AMERICAN ACADEMY of ACTUARIES

ANNUAL MEETING AND PUBLIC POLICY FORUM

NOVEMBER 5-6 2020

CYBER RISK INSURANCE

Housekeeping

- The statements and opinions expressed by moderators/presenters do not necessarily represent the statements or opinions of the American Academy of Actuaries, the Actuarial Standards Board, the Actuarial Board for Counseling and Discipline, or any Academy boards, councils, or committees.
- The Academy operates in compliance with the requirements of applicable law, including federal antitrust laws. The Academy's antitrust policy is available online at https://www.actuary.org/content/academy-antitrust-policy.
- Academy members and other individuals who serve as members or interested parties of any of its boards, councils, committees, etc., are required to annually acknowledge the Academy's Conflict of Interest Policy, available online at https://www.actuary.org/content/conflict-interest-policy-1.
- Use the chat feature at the right of the video screen to type in questions.
- This program, including remarks made by attendees, may be recorded and published. Additionally, it is open to the news media.

Continuing education credit

- The Academy believes in good faith that attendance at this program constitutes an organized activity as defined under the current *Qualification Standards for Actuaries Issuing Statements of Actuarial Opinion in the United States*, and that attendees may earn up to 1.5 organized continuing education (CE) credits for attending this program.

Today's Presenters

- Norman Niami, moderator
  - Chairperson, Academy Cyber Risk Task Force (CRTF)
- Laura Maxwell, CRTF member
- Taylor Krebsbach Davis, CRTF member
- Eduard Alpin, CRTF vice chair
- Christopher Loza, Academy senior research analyst

Today's Program

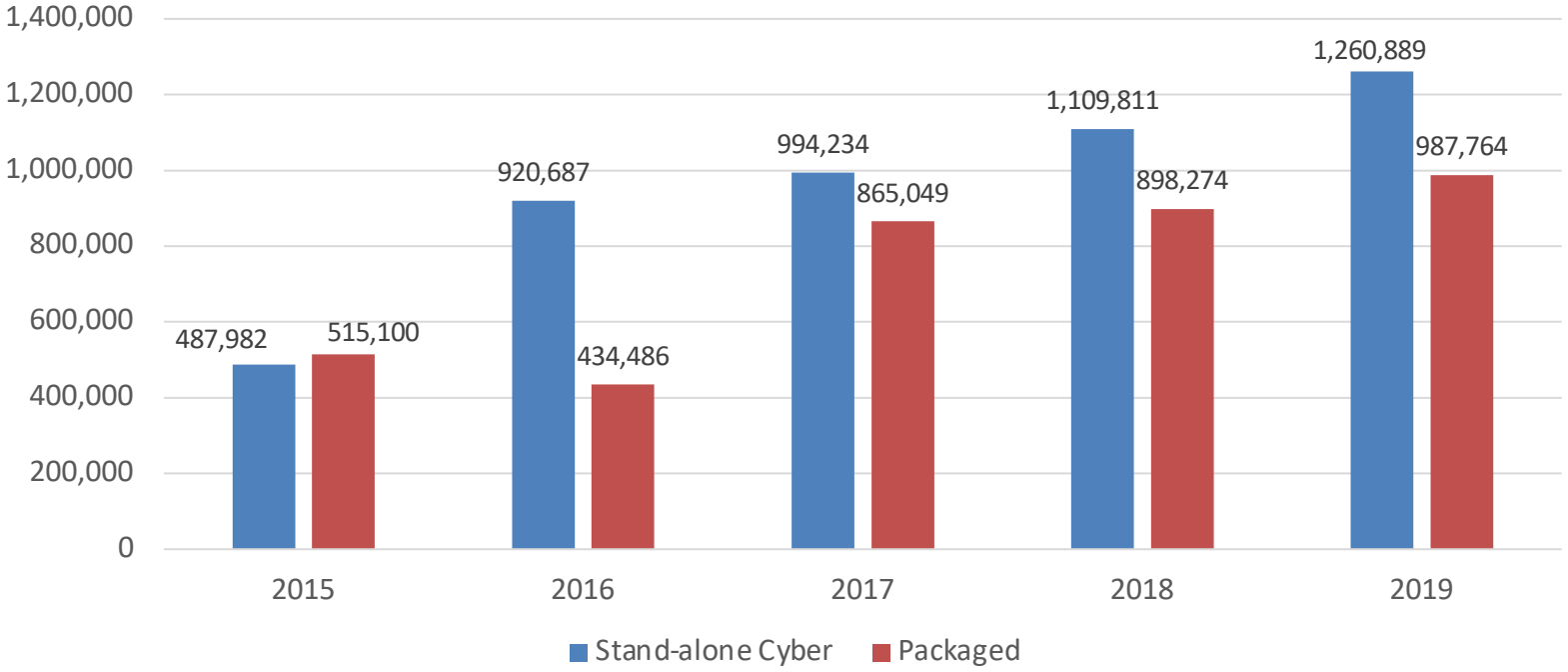
- Introduction/Overview
- Silent Cyber
- Cyber Threat
- Cyber Data
- Cyber Breach Reporting Requirements

