

## Cyber Insurance as a risk mitigation strategy

### Stuart Madnick

- John Norris Maguire Professor of Information Technology & Professor of Engineering Systems
- Co-founder and Director of MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity – MIT-(IC)<sup>3</sup>
- MIT Sloan School of Management (smadnick@mit.edu)


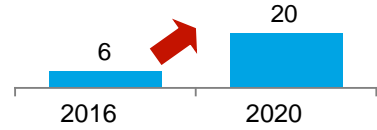







### Michael Coden

- Co-founder and Associate Director MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity – MIT-(IC)<sup>3</sup>
- Head of Cybersecurity Practice, BCG Platinion a company of The Boston Consulting Group (coden.michael@bcgplatinion.com)

With valuable assistance from GA (Fabian Sommerrock, Dominic Harington), MIT (Michael Siegel, Juan Jose Carrascosa Pulido, Mohammad Jalali), BCG (Nadya Bartol, Michael Bernaski) and special thanks to all of the interviewees and GA reviewers.



# Clear trends are shaping and growing the future cyber security market

Trend	Description	What we observe
 <b>Technology proliferation</b>	<ul style="list-style-type: none"> <li>Greater cyber vulnerability, amplified through IoT, cloud, social media, digitization</li> <li>Artificial Intelligence &amp; big data drive new defense tools</li> </ul>	<p>"Internet of things" devices (B)<sup>1</sup></p>  <p>6      20</p> <p>2016      2020</p>
 <b>Hacking threat &amp; tools</b>	<ul style="list-style-type: none"> <li>Greater number and impact/cost of cyber crime (from nodes to networks &amp; disruption)</li> <li>New methods (ransomware) &amp; open source</li> <li>State sponsored, coordinated attacks (IP)</li> </ul>	<p><b>~\$11M</b></p> <p><b>is median cost per attack</b> <b>(+190% since 2010)</b></p>
 <b>Widening capability gap</b>	<ul style="list-style-type: none"> <li>Already large cyber capability gap widens</li> <li>Cyber talent remains in short supply; shortage of in-house cyber skills</li> <li>Increasing demand for cyber services</li> </ul>	<ul style="list-style-type: none"> <li>Demand for cyber talent will grow by <b>53%</b> through 2018<sup>3</sup></li> <li>A shortage of 1.8 million qualified cybersecurity personnel by 2021<sup>5</sup></li> </ul>
 <b>More prevalent regulation</b>	<ul style="list-style-type: none"> <li>Growing prevalence of cyber regulation</li> <li>Increasingly tough privacy laws</li> <li>Varied evolution expected per geography, e.g., mandatory/voluntary, descriptive/not</li> </ul>	<p> <b>GDPR<sup>1</sup></b>, application 2018</p> <p> <b>Gov Cuomo</b>, Sep 2016, Cyber req. for Financial Services</p> <p> <b>China Cybersecurity law</b>, Nov 2016</p>
 <b>Growth in litigation</b>	<ul style="list-style-type: none"> <li>Cyber litigation expected to be 'next big thing' in legal circles</li> <li>Increase in class-action lawsuits</li> <li>Expansion of legal pursuits beyond USA</li> </ul>	<p><b>"Cyber Class action lawsuits will be common place in 5 years time."</b> <b>(Partner—US Law firm)</b></p>

1. Gartner, 2015 2. McAfee Labs Threat report 2. McAfee Labs Threat report 3. MIT Technology Review 4. EU Regulation: "General Data Protection Regulation" 5. (ISC)<sup>2</sup>



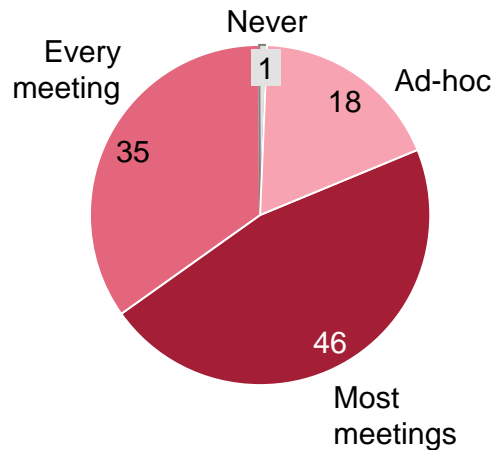
# Cybersecurity has become a board and c-suite imperative

Creating demand for cyber insurance – but upsetting the normal purchase dynamic



**99% of Boards discuss cybersecurity**

**Board survey:** How often is cybersecurity discussed during board meetings?<sup>1</sup> (%)



By comparison, in 2012, only 1/3 of boards were actively considering cybersecurity<sup>2</sup>

