Marsh

Quantifying the Cost of Cyber Risk

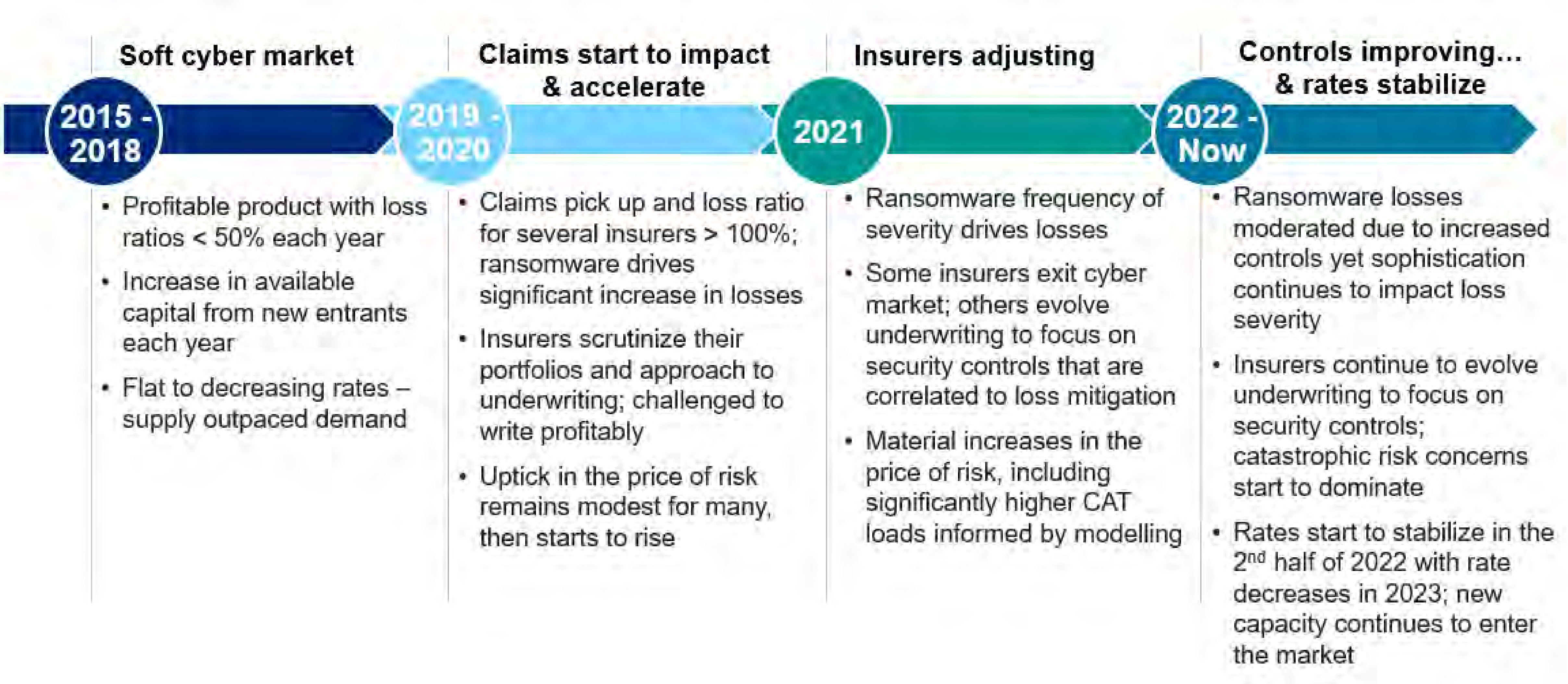
October 10, 2024

A business of Marsh McLennan

Agenda

- Quick cyber insurance overview
- The cyber data spectrum
- Correlations between cyber incidents and:
  - Questionnaire data
  - Outside-in data
  - Dark web data
- Summary and conclusions

Cyber Insurance Timeline



2015 - 2018: Soft cyber market

- Profitable product with loss ratios < 50% each year
- Increase in available capital from new entrants each year
- Flat to decreasing rates – supply outpaced demand

2019 - 2020: Claims start to impact & accelerate

- Claims pick up and loss ratio for several insurers > 100%; ransomware drives significant increase in losses
- Insurers scrutinize their portfolios and approach to underwriting; challenged to write profitably
- Uptick in the price of risk remains modest for many, then starts to rise

2021: Insurers adjusting

- Ransomware frequency of severity drives losses
- Some insurers exit cyber market; others evolve underwriting to focus on security controls that are correlated to loss mitigation
- Material increases in the price of risk, including significantly higher CAT loads informed by modelling

