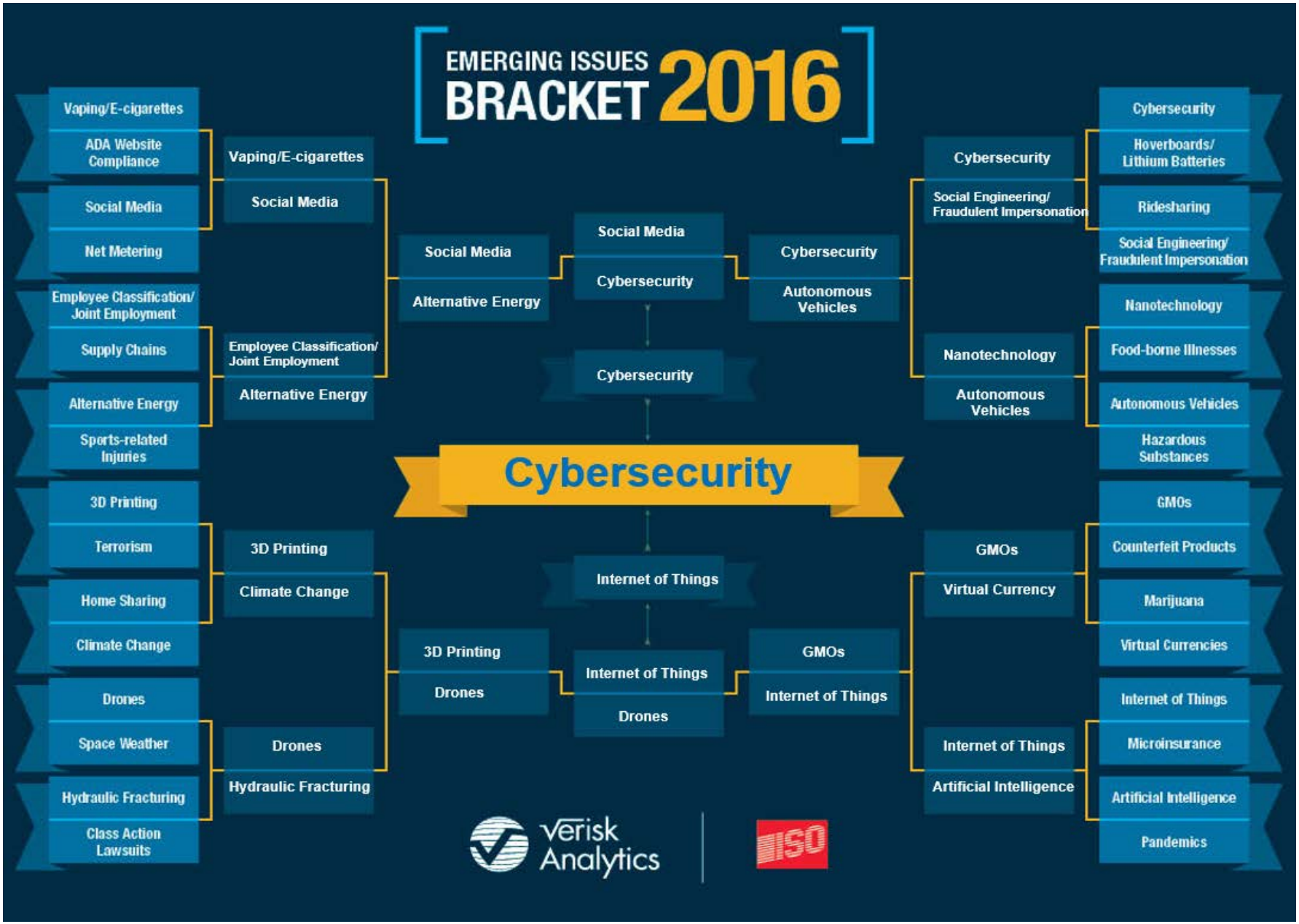
Cyber Statistics, Modeling & Pricing

Verisk Analytics

SERVE | ADD VALUE | INNOVATE

November 2017



Cyber Market and Coverage Overview

Cyber Market Overview

- Limits between $25K and $50M are common
- Businesses from all risk sizes and industries are seeking coverage
- Wide variation in pricing
- Lack of consistency in terminology
- Most cyber currently written on an E&S basis
  - Gravitating towards admitted market business

Cyber Insurance

- Insurance coverage approaches
  - Stand-alone insurance policies
  - Commercial Package Policies
  - Roll-on coverage to existing insurance policies (e.g., Businessowners, D&O, Professional Liability, etc.)
- Typical coverages and rating approaches
  - 1st and 3rd Party coverages
  - Revenue | Number of Records

