Cyber Liability Insurance: A No-Brainer?

Jake Kouns  @jkouns
CISO  jake@riskbasedsecurity.com
Risk Based Security  www.riskbasedsecurity.com
State Of Security
Data Breaches

Breaches Over Time

Records Lost Over Time

Source: CyberRiskAnalytics.com
Vulnerabilities

Source: VulnDB
Data Breach – Ticking Time Bomb?

Only a matter of when for most organizations?
Data Breaches cost organizations money?
Risk Management
Reality of Risk

Perfect Security?

NOT JUST SECURITY, THE RIGHT SECURITY
Reality of Risk

Law of Diminishing Returns

\[
\frac{1}{X} \sum_{i=1}^{x} \frac{1}{2^{i-1}} = D
\]
Reality of Risk

Accept

Mitigate

Risk

Transfer

Avoid

NOT JUST SECURITY, THE RIGHT SECURITY
Reality of Risk

Avoid

• Not always possible

Mitigate

• Controls are key, but...

Accept

• High level of certainty around the impact
Transfer Options

- Outsourcing
  - Contracts & Agreements
  - Insurance
Insurance
Insurance Drivers

• Insurance is purchased for numerous reasons:
  – Reducing liability
  – Loss recovery
  – Legal requirements
  – Securing loans and/or investments
  – Improving business image and stability
  – Peace of mind

• Typically purchased for most valuable assets
Insurance Coverage

NOT JUST SECURITY, THE RIGHT SECURITY
Insurance Coverage

NOT JUST SECURITY, THE RIGHT SECURITY
Insurance Coverage
Insurance Coverage

NOT JUST SECURITY, THE RIGHT SECURITY
Cyber Insurance Coverage

Why haven’t more organizations bought Cyber Liability?:

- They have “unbreakable” security controls?
- They think the coverage won’t last or respond?
- They don’t believe it’s a good spend of budget?
- They are not aware of the market?
- Something else?
- Perhaps, organizations don’t truly understand it?
Trust The Salesman!
But is it well deserved?

CLAIM DENIED

TRICKS OF THE TRADE

HOW INSURANCE COMPANIES DENY, DELAY, CONFUSE AND REFUSE

NOT JUST SECURITY, THE RIGHT SECURITY
Many Names, Little Commonality

- Cyber Liability
- Privacy Injury Liability
- Network Security Liability
- Data Privacy
- Theft of Digital Identification
- Cyber Extortion
- Internet Liability
• **Annual premium volume information about the U.S. Cyber Risk market is hard to come by,**
  – Estimated annual gross written premium is in the **$2.5 Billion range** (up from $2 Billion in last year‘s report).
  – Betterly Report June 2015
• **50+ Carriers have a stand alone Cyber Liability Product**
  – Many, many more with packaged policy or excess
Cyber Insurance

NOT JUST SECURITY, THE RIGHT SECURITY
Cyber Insurance

**First Party**
Pays to fix the things we own when damaged

**Third Party**
Pays others when our actions (or inaction) causes harm

As a result of a security event including data compromise
Cyber Insurance

Third Party

First Party

Michael Jastremski

NOT JUST SECURITY, THE RIGHT SECURITY
Why does this matter?

Because it means organizations can buy a policy that can cover *both*

- Security event recovery costs

&

- Protection from lawsuits arising out of a data compromise
Cyber Insurance

**Breach Notice Compliance**
- Forensics
- Legal fees
- Mailings
- Credit Monitoring
- Identity protection

**Liability**
- Defense costs
- Settlements
- Responding to regulatory investigations
- Costs to reissues credit or debit cards
- Website & Social Media

**Other 1st Party**
- System Restoration & Extra Expense
- Payment of Extortion Demands & Lost Business
Cyber Liability “Gotchas”
But I buy GL or professional liability insurance, so I’m covered for all this stuff, aren’t I?
Sony’s insurer is contesting any obligation to cover the electronics giant for costs related to lawsuits filed over its massive PlayStation Network breach earlier this year.

In a complaint filed with the state Supreme Court in New York, Zurich American Insurance Co. is seeking "declaratory relief" from having to defend and possibly compensate Sony over class-action lawsuits or state attorneys general actions filed in response to the breach.
Why You Shouldn't Count On General Liability To Cover Cyber Risk

Travelers Insurance's legal spat with P.F. Chang's over who'll pay breach costs will likely illustrate why enterprises shouldn't think of their general liability policies as backstops for cyber risk.