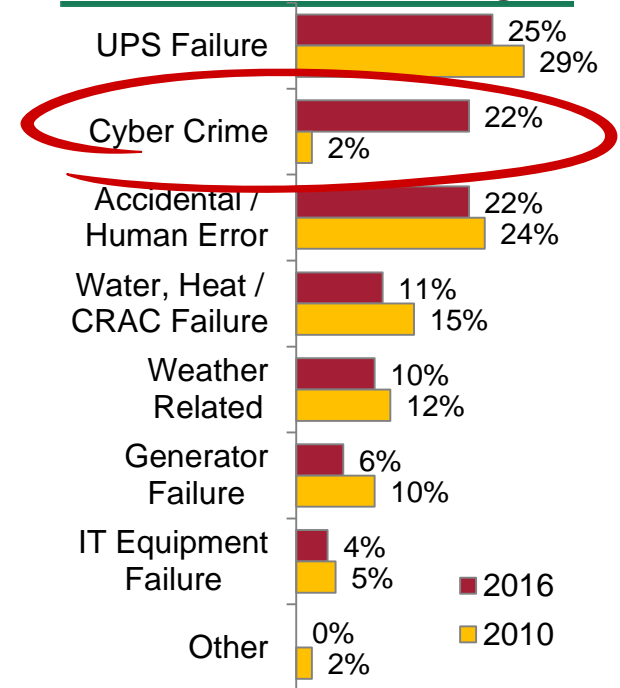


**CEOs see the strategic importance of security**



**Cyberattacks are now 2nd largest cause of business interruption**

## Root Causes of IT Outage



**Cyber crime increased 167%**

1. NYSE Governance Service Cybersecurity in the Boardroom 2015 survey 2. Georgia Tech Information Security Center: Governance of Cybersecurity 2015 Report 3. PWC 18th Annual Global CEO Survey (2015) 4. CIO.com 2016 State of the CIO Survey