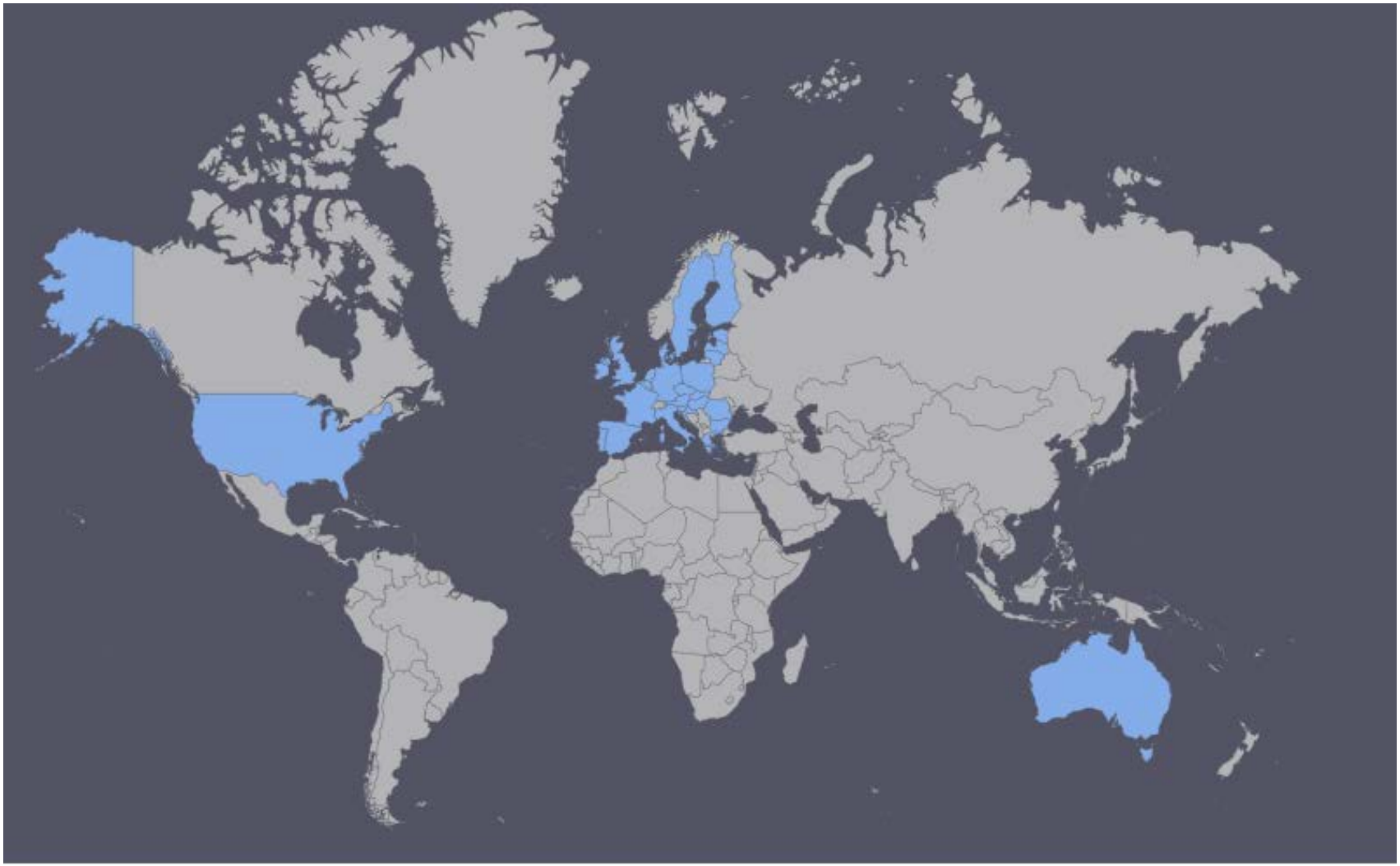
Both First Party and Third Party Loss Potential

Cyber Coverage Overview

Common Insuring Agreements in Cyber

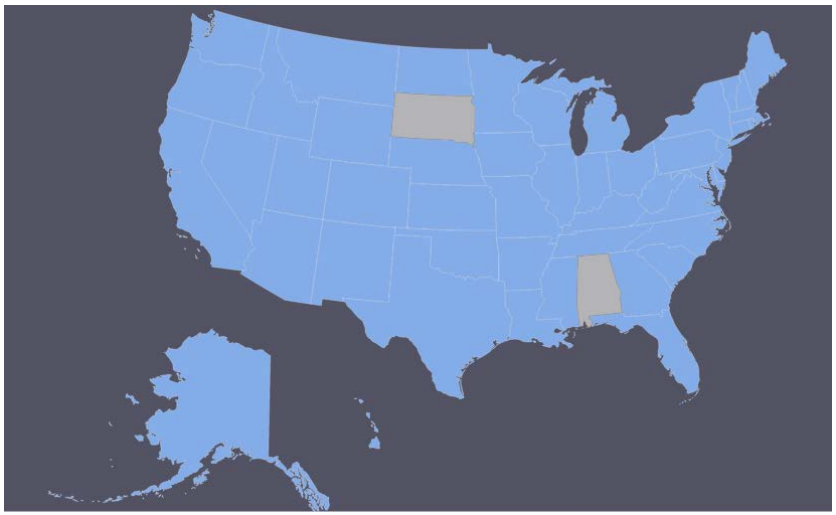
- Security Breach Expense
- Extortion Threats
- Replacement | Restoration of E-Data
- Business Income & Extra Expense
- Public Relations Expense
- Security Breach Liability
- Web Site Publishing Liability | Media Liability
- Programming E&O Liability

Regulatory Landscape International



Regulatory Landscape of the United States

- State Laws / Regulations
  - Data breach-related and notification laws in 48 States, the District of Columbia, Puerto Rico, U.S. Virgin Islands and Guam (as of April 2017)
  - Currently no U.S. federal law regarding notification standards



California was first state (2003).