2022 - Now: Controls improving… & rates stabilize

- Ransomware losses moderated due to increased controls yet sophistication continues to impact loss severity
- Insurers continue to evolve underwriting to focus on security controls; catastrophic risk concerns start to dominate
- Rates start to stabilize in the 2nd half of 2022 with rate decreases in 2023; new capacity continues to enter the market

Marsh

A business of Marsh McLennan

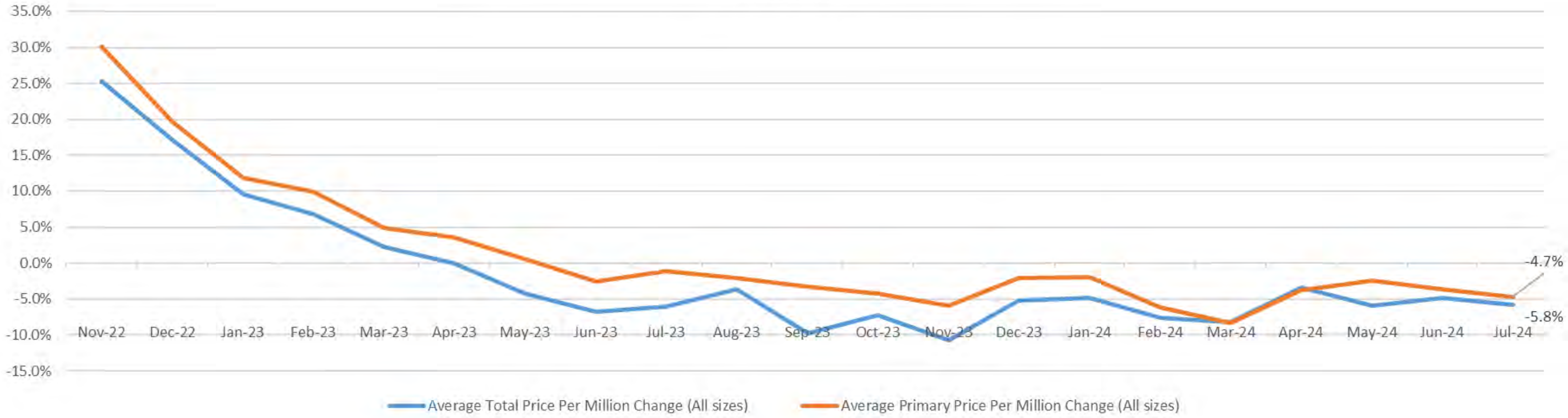
Competitive Rate Trend Through July

Improved pricing remains available despite evolving claims and risk environment

Average US Cyber Price Per Million Changes Over Time

Source: Marsh Global Placement & Specialties, Data and Analytics, PlaceMAP

Marsh Clients



July 2024 Renewals*	1st Quartile	Median	Average	3rd Quartile
Total price per mil	-11.8%	-2.7%	-5.8%	0.4%
Primary price per mil	-10.1%	-1.7%	-4.7%	0.9%

*Programs that renewed with expiring limits | Excludes 29% of June renewals due to limit changes.

All July 2024 renewals including those with limit changes**	Average
Total price per mil	-7.9%
Primary price per mil	-6.0%