INTRODUCTION
Laura Maxwell

Agenda

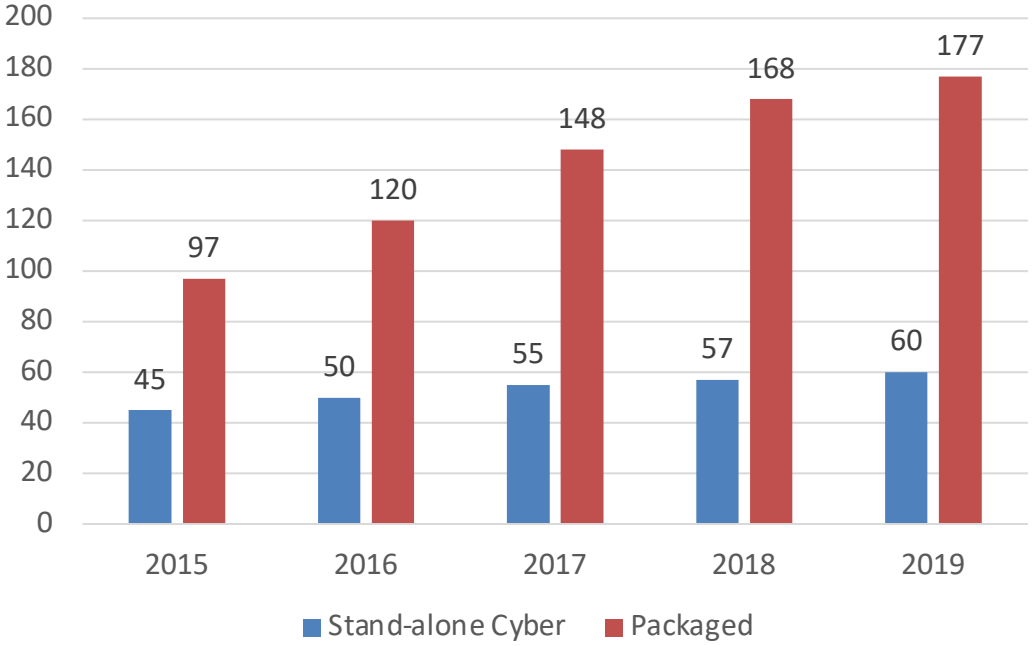
- Cybersecurity insurance market
- Coverage definitions
- Policy characteristics
- Case study

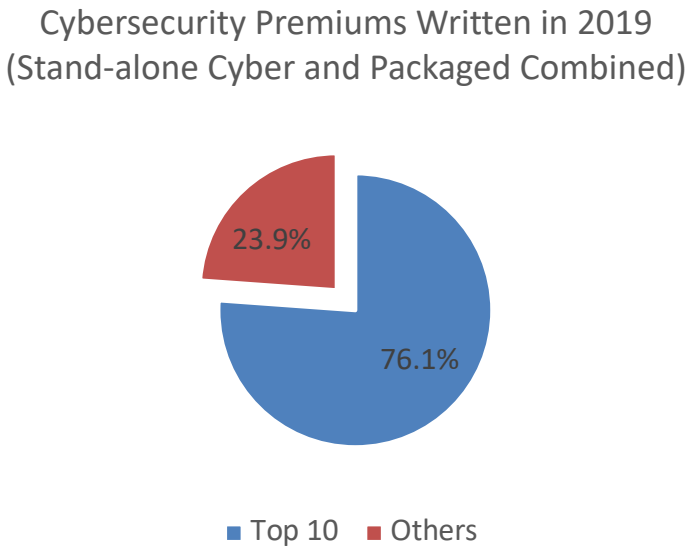
Cybersecurity Written Premium (000s)



The figures shown in the graph are limited to information reported to the NAIC by insurance carriers.