Today, Alabama and South Dakota are the only states without a current law

GDPR in the European Union

- Breach notification requirements
- Increased territorial scope
- Penalties up to 4% of global revenue
- Privacy by design
- Enforceable on May 25th, 2018

Australian Privacy Amendment Bill

- "Eligible data breaches" will require customer notification

- An eligible data breach occurs when:

  personal information held by an entity is subject to unauthorized access or unauthorized disclosure and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the personal information relates

Percent of Data Breaches by Nation

Country	Percent of Data Breaches Reported
United States	90.2%
United Kingdom	3.4%
Canada	1.7%
Australia	1.3%
India	0.7%
Ireland	0.7%
Japan	0.6%
Israel	0.5%
Germany	0.4%
Thailand	0.4%

Source: Symantec

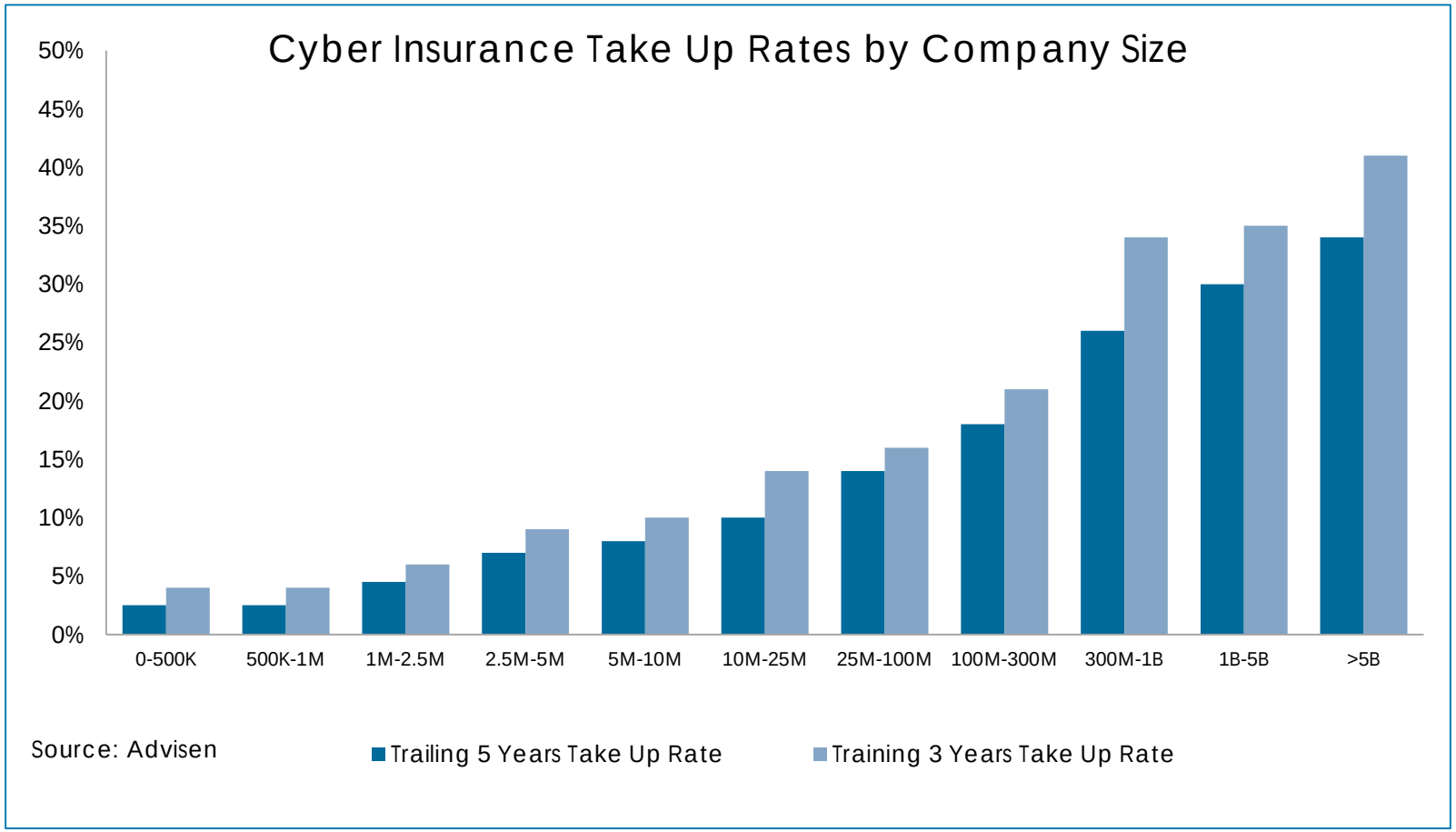
U.S. Cyber Market Performance in 2016 Based on NAIC Supplement Accounting Data

- Approximately $1.4B in reported premium
- 62% of premium is written by top 10 cyber writers
- Overall loss ratio - 54% (Max 1524%, Min 0%)
  - Stand-alone policies - 60%
  - Package policies - 43%
- Stand-alone Loss Ratios: Top 10 vs. The Rest
  - Top 10 Writers - 49%
  - The Rest- 83%

Source: National Association of Insurance Commissioners (NAIC) Supplement Accounting Data

Cyber is the Fastest Growing Segment of Insurance

- Market is growing both in scope of products offered and type of clients



Poll Question #1

- What percentage of small businesses go out of business in the 6 months following a data breach?

