Managing Technology Risk with Cyber Insurance

Paul Rohmeyer, Ph.D.
Associate Industry Professor

School of Business
Stevens Institute of Technology

FINCYBERSEC

Key Points

- The state of the cyber insurance marketplace
- An understanding of coverage types for cyber policies, as related to current threat models
- The practical limitations of relying on transfer as a risk treatment option
- How to incorporate cyber insurance in the enterprise risk management program
- Observations and key learnings from recent cases involving cyber insurance

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

Quick Review – Risk Treatment

Risk is part of all business and technology contexts, characterized by threats that may exploit vulnerabilities in systems and thereby produce negative consequences.

We can TREAT risk by…

- **Avoidance** by pursuing alternative solutions
- **Mitigation** via introduction of controls to reduce likelihood or impact
- **Acceptance** and establish continuous monitoring
- **Transference** via …
  - Contract – e.g. business partner assumes risk
  - Insurance

Risk Treatment represents a jump from theoretical to practical.

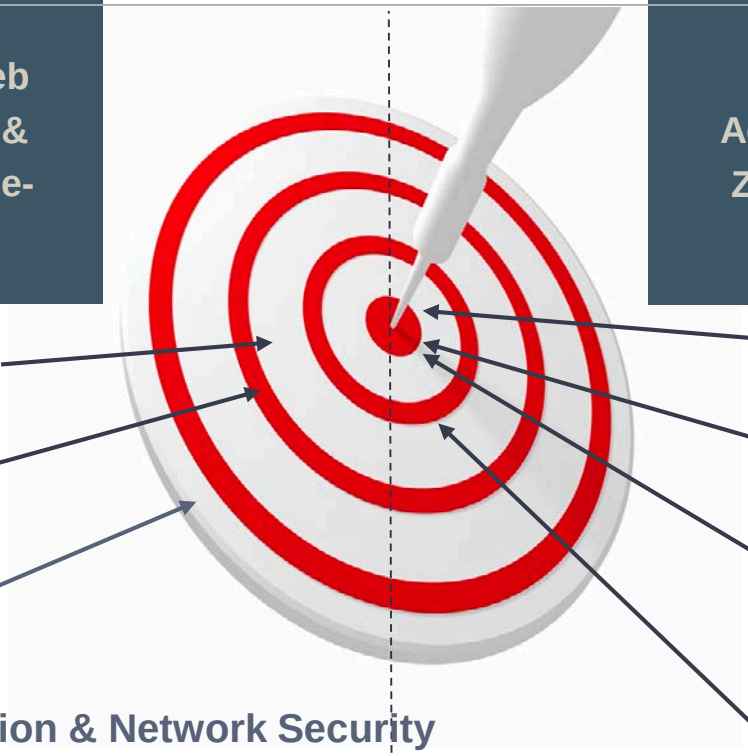
FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Attack Sophistication is Growing

Denial of Service, Hijacked Sessions, Web Defacements, Viruses & Malware, Known or One-Off Exploits

Stealthy Infiltration, Embedded Malware & Agents, Social Engineering, Zero-Day Exploits, Rapidly Changing



Hacker Groups

Hacker

Script Kiddies

State-Supported

Corporate / Criminal

Cyber Terrorist

Hacktivists

"1st Generation" Information & Network Security

- Security by prevention
- System & software vulnerability assessment
- Penetration testing
- Respond to most-recent event
  - Effectiveness rarely assessed
  - Prepared for the "last war"
- Hyper focus on technology & compliance

Emerging "2nd Generation" Threats

- Quickly evolving; seeks asymmetric advantage
- Persistent & patient; waging long-term campaigns
- Structured organization & planning
- Well-resourced (money, people, skill)

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Costs of Cyber Crime are Growing

- Average Cost of Cybercrime Per Company - $7.7 Million
- Time to Resolve Attacks
  - 2010 – 14 Days
  - 2015 – 46 Days
    - *A 229% Increase*
- Number of Attacks Per Year Per Company
  - 2012 – 68
  - 2015 – 99
    - *A 46% Increase*

Ref: Ponemon Institute based on studies of 252 companies in 7 Countries

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Current Cyber Insurance Marketplace

What is a Cyber Insurance Policy?

