Data and Methods for Managing Cyber Risk

NAIC Cybersecurity Working Group Meeting

Rebecca Bole, Head of Industry Engagement
Jon Laux, VP of Analytics

May 20, 2024

AGENDA

1. Introduction to CyberCube
2. The state of the cyber insurance market
3. Understanding cyber risk
4. Data & decisions at point of underwriting
5. Managing a dynamic risk over time
6. Conclusion

1. Introduction to CyberCube

The trusted partner on cyber risk quantification

Our Mission

To deliver the world's leading analytics to quantify cyber risk.

Our financial cyber analytics improve the resilience of organizations and society.

Our Impact

- Unlock capital for cyber risk to drive innovation
- Translate cyber risk into financial impact for organizations
- Enable societal resilience to systemic cyber risk

Trusted partner in building cyber resilience

We've partnered with over 100 leading institutions who leverage CyberCube's data and analytics to power their cyber (re)insurance growth, including over two-thirds of the global cyber (re)insurance market.*

beazley
AON
Munich RE
LOCKTON
SCOR
CHUBB
KOREAN RE
QBE
HISCOX
GuyCarpenter
AXA

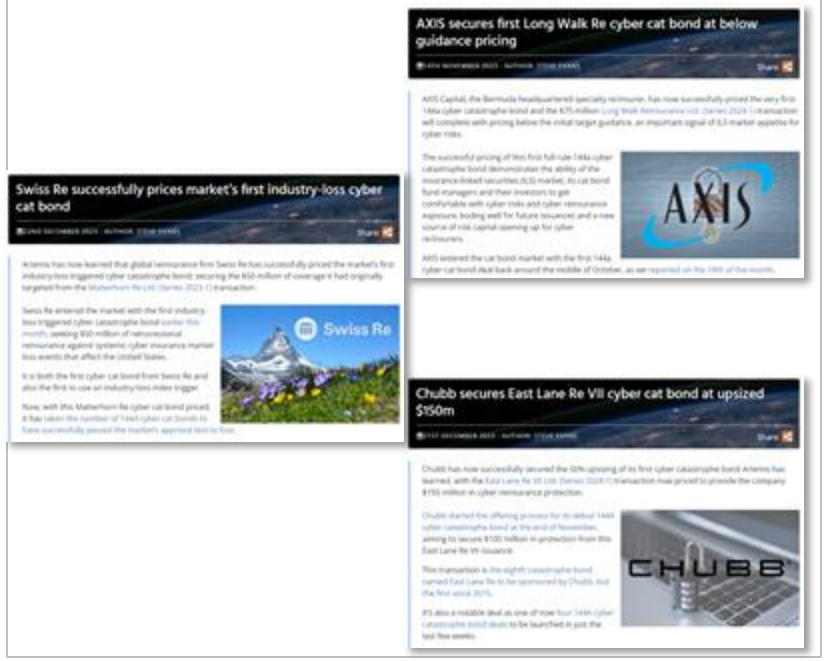
*Sources: NAIC, AM Best, S&P. Data estimated by premium written)

We actively partner with public and private sector organizations to improve the resilience of organizations and society to cyber risk.

We help develop clear, actionable cyber risk strategies for the insurance and financial sectors, for enterprise-level businesses, regulators and policymakers.

FitchRatings
BMA BERMUDA MONETARY AUTHORITY
UNITED STATES OF AMERICA
IAIS INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS
S&P Global
BANK OF ENGLAND PRUDENTIAL REGULATION AUTHORITY
LLOYD'S

CyberCube's analytics are the currency of risk for the financial services industry. CyberCube was used by all 4 Rule 144A cyber cat bonds placed in 2023, with 3 of the 4 selecting CyberCube's view of risk as the basis for pricing. These deals have brought $400M+ in capital into the cyber insurance market.

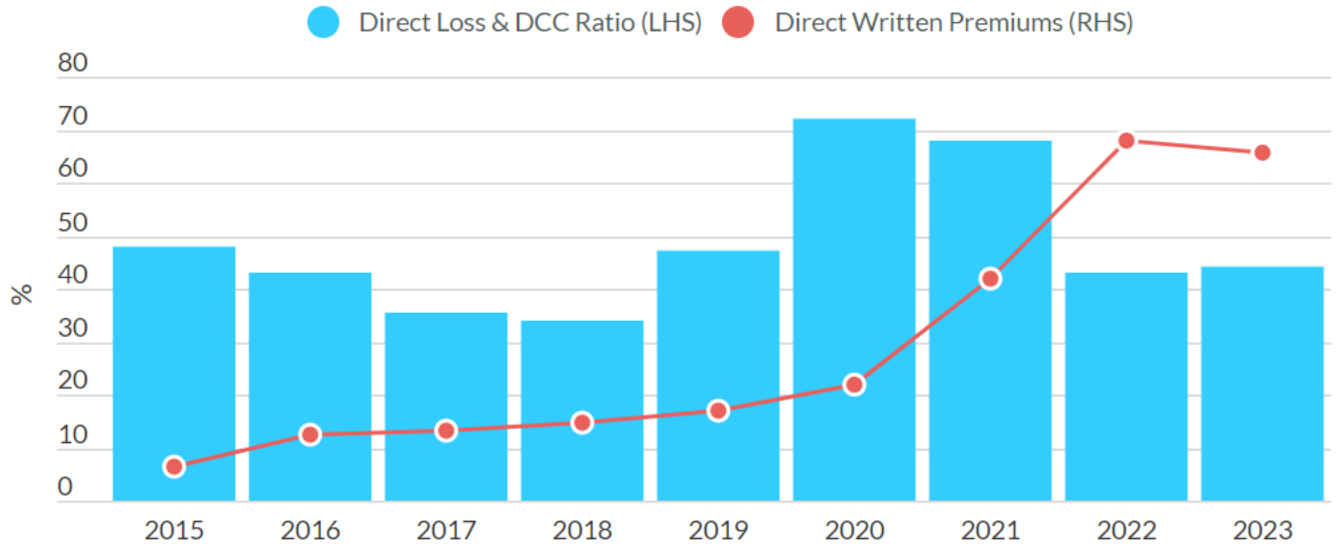


2. The state of the cyber insurance market

State of the cyber market: 2023 reflections

Standalone Cyber Coverage Direct Loss & DCC Ratios

Direct Written Premiums Declined for the First Time in 2023



Source: Fitch Ratings, S&P Global Market Intelligence
Statutory Cybersecurity and Identity Theft Insurance Coverage Supplement Data

