



# black hat<sup>®</sup>

## USA 2019

**AUGUST 3-8, 2019**  
MANDALAY BAY / LAS VEGAS

# How Do Cyber Insurers View the World

- Matt Prevost
  - Cyber Product Manager, Chubb





Adam Smith, The Wealth of Nations, 1776

“...the chance of loss is frequently undervalued, and scarce ever valued more than it is worth, **we may learn from a very moderate profit of insurers...**”

“in order to make insurance...a trade at all...the common premium must be sufficient to compensate for losses, to pay the expenses of management and to afford such a profit as might

“the person who pays no more than this evidently pays no more than the real value of the risk, or the lowest price at which he can reasonably expect to insure it.”

“many people despise the risk too much to pay for it...”

“sea risk is more alarming to the greater part of people, and the proportion of ships insured to those not insured is much greater...

“many fail however, at all seasons, and even in time of war, without insurance”...



# Combined Ratio

$$\text{Combined Ratio} = \frac{\text{Incurred Losses} + \text{Expenses}}{\text{Earned Premiums}}$$

<100%



>100%

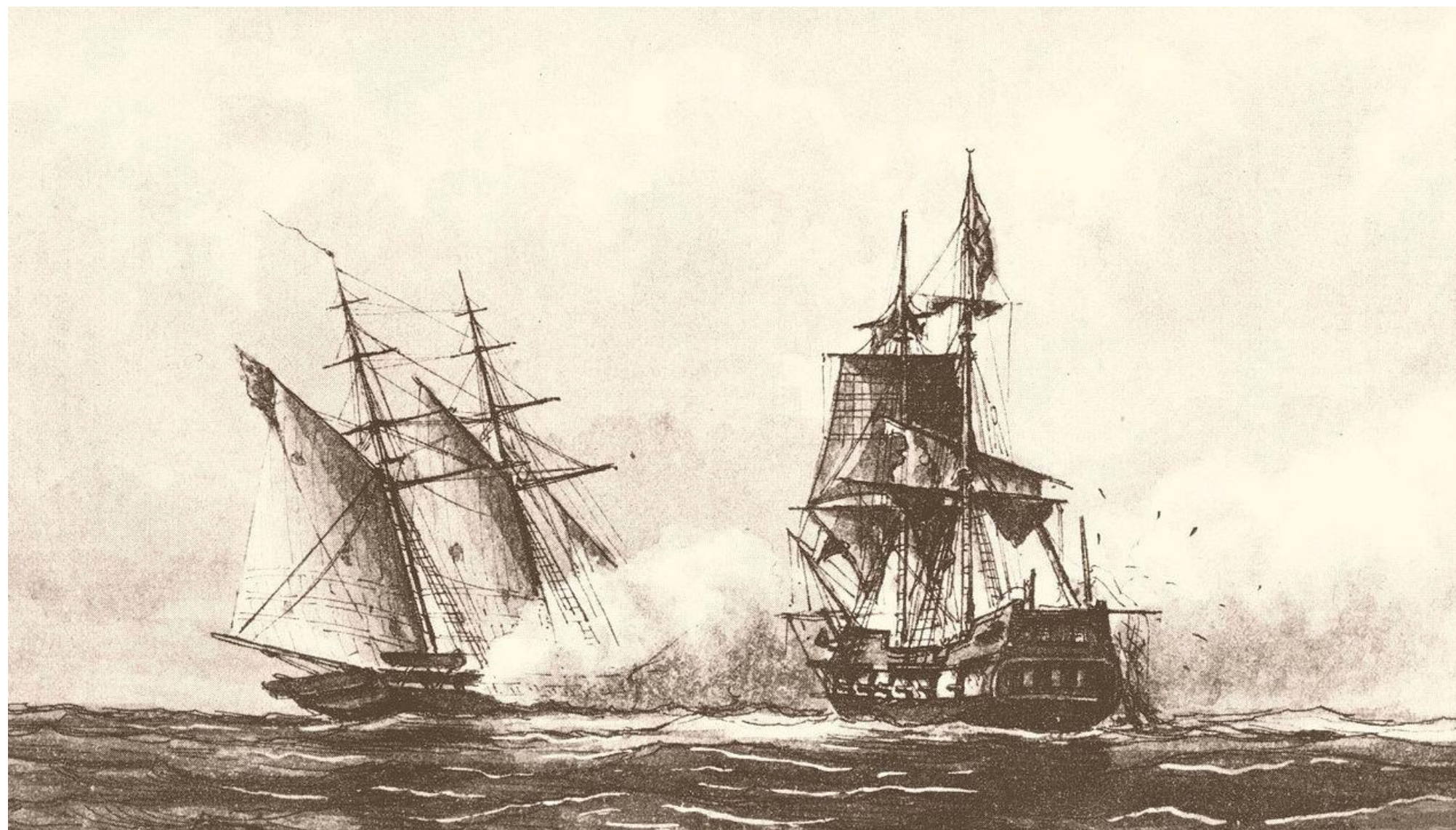
A combined ratio of less than 100% is good, over 100% is bad.