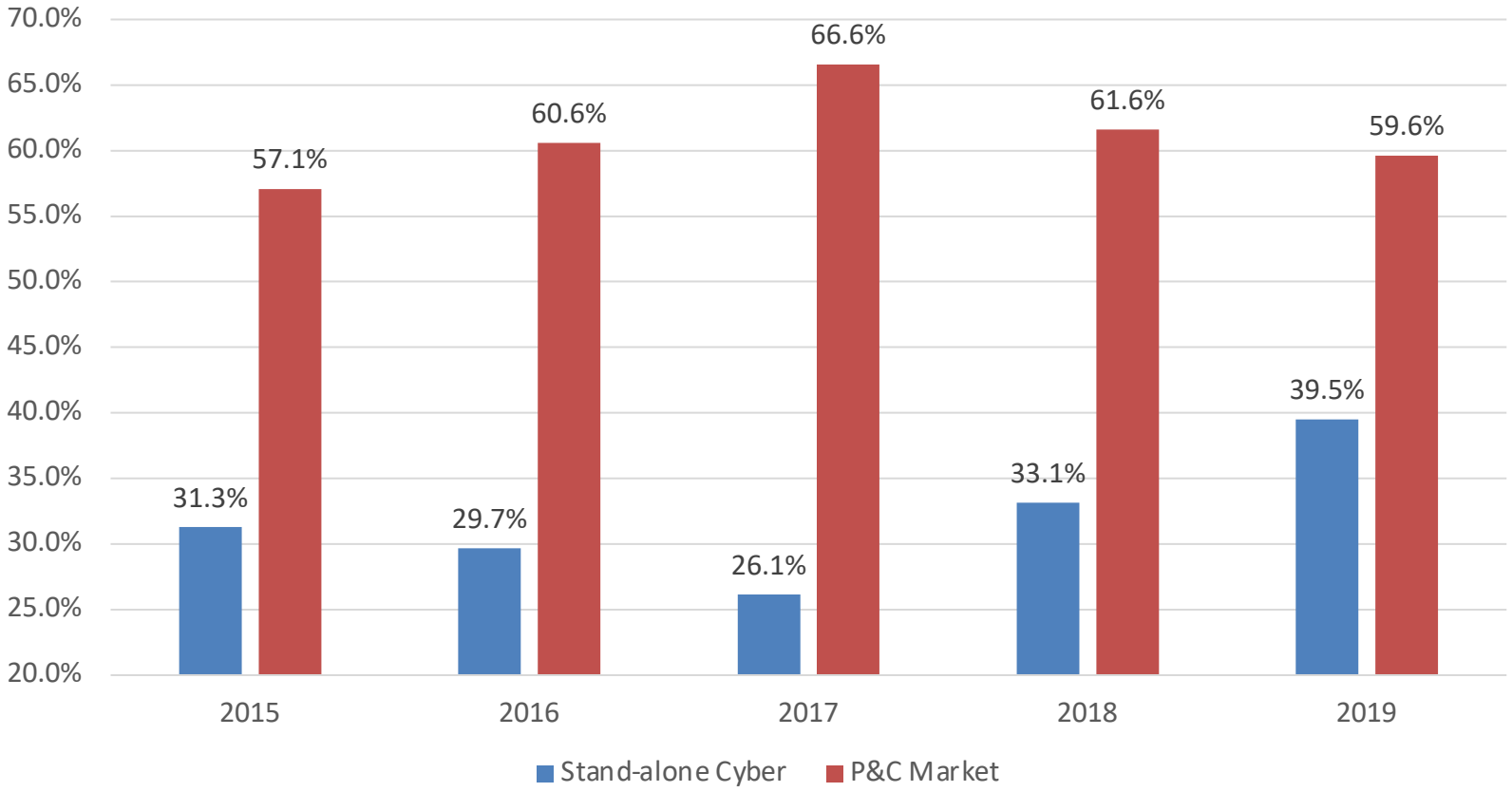
Companies Writing Cybersecurity Policies





The figures shown in the graphs are limited to information reported to the NAIC by insurance carriers.

Direct Incurred Loss Ratios



COVERAGE DEFINITIONS

First-Party Coverage

Business Interruption

Identity Recovery

Privacy Breach Response Services

Property Damage

Computer Attack and Cyber Extortion

Computer and Funds Transfer Fraud

Third-Party Coverage

Electronic Media Liability

Regulatory Defense & Penalties / PCI Costs

Information Security & Privacy Liability

Network Security Liability

Service Offerings

Risk Management	Education	Response Readiness Assessment
Simulation & Vulnerability Scans	Benchmarking	BYOD Coverage
Threat Intelligence	Expert Guidance	Ongoing Monitoring

GENERAL COVERAGE CHARACTERISTICS

Premiums

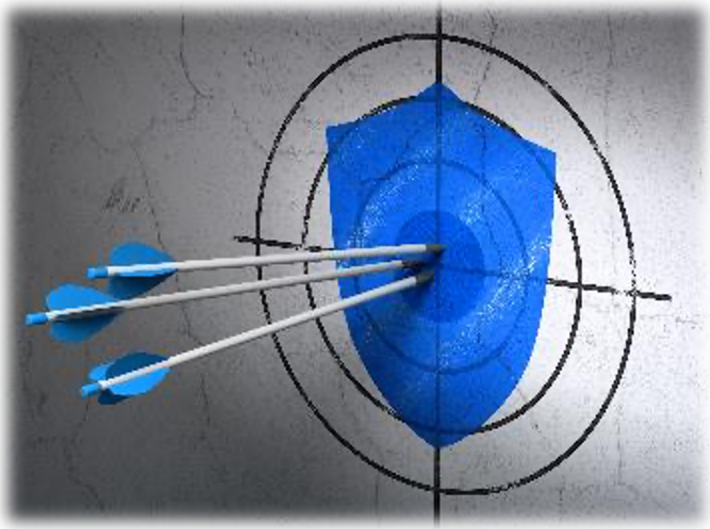
Base Rate

x Increased Limits Factor (ILF)