- 2023 saw a general trend of rising claim severity related to "double extortion" claims
- Frequency of *attacks* also increased, but policyholders' resilience has improved
- The extortion campaign involving MOVEit software contributed a measure of Cyber CAT loss in 2023
- Despite this, we believe carriers realized a significant amount of favorable rate movement building on several years of market hardening
  - US Standalone loss ratio of 44% (2022: 43%)
- US Standalone premium leveled off, -2% yoy

State of the cyber market: 2024 outlook

Threat Landscape

- Ransomware attacks continue
- “The breach is back”: increased activity focus on exfiltration and/or double extortion
- Much more public comm’s from threat actors: media leaks, SEC reporting
- Potential for widespread public sector attacks as geopolitical tensions rise

Insurance Market

- Market showing signs of softening, but claim trends remain a worry
- 'Change Healthcare' event illustrating systemic risk potential as well as large-scale remediation efforts
- CAT/systemic risk a major concern – many approaches being explored to identify & contain it
- Increased reliance on models for risk tolerance, reinsurance & capital

Reinsurance Market

- Demand neutral, supply more abundant
- Market has “caught up” with primary writers – improved terms for cedants
- Challenges over exclusions, esp. war
- Cedants willing to retain more
- Event XOL cover finding favor
- 1st successful Cyber ILS placements

3. Understanding cyber risk

Cyber risk has similarities to other P&C lines, but is unique to itself

How cyber risk is like:

Property

- Short tail
- Catastrophe-exposed line
- Embrace of catastrophe modeling & exposure management
- Focus on risk tolerance at the extreme tail: 1-in-100, 1-in-250

Casualty

- Social science, not natural science
- Managed within Specialty / Professional Liability / E&O
- Concern about systemic risk (theoretically cannot be diversified)
- Pricing volatility & underwriting cycle
- Mean vs median vs mode loss ratio

Terrorism

- Man-made peril
- Sensitive to political environment
- Dynamic & rapidly evolving threat

Observations indicate that cyber insurance is among the most volatile P&C lines

Cyber insurance is a very dynamic environment:

- Fluctuations in loss frequency & severity
- Underwriting cycle – rapid changes in rates, T&C's
- Measured volatility exceeds many P&C lines…
- … plus CAT risk!

CHANGE HEALTHCARE

Progress MOVEit

Exhibit 27: Comparison of Cyber volatility to selected Schedule P lines

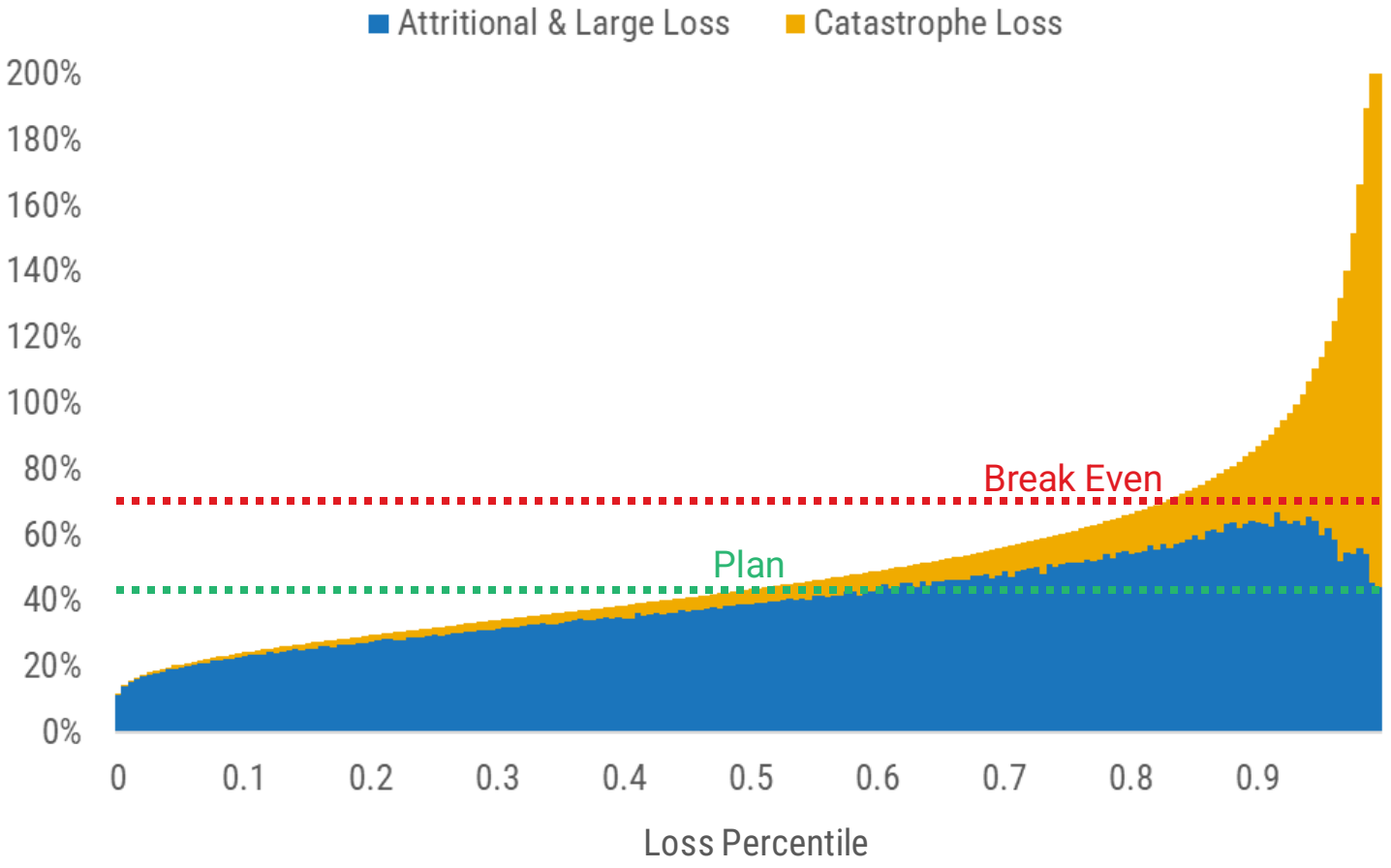
Line of Business	CV
Private Passenger Auto	14%
Commercial Auto	22%
Workers' Compensation	26%
Commercial Multi Peril	34%
Other Liability Claims-Made	37%
Homeowners	44%
Cyber	**61%**
Fidelity and Surety	63%
Reinsurance - Liability	67%
Reinsurance - Property	78%