‘Underwriting’ was working...and ships had smooth sailing...





Until American ships didn't have protection in late 1770s....





# Insurance History 101 (Lessons Learned)

- Fire Insurance\*
  - **"New Factors" Phase**
    - **1837:** First industry classification and new factors were required. Mutuals and those that focused on 'knowledge, inspection and improvements'
    - **1853:** Proofs of loss established
    - Many mistakes were made in this period, because there was little co-operation, but still there was a gradual approach toward better conditions and a larger and more comprehensive development.
  - **"Cooperations" phase**  
(post civil war, Chicago/Boston fires)
  - Conditions were very unsatisfactory; rates were low, and prosperity for the companies was not very apparent. Special agent has scope change beyond that of just handling losses.
  - Fire insurance had been going through an evolution, and step by step, the scope had become broader and better calculated to assist the business development of the country.

- Cyber Insurance

- What can we learn?



\*Historical Study of Fire Insurance in the United States F. C. Oviatt (Sep., 1905)



	Property (last century)	Cyber (today)
Market GWP (2018 Dollars)	\$40M	\$4B
Predominant Loss Driver	Fire	Data Breaches & Business Int.
Other Perils Insured	Quake, Many More	Interruptions, Cyber Extortion
Cat Perils Excluded/Controlled?	Yes	Yes
Cat Event	1906 San Francisco Earthquake	2017 examples...
Geography	San Francisco Area	Global.
Affected Insureds (Claims)	100,000	TBD
Loss (2018 Dollars)	\$4B (100x GWP)	TBD
Insolvencies	14+	TBD
Percent of Insured Losses Paid	76%	TBD
Prior Years' Profits Erased	47 Years	TBD

\*Historical Study of Fire Insurance in the United States F. C. Oviatt (Sep., 1905)



...but a cyber insurance underwriter's algorithm is too new... right?

0%

## Combined Ratio


















$$\text{Combined Ratio} = \frac{\text{Incurred Losses} + \text{Expenses}}{\text{Earned Premiums}}$$

**<100%**  **>100%** 

A combined ratio of less than 100% is good, over 100% is bad.

400%



	Merck	US Pharmaceutical Company	
	Maersk	Global shipping and logistics	
	Saint Gobain	French construction materials company	
	FedEx TNT Express	Global parcel delivery company	
	Mondelez International	World's second-largest confectionery company	
	Reckitt Benckiser	British consumer goods maker	Halted production lines
	Beiersdorf	German consumer product manufacturer	Product shipping and production delays, Nivea product line impacted
	WPP	UK Ad Agency (Largest Ad agency in the world)	WPP agency network disabled
	Nuance Communications	US Healthcare company	Healthcare data system disabled
	Home Credit	Consumer lending	All Russian branches closed
	Evraz	Steel manufacturing and mining company	Information systems affected
	Oschadbank	Ukraine's state-owned bank	
	Rosneft	Russian state oil company	
	Deutsche Post DHL	Global parcel delivery company	
	Boryspil International Airport	Ukraine International Airport	
	UKRENERGO	Ukrainian state power distributor	No impact on power supplies
	Metro	German wholesaler	Ukrainian Stores affected
	Chernobyl Radiation Monitoring	Nuclear Power Plant Safety	Automatic monitoring systems disabled, forcing switch to manual
	DLA Piper	Multinational law firm	Internal systems and phones disabled
	Ukrainian Supermarkets	Retail - multiple?	Point of Sale systems disabled
	Heritage Valley Health Systems	US Hospitals and Healthcare, Pennsylvania	Systems disabled
	Ukrainian Banks	Banks, possibly 5	Disruption to operations
	Russian Banks	Banks, multiple	Disruption to operations