SMEs – The Next Big Growth Area in Cyber Insurance

64% of Cyber Breach victims are small to mid-size businesses*

Over 60% of those attacked go out of business**

- What is a Small / Medium Enterprise?
  - Companies with under $250 million in annual revenue
- Why are SMEs Vulnerable?
  - Financial gain is a primary motivation for committing cyber attack – SMEs often have the lowest defenses, making them attractive targets
- Costs of Breach (forensics and notification) alone can bankrupt an SME
  - Proliferation of Ransomware (Cyber Extortion) increases risk

*Based on ISO Analysis
**SBIR STTR The Impact of Cybercrime on Small Business

How Might an SME be Impacted by Cyber - Illustrative Events

- Offering explicit cyber insurance coverage minimizes uncertainty and provides protection for insureds in events such as:

Breach of sensitive customer data due to social engineering, phishing incident targeting individual company employees

A virus leads to corruption of external facing website of a niche market online retailer, leading to 48 hours of downtime and lost sales

Ransomware indecent impacting the computer of an employee which contains clients' personal information leading resulting in extortion payment to release encrypted files

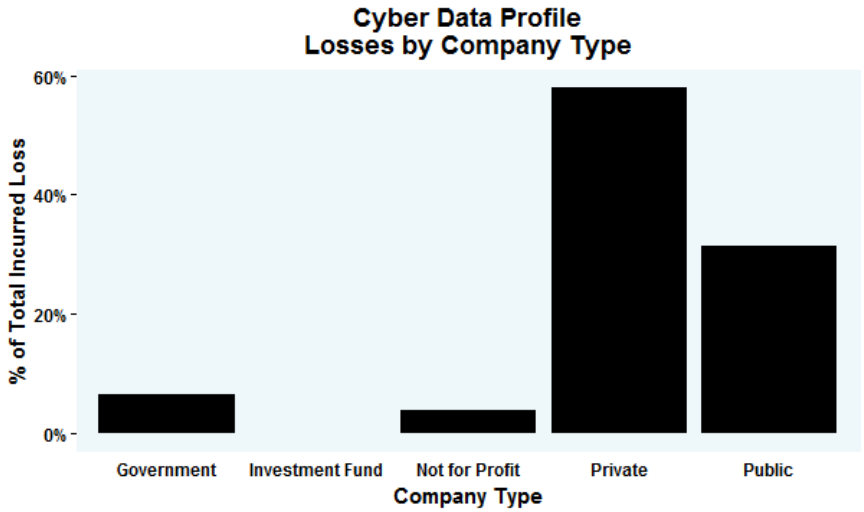
New ISO Cyber SME Coverage Form – Filed June 2017

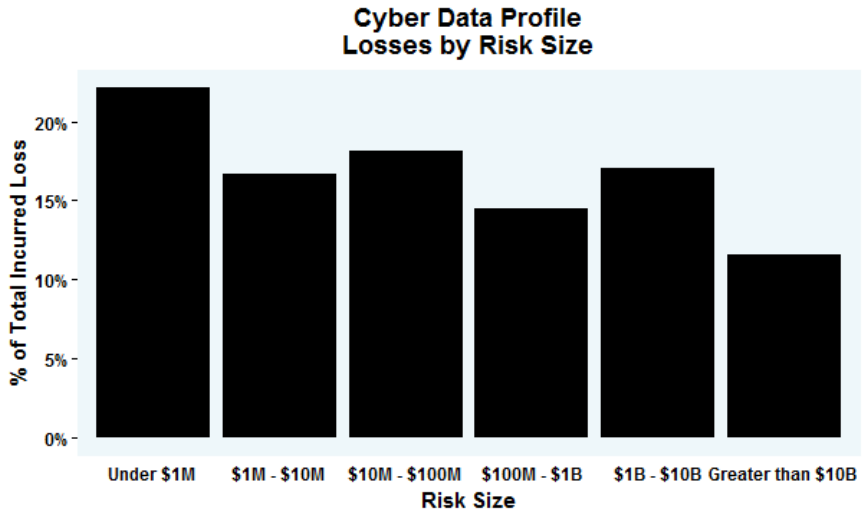
- Filed in 48 states plus DC & Puerto Rico
- Short form SME specific application
- Simplified limit and deductible structure - Base $100k with flexibility to adjust from $50k to $1M
- “Discovery” loss trigger
- Detailed Rating plan informed by analysis of over 20,000 historical cases explicitly impacting SMEs