Source: Aon, *U.S. Cyber Market Update*, September 2023

Key questions for insurers

- How much capital is needed to support this line?
- What do we *expect* this year? ("plan")
- How much could our view of risk *change* over 1 year? ("plan" vs. "actual")

Representative Loss Ratio Distribution



4 choices for risk

1. Accept

2. Avoid

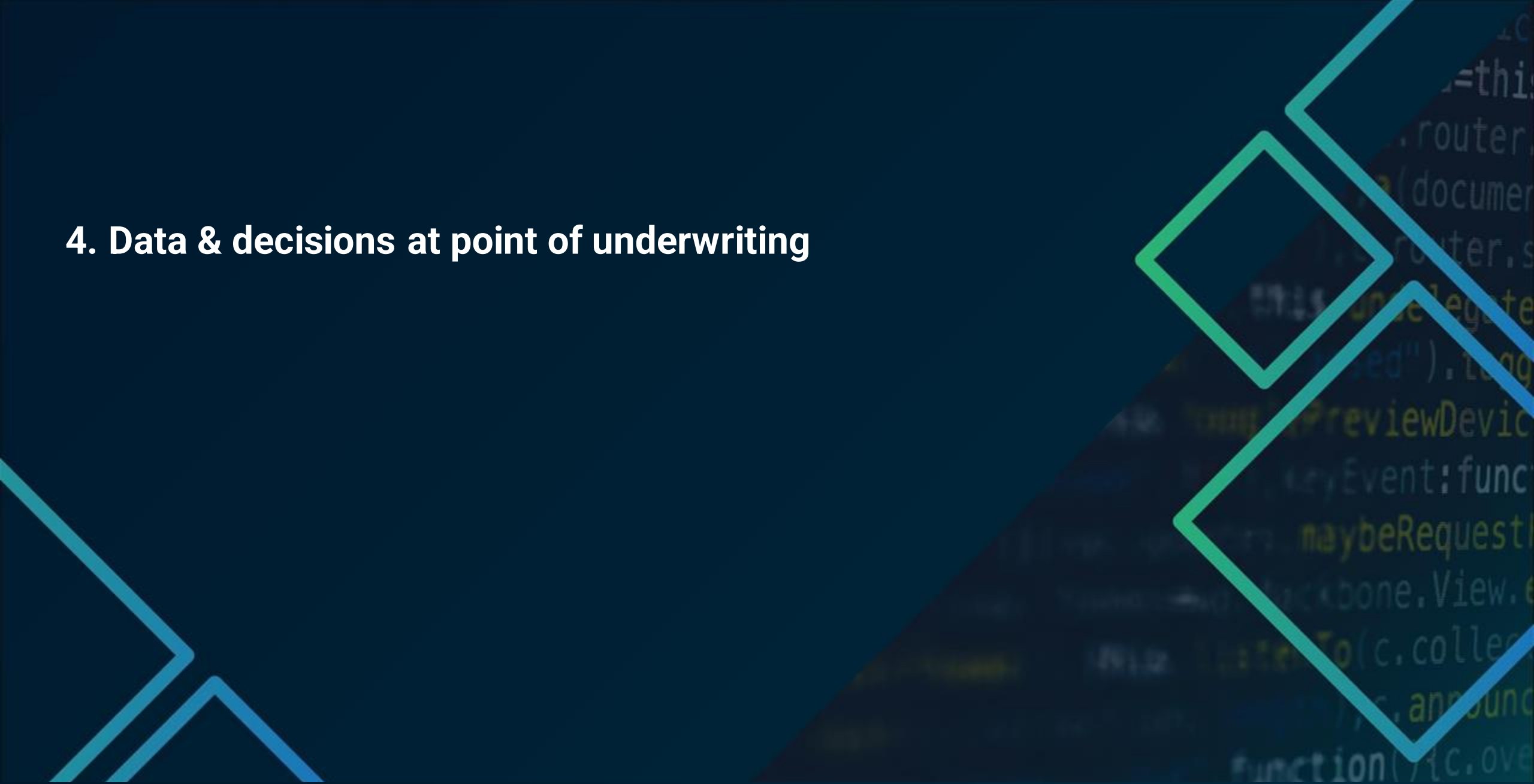
3. Mitigate

4. Transfer

Timeframe

“How long am I committed to my decision before I can revisit it?”