- Can be a separate policy (most common)
- May appear as an endorsement to Errors and Omissions
- Largest carriers are limiting policies at $100 million
- Coverage is very specific – not blanket protection for all cyber assets!
- Relatively more complex than other types of insurance
- Individual policy characteristics can be negotiated
- May require specific practices/capabilities such as incident response

Ref: Fogle Law Firm PLC

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

State of Cyber Insurance Market

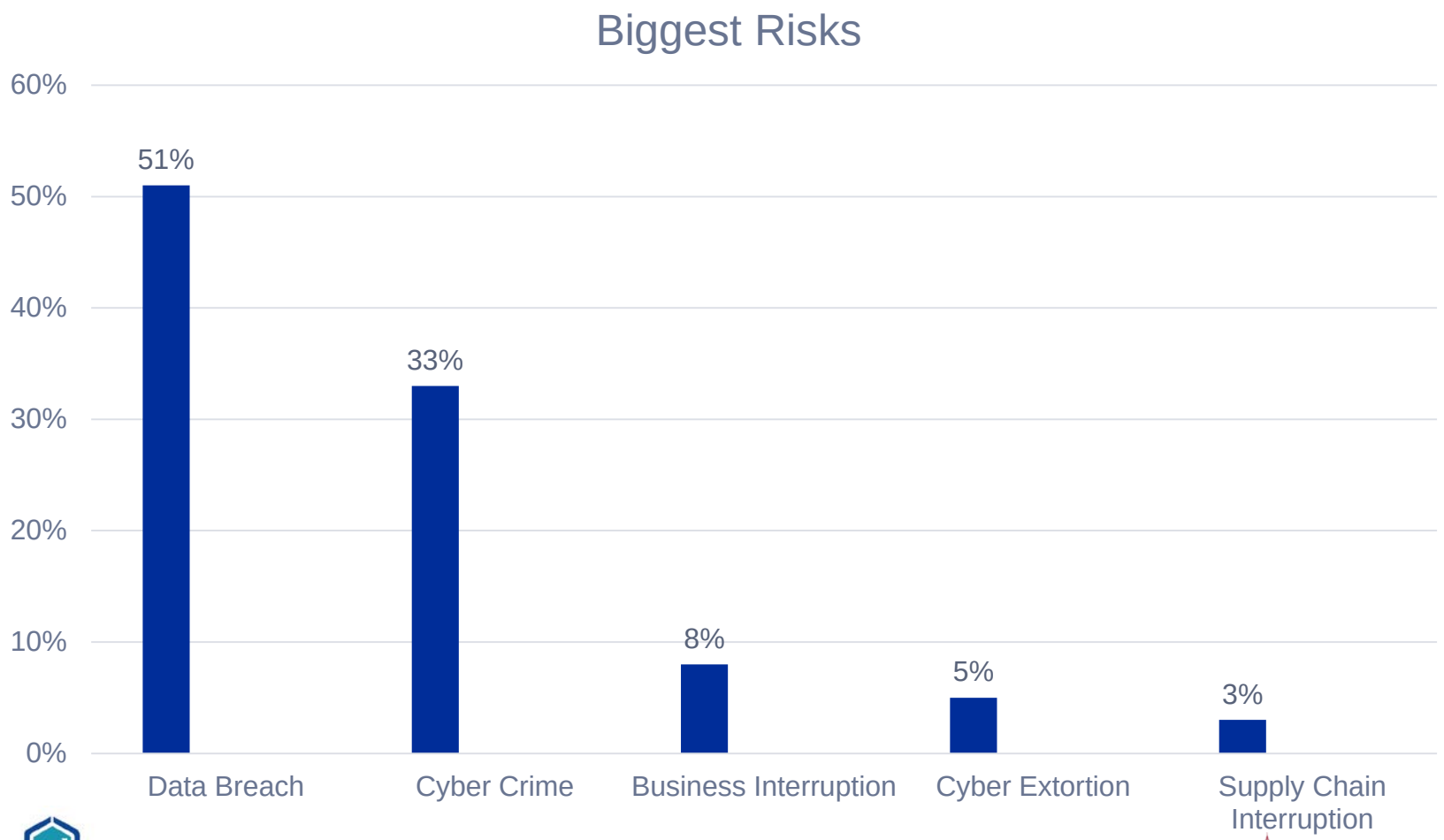
- Global Marketplace is estimated at $1 Billion to $1.5 Billion
- 70% of Global Carriers are based in USA
- European Carriers Account for approx. $150 million

