RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CRWD-W16

Cybersecurity Insurance: The Catalyst We've Been Waiting For

Mark Weatherford
Chief Cybersecurity Strategist
vArmour
@marktw

#RSAC

Agenda

- Insurance challenges in the market today
- 10 reasons to invest in cyber insurance
- Cyber risk assessment tools and services
- 10 key coverage items
- So, why is insurance a catalyst for security?
- Weatherford predictions - the future of cybersecurity insurance

Cybersecurity insurance challenges

- A static underwriting process for a dynamic risk
- Risk aggregation is global, not local
- Limited capacity
- Pricing risk – not for the faint of heart!

Insurance is an historically static business

- Historically, the majority of assessments have been based on a snapshot in time through completion of a written questionnaire, a telephone interview, or a presentation.
- This static approach is irrelevant in the cybersecurity market. Insurers are investing in, and partnering with, the security industry to develop and use risk tools to predict and monitor the threat and vulnerability landscape in real time.

Cybersecurity threat intelligence capabilities are becoming a standard component of the underwriting process.

Aggregation of risk

- Aggregation refers to the consequences of concentrated and cascading cyber risks where key aggregation attributes such as internet failure, compromised service providers, or a number of companies in the same (or different) sectors using the same IT system where something happens to that system and affects all of the companies in that industry.
- As cloud computing becomes more ubiquitous, one successful attack or the failure of a cloud host could cause losses to hundreds of thousands of parties who hold their data within the cloud.

Limited capacity

- Capacity refers to the supply of insurance available to meet market demand and depends on the financial ability to accept risk. For an individual insurer, capacity is the maximum amount of risk it can underwrite based on its financial condition.
- The cybersecurity insurance market only dates back to 1998 so very little actuarial actuarial data exists, which means capacity is still growing. As the cyber insurance market capacity grows, more meaningful limits will develop as loss data accumulates and risk modeling matures.

How do insurers price risk?

- A lack of sufficient metrics with respect to frequency and severity of loss, specifically with PII and PHI assets, and physical destruction as a result of cyber events makes pricing risk a challenge.
- Fundamentally, insurers look for a strong security culture within the company as a first step in risk triage. Additional factors such as industry, revenue size, geography, and actual assets at risk contribute to how risk is priced.

The evolving nature of cyber-threats (DDoS, APT, Ransomware) and the IT environment (virtualization, the Internet of Things, and the Cloud), compounds the problem of developing accurate actuarial data.

10 reasons to invest in cyber insurance

1. Changing threat landscape
2. Governance and an enterprise-wide risk management strategy
3. Increasing regulatory risk
4. Financial incentive
5. Vicarious risk to vendors, business associates
6. Insider threat
7. Compliance does not equal security
8. Monetizing the cost of cybersecurity
9. M&A activity
10. Operational technology

10 reasons to invest in cyber insurance

1. Dynamic threat landscape and growing number of adversaries

- Private sector companies are out-matched in their ability to combat cyber-attacks from nation states, global criminals and malicious insiders.
- In no other arena are private companies expected to do battle with:

10 reasons to invest in cyber insurance

2. Governance and an enterprise-wide risk management strategy

Cybersecurity has become a governance issue for Boards and they are increasingly looking to cybersecurity insurance as a financial instrument for transferring risk.

Cybersecurity involves the entire enterprise, including stakeholder domains outside the IT department. Driving a culture of collaboration between stakeholders is challenging, but the underwriting process can be the catalyst for better security throughout the organization.

10 reasons to invest in cyber insurance

3. Increasing regulatory risk

Board of Director liability is resulting in new focus on cybersecurity governance. 2011 SEC guidance highlights that regulators see cybersecurity insurance as part of a strong enterprise risk management strategy.

The NIST Framework is increasingly being viewed by many in the legal community as creating a standard of care to be used by plaintiff attorneys to allege lack of sufficient oversight and even negligence.

10 reasons to invest in cyber insurance

4. Incentives

Even though they have failed to pass legislation that drive stronger enterprise security, Legislators are beginning to give greater legitimacy to the role of cybersecurity insurance.

