacks which are considered an act of terrorism or war
“There’s so much new coverage out there that hasn’t been tested. . . . One day there will be certain claims and we’ll figure [out] if the words we used to convey coverage actually say what we thought they meant, which is often up to a lot of lawyers.”
The 2011 Sony PlayStation network breach

• Cost an estimated $170 million
• Sony thought its general liability policy would cover
• Court ruled against Sony
• Case settled while on appeal
2013 Target breach

- Approximately $300 million in costs
- Hefty percentage of costs paid under cyberinsurance policy
First Party Coverages

Privacy Breach Response
- Legal
- Forensic
- Notification
- Credit Monitoring
First Party Coverages

• Business Interruption
• Contingent Business Interruption
• Data Restoration
• Extortion
• Social Engineering
• Telecommunications Fraud
Third Party Coverages

- Privacy and Network Liability
- Media Liability
- Regulatory Liability
- PCI-DDS Fines
- Payment card Issuer Liability
Market Challenges

• No Standard Forms
• Tremendous Variation Among Available Policies
• Frequent Updating of Forms by Insurers
• Varying Degrees of Knowledge Among Brokers
• Appropriate Fit with Entire Insurance Program
Potential Pitfalls

- Application Responses
- Prior Consent Requirements
- Panel Firm Requirements
- Notice Conditions
- Other Insurance Condition
- Liability Assumed Under Contract
The 10 most common costs that people mistakenly believe are automatically covered

- Losses incurred during a policy "waiting time"
- Third-party mistakes
- New hardware
- Software upgrades
- Social engineering, including business e-mail compromise (BEC) attacks
- Bodily injury/property damage
- Fines and penalties issued by the Payment Card industry
- Reputation damage
- Financial loss during downtime
- Loss from account takeover schemes
A new challenge: GDPR coverage

- General Data Protection Regulation – May 25, 2018
- Data breach liability
- Data practices liability – collection, storage and usage of protected data
- Fine and penalties up to 20 million Euros or 4% of the total worldwide annual turnover of the preceding financial year
What insurance companies may want to know

• Had a 3rd party audit? Produce
• E-mail encrypted when warranted?
• Full disk encryption?
• How is your backup engineered?
What insurance companies may want to know

- Cybersecurity training? Mandatory? How often?
- Phishing tests?
- What security policies do you have?
- Penetration testing? Results?
What insurance companies may want to know

• Security software and hardware? Anti-malware, data loss prevention, incident detection, etc.
• Had a data breach? Full details
• Physical security
• Compliance with national/international security standards? NIST cybersecurity framework, ISO 27001
• Compliance with GDPR?
What insurance companies may want to know

• Mobile device security? BYOD allowed? Mobile device management in place?

• Ever made an insurance claim involving cybersecurity?

• Any other insurer canceled your cybersecurity policy or refused to renew your policy?
What insurance companies may want to know

• Vendor management
• Out-processing employees – security steps
• Background check on new employees
• Aware of facts giving rise to possible claim at time of application?
What insurance companies may want to know

- Annual cybersecurity budget?
- Practices regarding passwords, access control, patching, upgrading outdated software
- What kind of data do you hold? PII, health data, financial data, etc.
- Assets, revenues, number of employees, proposed merger or acquisitions?
- Logging enabled? Retention period for log files?
What you should be asking an insurer

- Are the terms of the policy negotiable?
- Is the coverage retroactive? How far back if so?
- How much coverage do you need, given size, data held, etc.?
- Does the policy cover regulatory fines?
What you should be asking an insurer

• Discount if you have a 3rd party audit and remediate any critical vulnerabilities?
• Other discounts?
• Are you covered if a vendor holding your data is breached?
• What actions (or inactions) of yours might void coverage?
• Misrepresentations on application
Cyberrisks in the courts

- A number of cases, insurers winning much of the time
- 2017: Moses Afonso Ryan – 10-lawyer R.I. firm struck by ransomware
- Sued in federal court for $700,000 in lost billing
- Crippled for 3 months, paid over $25,000
- Insurer Sentinel paid $20,000 (the limit) for certain computer-related losses, law firm argued that Business Income coverage required it to pay actual losses over a 12-month period
Cyberrisks in the courts

- Medidata Solutions wired $4.8 million after receiving e-mail from its president (not) who introduced her to an attorney (not) in an acquisition
- July 2017 – District Judge held that e-mail spoofing constituted fraudulent entry of data, triggering protection under the computer fraud provision
- Also covered under the funds transfer fraud policy
- Appeal pending in 2nd Circuit
- 2018 – The Year of the Phish
Insuring companies “shaming”

- “We don’t insure stupid”
- Cottage Health Systems
- Medical data exposed on Internet
- Columbia Casualty – Cottage failed to follow “minimum required practices” spelled out in the policy
- Stored data unencrypted on a system accessible on the Internet
- The first of many sins . . . .
Cyberinsurance companies (some of the leaders)

- Liberty Mutual
- Beazley Insurance Co.
- Chubb Ltd.
- Travelers
- Hiscox
- CNA
- AIG
Apple, Cisco team up with insurance companies to offer cyber policy discounts

• February 5, 2018 - teaming with insurer Allianz SE
• Primarily for businesses using their equipment, which is regarded, at least by them, as more secure
• Requires cybersecurity evaluation by Aon, a risk management firm
Walk carefully – it’s dangerous out there!
• YOU play the most important part in keeping TECHSHOW exciting. *Please complete the Speaker evaluation before you leave.*

• Reserve the dates!

TECHSHOW 2019: February 27 – March 2, 2019