As the legal troubles for P.F. Chang's restaurant chain kept piling up over the breach discovered this summer affecting 33 of its locations, its legal team made an insurance end-around play that many enterprises try after a breach. It filed a claim for coverage under its comprehensive general liability (CGL) policy. But a lawsuit filed earlier this month from its general liability insurer, Travelers Insurance, offers a good lesson to organizations on why this ploy rarely works.

Travelers asked the US District Court in Connecticut to clear it of any obligation to defend or indemnify the restaurant company during breach litigation. Its argument to the court: that not only is a breach like this not covered in its general policy definitions, but that even if it were, the restaurant company hadn't met a $250,000 basement floor limit up to which the firm needed to self-insure for covered events.
Cyber Insurance

As helpful as some of these policies can be, expect some things not to be covered
Reputation Damage
Cyber Insurance

Regular maintenance        Upgrades        Fixes

NOT JUST SECURITY, THE RIGHT SECURITY
Cyber Insurance

The economic value of data

Data or systems in the care, custody or control of others
Coverage – Common Exclusions

• Infringement of intellectual property/trade secret or value of proprietary information
• Fraud, but look for severable & final adjudication
• Employee theft of monies or securities
• Cost of upgrading the system
• EPLI, Pollution, Discrimination, Contractual
Coverage – Not So Common Exclusions

- Failure to encrypt data (mobile devices)
- Failure to maintain or take reasonable steps to maintain security
- Coverage limited to web site and Internet activities only
- Widespread virus / Spyware
- Failure to comply with PCI standards
- Wireless
- Cloud / SaaS
- Business Income Loss
Sublimits

- Notification Costs
- Credit Monitoring
- Public Relations Expenses
- Forensic Costs
- Extortion Costs
- Reward Reimbursement
Underwriting and Pricing
Typical Underwriting Considerations

• Basic security controls
• Type of data processed, stored or transmitted
• Back up procedures for 1st party cover
• History of prior incidents
• Underwriting is far from a science
• Most underwriters are not security experts
• Typically written applications
• Model encourages less information not more
• Minimal security controls required are... LOW
• Typically no scans or audits performed
Cyber Insurance

Applications can be a single page or run up to 12 pages & require input from multiple departments.
Cyber Liability Underwriting

- Carriers do have prohibited classes/industries
- Most of the market rates on revenues
- Prices currently vary wildly depending on:
  - Revenues
  - Class of business / industry
  - Records / Data types
  - Controls
- Price may not be appropriate for all organizations
- Deductibles can vary
Willis Fires First Salvo in the Cyber Risk Model Race

FEBRUARY 4, 2015

In announcing what it describes as the “insurance industry’s first cyber risk modeling tool,” Willis Re’s new product may be the first shot in a battle among reinsurers and modeling firms to measure and underwrite the growing field of cyber risk.

The new model – PRISM-Re – will offer an analysis of the susceptibility to data breach events across the insurer’s portfolio using a ‘common shock’ methodology to encompass the possibility of contagion behavior, according to a company statement issued yesterday. Based upon the latest exposure data, the model estimates the “frequency of data breaches and the potential severity of insured losses arising from those events.
What’s the Cost of a Cyberattack?

A flurry of attempts to model the risk of a corporate cyberattack hasn’t provided many answers.

Modeling Cyber Risk

That, however, may be the easy part of the assessment. Much tougher is gauging the likelihood that a company’s most valued data will be threatened—that is, how alluring a target is it for cybercriminals? To answer that question, a growing number of insurance-related firms are developing models of the risk fed by data on corporate cyber break-ins. The models represent a chance for finance chiefs and risk managers to get a better sense of their companies’ risks of being hacked.

The history of cyberattacks is short, however, and information of which such events can cost a company is hard to come by. Relative to hazards like earthquakes, fires, and lawsuits—not to mention economic perils like capital-market volatility—the threat of bad actors breaking into computer systems and stealing vital information or creating havoc is in its infancy. Unlike, say, the knowledge amassed about hurricanes in the United States, which have been tracked for about 165 years, data about corporate cybercrime has only been recorded since the emergence of the Internet as a vehicle of commerce in the mid-1990s.
Integrating Cyber Liability Insurance
Integrating Insurance

• Executives understand risk:
  – Avoid, Mitigate, Accept and Transfer

• Organizations understand the need to protect their most important assets and transfer risk already:
  – Property (Buildings)
  – Casualty Coverage (Accidents)
  – Employment Practices Liability & Workers Comp (People)
  – Professional Liability - Errors and Omissions