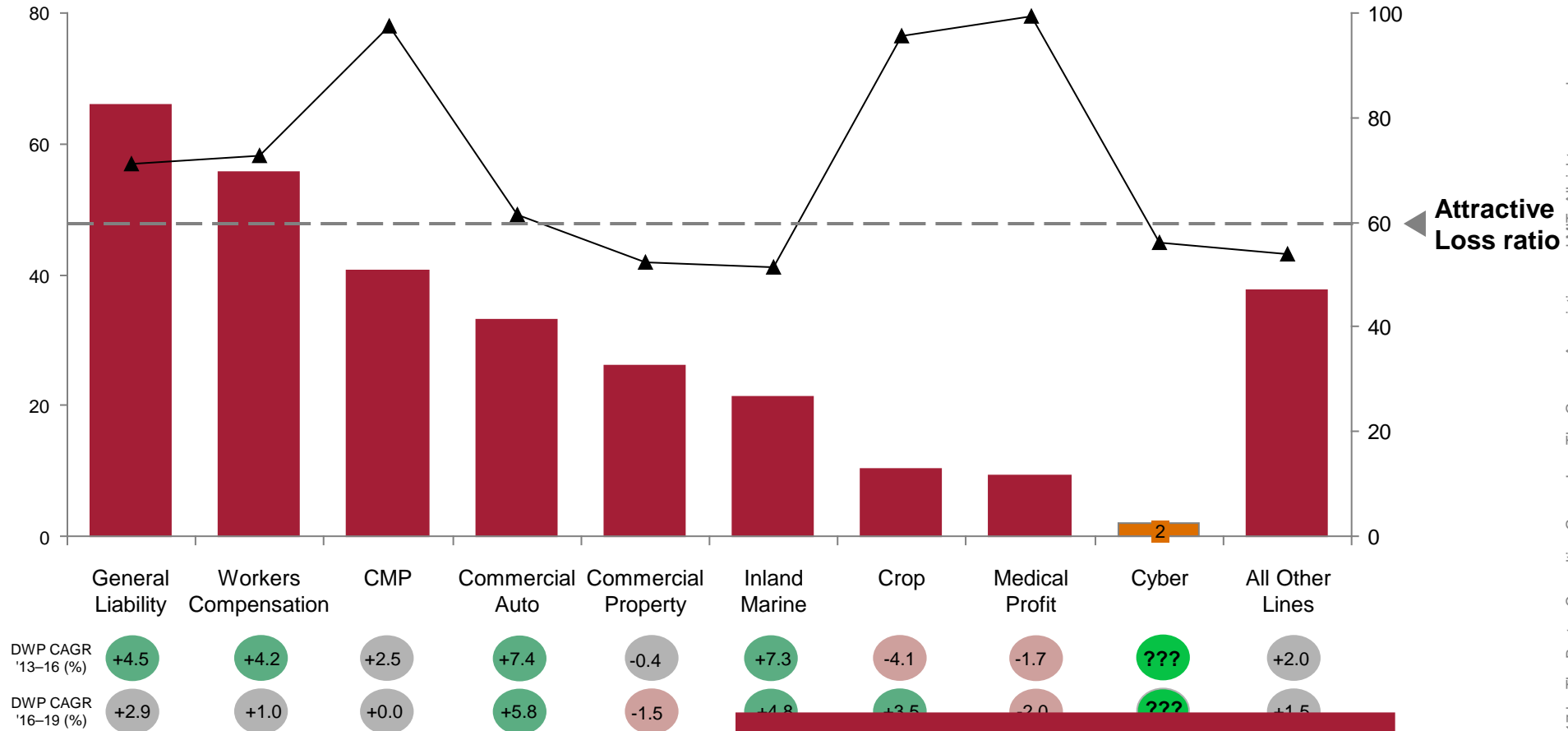


# Cyber insurance not material however profitable & highest growth LOB in commercial insurance



2016 Direct US commercial property & casualty  
Written premiums, \$Bn

Average  
COR '13-'16



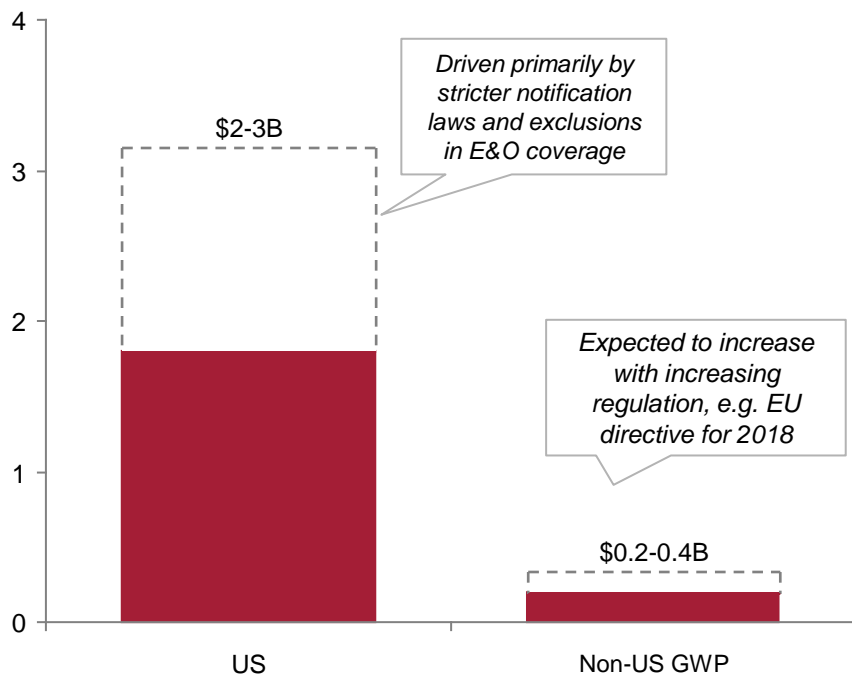
**Current cyber policies are mostly data protection  
New demand for cyber-physical property/casualty**



# Uptake so far has been limited outside large us companies, indicating substantial opportunity in SME & non-us markets

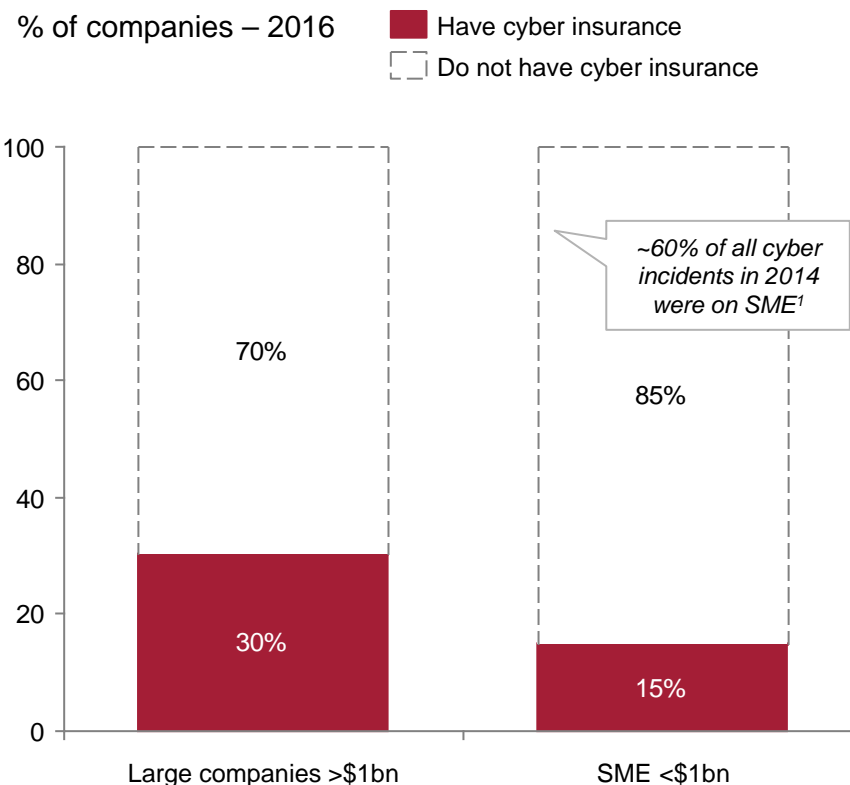
**US is currently ~90% of total gross written premiums, driven by regulation**