**Maersk: 51% of devices on networks infected. Reinstallation of 45,000 machines took 10 days. \$450m loss.**

**Rosneft: 1% of devices on network infected. ICS systems unaffected. \$5m loss**



Share of **\$2.2 Billion** Loss



**“Cyber insurance doesn’t pay claims” is to cyber insurance as  
“my cyber security tool didn’t work so none do” is to Cyber security.**

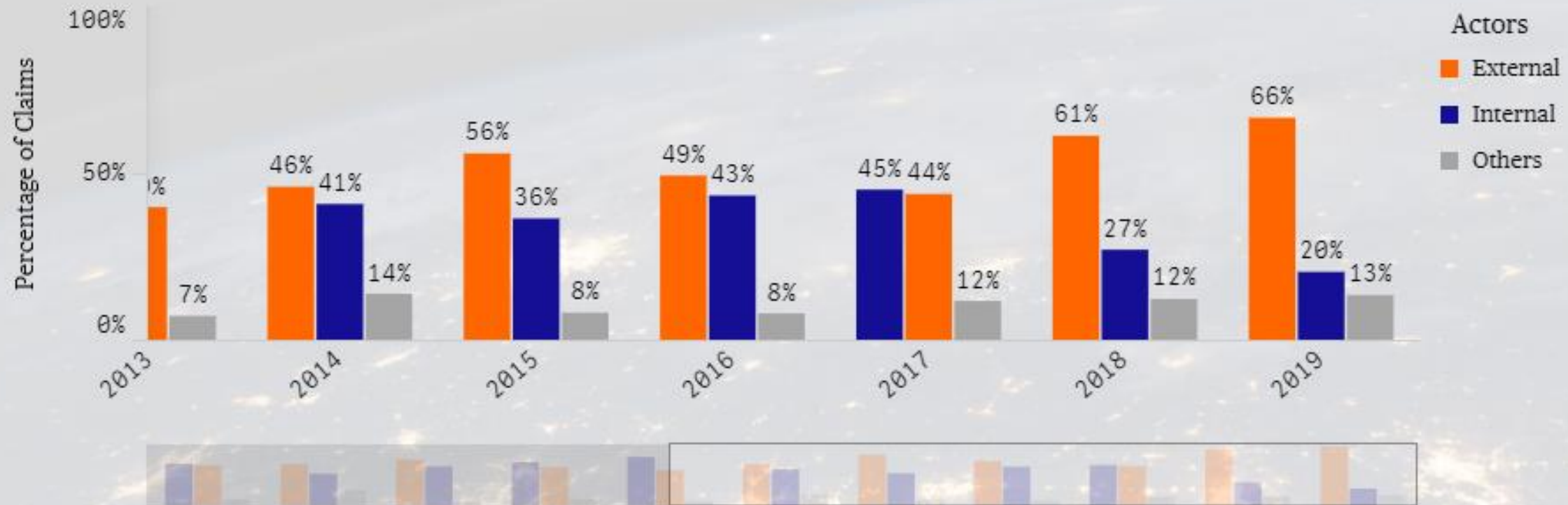
Data Source:

☒ Chubb ☐ R

View Claims by:

☒ Industry☐ \$ Company Revenue☐ Date Range

## Chubb Top Actors Causing Cyber Incidents for All Available Data

*All Industries and All Revenue Sizes*





## September 2018

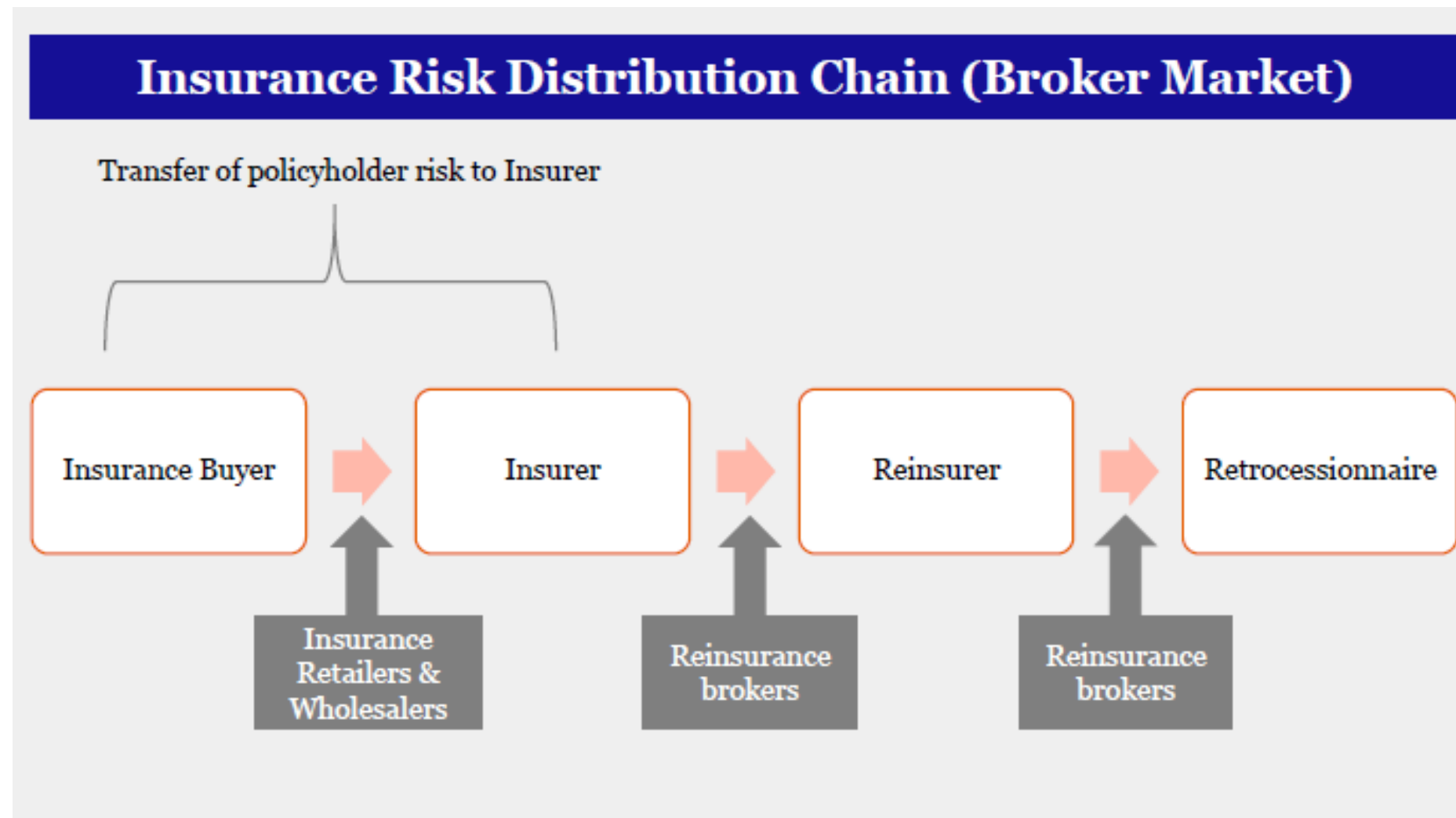
“It’s kind of crappy to be a Chief Security Officer.. It’s like being a Chief Financial Officer before accounting was invented..”

“When you take the job, you decide that you’re going to run the risk of having decisions made above you or issues created by tens of thousands of people making decisions that will be stapled to your resume.”

- Alex Stamos, Facebook’s former Chief Security Officer



- How do cyber underwriters 'view' companies?



## The Underwriting Presentation

---

- Introduction (individuals, roles)
- Operational Overview: What does the company do?
  - How does the company make money / who is the customer
  - PR opportunity

*TIP: underwriters want a sense of “crown jewels” – is it pii, phi, trade secrets*

*TIP: underwriters will likely ask for a record count*
- E&O – focus on contracts/legal; testing protocols
- Security Portion
- Privacy Portion
- Governance (optional)
- Litigation/Claims Activity



## Security Presentation

---

- Overview of information security structure/and how it fits in to rest of organization
- Vision/Strategy/Framework
- What are your current strategic initiatives?
- Network architecture (data centers, segmentation)
- Information Governance
- Data Protection (encryption, tokenization, segmentation, masking/separation)
- Identity Management – Active Directory; Privileged Access Management (incl behavioral)
- Incident Response: SOC, SIEM
- Vulnerability management (patching)
- Business Continuity /Disaster Recovery
- Vendor Compliance
- Security Awareness
- Active Defense
- Threat Intelligence

## Privacy Presentation

---

- Overview of privacy organization, incl. entities & individuals who help serve function
- Vision/Strategy/Framework
  - What are the crown jewels?
- Information governance
- Classification scheme; technological protections (encryption) as well as procedural/HR
- Regulatory compliance, incl GDPR Readiness/Data Handling
  - Tip: explain the “how”*
- Sharing, selling with business associates and other third parties; contractual protections
- Involvement of key stake holders (legal/compliance w/business units; audit function)







## Why do insurers have to worry about Cyber Risk Aggregation?

---

Not surprisingly, in recent months, Enterprise Risk and Underwriting have jointly received inquiries from key stakeholders on potential risk aggregation arising from cyber.