Ref: Advisen Cyber Liability Insurance Market Trends Survey

FINCYBERSEC

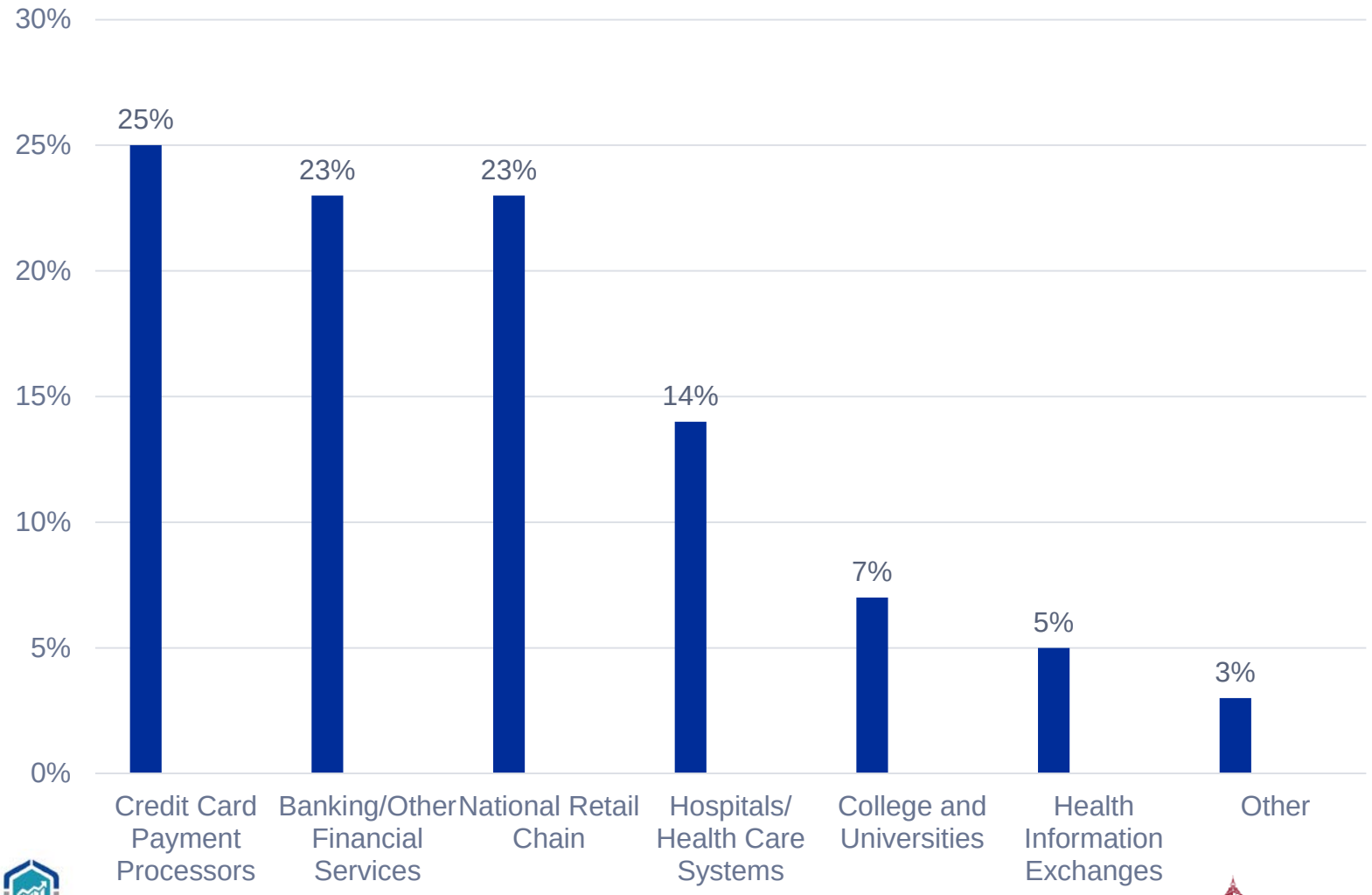
STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