**Includes 19% of renewals with limit changes:

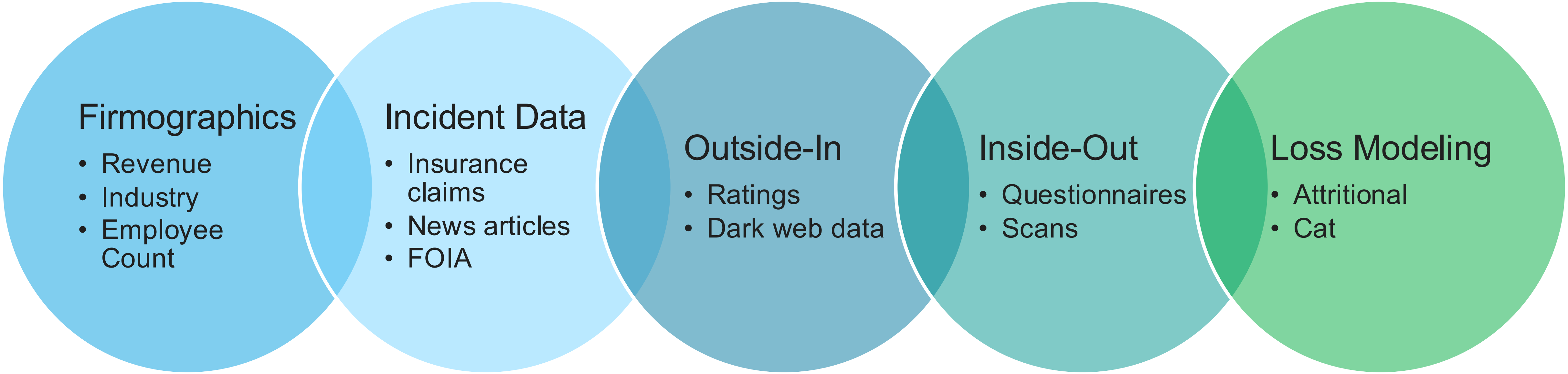
15% increased limits

4% reduced limits

Takeaways:

1. Premium decreases continue into July
2. Clients are using savings to invest in additional cyber limits.
3. Opportunity to evaluate cyber limits against total cost of risk.