### **Senior Management and Board of Directors:**

- What insurance coverages are triggered by cyber attacks?
- How many customers are potentially impacted by an event?
- How do we model cyber risks?
- What is our risk appetite for losses arising from cyber risks?
- Are we getting paid to cover cyber risks?
- What is the appropriate policy language to address cyber risks?
- What guidelines/authorities should we have in place to manage this risk across the organization?

**Regulators and Rating Agencies** are interested in controls in place to manage cyber risk aggregations to preserve long term solvency of the insurer.

- Is Cyber the next Asbestos or Long Term Care?



LLOYD'S



STANDARD  
& POOR'S



**HURRICANE ANDREW 25 YEARS LATER ... CAT EVENT THAT CHANGED THE P/C (RE)INS INDUSTRY  
Catalyst For The Modern Day Cat Mkt With Modeling / Exposure Based Pricing. Bermuda Cat Re "Wave" Formed  
Uncapped QS Goes Away. Primary Carriers Withdraw From The Coasts While Wind Pools / FAIR Plans Expand**

---

Hurricane Andrew struck South Florida (Homestead) 25 years ago today, making landfall on August 24, 1992 as a Category 5 hurricane (it was re-classified from Category 4 in 2002), causing \$15.5B in insured losses (~\$26B indexed to today's \$s). This single event exceeded the cumulative profit on all property lines beginning with biblical times. The loss remains the 2<sup>nd</sup> costliest natural disaster, after Hurricane Katrina (2005). Eleven property/casualty insurers became insolvent due to Hurricane Andrew and many others were financially impaired. Looking beyond the immediate impact of the event, Hurricane Andrew was a tremendously important event for the industry as a whole, bringing about significant changes that affect the (re)insurance market to this day. Among a number of other things (described in more detail below), Hurricane Andrew triggered the widespread use of catastrophe modeling / exposure quantification and prompted the launch of the Bermuda Class of 1993 (RenRe is the last independent company from this wave). On the 25<sup>th</sup> anniversary, we highlight what we view as the most significant changes for the (re)insurance industry as a result of Hurricane Andrew.

*IBRN weekly (8/24/2017)*

## What information is required to build a catastrophe model for cyber risks?

Catastrophe models help insurers estimate losses under extreme events. In addition to contract terms like coverages, limits, deductibles, insurers would require the following data to properly aggregate risks:

Cyber Catastrophe	Natural Catastrophe Property
<ul style="list-style-type: none"><li>• Event Type (Threat Actor, Threat Vector, Target)</li><li>• Accounts potentially exposed to Target (Cyber eco-system)</li><li>• Cyber Hygiene Score (outside-in view)</li><li>• Other security considerations (account level controls like data encryption, two-factor authentication)</li><li>• Other hazard considerations (motivation of bad actors to attack target)</li></ul>	<ul style="list-style-type: none"><li>• Event Type (Hurricanes, Fire, Flood, Earthquakes, etc.)</li><li>• Occupancy</li><li>• Location</li><li>• Structural Engineering, Age</li><li>• Other hazard information (proximity to coast line, proximity to bedrock, etc.)</li></ul>

The insurance industry is working with a number of vendors to develop cyber catastrophe models; however we have yet to achieve a level of risk aggregation maturity consistent with Natural Catastrophe Risks impacting the Property product line.



# Evolution within cyber underwriting

- Actual strategies proving successful and unsuccessful
- More 'tools' at our disposal
  - Aggregation
  - Account specific
- More insights into events themselves across the market
  - Attritional Losses (the everyday risks)
- Importance of Education
- Services to mitigate risk
- Advancing transparency of claims and underwriting process itself
- Back-casting seemingly systemic events
  - NotPetya
  - Wannacry
  - Third party distributed