The Insurers' Concerns - Biggest Challenges Facing Business



Verisk Cyber Insurance Survey

Most Vulnerable Sectors to Insure



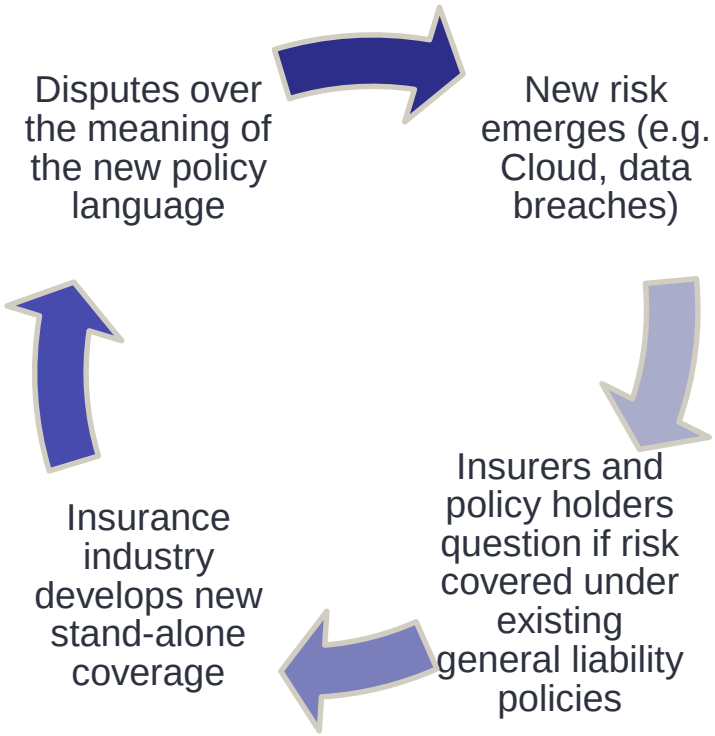
Verisk Cyber Insurance Survey

Common Causes of Loss/Damages

- Direct, actual losses resulting from a cyber event
- Liability (e.g., fiduciary duties)

Summary of the Current Marketplace

- Insurance industry is wrestling with determining how much risk they have underwritten – lack of actuary data and robust metrics – and accurate ways to measure them
- Insurance premiums are skyrocketing
  - The insured want to lower their premiums
  - The insurance companies want to be competitive and reasonable
- "Coverage exclusions" are part of the scenery



Ref: Delta Risk LLC, Adapted from "The Future of Cyber Coverage Disputes"; Thomas Bick, in US Cybersecurity Magazine, Winter 2016

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Summary of the Current Marketplace

- Cyber crimes impacted even the biggest corporations with the most sophisticated controls environments
  - Note: Organizations with underutilized or misconfigured technologies will not achieve security effectiveness; *simply buying tools does not make you more secure!*
- There is a growing demand for cyber insurance due to increasing volume of attacks and breaches and, perhaps, regulatory oversight
- Due to the high demand…
  - Premiums are going up as carriers recognize they may not have sufficient capital to cover claims
  - Deductibles raised

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Lack of Providers Offering Cyber Insurance