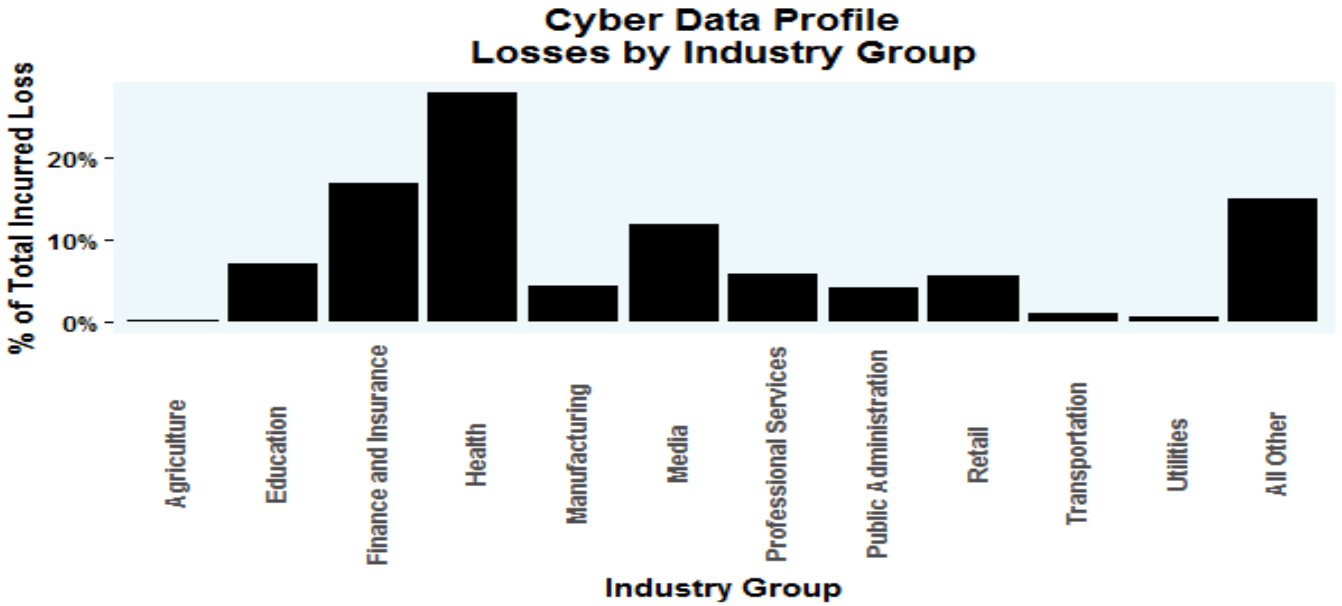
Poll Question #2

- What percentage of cyber losses today affect businesses with less than $10M in revenue?

Cyber Data Profile | Loss



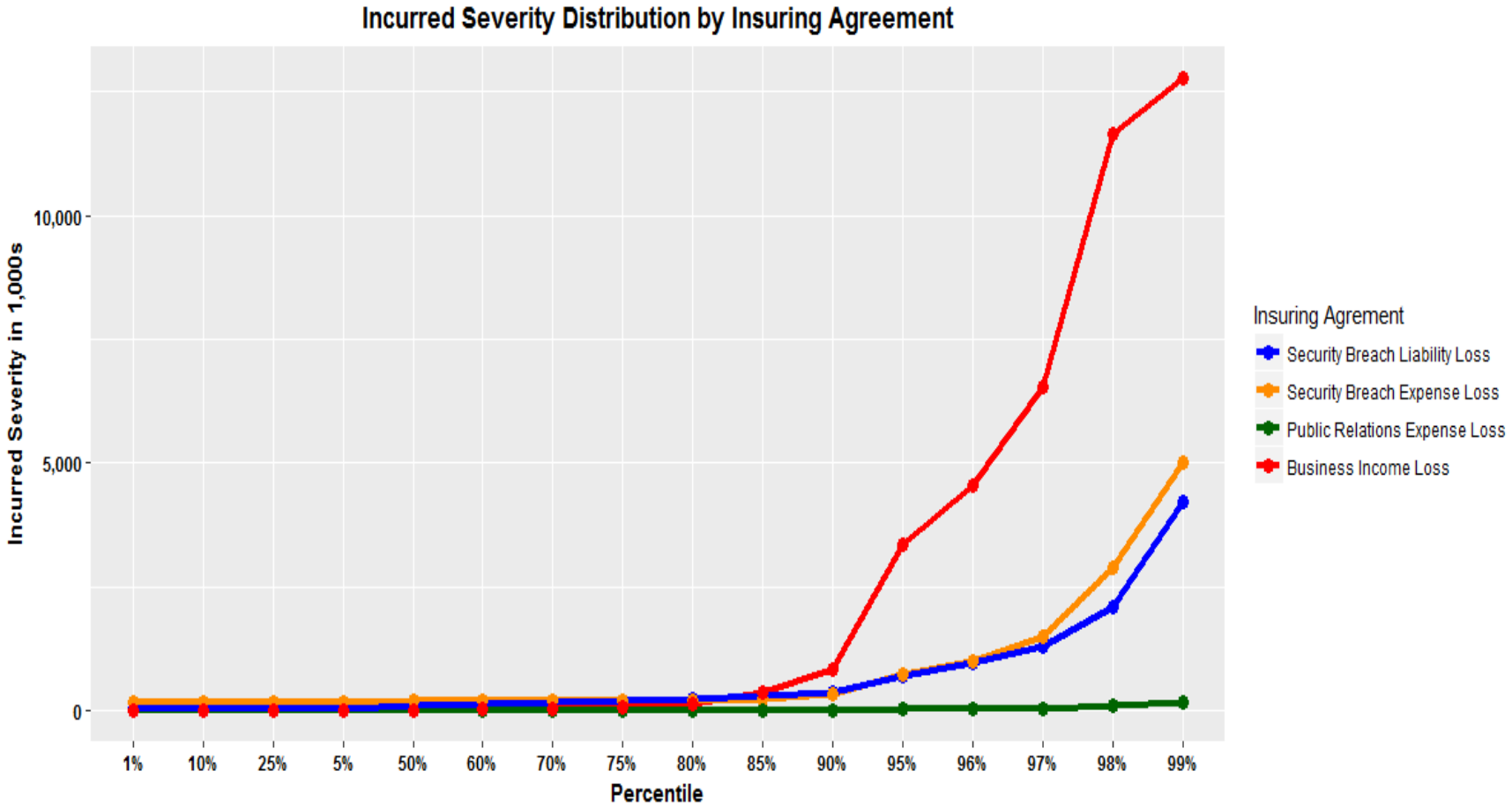




Poll Question #3

- Which insuring agreement has the greatest likelihood of experiencing a cyber loss greater than $10M?