Estimated 2016 Cyber GWP



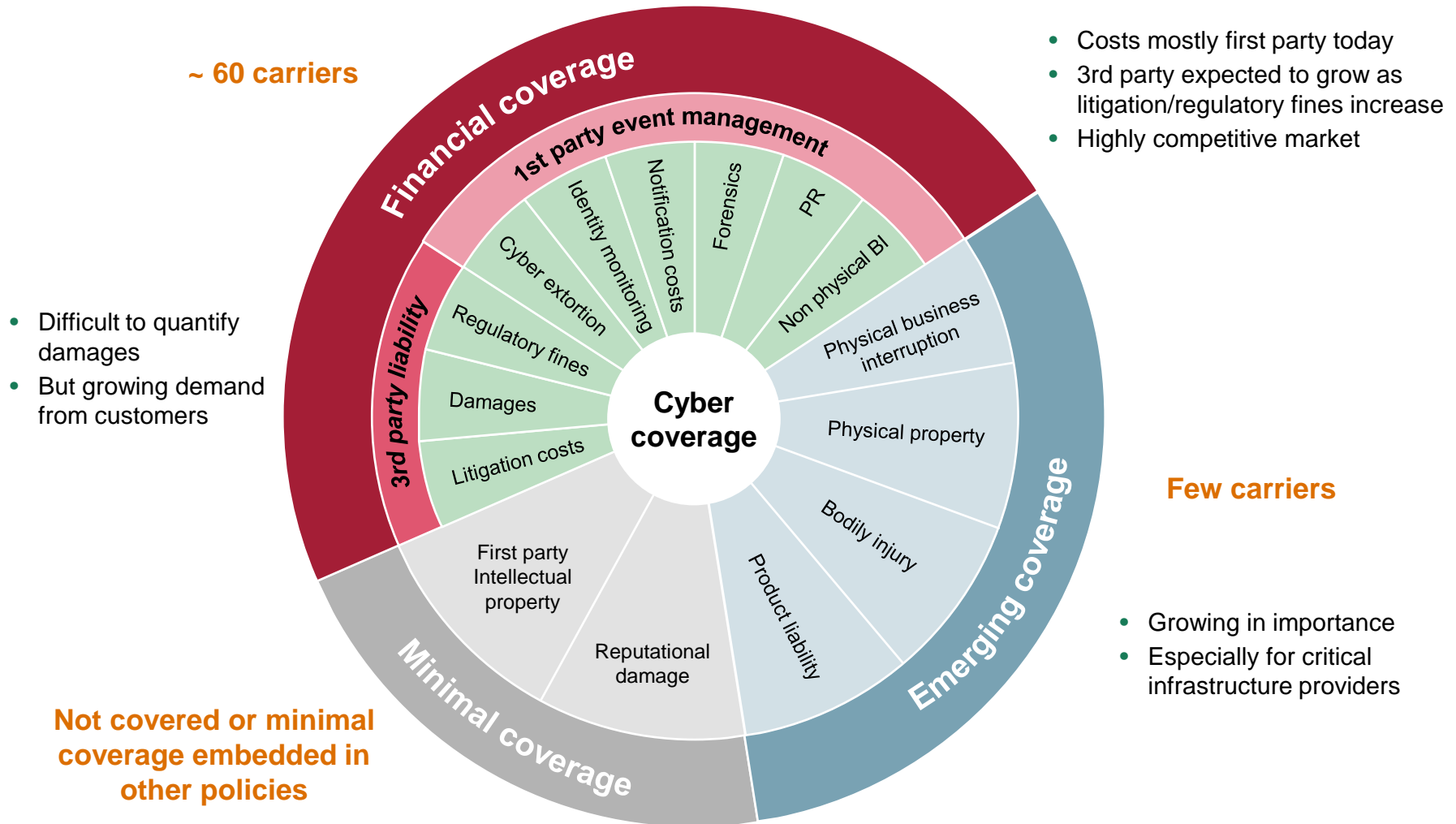
Source: 2015 Aon Global Risk Management Survey (n=1,41); Morgan Stanley, Allianz, Betterly  
1. Symantec (2015 report)