x Deductible Factor

x Cyber Specific Rating Factors

x Schedule Modification Factors



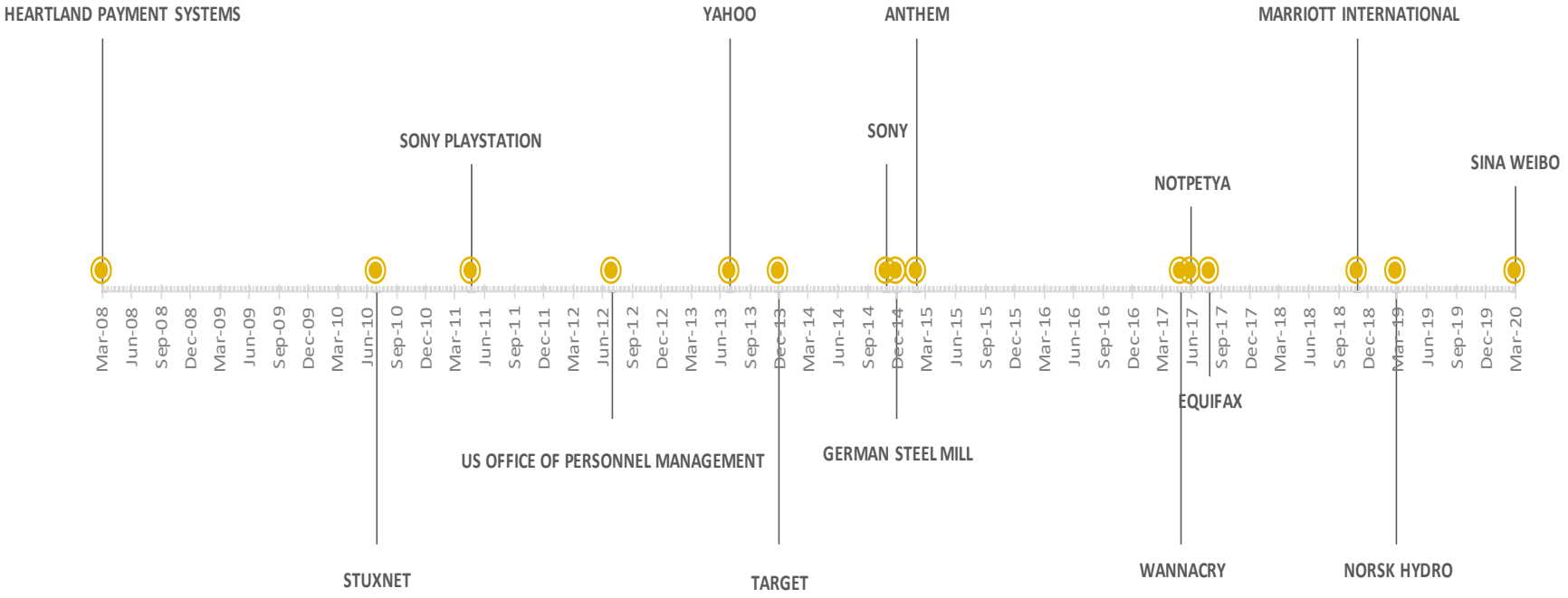
Other Considerations

- Extended Reporting Period
- Exposure Base
- Hazard Groups
- Schedule Rating

Policy Exclusions

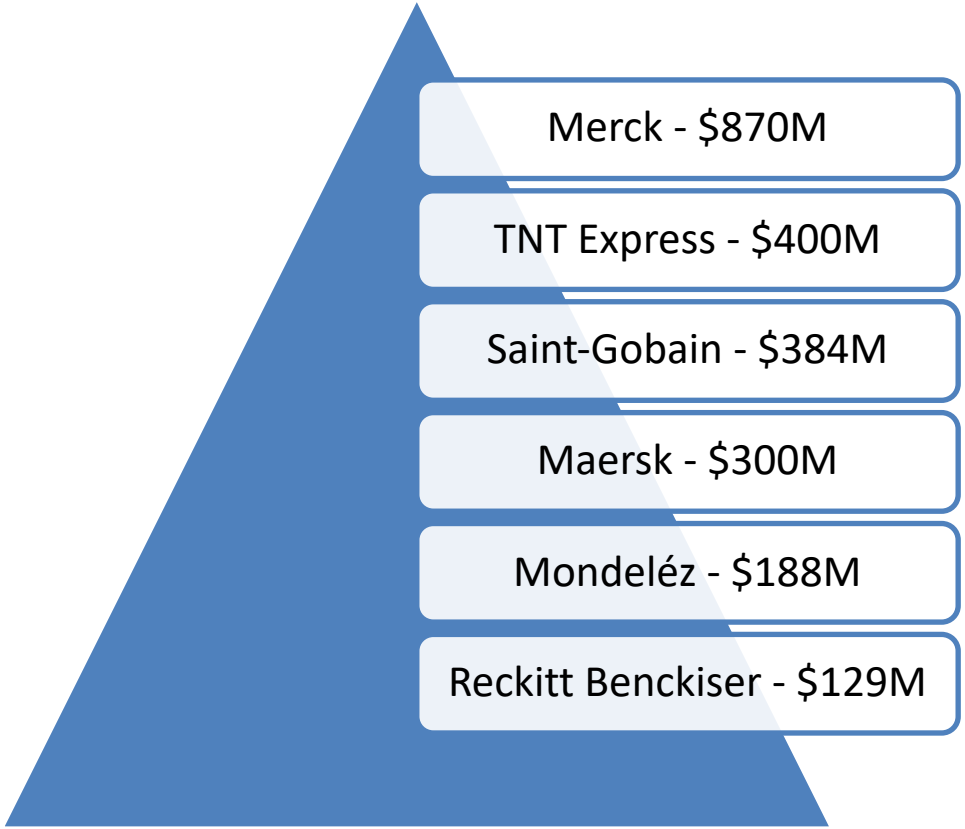
- War
- Infrastructure Outage
- Nuclear

CASE STUDIES



NotPetya

- June 27, 2017
- Caused massive destruction
- Spread quickly
- $10 billion total damages
- First party coverage?
- Act of war?