Severity Distribution



*A basic limit of $1M overall captures roughly 85% of the variance in the severity distribution

*A basic limit of $100K only captures less than 10% of the variance in the severity distribution

Challenges in Pricing SMEs

Insurance Industry Faces Additional Challenges in Pricing Small to Midsize Enterprises

Lack of insurance data	Short Application Forms for SMEs	Specialized Coverage Forms for SMEs
Different Security Standard for SMEs	Risk Aggregation Exposure	Competitive and Heterogeneous Market

Lack of Insurance Data

- ~40% of cyber premium is written for SMEs despite SMEs representing 99.7% of U.S businesses
- SME policies are frequently written at very low limits often as low as $25K
- Less information is gathered in SME underwriting systems

Short Application Forms for SMEs

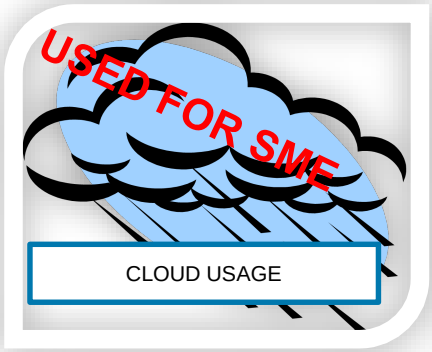
Application Form Length Varies Dramatically by Risk Size:

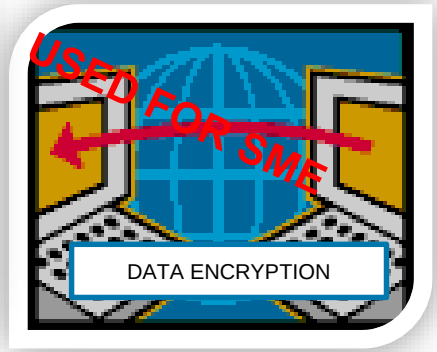
- Small commercial – 15 to 25 questions
- Middle Market – 35 to 45 questions
- Large commercial – 60 to 70 questions

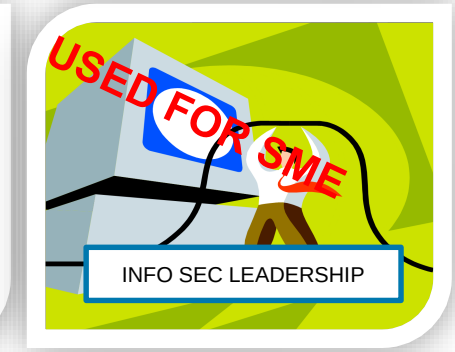
Specialized Coverage Forms for SMEs Part 1

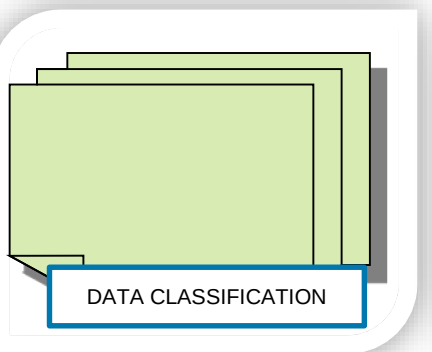
- Typically policy form is rated on a combined basis rather than separately by insuring agreement
- Often additional exclusions are added for SMEs – for example, coverage for DDOS attacks may be excluded
- Basic limit is often much lower than much lower for SMEs

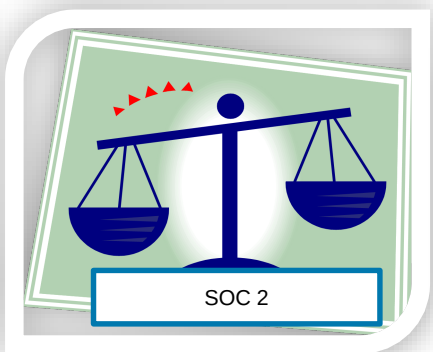
Different Security Standard for SMEs











Risk Aggregation Exposure

- Business Income has the most risk aggregation exposure

- Risk aggregation exposure can be generated via:
  - Cloud usage
  - Internet service provider usage
  - Mass ransomware attacks

- Important to map which cloud service providers your SME book is using to prevent excessive exposure with one provider

Cyber Data Resources for Pricing SMEs

Data Source Types for Cyber

1. Cyber insurance historical premium and loss information

2. Historical insurance premium and loss data from other lines of business including general liability and crime

3. Cyber third party data vendors

4. U.S. businesses distributional data

Drawbacks of Cyber Insurance Databases

- Cyber is often written at low limits (often as low as $50K for small commercial)
- Most businesses do not have cyber insurance, so databases are quite small
- Not useful when developing new coverages, such as reputation protection
- Certain segments are underrepresented
  - Small commercial
  - Manufacturing
  - Education
  - Transportation
  - Utilities

Third Party Data Vendors Overview

Outside In Scan

- Cyber Health and Hygiene
- Ongoing Infections
- IT policies

Incident Data

- Past Incidents
- Losses
- Trend over time

Connectedness

- Cloud Providers
- Software/Hardware Providers
- Degrees of Separation

Threat Intelligence

- Vulnerabilities
- IRC communications
- Leaked credentials

Inside Out Scan

- Evaluate access paths within network
- Evaluate difficulty for hacker to move laterally
- Internal device configurations