The Cyber Data Spectrum



Firmographics

- Revenue
- Industry
- Employee Count

Incident Data

- Insurance claims
- News articles
- FOIA

Outside-In

- Ratings
- Dark web data

Inside-Out

- Questionnaires
- Scans

Loss Modeling

- Attritional
- Cat

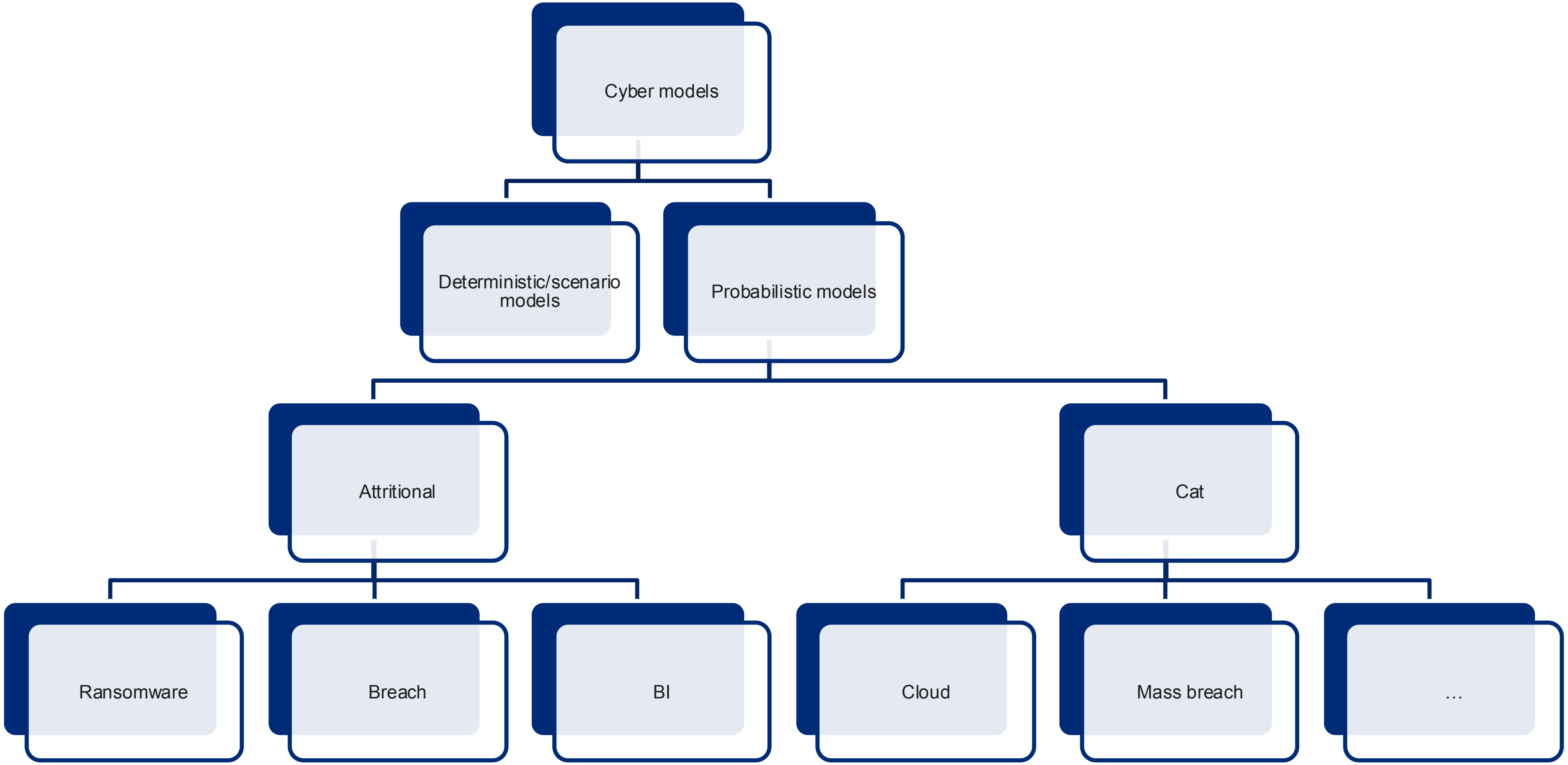
Advantages of Using Insurance Data