- Most carriers do not sell cyber insurance
- This leads to higher prices as the number of insurers is low, although competition among them is significant
- In a survey by Verisk ISO of 271 insurance companies only 46% indicated they offered cyber insurance
- Not a single company expected to underwrite less cyber insurance in the next year as compared to the previous one
  - About 75% of the companies expected an increase in the amount of cyber insurance they expected to sell

Verisk Cyber Insurance Survey

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Lack of Data - The Carriers' Challenge

- Insurance of all types has always been designed and priced according to actual historical event experience
- Actuaries analyze the actuals to determine incident frequencies, reported losses, and other important factors
- This is compounded by organizations struggling to capture the complete costs of a cyber event
- The lack of consistent and reliable historical data sources makes actuarial analysis challenging if not impossible, thereby providing little or no use to the underwriting process
- The result is a reliance on incomplete data

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Multiple Carriers Can Share Risk in “Towers”

- Insurance “towers” spread risk across carriers and provide coverage/protection in the event an event overruns risk forecasts.
- Most large companies align their policies in towers because the big carriers are reluctant to shoulder the whole risk.
- Interestingly, this is where the second level of competition to underwrite exists (the first being a seat in the tower). Carriers are bidding aggressively to be the first $10M paid out because the first one gets to collect higher premiums, and they are all assuming the entire tower will be paid out.

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Why More Companies are Not Buying

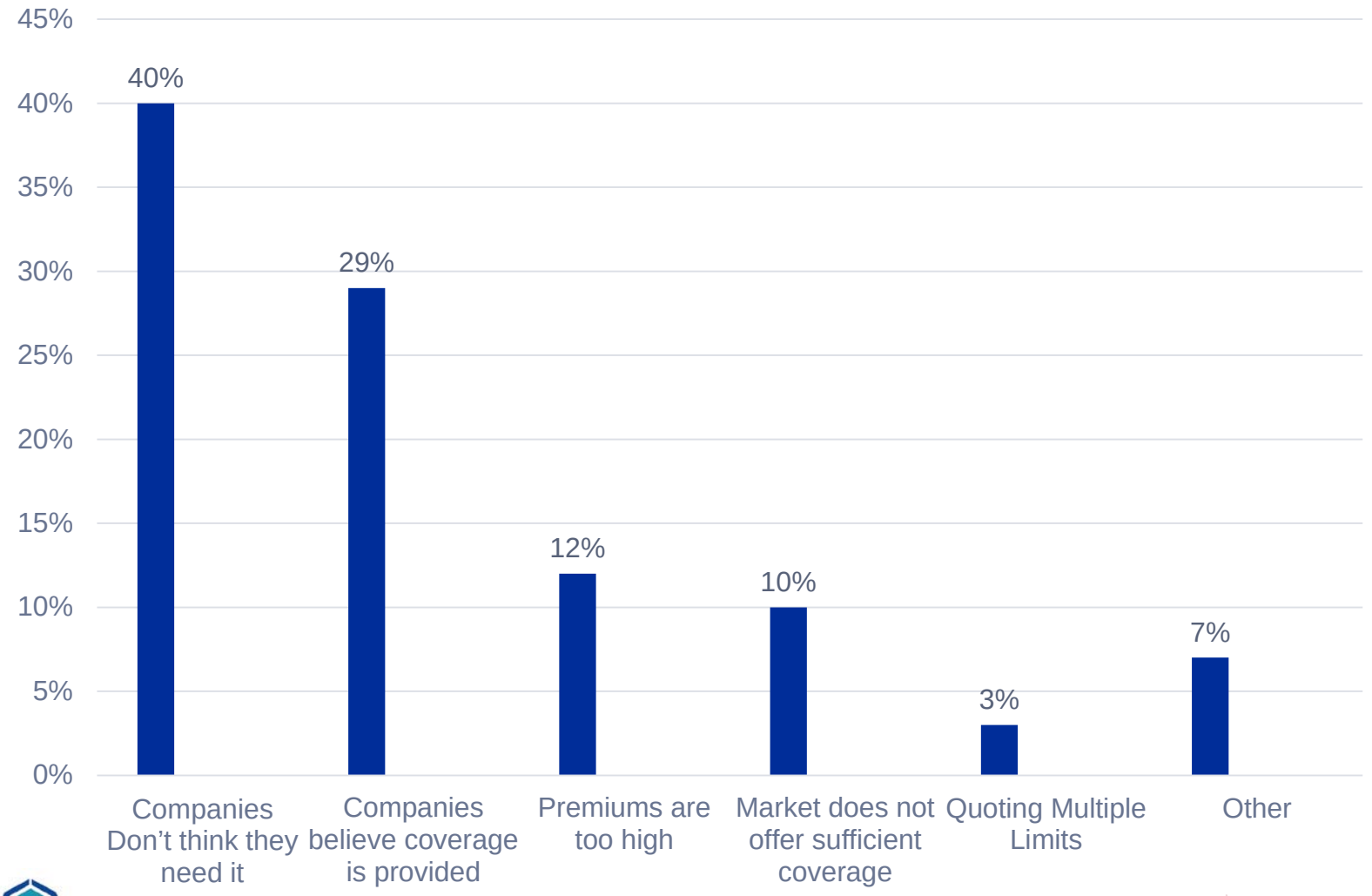
- You may suspect the most common reasons why more companies don't buy cyber insurance is because premiums are rising, or sufficient coverage is not being offered.
- But survey data points to a lack of awareness of the actual risks, causing companies to conclude they don't require cyber insurance.
- Many that feel that cyber insurance is already covered in their existing policy.