Process and Policy

- Self described process and policy evaluation
- Vendor management platform
- Phishing simulations

Endpoint/Mobile

- Security providers have data on risks
- Privacy protection
- Aggregated Information

Cloud Hosting

- Hosting providers have data on security settings of their customers
- They want to incentivize better security

Challenges of Using Third Party Cyber Incident Repositories

- Data is generally missing loss information
- Data only contains cyber incidents that are publicly known
- There is not a simple mapping of losses with exposures

Imputing Missing Loss Information: Overview

Cyber Claims Model: A model that translates the characteristics of a cyber event into estimated insurable loss by insuring agreement

Example Predictors for Business Income Loss:

- Revenue
- NAICS
- Number of Employees
- Event Type

Example Predictors for Non Business Income Loss:

- Number of Records Affected
- Type of Records Affected
- Risk Size
- Event Type

Data Sources for Claims Model Construction

- White papers
  - Verizon
  - Net Diligence
  - Symantec
- Internal cyber insurance databases
  - Claims data
- Third party incident repositories
  - Court records with lawsuit amounts can be used to estimate security breach liability losses

Cyber SME Rating

Cyber Exposure Bases in the Marketplace

- Revenue
- Assets
- Budget
- Net Operating Expense
- Limit
- Number of Records Stored

Segmentation at the 4 Digit NAICS Level Is Critical

Classification Description	4 Digits NAICS
Offices of Physicians	6211
Offices of Dentists	6212
Offices of Other Health Practitioners	6213
Outpatient Care Centers	6214
Medical and Diagnostic Laboratories	6215
Home Health Care Services	6216
Other Ambulatory Health Care Services	6219
General Medical and Surgical Hospitals	6221
Psychiatric and Substance Abuse Hospitals	6222
Specialty (except Psychiatric and Substance Abuse) Hospitals	6223
Nursing Care Facilities (Skilled Nursing Facilities)	6231
Residential Intellectual and Developmental Disability, Mental Health, and Substance Abuse Facilities	6232
Continuing Care Retirement Communities and Assisted Living Facilities for the Elderly	6233
Other Residential Care Facilities	6239
Individual and Family Services	6241
Community Food and Housing, and Emergency and Other Relief Services	6242
Vocational Rehabilitation Services	6243
Child Day Care Services	6244