SILENT CYBER
Taylor Krebsbach Maxwell

What Is “Silent Cyber”?

- Unintentional, non-affirmative coverage of losses caused by cyber perils.
- Risk that a cyber event could trigger unexpected payouts under existing policies where the cyber risk was not considered and/or priced.
- Policy wording has not evolved at the rapid pace of technology
- There are two major aspects of silent cyber risk: **unintentional** coverage and **unpriced** coverage.

Consider a Hypothetical Example…

- A cyber-attack that hacked the industrial control system of a dam, resulting millions of dollars of property and flood damage losses covered by the policy language where flood is the covered cause of loss.
- Many lines of business covering the dam and its operator could have potential exposure to silent cyber losses due to unintentional coverage. In today's connected world even many cars and homes have significant cyber exposure.

Unintentional Coverage

- Occurs when a policy language does not explicitly address the loss caused by a cyber incident or a cyber-attack.
- In the dam flooding example, many lines of business covering the dam and its operator could have potential exposure to silent cyber losses due to unintentional coverage.
- In today's connected world even many cars and homes have significant cyber exposure.

CYBER THREAT
Norman Niami

Agenda

- Many Risks
- Bad Actors and Motives
- Threat Vectors
- Examples of Incidents

Many Risks

- Today's connected word increases risk to critical network infrastructure and a businesses can be impacted in a numerous ways such as:
  - Business Interruption
  - Loss of proprietary business information
  - Liability risk from loss of personal data
  - Direct costs (investigation, ransom, regulatory fines or penalties, restoration or replacement of digital assets, legal, etc.)

Bad Actors and Motives

- The list of bad actors keeps growing and can range from foreign governments and competitors, to criminal syndicates and disaffected employees/contractors
- Hacking software is now available for sale; Hackers are available for hire
- A large majority of attacks have had financial motives - bundles of personal identifiable information and protected health information are available for sale with somewhat set market prices; ransomware has been growing significantly
- A number of attacks without financial motivations have been quite severe - Sony, NotPetya

Threat Vectors

- Phishing – has been the largest portion of methods for successful attacks
- Delayed software patch installation
- Zero-day vulnerability -- exploits software vulnerability before developers know about and/or can fix the issue
- Disgruntled and disaffected employee or contractor

Examples of Incidents

- 2013 Target Data Breach – Stole around 40 million credit and debit card numbers and 70 million customer records; phishing email via network of a refrigeration contractor; a few hundred million dollar loss with close to a $100 insured loss

- 2017 NotPetya Attack – Attack started in Ukraine and spread globally; disguised as a software update; a known vulnerability was used to gain access to unpatched systems and then another vulnerability allowed the malware to use compromised system to find usernames and passwords, taking over a target machine and altering hardware stored information, destroying software and data; total cost estimate of $10 billion; cost FedEx and Maersk a few hundred million dollars each