4. Data & decisions at point of underwriting



At point of underwriting: all 4 risk choices available

1. Accept

2. Avoid

3. Mitigate

4. Transfer

Point of Underwriting

1-Year Outlook

As a digital risk, data about cyber risk is abundant

Data categories (CyberCube examples):

Enterprise Data

Database of over 20 million companies' specific details:

- Location, revenue, industry
- Number of employees
- Company URL, TLD and subdomains

Digital Supply Chain

Technology dependencies at a company level:

- 40,000+ unique technologies and services captured
- Maps to individual company, 1B+ tech-to-company mappings

External Network Scans

Trusted data partners providing:

- Malware infections
- CVE identification
- Misconfigurations
- Dark Web intelligence
- Tech stack mapping
- Port scanning

Internal Network Scans

Behind the firewall data:

- MFA
- SIEM
- Backup Technologies

Internal Cyber Hygiene:

- Vulnerability Mgmt
- Configuration Mgmt
- Network Security

Expert Intelligence

Internal and external expert surveys:

- Patching levels
- Security awareness
- Event monitoring
- Best practices
- Industry standards

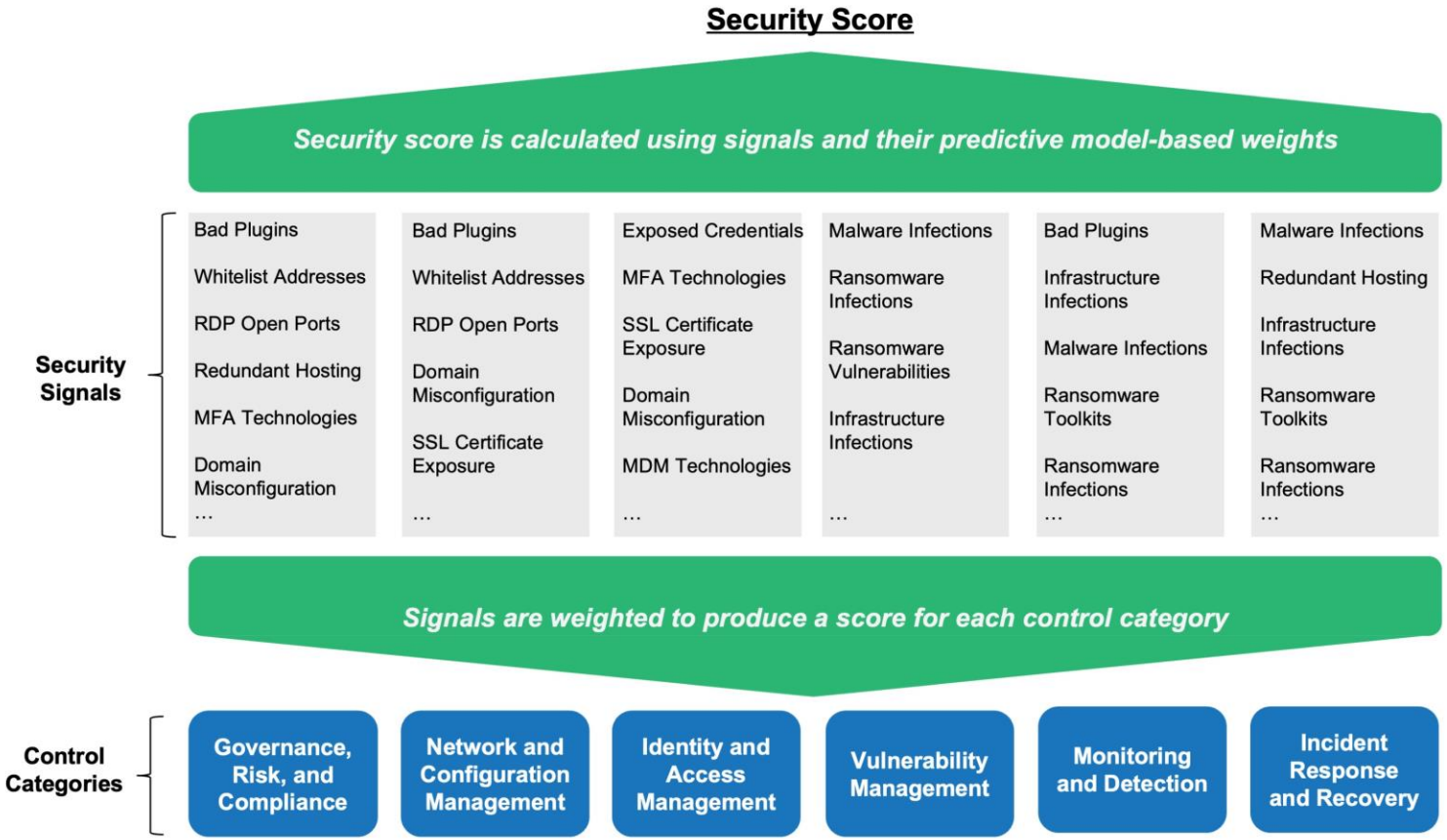
Historical Data

Cyber incidents:

- Historic events
- Public disclosures
- Media articles
- DFIR reports
- IR partners
- Industry data

Data is abundant. The important question is, can we make sense of it?