**Significant whitespace in SMEs, with half the penetration of companies \$1bn+**





# Initial risk transfer policy coverage is expanding to cover BI, property damage and physical injury – but gaps remain



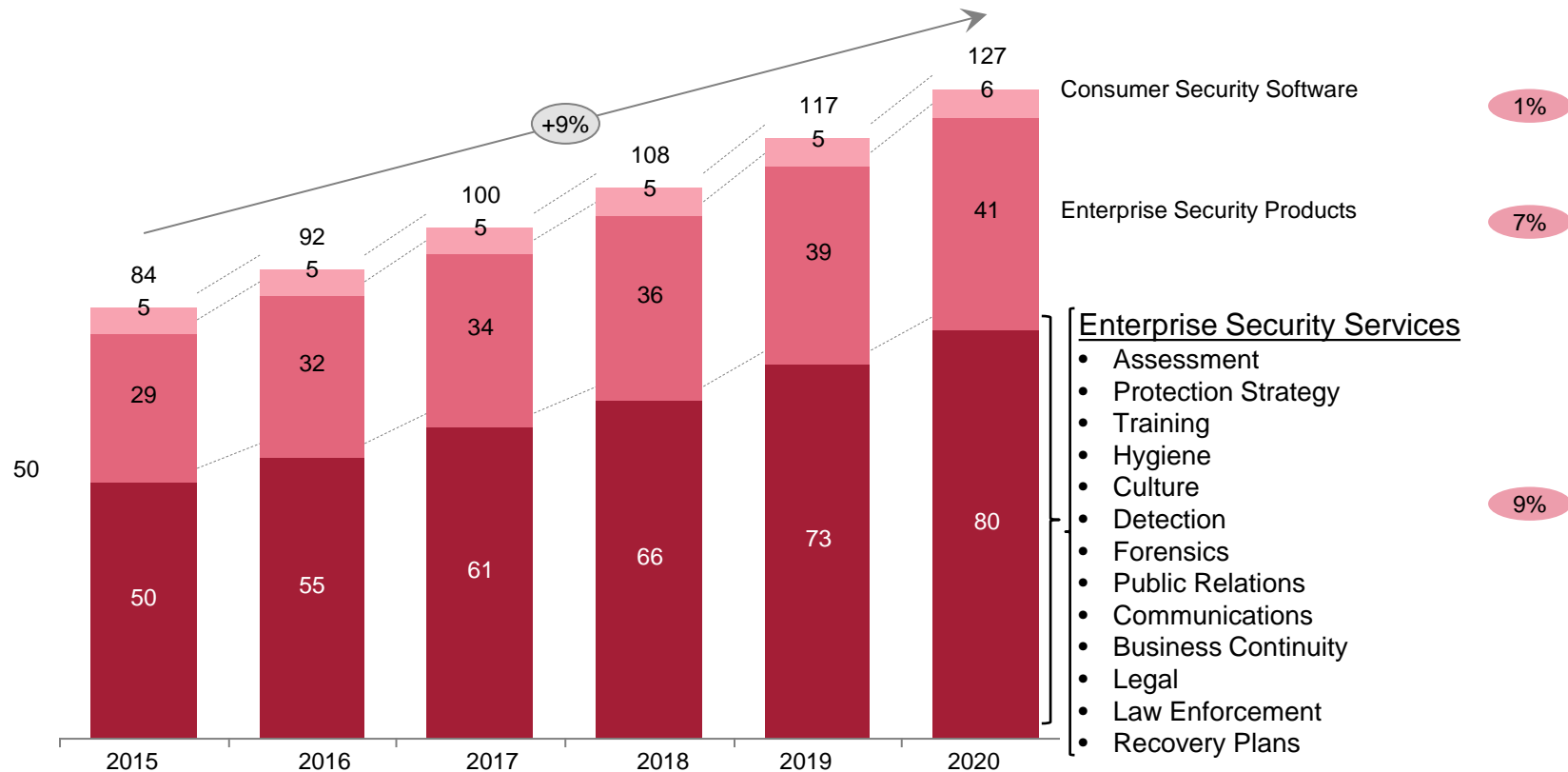
Source: BCG, Core team analysis



# Additional revenue/profit in enterprise security services, the largest and fastest growing part of the cybersecurity market