Unbiased dataset

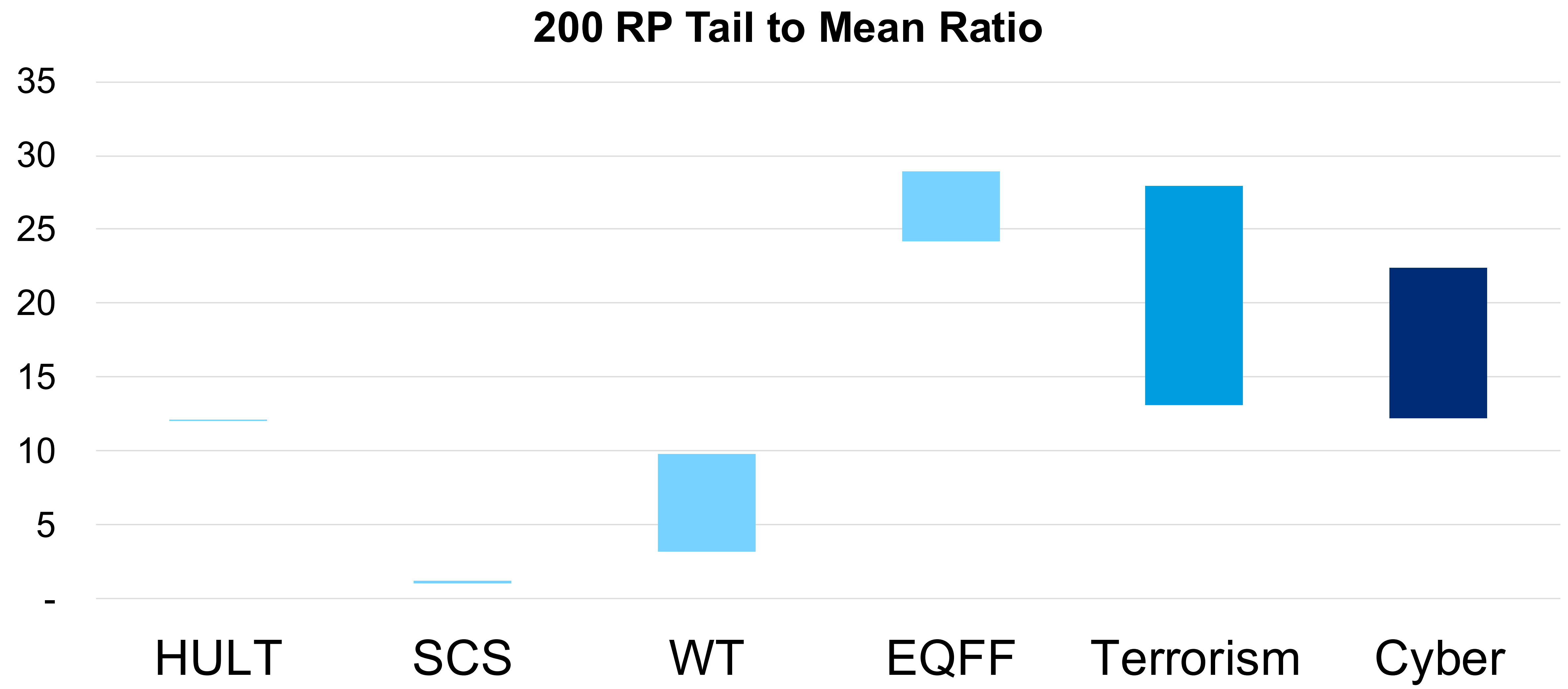
Global coverage

High fidelity in reported incidents

Cyber Modeling Overview



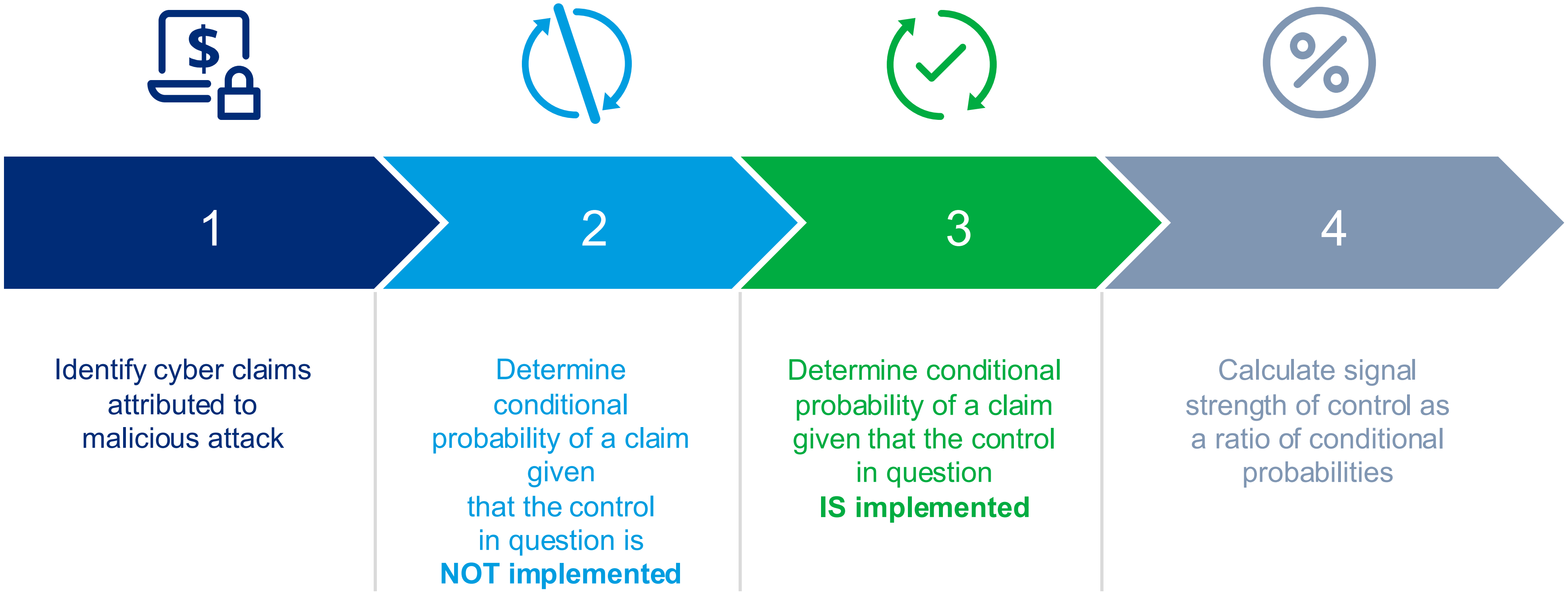
Cyber Tail Losses vs Other Perils



Marsh

HULT – Hurricane Long-Term; SCS – Severe Convective Storm; WT – Winter Storm; EQFF – Earthquake with Fire Following