Security control frameworks provide a guide



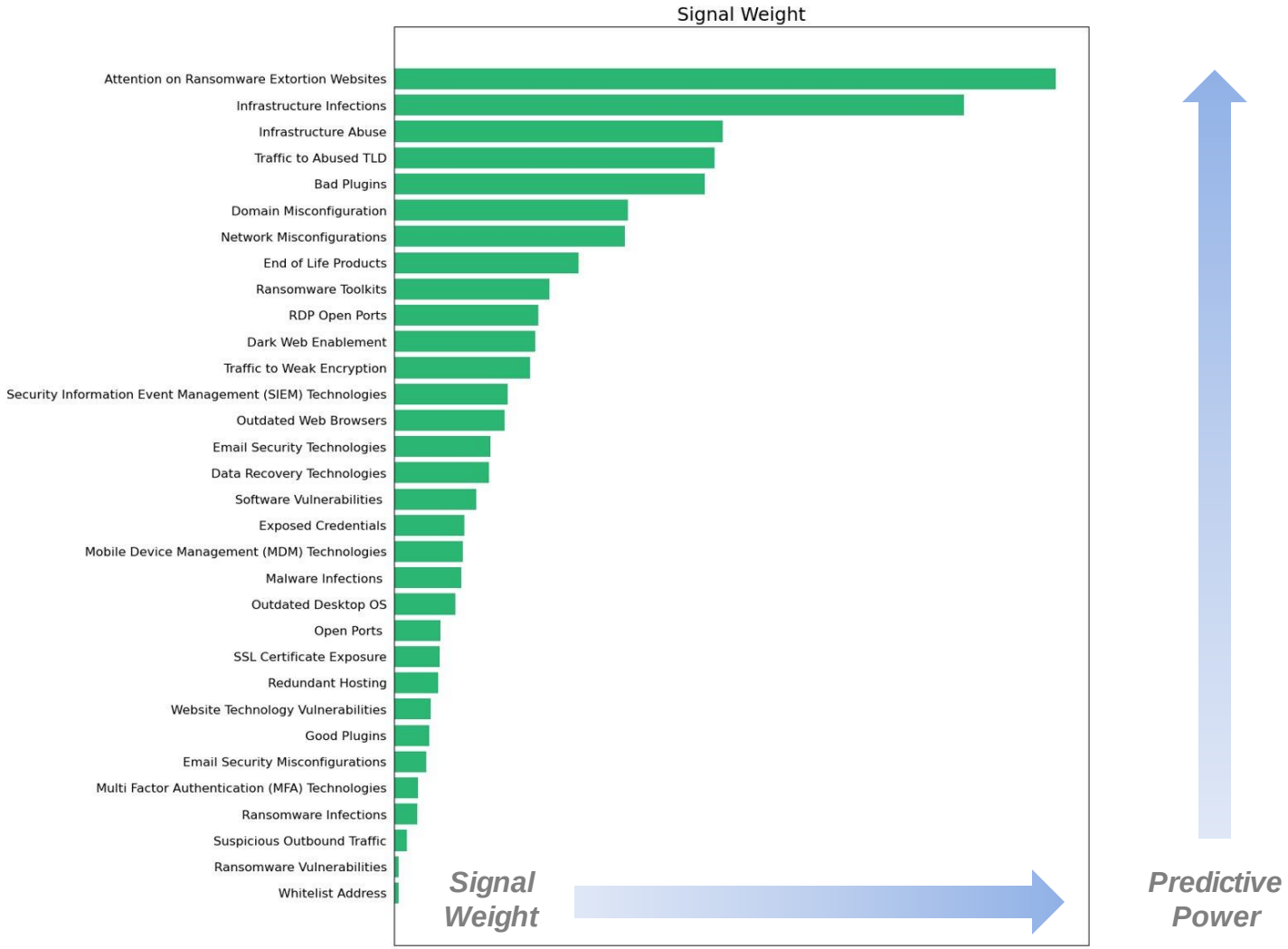
- NIST, CIS, and ISO control frameworks all commonly used
- Security control questions are commonly asked in underwriting questionnaires, esp. for larger accounts
- Security control data can be a challenge for underwriting small businesses, when efficiency is key
- Important to understand:
  - Efficacy of security controls ("does it work?")
  - Scalability of using controls in underwriting ("can we use it?")

Detailed analysis can inform decision making and quantify the importance of many security signals

There are many potential signals of a company's security health, including:

- Active cybersecurity measures undertaken to mitigate risk
- Signs of active or prior compromise
- The value of the company as a target for cyber threat actors (exposure to loss)

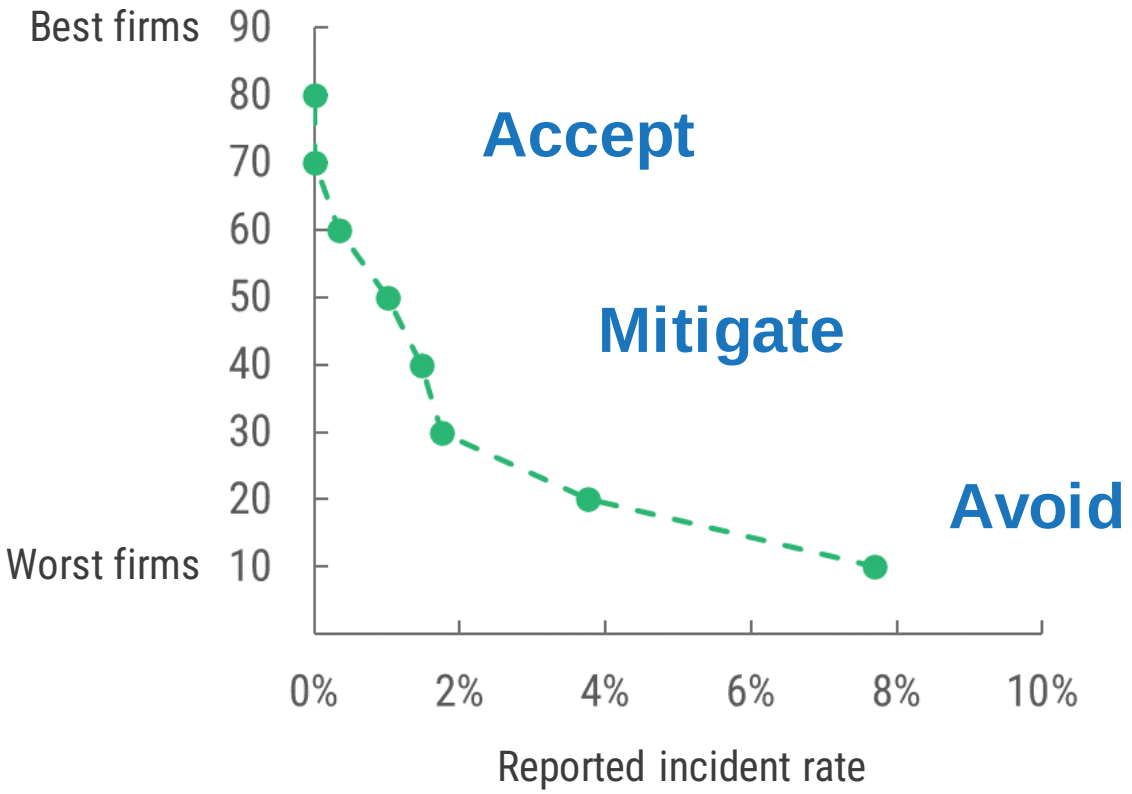
CyberCube applies weightings to signals it monitors, to indicate the predictive power of the signal to a cyber loss.



Notes
1. Signal weights are derived from our data science analysis, relating various risk and exposure signals to the likelihood of an incident:
2. Signals are weighted by their predictability based on correlation coefficients. Higher Weight = stronger correlation with a security incident.