There is growing support for market-based incentives such as insurance, that reward strong cybersecurity programs with discounted premiums and broader coverage.

The lack of robust actuarial data to model risk, and a changing underwriting process that validates the dynamic threat environment is a growing priority for the insurance industry.

10 reasons to invest in cyber insurance

5. Interdependencies and third party risk

Adversaries are increasingly focused on third parties such as Managed Service Providers, off-prem maintenance, and even cloud services that have access to sensitive information and other critical assets of the target enterprise.

Liability for PII or PHI typically still rests with the enterprise data owner, even though a breach may have occurred at, or been the fault of, the third party.

10 reasons to invest in cyber insurance

6. Insider threat

Attacks from the inside continue to be difficult to prevent. Cybersecurity insurance typically provides coverage when the employee is the perpetrator, just like when the attack is from the outside. This probably will not extend to acts involving the Board or members of the executive team however.

When asked who posed the biggest internal threat to corporate data, 55% of the respondents to the 2015 Vormetric Insider Threat Report identified Privileged Users, followed by contractors, service providers, and business partners.

10 reasons to invest in cyber insurance

7. Security Compliance

Treating security as a compliance issue distracts from real security and ultimately results in a false sense of security. Many companies have been in compliance with their required standards and still fell victim to a data breach or a security incident.

10 reasons to invest in cyber insurance

8. Monetizing the cost of cybersecurity

One of the biggest CISO challenges continues to be the ability to quantify cybersecurity risk to the executive team in terms of dollars and cents. The premium charged by an insurance company can help solve this problem, especially when implementation of security controls and policies reduces overall risk.

10 reasons to invest in cyber insurance

9. Merger and Acquisition (M&A) activity

The difficulty in evaluating the cybersecurity posture in any acquisition target leaves the acquirer vulnerable. A comprehensive due diligence risk assessment can go a long way in identifying threats and vulnerabilities that can satisfy the demands of cybersecurity insurance.

10 reasons to invest in cyber insurance

10. Operational technology

Industry sectors dependent on operational technology and industrial control systems are particularly vulnerable due to the often very distributed nature of the OT/ICS environment. Built primarily for 24/7/365 availability and to operate in remote and isolated environments, these systems and devices have historically been air-gapped but are increasingly being connected to the corporate information technology network and the Internet.

Cyber risk assessment tools and services

- A number of product and service companies have joined the market for automating the risk assessment process for cybersecurity insurance
- Underwriters are using (and developing) risk assessment products and services to require a higher level of risk maturity for potential customers
- Cybersecurity insurance customers are using risk assessment products and services to validate their maturity for underwriters and to drive down the cost of premiums

Exclusion is the name of the game

An exclusion clause, i.e., *"the fine print,"* is a clause in an insurance contract that eliminates coverage for specified events.

It's important that you understand what the restrictions are in the policy, including exclusion clauses, before you execute the contract.

EXAMPLE: The Company shall not be liable for Loss on account of any Claim based upon, arising from, or in consequence of any fact, circumstance, situation, transaction, event, act or omission of which any Insured had knowledge prior to the inception date of the first Liability Insurance Policy issued and continuously renewed by the Company to the Parent Organization.

10 key coverage items

1. Full prior acts coverage
2. Restrict knowledge and notice of a circumstance to the executive team
3. Security warranty
4. Operational technology
5. Outside counsel
6. IT Forensics
7. Law enforcement
8. War and Terrorism
9. Intentional Act
10. Continuity of Coverage

Ten key coverage items

1. Full Prior Acts coverage

Insurers typically try to limit coverage to acts from the first day that the policy begins, known as the retroactive date. However, in the context of the challenges in detecting an attack, buyers should seek to remove this exclusion and avoid the risk of a claim denial.

Ten key coverage items

2. Restrict knowledge and notice of a circumstance to the executive team

An insurer should not be allowed to attribute liability to the whole enterprise because enterprise-wide detection has proven to be a challenge for most organizations.