Cyber Controls Study Design



1 Identify cyber claims attributed to malicious attack

2 Determine conditional probability of a claim given that the control in question is **NOT implemented**

3 Determine conditional probability of a claim given that the control in question **IS implemented**

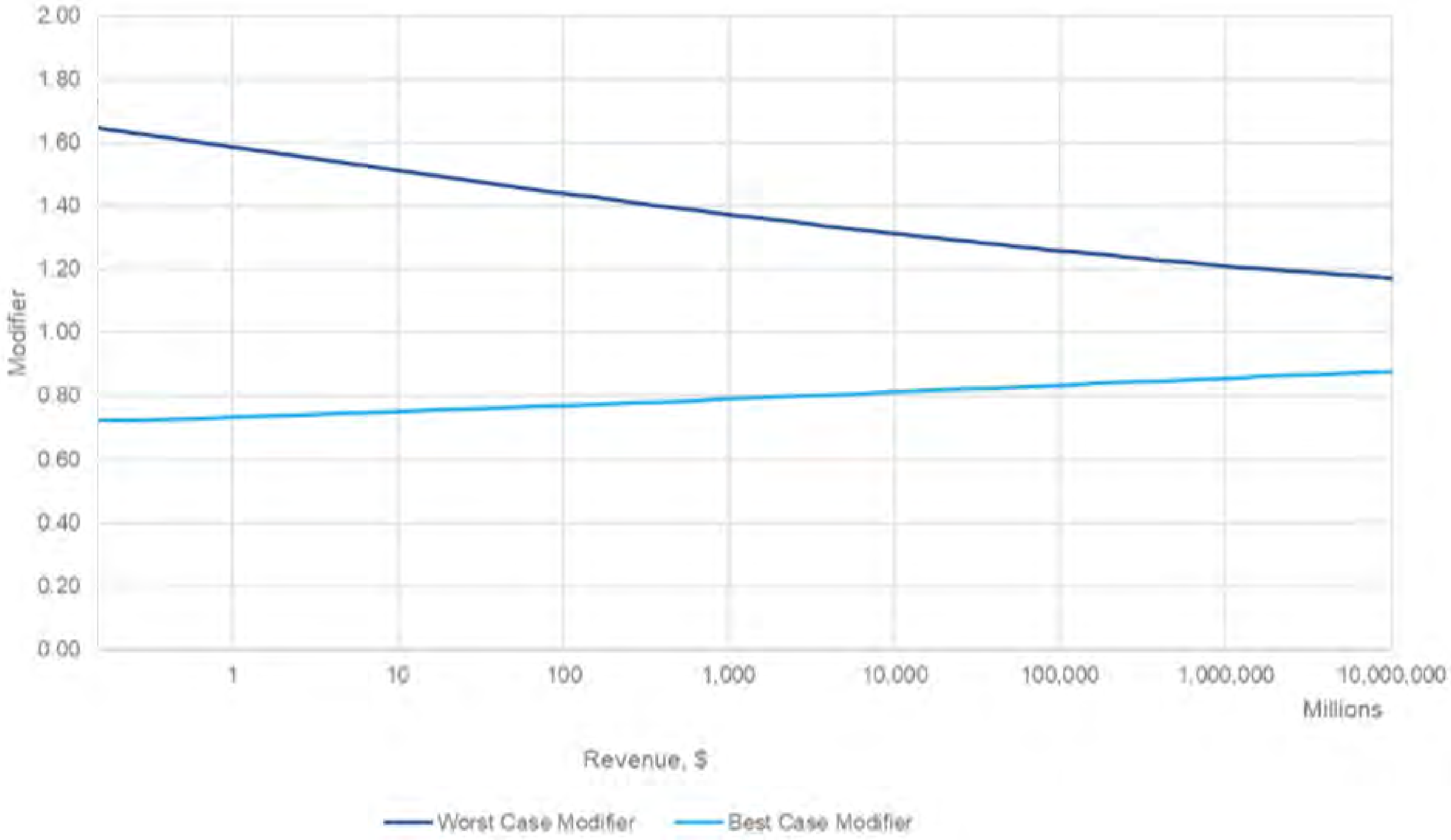
4 Calculate signal strength of control as a ratio of conditional probabilities