Verisk Cyber Insurance Survey

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Why More Companies are Not Buying



FINCYBERSEC

Verisk Cyber Insurance Survey

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

First Party Coverages: Pays for Your Losses

- Theft and Fraud Coverage
- Forensic Investigation
- Network/Business Interruption
- Extortion
- Data Loss and Restoration
- Etc.

Raptis, S. (2015, March 13). Analyzing Cyber Risk Coverage. Retrieved from http://www.riskandinsurance.com/analyzing-cyber-risk-coverage/

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Third Party Coverages: Pays Others for Losses They Say You Caused

- Privacy Liability Coverage
- Regulatory Actions
- Notification Costs
- Crisis Management
- Call Centers
- Credit/Identity Monitoring
- Transmission of Virus/Malicious Code

Raptis, S. (2015, March 13) Analyzing Cyber Risk Coverage. Retrieved from http://www.riskandinsurance.com/analyzing-cyber-risk-coverage/

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Need to Define the Policy Triggers

- Loss – Insurance is triggered as soon as we incur a loss due to a cyber attack.
- Claim – In this case, insurance is triggered when a claim is made against the insured during the policy period.
- Suit – In some cyber policies, insurance is triggered when a defense suit is brought against the insured.

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Challenge: Insuring Intangible Assets

- Insurers can easily value products which are tangible, like land, vehicle, property etc., and provide you with detailed insurance information.
- However, increasingly our most valuable assets are intangible
- Insurers do not have a consistent basis to assess the value of your data.

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Challenge: Calculating the Premiums

- How do most companies decide premiums for your cyber insurance policy? They assess the readiness of your system to avert cyber attacks!
- How do they check the readiness of your systems to avert cyber attacks?
- Historically the pricing process has relied on questionnaires and interviews.
- An industry-wide challenge is the lack of data to support the actuarial analyses typically completed by carriers to price traditional insurance lines… *this is all new!*

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Challenge: Calculating the Premiums

- Cyber Insurance focuses our attention on **big picture outcomes** to inform businesses on prevalent risk dimensions
- Therefore, we need to be concerned with **overall effectiveness** in cyber security
- Demonstration of overall effectiveness requires testing the full architecture - personnel, processes, technologies – by completing drills and tests that mirror real-world conditions such as **cyber war gaming**
- **In other words… Insurers will not base your cyber insurance premiums on how well your last pen test went! Organizations will need to demonstrate robust capabilities to protect against high impact, emerging threats!**