Ten key coverage items

3. Security warranty

Remove any language that tries to warrant that security is maintained to the same level as represented in the underwriting submission. The dynamic nature of the risk leaves this too open to insurer interpretation in the event of a loss.

Ten key coverage items

4. Operational technology

The majority of insurance policies provide coverage only to the corporate IT network. If relevant, ensure that language is broadened to also address operational technology such as SCADA and industrial control systems.

SCADAhacker

Think like a hacker ...

Ten key coverage items

5. Outside counsel

Choice of counsel must be agreed upon at the outset. In the event of a security breach, a dedicated legal expert must take the response lead, including attorney client privilege. Negotiating with an insurer during a security incident is a very bad idea.

Ten key coverage items

6. IT Forensics

Similarly to choice of counsel, the preferred forensics firm must be agreed upon up front and the decision should not be left to the underwriter. Incident response and forensics can be very expensive and and a significant part of the overall incident cost.

Ten key coverage items

7. Law enforcement

Law enforcement is typically involved in major security breaches and oftentimes the first time a company knows they've been a victim is when the FBI knocks on the door. A claim should not be excluded by an insurer for "failure to disclose as soon as practicable" if law enforcement had advised nondisclosure during the investigation.

Ten key coverage items

8. War and Terrorism

Many insurance policies exclude coverage for acts of war such as invasion, insurrection, revolution, military coup and terrorism. With the emergence and growth of the nation state adversary's, this clause must be eliminated from any insurance contract.

Ten key coverage items

9. Intentional Act

Coverage that addresses the employee or insider as perpetrator acting in isolation of the executive team.

Ten key coverage items

10. Continuity of Coverage

When renewing the insurance policy with the same insurer, you should always avoid signing a warranty regarding a circumstance or claim.

So, why is insurance a catalyst for security?

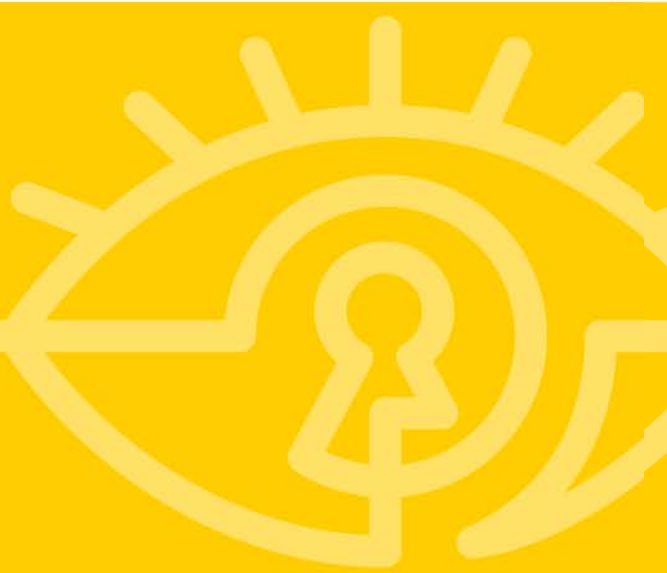
- Shareholders expectations are rising
- CEO's are paying attention
- Boards don't understand security and are nervous
- Regulators are enforcing compliance
- Legislators want to legislate
- Underwriters are incentivizing better security behavior

The future of cybersecurity insurance

- Continuous monitoring and risk scoring will be the new norm. This is the process of maintaining real time awareness of security threats and vulnerabilities that support organizational risk management decisions.
- Premiums and rates will vary monthly, weekly, daily, and hourly based on dynamic threat and vulnerability environment
- Underwriters will establish new relationships with security product vendors to incentivize spending
- Insurance brokers will become your new best friend

Apply what we've discussed today

- Next week you should ask about and review your corporate cybersecurity insurance policy (if you have one)
- In the next three months you should:
  - Review your most recent enterprise risk assessment
  - Discuss your corporate cyber risk appetite with CEO and CRO
  - Meet with your insurance broker to discuss your cybersecurity insurance policy
- In the next six months you should begin budgeting and scheduling an enterprise risk assessment and considering potential tools or services to automate and provide visibility into your risk environment.



Thank You

mark@varmour