CYBER INSURANCE DATA

Eduard Alpin

Verisk Cyber Solutions

Cyber Policy Management Platform

Integrated policy pricing, underwriting, and distribution platform

Cyber Risk Modeling

Exposure management; deterministic + probabilistic modeling

Underwriting Platform

Qualitative + quantitative detailed scoring for risk selection

Insurance Program

Forms, rules, and loss costs for cyber insurance

Industry Loss Estimates

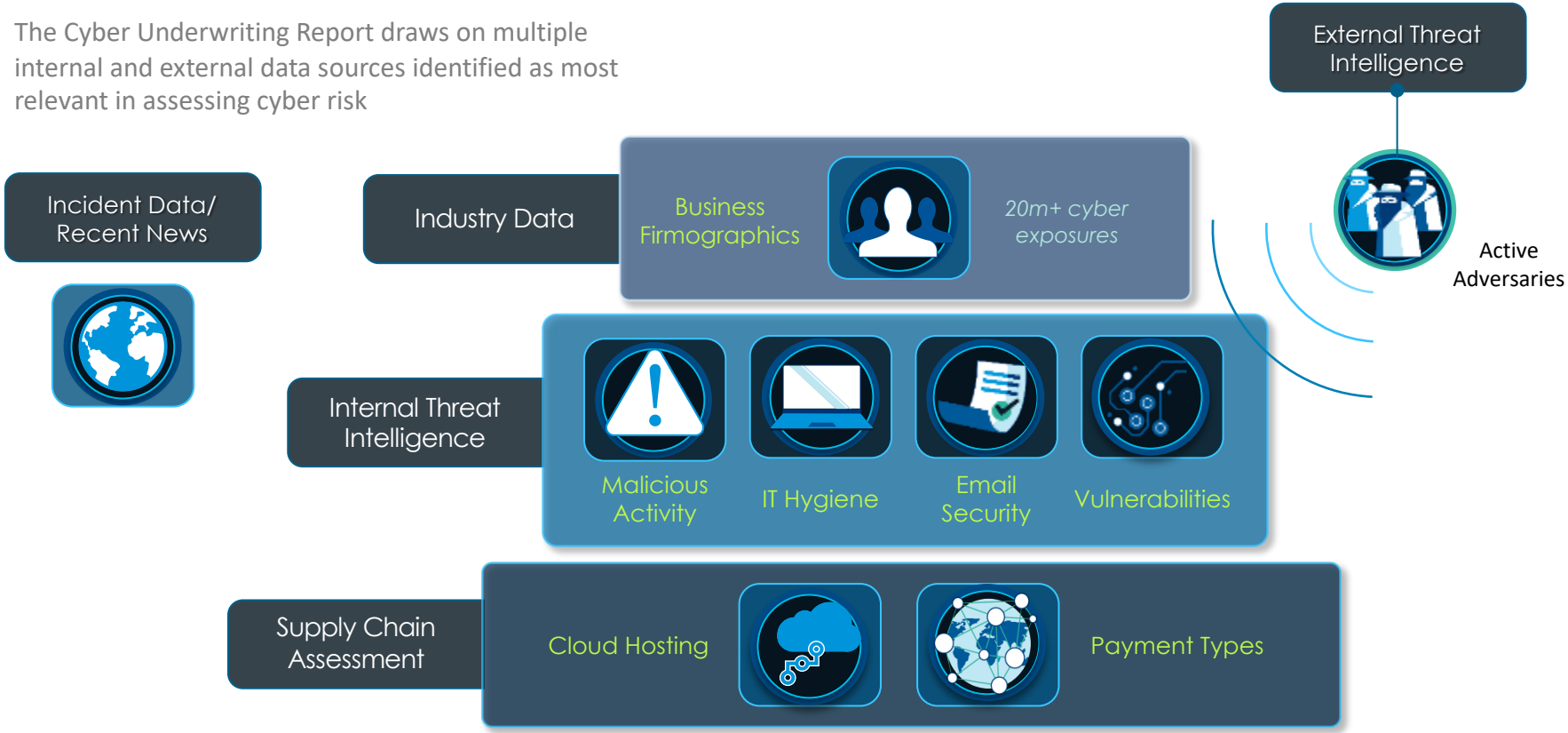
Independent estimates of large-loss events

Cyber Data Exchange

Accessible platform for sharing and accessing aggregate cyber data across the industry

Cyber Data To Support Underwriting

The Cyber Underwriting Report draws on multiple internal and external data sources identified as most relevant in assessing cyber risk



Cyber Data To Support Ratemaking

- Vendor exposure and incident data:

Incident #	Company Type	Revenue	Industry	# Records Exposed	Type of Record	Loss Amount	GLM	Modeled Loss
1	Not-for-Profit	98,327,000	Healthcare	589,760	PHI	2,527,323		
2	Investment Fund	61,989,000	Finance	8,583,411	PFI		→	16,982,782
3	Private	97,098,000	Information	7,335,013	PII		→	9,242,811
4	Private	44,135,000	Accommodation	3,667,507	PFI	3,509,994		
5	Public	94,282,000	Retail	3,613,102	PFI		→	6,595,370
6	Private	67,091,000	Healthcare	3,527,682	PHI		→	7,250,002
7	Government	51,169,000	Government	6,417,107	PII		→	4,770,184
8	Government	59,014,000	Government	6,875,762	PII	5,557,318		
9	Public	17,360,000	Retail	263,907	PFI		→	1,047,117
10	Private	56,914,000	Finance	4,583,841	PFI			2,513,080
11	Public	89,617,000	Healthcare	638,163	PHI		→	2,270,882

- Advantage:
  - >100k incidents allows for credible modeling and granular factors
- Disadvantages:
  - Events fall under a limited number of coverages
  - Losses are skewed by larger events

Cyber Data To Support Ratemaking

- Cyber insurance data:

Policy #	Policy Eff Date	Policy Exp Date	Coverage	Limit	Premium	Claim #	Coverage triggered	Loss Amount
12345678	1/1/2020	12/31/2020	Breach Expense	$5,000,000	$10,000			
12345678	1/1/2020	12/31/2020	Breach Liability	$5,000,000	$12,000			
12345678	1/1/2020	12/31/2020	Extortion	$5,000,000	$7,000	XYZ1234567	Extortion	$2,000,000
12345678	1/1/2020	12/31/2020	Business Interruption	$5,000,000	$5,000			
12345678	1/1/2020	12/31/2020	Data Restoration	$5,000,000	$3,000			