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Using Cyber Insurance as a Layer in the Enterprise Risk Management Program

Hopefully this point is Obvious: Insurance should not be used as a Primary Risk Treatment Option

- Cyber insurance should not be relied on as a primary risk treatment option, but deployed to complement the protective and detective controls architecture, and primarily be used as a source of funding for response and recovery

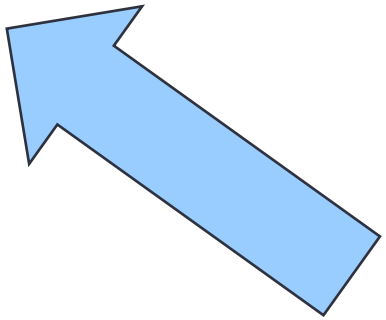
FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Cyber Insurance as a Control Layer

Enterprises must deploy complementary layers of controls to effectively treat risk

- Protective/Preventative –firewalls, access controls
- Detective – IDS, system log monitoring
- Response – Incident Response & Forensics
- Recovery – Return to Business as Usual



Cyber Insurance can provide funding to address many recovery concerns

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Cases

Sony Data Breach

- Sony Pictures suffered a massive attack on its systems.
- A group of hackers who called themselves Guardians of Peace(#GOP) leaked internal documents including spreadsheets containing information and data about company's employees and senior executives.
- Also, a copy of the unreleased movie, *The Interview*, was leaked by the group, which led to Sony cancelling all screenings of the movie in the USA.
  - The hackers made unspecified threats of violence against theater owners, which led to most theatres refusing to show the movie.
  - The film's production cost was $40 million.
- Documents that were released included sensitive information about the employees, salaries of senior executives, and even emails exchanged between employees.

FINCYBERSEC

The Hack of Sony Pictures: What We Know and What You Need to Know. (2014, December 8). Retrieved from http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Sony – Insurance Perspective

- One of the leaked documents contained detailed information on Sony's cyber insurance.
- Sony held a $60 million cyber insurance cover with Marsh at the time of the leak.
- When Sony was breached in 2011, it had made a claim of $1.6 million with Hiscox, its cyber insurance company at the time, but Hiscox declined to renew their insurance.
- Sony turned to Lockton, which provided a policy of $20 million, which $10 million in self retention.
- In April 2014, Sony took out insurance with AIG worth $10 million.
- In May, Sony took out insurance with Marsh worth $60 million.
- Marsh reached out to Brit Insurance, Liberty International Underwriters, Beazley and other carriers to secure the insurance amount.

Hillebrand, Melissa. (2014, December 8). 2016 Sony Pictures holds $60 million Cyber policy with Marsh. Retrieved from http://www.propertycasualty360.com/2014/12/18/sony-pictures-holds-60-million-cyber-policy-with-m?slreturn=1455313471

Target Data Breach

- Attack took place from November 27 - December 15 of 2013.
- The credit and debit card information of about 42 million customers was stolen including card numbers and three digit CVV code and even the PIN number
- But total number of people who had some kind of personal information stolen was around 70 million
- The attack was carried out by hacking compromised point of sales terminals to get to customer data
- Financial impact was substantial

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Target – Insurance Perspective

- Target offset much of the losses they incurred by a strong cyber insurance… of the initial $61 million in damages they incurred, $44 million was covered by their cyber insurance
- Target disclosed that breach related expenses included costs for reissuing cards, lawsuits, government probes and enforcement proceedings, legal expenses, investigative and consulting fees, and capital investments.
- …however, Target declined to clarify what type of costs its insurance will cover and who are its insurers.