• Speak to executives in terms they understand
Integrating Insurance

• Lets estimate costs for a security program for a small business (Approximately $2-5M revenue)
  – Security Staff
  – Security Software / Hardware
    • Antivirus, Encryption, Firewall, IDS, DLP, Compliance, Scanners, etc.
  – Security Consulting
    • External Vuln Scans, Pen Tests, PCI compliance, Legal, Awareness, etc.
Integrating Insurance

• For sake of argument..........  
• Lets say it costs a business with $2-5M in revenues spends approximately $200,000/per year on security  
• Not including initial investment costs  
• This estimate is extremely low if they are to implement proper security  
• Should they be spending more?  
• Does this ensure that they won’t have a breach?
Integrating Insurance

• Typical costs for Cyber Insurance are currently extremely reasonable
• Minimum premiums can be $1,500 for $1M in coverage
• Includes many Risk Management Services
• Pricing can change based on industry and controls
• Preferred pricing for critical services:
  – Forensics, notification, credit monitoring, legal, etc.
• Many smaller companies confused by security and are not yet doing anything
Integrating Insurance – Perfect Security
Integrating Insurance

- Larger organizations can also get Cyber Insurance for a reasonable cost
- Large hospital with $2B in revenues premium estimates:
  - $100,000 for $1M in coverage
  - $200,000 for $5M in coverage
- Limits are available up to $250M
- Pricing can change based on industry & controls
- Larger organizations have not shown much interest thus far in actually using Risk Management Services, but like them available
Despite some limitations, there is real value found in these cyber insurance policies.
Incident Response

Who you gonna call?

GHOSTBUSTERS
For professional paranormal investigation and eliminations

NOT JUST SECURITY, THE RIGHT SECURITY
Incident Response
Incident Response

- 24 million customers warned by shoe retailer their personal information compromised - January 2012
- Unauthorized access to the following customer account information:
  - names
  - e-mail addresses
  - billing and shipping addresses
  - phone numbers
  - last four digits of credit card numbers
  - cryptographically scrambled passwords
Company is known for their customer service!

Statement from CEO:

“Due to the volume of inquiries we are expecting, we realized that we could serve the most customers by answering their questions by email. We have made the hard decision to temporarily turn off our phones and direct customers to contact us by email because our phone systems simply aren't capable of handling so much volume.”

Breach Mitigation includes services such as hotlines!
Cybersecurity Insurance

Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured’s level of self-protection. Many companies forego available policies, however, citing as rationales the perceived high cost of those policies, confusion about what they cover, and uncertainty that their organizations will suffer a cyber attack.

In recent years, the Department of Homeland Security’s (DHS) National Protection and Programs Directorate (NPPD) has brought together a diverse group of private and public sector stakeholders – including insurance carriers, risk managers, IT/cyber experts, critical infrastructure owners, and social scientists – to examine the current state of the cybersecurity insurance market and how to best advance its capacity to incentivize better cyber risk management.

<table>
<thead>
<tr>
<th>Attachment</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2014 Insurance Working Session Readout Report</td>
<td>730.99 KB</td>
</tr>
<tr>
<td>February 2014 Cyber Insurance Health Care Use Case Roundtable</td>
<td>834.43 KB</td>
</tr>
<tr>
<td>May 2013 Cyber Risk Culture Roundtable</td>
<td>831.32 KB</td>
</tr>
<tr>
<td>November 2012 Cybersecurity Insurance Workshop Readout Report</td>
<td>943.02 KB</td>
</tr>
</tbody>
</table>
Cyber Insurance

Could insurance force uniform standards and increase security for all?
• Recommended Actions:
  – Continue to invest in the appropriate security controls
  – Define a response plan in case of a data breach
  – Understand your exposures
  – Understand your data types stored and amount (number of records)
Recommended Actions (cont):

- Discuss transferring a portion of risk in the form of Cyber Liability insurance with management
- Determine coverage that would be important to your organization
- Determine amount of desired coverage
- Obtain a Cyber Liability quote
- If appropriate, integrate Cyber Liability into your risk management plan
Integrating Insurance – Wrap Up

• Effective security programs cost $$$
• Yet, can still be compromised
• Cyber Liability insurance is cheaper than most controls and provides serious financial coverage including security services & preferred pricing.
• While there are “gotchas”, there are legit policies out there
• If you are a CISO and you have a breach. What do you want to say?
  – Whoops? Sorry.
  – We have a partner and coverage. Lets file a claim.
Discussion!
Cyber Liability Insurance: A No-Brainer?

Jake Kouns  @jkouns
CISO        jake@riskbasedsecurity.com
Risk Based Security  www.riskbasedsecurity.com