Potential Rating Variables for SMEs

General Rating Variables

- Revenue
- NAICS
- Years in Business

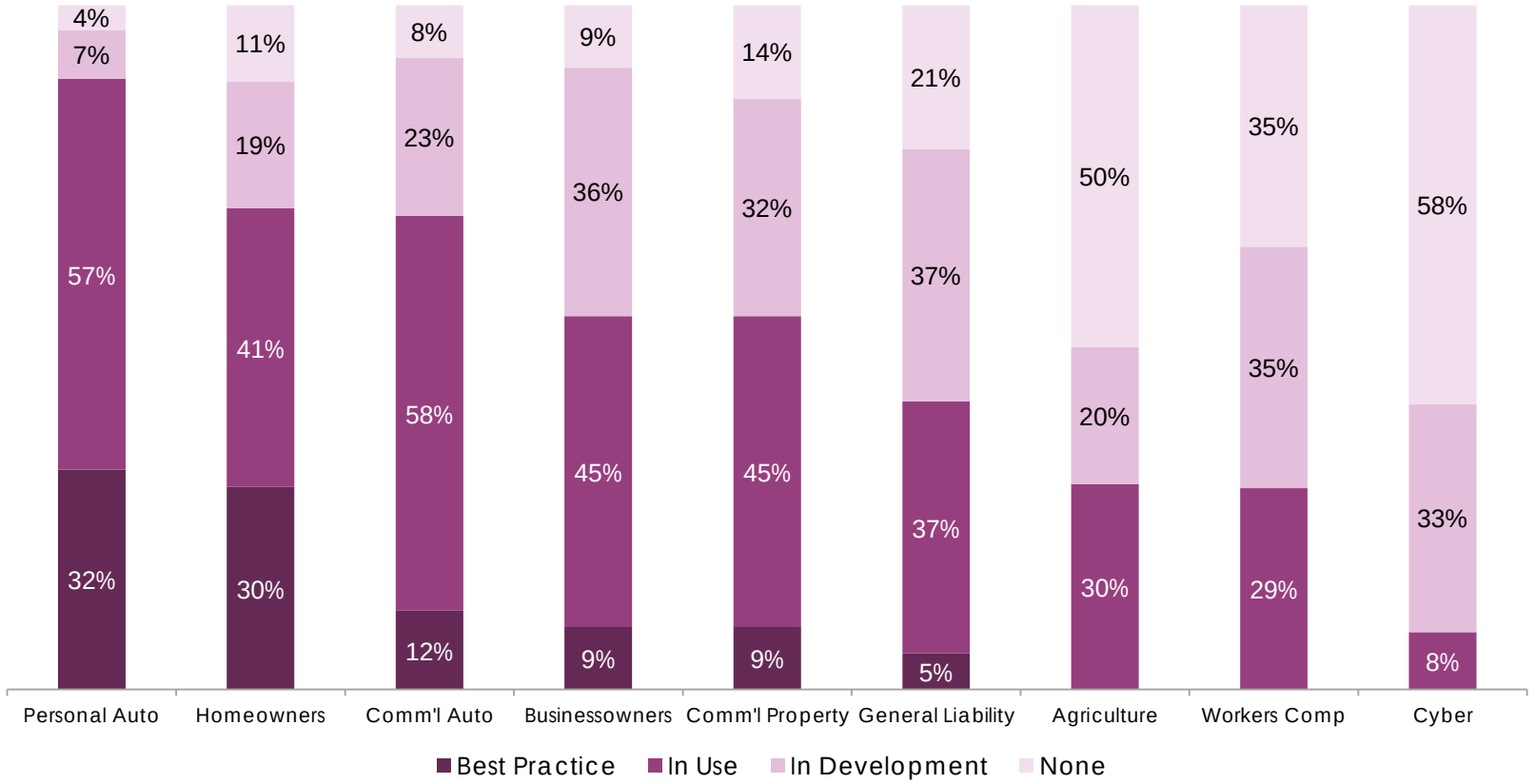
Technical Control Rating Variables

- Email Encryption
- Data Encryption
- Cloud Usage

Administrative Control Rating Variables

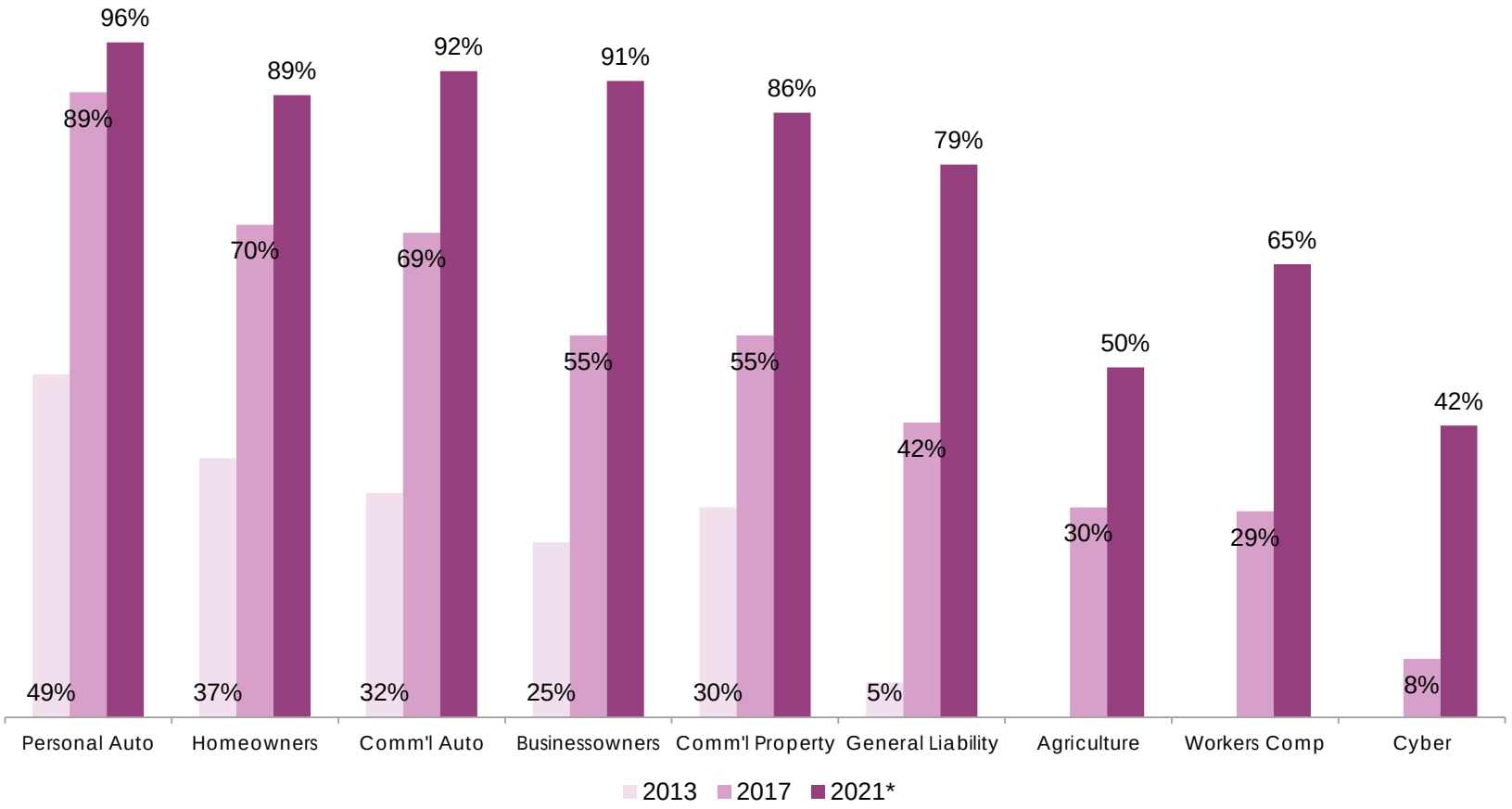
- Employee Training
- Business Continuity Planning
- Information Security Leadership

Analytic Maturity by Line of Business



Preliminary findings from 2017 ISO-Earnix Predictive Modeling Survey (n=40). Want to take it? http://bit.ly/2l4v7hr.

Analytics Growth Projections



Findings from 2013 and preliminary 2017 ISO-Earnix Predictive Modeling Survey (n=269 and n=40).
** - 2021 is projected, based on responses that capabilities are in development over the next two to three years.*

Thank You!

Verisk Analytics