Risk scores allow significant potential to recognize differences in risk quality at point of underwriting

Risk Scoring vs. Cyber Incidents



Source: analysis by CyberCube

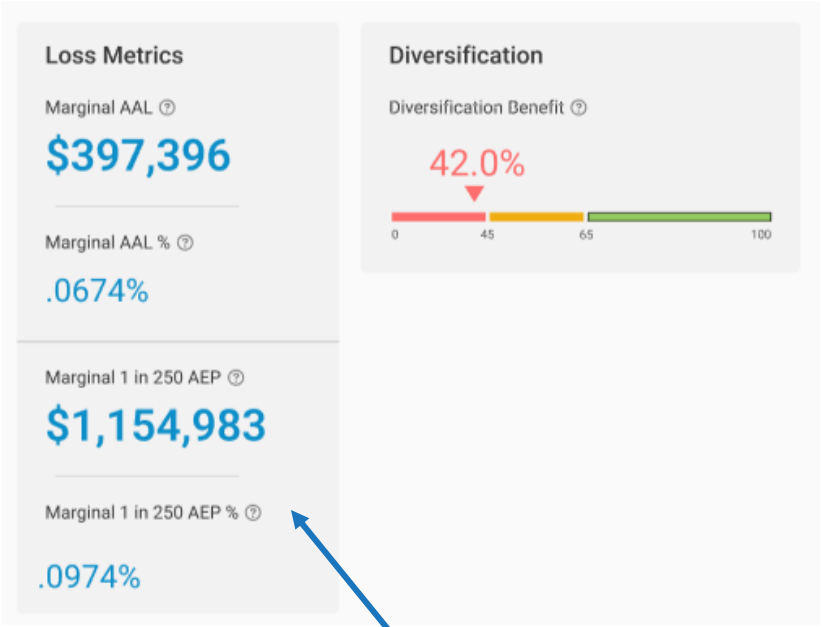
- Analysis shows clear relationship between companies' security posture and their propensity to fall victim to cyberattacks
- Security signals externally observable – incorporates positive & negative hygiene, suspicious activity, & signs of prior infection (see below)
- With disciplined attention to signals and scoring, insurers can make efficient underwriting decisions, evaluate pricing, & assess the cost/benefit of helping insureds mitigate risk

Signal Category	Scoring Weight
Positive Hygiene	10-15%
Negative Hygiene (mitigatable)	35-40%
Suspicious Activity (possible mitigation)	15-20%
Infection Signals	30-35%

With insurers' accumulations rising, it is beneficial to consider Accepting or Avoiding CAT risk at the point of underwriting

- With sizable portfolio accumulations, managing potential CAT impact is of heightened importance
- Objective: proactive action at point of underwriting to diversify portfolios, use capital efficiently & generate better returns
- Use cases
  - North star metric thresholds
  - Return on risk capital thresholds
  - Tail diversification thresholds

Marginal Risk Metrics (example)



- E.g. target accounts with lower contribution to 1:250 AEP
- Refer accounts with >0.08% or over $1M contribution

Markets are exploring "Avoid" strategies for CAT risk: War & infrastructure exclusions, & widespread event triggers

Key questions the industry is asking:

- What role can policy language play to contain (re)insurers' exposure to CAT scenarios?
- What would this do to reduce capital requirements?

Exclusions commonly used to limit scope of Cyber "systemic" risk

- Critical infrastructure: commonly excluded via several wordings
- War: ongoing debate over definitions, including recently at 1/1

"Widespread event" triggers being explored:

- Sublimits vs. exclusions, focus on key scenarios vs. broadly
- Tradeoffs between tail reduction & AAL reduction
- Results vary greatly depending on approach (see right)

Cyber Tail Values & Widespread Trigger Approach

1:100 Tail Value at Risk

Source: CyberCube
Results based on representative market wordings applied to a diversified industry portfolio

5. Managing a dynamic risk over time

On risk: more limited options during policy year

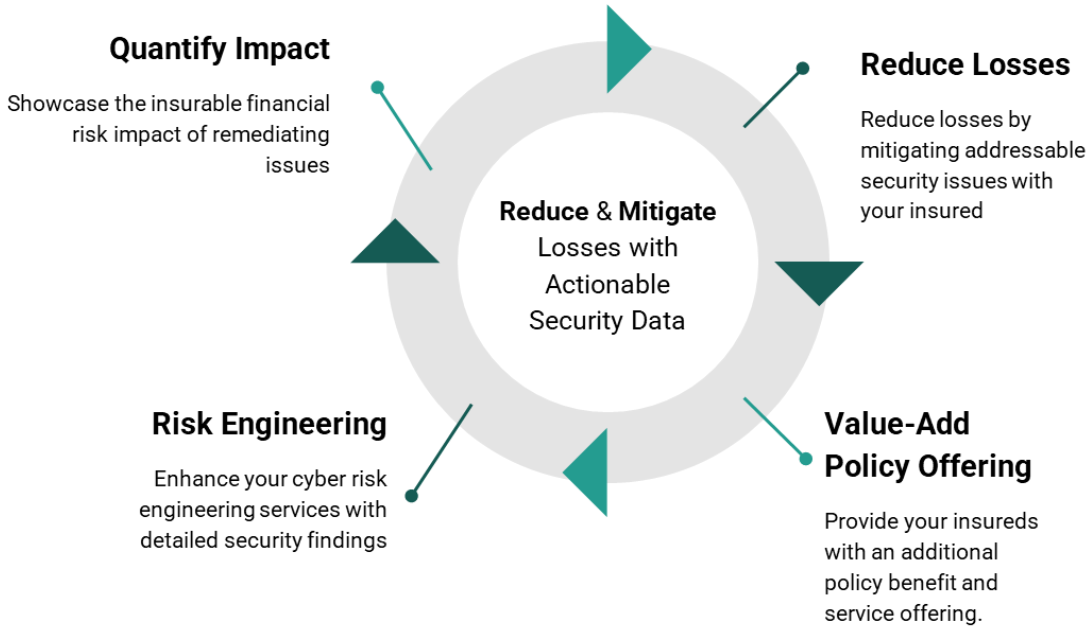
1. Accept
2. Avoid
3. Mitigate
4. Transfer

Policy Year

- Risks already accepted
- Pricing decisions made
- Reinsurance program in place
- Volatility now a primary concern
- Choices: accept or mitigate!