- Advantages:
  - Perfect match of claims to exposures – results in an accurate frequency estimate
  - No claims bias towards certain coverages, or risk characteristics
- Disadvantages:
  - Companies lack ample claims data for modeling
  - Reported losses are capped at the limit, not ground up like with vendor incident data

Cyber Data To Support Ratemaking

- Carriers need to assess a company's cybersecurity culture, governance and cyber hygiene
- Questionnaires are often used. Examples:
  - Does your organization encrypt sensitive information sent to external parties?
  - Does your organization have an individual officially designated for overseeing information security?
- Credits/debits are assigned based on responses
- Advantage: simple to implement and can ask about a variety of topics
- Disadvantages:
  - Responses can be anecdotal, not data driven
  - Risk manager filling out the questionnaire may not know or not share all of the information

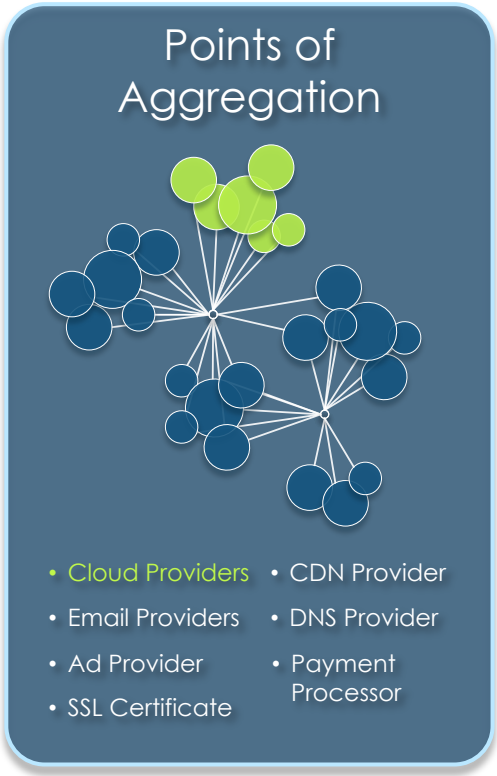
Cyber Data To Support Ratemaking

- Ideally a rating plan would employ factors based on observed technographic datapoints such as:
  - Email security (DMARC, DMARC, DKIM implementations)
  - IT Hygiene (Open ports, P2P file sharing, OS & Browser data)
  - Vulnerability (Software and Server CVEs, SSL/TLS certificate)
  - Adversarial Activity (botnets, brute force attempts)
  - Internal Malicious (traffic to known malicious sites)
- As a hypothetical example:
  - If an organization uses outdated Windows XP software, they would receive a debit of 10%
  - If an organization has DMARC implemented they would receive a 5% credit

Policy #	Policy Eff Date	Policy Exp Date	Insured	DMARC?	# of High Severity CVE	Average time to patch	Open Ports	Limit	Premium
12345678	1/1/2020	12/31/2020	ABC Shipping Co	Yes	0	30 days	5	$10,000,000	$100,000
56789012	1/1/2020	12/31/2020	XYZ Finance Corp	No	5	50 days	20	$5,000,000	$120,000

Cyber Data To Support Accumulation Modeling

- Exposures
- Cyber incidents – individual organizations
- Insurance policies and claims
- Technographic data on individual companies
- Cyber incidents – multiple organizations involved
- Technographic data – points of aggregation



Cyber Data Exchange

Challenge: Lack of credible and relevant cyber insurance data that carriers need to make informed decisions

Solution: Verisk aggregates cyber insurance data from across the industry and provides summarized metrics delivered via dashboards back to participating companies.

Open to:

- Admitted Carriers
- Excess & Surplus
- MGAs
- Syndicates
- Reinsurers
- Brokers

Data Collected:

- Policy & Claims
- Transactional
- Historical
- Quarterly submissions

Metrics:

- Average Premium
- Claim Frequency
- Loss Severity
- Loss Ratio

Dimensions:

- Policy Year
- Insuring agreements
- Account size
- Industry Class

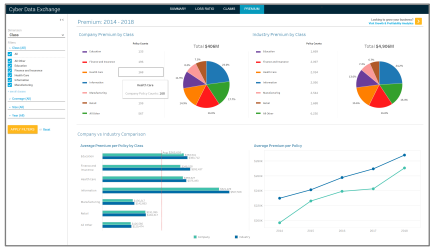
Product Details:

- Anonymity
- Flexibility
- Credibility
- Balance

Use Cases:

- Benchmarking
- Strategic Decisions
- Analytics
- Risk Selection

Dashboards: cde.iso.com



Cyber Breach Reporting Requirements:

An Analysis of Laws Across the United States

A Report of the Cyber Risk Task Force,
Presented by Christopher P. Loza
Senior Research Analyst
American Academy of Actuaries

Background

- “[M]alicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.”—U.S. Council of Economic Advisers
- According to the National Association of Insurance Commissioners (NAIC), between 2015 and 2018, total premiums written for cyber coverage increased from $1.4 billion to $3.6 billion.
- Reducing and managing risk efficiently requires information, including that drawn from compliance with laws regulating reporting of cyber breaches

Background (cont'd)