## Global cybersecurity market by security segment (\$ B)

**CAGR**  
(2015-2020)



Source: Gartner and BCG Analysis



# Cyber risk quantification data and models are lacking, underwriters must overcome for future sustainable growth



## Nature of the threat

## Dynamic

*Cyber threats are constantly evolving*

## Potentially systemic

*Single attacks could cause loss across multiple clients*



## Difficult to translate past incidents to the future



## Risk assessment

## Competitive market

### Market dynamics create barrier for detailed UW assessment

## Limited incident modeling

*Impact of risk management processes not well understood*



## Difficult to predict likelihood of incident



## Cost impact

## Short history

### Limited claims data compared with other insurance types

## Limited data sharing

*No mechanism for sharing loss data across the ecosystem*



## Difficult to quantify financial impact

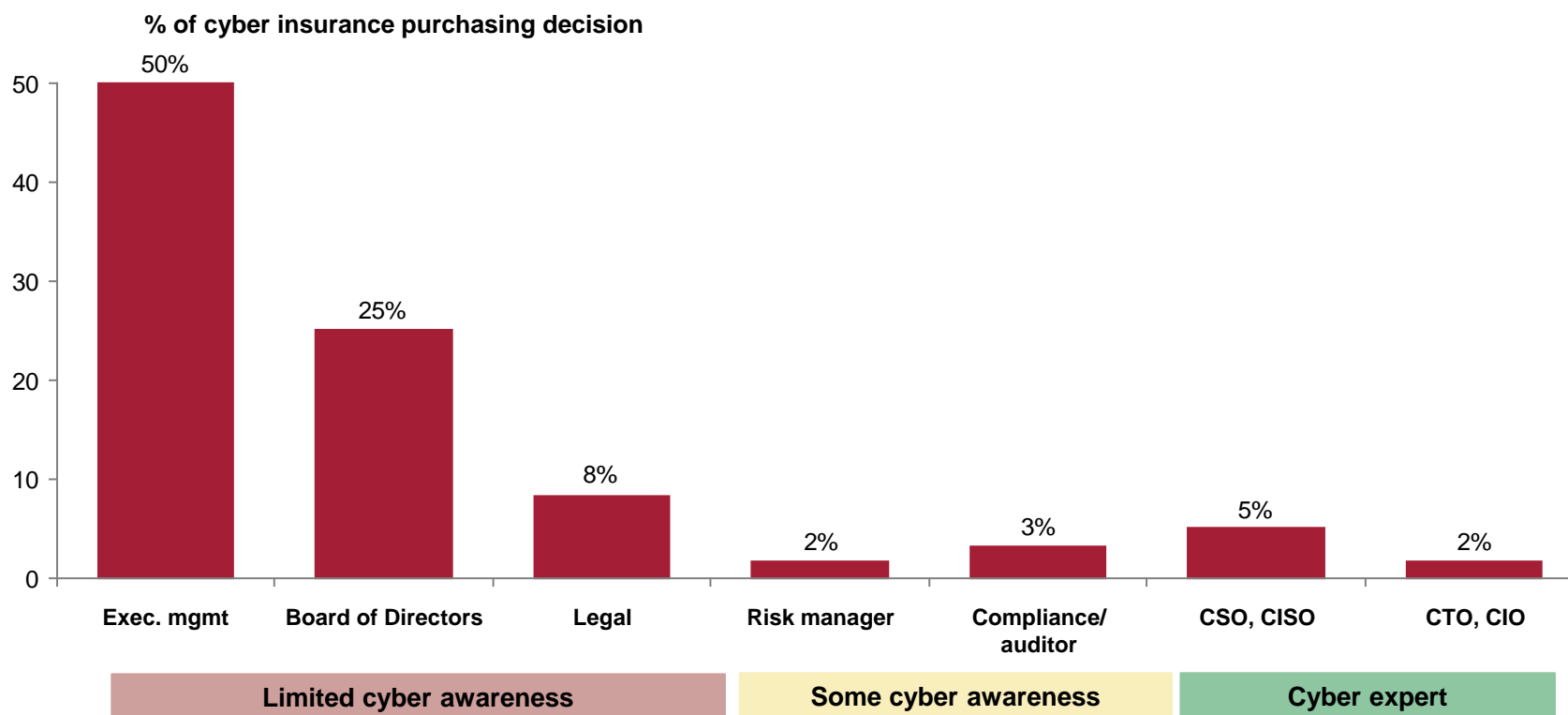
Source: Core team analysis



# Client organizations are not set up for insurance purchase

Disconnect between purchase decision maker and expertise

**Cyber security experts** have minimal purchasing and decision power, while **less-cyber-savvy executives** drive decisions



Source: "Bridging the insurance gap Info sec cyber insurance survey 2016"



## Based on Literature and Initial Interviews: Our hypotheses:

**A**

***Cyber insurers are moving from providing simply risk transfer to offering prevention, mitigation and resolution services***

**B**

***The new collaborative model and the larger presence of insurers can be leveraged to create cyber risk awareness and coordination within organizations***

**C**

***The cyber insurance market is an immature market in constant transition***



# Example: Impact of WANNACRY Ransomware Attack on Spain



- Ransomware attack to Telefónica blocked 80% of its computers!
- All employees sent to home
- Other companies attacked in Spain, included Banco Santander, BBVA, etc.
- Over 200,000 computers in over 100 countries disrupted within hours.



# A The expanding role of cyber insurance: the value chain

NIST framework functions



IT Vendors



Telcos



Consulting firms



Law firms



Insurers



Brokers





# A The expanding role of cyber insurance: What services?

## Examples of additional services (by AIG)

### Risk Insurance Resolution

Risk Consultation and Prevention	Insurance Coverage	Breach Resolution Team
Education and Knowledge 	Third-Party Loss Resulting From a Security or Data Breach 	24/7 Guidance: 1-800-CYBR-345 
Training and Compliance 	Direct First-Party Costs of Responding to a Breach 	Legal and Forensics Services 
Global Threat Intelligence and Assessment 	Lost Income and Operating Expense Resulting From a Security or Data Breach 	Notification, Credit, and ID Monitoring Call Center 
Shunning Services 	Threats to Disclose Data or Attack a System to Extort Money 	Crisis Communication Experts 
Expert Advice and Consultation 	Online Defamation and Copyright and Trademark Infringement 	Over 15 Years' Experience Handling Cyber-Related Claims 

## Partners providing services



### Infrastructure Vulnerability Scanning: Powered by IBM

ILLUSTRATIVE

- Remote scan
- Detect risk in public facing infrastructure
- Help speed vulnerability remediation

### Consultations: Access to vendors and partners

- 2 hours with **specialized law firm**  
-> address regulations
- 1 hour with **forensic firm**  
-> advise technical response
- 1 hour with vetted **public relations firm** -> address reputation risk

SOURCE: AIG Cyber Cyberedge brochure; <http://www.aig.com/business/insurance/cyber-insurance>



# A The expanding role of cyber insurance: Why?

## Attractiveness

### Findings

- **SMEs** without cyber security pa**Target** rtners
- **Increase value added** perception
- Help companies to **better understand cyber risk**

### Quotes

***“Insurers are the best companies to understand risk, so it’s in their best interest to provide the best advice to their customers”***

## Profitability

**Lower losses**

- **Prevent high losses and reduce impact** (lower coverages)

**Longer contracts**

- **Retain customers**, after a long sales process (3-6 months)
- **Prevent customers from going to competitors** who offer additional services

***“Companies are overwhelmed by Cyber. After an attack they don’t even know how to submit a claim”***

## Knowledge

- The presence of insurers throughout the cyber risk value chain enables **capture of broad spectrum of insights and knowledge**
- **Cope with the challenge of data availability**