Many carriers seeking “Mitigate” strategies via Active Risk Monitoring

- Loss control not a new concept, but uniquely important at scale for Cyber given its time-sensitivity
- Carriers can improve loss ratios while increasing value and partnership for policyholders
- Achieved by combination of:
  - Proactive routine assessments
  - User-defined thresholds for security conditions
  - Autonomous alerts & notifications to insureds
  - Quantification of loss control measures

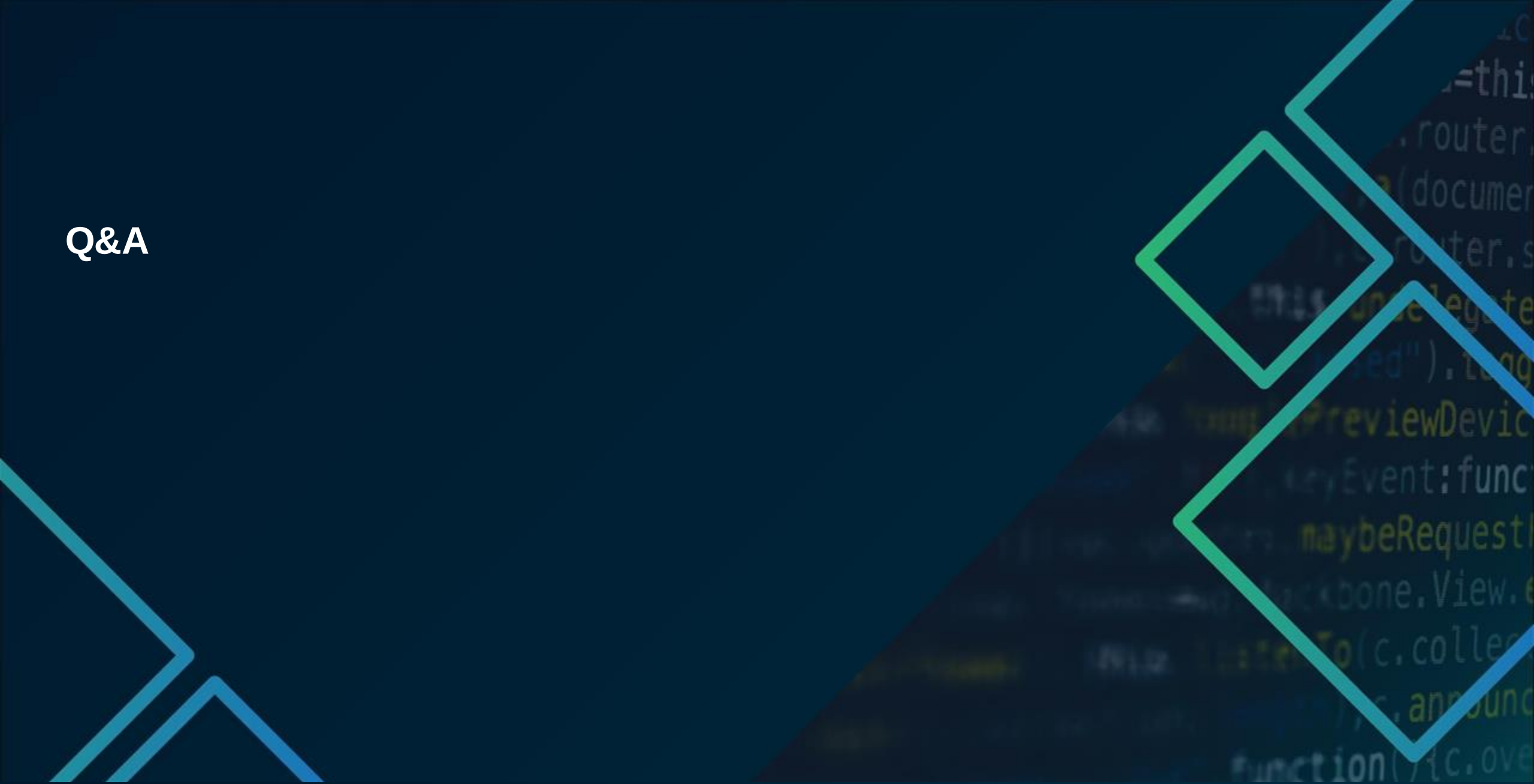


6. Conclusion

Conclusion

- Abundance of data available to cyber insurers for underwriting and risk management
- Cyber insurance requires adaptiveness and ongoing engagement with policyholders to improve resilience and reduce potential claim costs
- Understanding insurers' use of data, level of testing and adaptability to change are important criteria for underwriting maturity