Individual Cyber Controls Impact

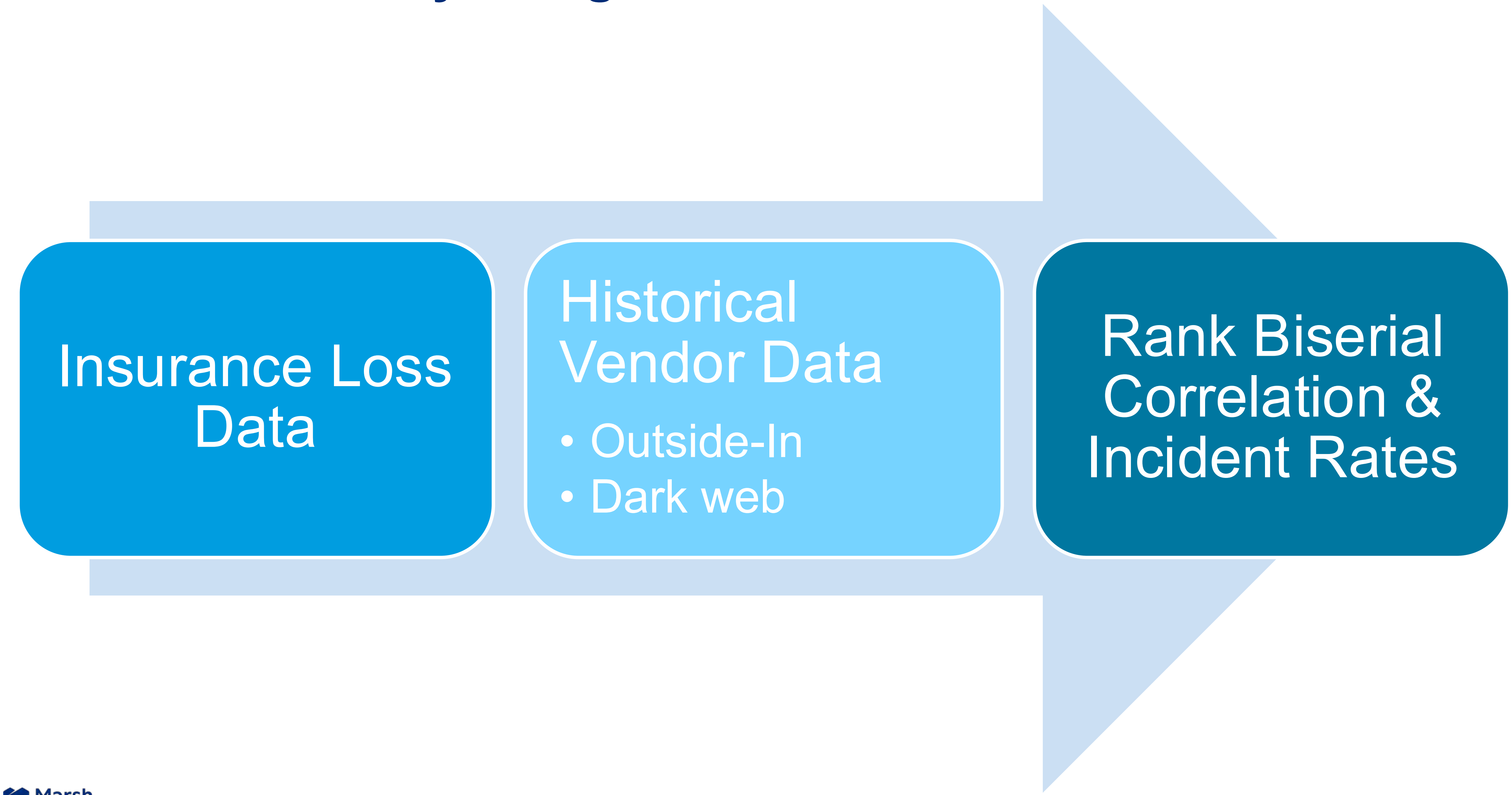
Marsh Key Control	Question	Signal Strength	Implement-ation Rate
Hardening techniques	Our system configuration management tools (such as active directory group policy) enforce and redeploy configuration settings to systems.	5.58	96%
Privileged access management	The organization manages desktop/local administrator privileges via: endpoint privilege management (EPM).	2.92	35%
Endpoint detection and response	The organization operates the following information technology (IT) and information/cybersecurity tools and capabilities: advanced endpoint security.	2.23	82%
Logging and monitoring	The organization operates its own security operations center (SOC) and/or has an outsourced managed security service provider (MSSP) with the following capabilities at a minimum: a) Established incident alert thresholds. b) Security incident and event management (SIEM) monitoring and alerting for unauthorized access connections, devices, and software.	2.19	85%
Patched systems	The organization's target timeframe to patch common vulnerability scoring system (CVSS) v3 high severity 7.0-8.9 vulnerabilities across your enterprise is: Minimum of within 7 calendar days of release.	2.19	24%

Cyber Controls Loss Impact

Increase/decrease in cyber incident frequency for the very best and worst cyber controls for various revenue companies