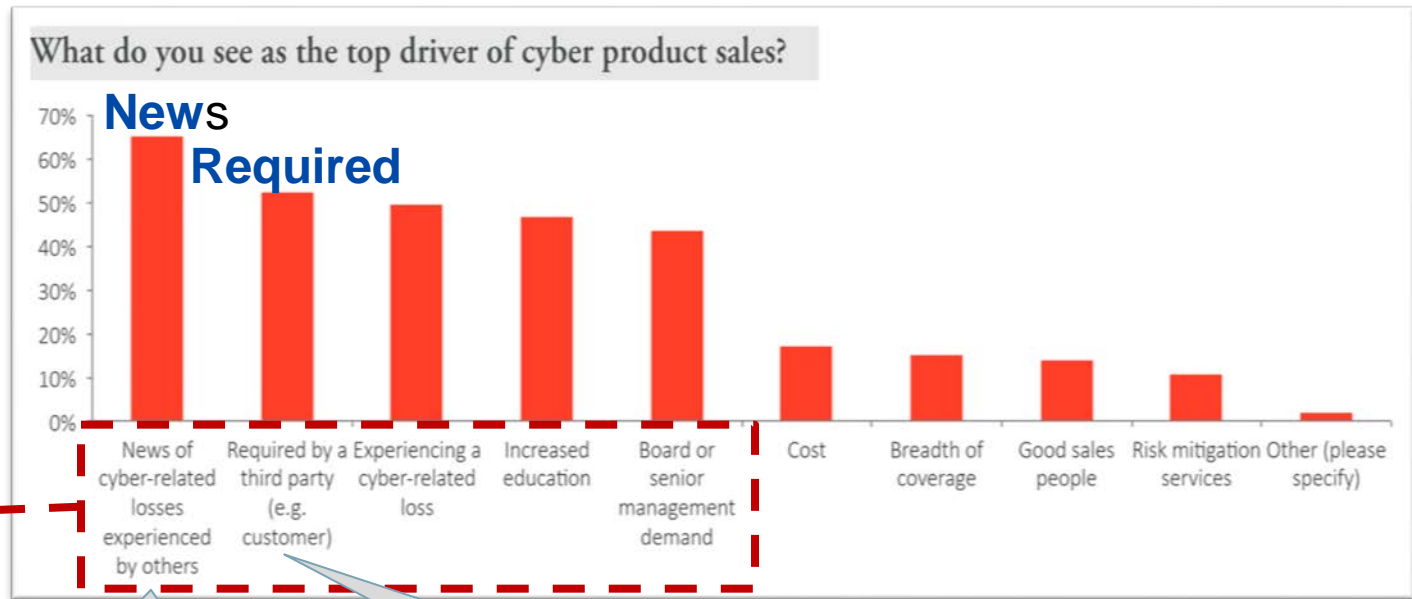
## B Accessing the right actors: CISO and CRO as advocates – though they are very different

	Characteristics	Insight
<b>CISO/ Head of security</b>	<ul style="list-style-type: none"> <li>▪ <b>Cost-driven</b> incentives</li> <li>▪ <b>Short-term focus</b></li> <li>▪ <b>CISO is not standardized across companies</b></li> <li>▪ <b>Stressful position</b></li> <li>▪ <b>Usually no direct reporting to top level management</b></li> </ul>	<ul style="list-style-type: none"> <li>▪ <b>Prefers to buy new tools than purchasing cyber insurance</b></li> <li>▪ <b>Limited empowerment to convince CEO or Boards to buy cyber insurance</b></li> </ul> <p><i><b>“CISO does not want to hear that he is doing a poor job”</b></i></p>
<b>CRO/ Risk manager</b>	<ul style="list-style-type: none"> <li>▪ <b>Focus on risk in general</b>, not only cyber</li> <li>▪ <b>Usually report to CFO</b>, though lately the role downgraded</li> <li>▪ <b>Already has interacted with insurance companies for other types of risks</b></li> </ul>	<ul style="list-style-type: none"> <li>▪ <b>Potential advocate for cyber insurance</b></li> <li>▪ <b>Language barrier with final decision-maker</b></li> </ul> <p><i><b>“CRO does not speak same language as the decision maker”</b></i></p>