Q&A



Questions? Email us at info@cybcube.com

CyberCube Analytics, Inc., 58 Maiden Lane, 3rd Floor, San Francisco, 94108

Appendix

CyberCube US insurance industry loss modeling study, Q4 2023

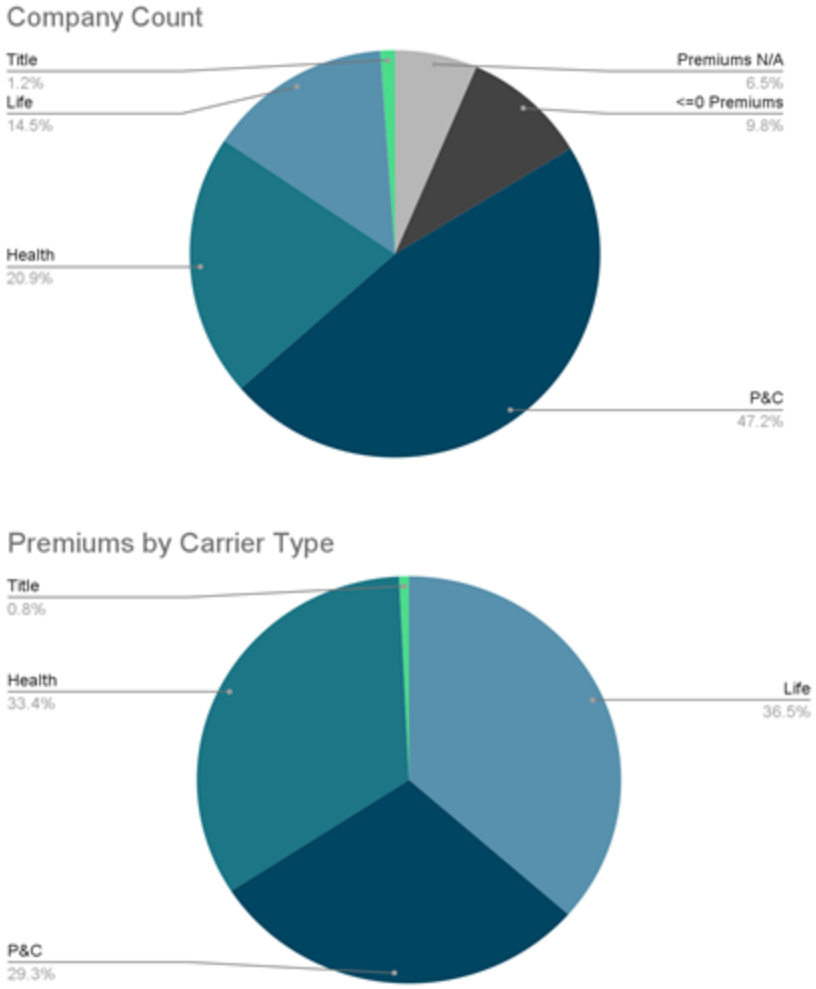
1. **Which companies are most vulnerable from a security perspective?**

2. Which insurer technology dependencies are likely to drive losses?

3. What types of events are most likely to cause losses across the insurance industry?

4. What is the financial cost of cyber attacks on the US insurance industry?

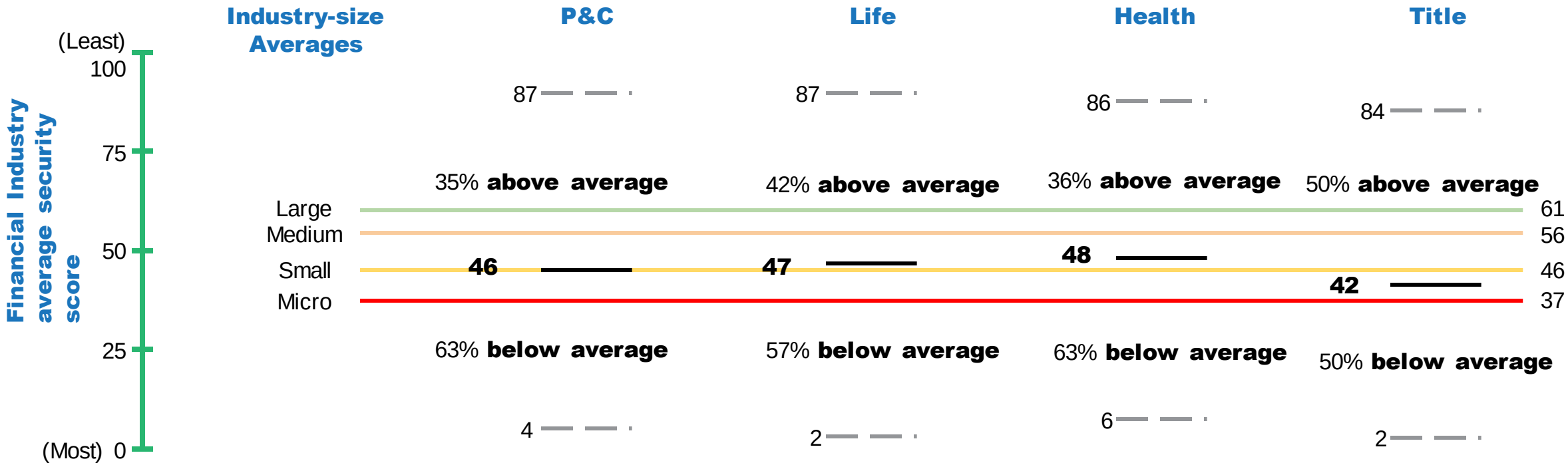
5. Which companies present the largest risks?



Total of 4,156 US carriers, writing $2,891bn in Direct Written Premium in 2022

1. Which segment is the most *vulnerable* from a security perspective?

> CyberCube Security Score averages show *all* Financial industry companies
> For all insurers, the averages by segment range from 42-48, therefore slightly below average Financial companies
> For P&C and Health insurers, two-thirds are below average for all Financials
> Life and Title insurers sit around the Financial industry average
> Overlaying company size, Large and Medium companies have above average scores. Small are average and Micro are below average



2. Which insurer technology dependencies are likely to drive losses?

- CyberCube loss modeling is based on Single Points of Failure (SPoF) technology dependencies that act as vectors to cause loss

- We show here the top SPoF groups for the insurance industry

- Research highlights 4 main SPoF types as vulnerabilities for attack: Certificate Authority, File sharing providers, Email services providers and Content Management Systems

Insurer technology dependency groups

- **Cloud Service Provider** (Omni)
  - AWS, Azure, Salesforce
- **Content Delivery Network** Provider
  - Cloudflare, Akamai, Amazon CloudFront
- **Certificate Authority**
  - DigiCert, Let's Encrypt, GoDaddy
- **Cloud-based Enterprise File Sharing Provider**
  - MS OneDrive/Azure, Google Drive, Apple iCloud
- **Email Services Provider**
  - MS Exchange, Gmail for Business, Zoho Mail
- **DNS Provider**
  - Route53, Cloudflare, GoDaddy
- **Operating System - Server**
  - Ubuntu, Unix, Linux
- **Content Management System Provider**
  - WordPress. Adobe Experience Manager, HubSpot CMS
- **E-Commerce Platform**
  - Shopify, Magento, Amazon