Skarichan, D., & Finkle, J. (2014, February 26). Target's Cyber Insurance Softens Blow of Massive Credit Breach. Retrieved from http://www.insurancejournal.com/news/national/2014/02/26/321638.htm

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Home Depot Data Breach

- Hackers used a vendor's log on credentials to penetrate Home Depot and installed a sophisticated custom-built malware that stole customers' credit cards information and email addresses.
- The malware was installed on self-checkout registers and was designed to evade any kind of detection from any anti-virus software.
- Company initially stated in September that information about 56 million credit cards were stolen; in November it announced that an additional 53 million email addresses were also compromised.
- Home Depot said personal data that may have been compromised included customers' names, credit card numbers, expiration date, cardholder "verification value," and "service code."
- This makes it a larger attack than even Target's cyber attack and the largest attack on a US retailer.

Winter, Michael. (2014, November 17). Home Depot hackers used vendor log-on to steal data, e-mails. Retrieved 12 from http://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/

Home Depot Data Breach Cost

- In October 2015, Home Depot released data stating that attack had cost them $232 million by that time.
- Much of this was because of lawsuits filed against Home Depot by small community banks and Credit Unions that were affected by the data breach.
- These lawsuits accused Home Depot of ignoring warnings from security experts that its computer systems were vulnerable to attack
- But this cost could go into the billions as more lawsuits are being filed against Home Depot

Bronson, Caitlin. (2015, October 15). Home Depot cyber attack costs could reach into the billions. Retrieved from http://www.ibamag.com/news/home-depot-cyber-attack-costs-could-reach-into-the-billions-25358.aspx

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Home Depot – Insurance Perspective

- Home Depot had a Cyber Insurance coverage of $105 million at the time of the attack.
- The first layer is a $10 million coverage from AIG .
- After the AIG layer, there are two $10 million coverages from each from two Zurich Insurance Group Ltd. U.S. and international units.
- There is $15 million from Liberty Mutual Insurance Co. and $10 million from a unit of Houston-based HCC Insurance Holdings Inc.
- Above that are two $25 million layers of coverage written on a quota share basis.
- Home Depot had a self-insured retention of $7.5 million.

Greenwald, J. (2014, February 9). Home Depot has $105 million in cyber insurance to cover data breach. Business Insurance. Retrieved from http://www.businessinsurance.com/article/20140914/NEWS07/309149975

Conclusions

- Cyber Insurance can be a valuable tactic in your risk management strategy
- Risk transfer via insurance should be layered behind appropriately designed protective, detective, and response controls, respectively
- The cyber insurance market continues to evolve due to a general lack of reliable data to support traditional actuarial methods
- Coverage needs should be expected to change in response to shifts in threat and vulnerability landscape
- Carriers will educate and perhaps transform the cyber security landscape by introducing practices to reduce loss exposure
- Breach consequences, notably substantial financial losses, are becoming more visible

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

THANK YOU!

Paul Rohmeyer, Ph.D.
prohmeye@stevens.edu
Tel: 1.201.216.3814
Twitter: @paulrohmeyer
www.fincybersec.org

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

About the Speaker

Dr. Paul Rohmeyer, Industry Associate Professor, Stevens Institute of Technology, has over 20 years of professional experience in IT Management, IT Audit, Information Security, Disaster Recovery Planning, and Vendor Management among other areas. Paul is a faculty member at Stevens in the School of Business and has presented and published on information security, decision-making and business continuation. He has consulted since 2000, delivering executive-level guidance in the areas of risk management, information assurance and network security to premier corporate clients in the financial services, pharmaceutical and energy industries. Prior to his consulting career, Paul served as Director of IT for AXA Financial and Director of IT Architecture Planning for SAIC/Bellcore. Paul holds a MBA in Finance from St. Joseph's University, M.S. and Ph.D. degrees in Information Management from Stevens Institute of Technology and a B.A. in Economics from Rutgers University. Paul has achieved the CGEIT (Certified in the Governance of Enterprise IT), PMP (Project Management Professional), and NSA-IAM (U.S. National Security Agency Information Assurance Methodology) credentials.

FINCYBERSEC

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

STEVENS

INSTITUTE *of* TECHNOLOGY

THE INNOVATION UNIVERSITY®

stevens.edu