- No uniform national standards exist for notifying consumers and authorities of data breaches
- Each state and territory has its own statute(s) with notification requirements.
- In 2017, the NAIC adopted the Insurance Data Security Model Law
  - To establish common data security and breach notification standards
  - States encouraged to adopt by the NAIC and U.S. Department of the Treasury
- In 2018, a U.S. Department of the Treasury report concluded:
  - Differences in state laws can make compliance overly burdensome for companies doing business in more than one state
  - U.S. Congress should enact data security and breach notification legislation that supersedes state law and applies uniform standards across the states

Objectives

- Academy Cyber Risk Task Force examined the current status of state reporting requirements in a paper just published
- Verify essential aspects of each jurisdiction's relevant statute(s), and summarize each in a consistent manner for comparison
- Compare statutes across jurisdictions and report key metrics
- Contrast current statutes with NAIC Model Law

Four Law Firm Summaries

State Law Survey 1	State Law Survey 2	State Law Survey 3	State Law Survey 4
Scope of this Summary	Application	Definition of "Personal Information"	Persons Covered
Covered Info	Personal Information Definition	Definition of "Personal Information"	Personal Information Definition
Form of Covered Info			
Encryption Safe Harbor		Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	
Breach Defined	Security Breach Definition	Definition of "Breach"	Encryption/Notification Trigger
Consumer Notice	Timing of Notification	Timing of Notification to Individuals	Specific Content Requirements
	Notice Required		Timing
	Substitute Notice Available		
Delayed Notice	Exception: Compliance with Other Laws		
Harm Threshold	Notification Obligation	Analysis of Risk of Harm	
Government Notice	Attorney General/Agency Notification		
Consumer Reporting Agency Notice	Notification to Consumer Reporting Agencies		
Third-Party Notice			
Potential Penalties		Enforcement/Private Cause of Action/ Penalties	Penalty/Private Right of Action
	Other Key Provisions		Other Provisions

Statute Categories

- **Scope**—entity or entities to whom notification requirements and other aspects of the law are applicable
- **Covered Information**—the personal identifying information (PII) that would trigger the statute if exposed to breach
- **Form of Covered Information**—whether electronic, written, or other form is covered
- **Breach Definition**—how a violation is defined by the statute
- **Safe Harbor/Exceptions**—exceptions that exempt a breach from statute requirements
- **Harm Threshold**—whether the statute sets a threshold for a reasonable expectation of harm before triggering remedies

Statute Categories (continued)

- **Consumer Notice**—how and when affected consumers should be notified of the breach
- **Government Notice**—how and when a government agency, such as the office of the attorney general, should be notified of the breach
- **Consumer Reporting Agency (CRA) Notice**—how and when CRAs should be notified of the breach
- **Third-Party Notice—**if responsible party is maintaining covered PII for a third party, how and when the third party should be made aware of the breach
- **Notification Delay**—circumstances when the mandated notification to consumers may be delayed
- **Potential Penalties**—additional liabilities potentially borne by responsible party, including monetary penalties and exposure to private litigation

Findings

- **Scope**—All cover PII of state residents
- **Covered Information**—All states use name in tandem with one other trigger. Twenty-three states only have 3-4 triggers. The rest vary between 5 and 15.
- **Form of Covered Information**—All include electronic records. Only six include written records.
- **Breach Definition**—"Unauthorized" or "illegal" access; good-faith exceptions in all but three jurisdictions
- **Safe Harbor/Exceptions**—In every jurisdiction, for encrypted data
- **Harm Threshold**—All but 14 states only require notification if some level of harm is likely

Findings (cont'd)

- **Consumer Notice**—Notice required as soon as possible. Only 15 states stipulate deadline, ranging between 30 and 90 days. Substitute notice available in 50 of 54 jurisdictions for varying cost thresholds.
- **Government Notice**—Only 36 states explicitly require notification to authorities.
- **Consumer Reporting Agency (CRA) Notice**—Often required if certain number of consumers are affected, ranging from 500 to 10,000 with a median threshold of 1,000.
- **Third-Party Notice**—Data owner must be notified immediately in all but two states.
- **Potential Penalties**—Civil penalties may be imposed for violation in all cases.

NAIC Model Law Requirements

- Provides considerations for implementation of data security program, including assessment of pertinent risks
- Primary objective is protection of "nonpublic information"
  - Information that identifies consumer along with any one of following:
  - Social Security number,
  - Driver's license number or any identification card number,
  - Any access number, code, or password that would permit access to a financial account,
  - Biometric records
- Provides necessary steps for investigation and assessment
- Required notification if "reasonable likelihood" of material harm
  - Within 72 hours to state insurance commissioner if at least 250 consumers affected
  - For consumer notification, follow relevant state law

Key Takeaways

- Typical statute may create issues due to arbitrary threshold and vague language.
- Variability may create uncertainty for pricing and designing cyber coverage, requiring higher margin components in premiums.
- Variability may also make mitigation and prevention more difficult, raising losses due to cyber risk, requiring higher cyber coverage premiums.
- Actuaries, insurers, regulators, and public might benefit from increased harmonization.

Questions?