**Risk managers and CROs can be the access window to top management teams (i.e., CEOs, board members)**



# C Cyber insurance market dynamics: Big cyber-attacks and regulation are important drivers of the market



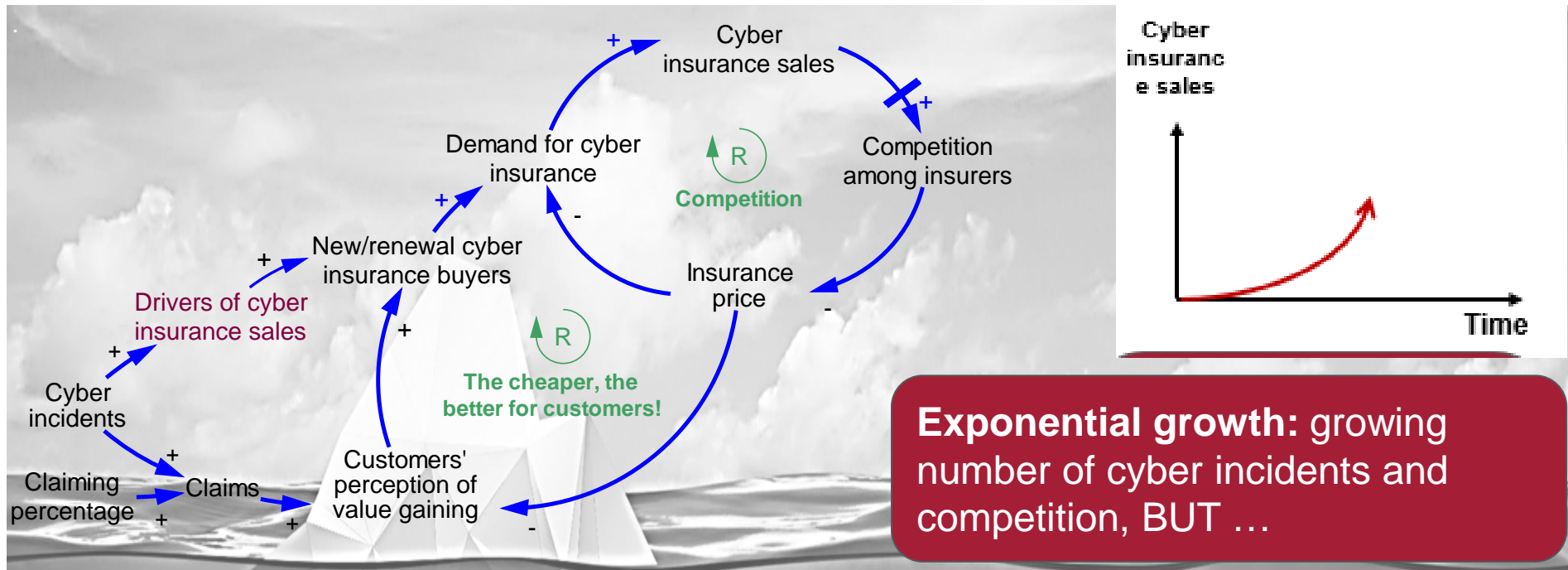
Main drivers of cyber insurance sales

***“After Target and Sony Network attacks an important number of companies started demanding our cyber insurance services”***

***“The EU 2018 Data Protection Directive GDPR is starting to drive the explosion of the market in EU”***



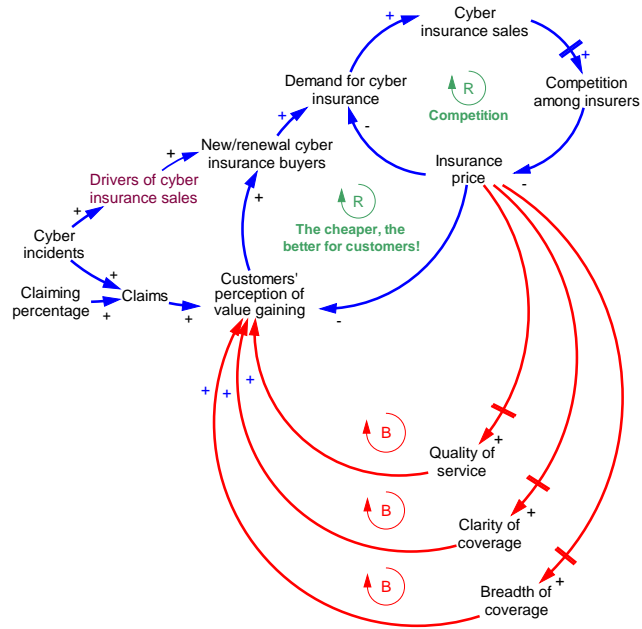
# C Cyber insurance market dynamics: modeling the market behavior



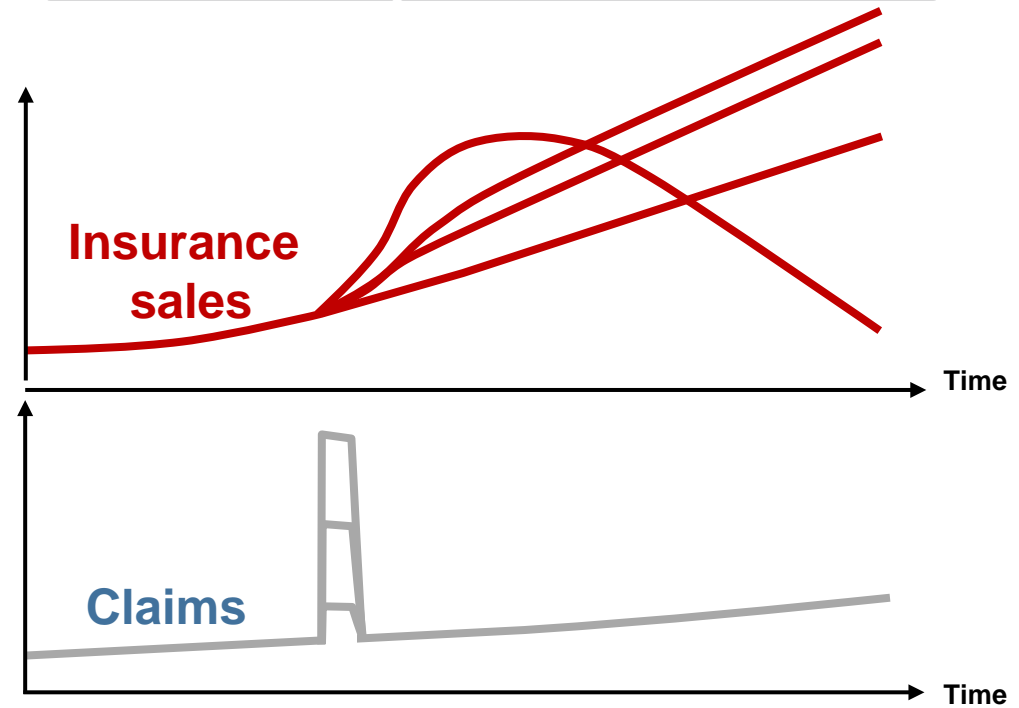
- ***“Customers do not understand what is covered under our cyber offer, language is complex”***
- ***“Customers feel that even if something seems covered, **insurers will not respond if there is a claim**”***
- ***“We think that our insurance is not making us better against cyber risk, we **see little value added**”***



# C Cyber insurance market dynamics: modeling the market behavior – focusing on impact of increasing events/claims



The tradeoff creates tipping dynamics...



- Data shows that increases in number of events and claims, insurance sales increase.
- However, the tipping dynamics in model reveal that the market can potentially crash if large spikes in the number of claims (e.g., Hurricane Andrew)
- This is preliminary dynamic model, more analysis needed.