Vendor Data Study Design



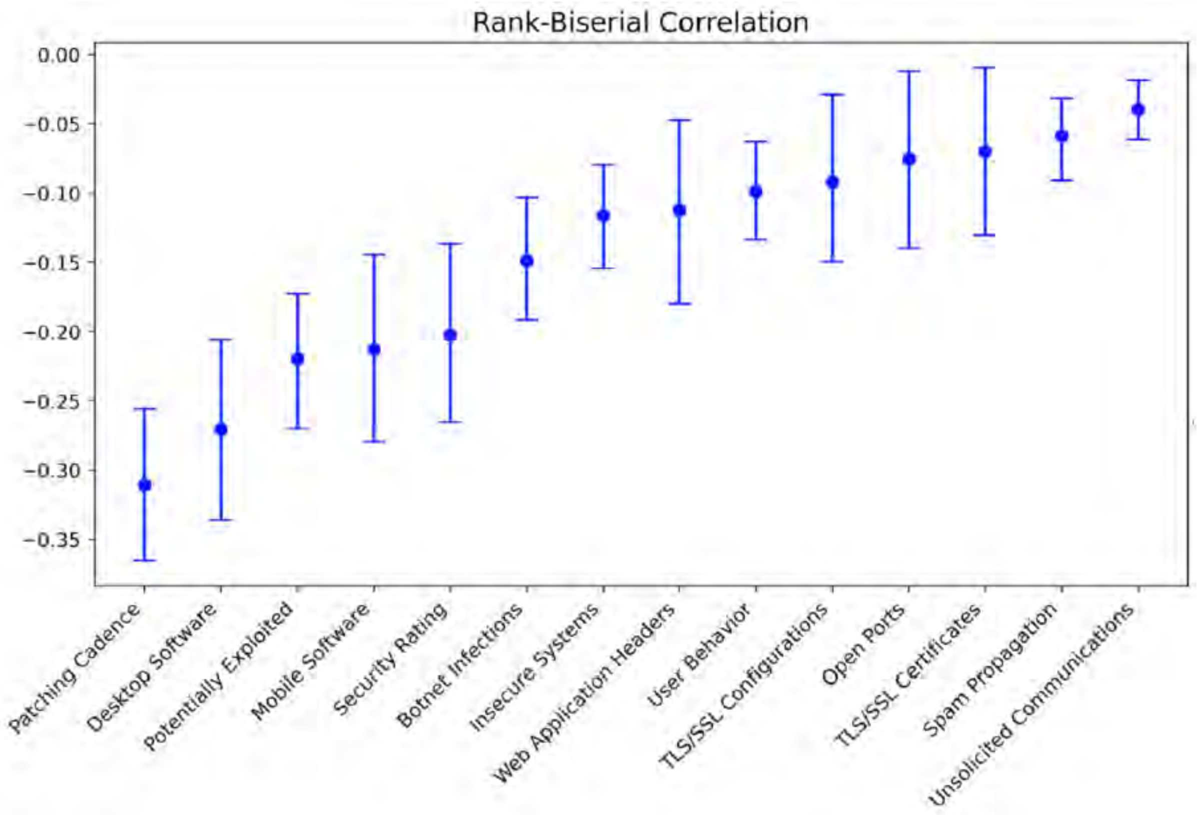
Insurance Loss Data

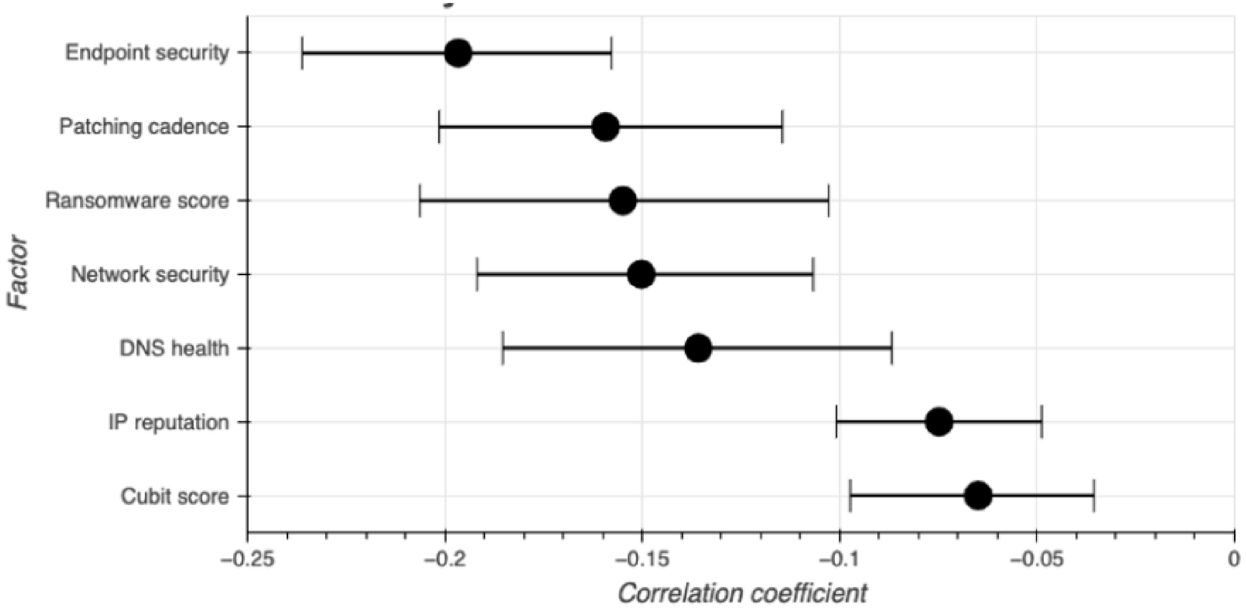
Historical Vendor Data

- Outside-In
- Dark web

Rank Biserial Correlation & Incident Rates

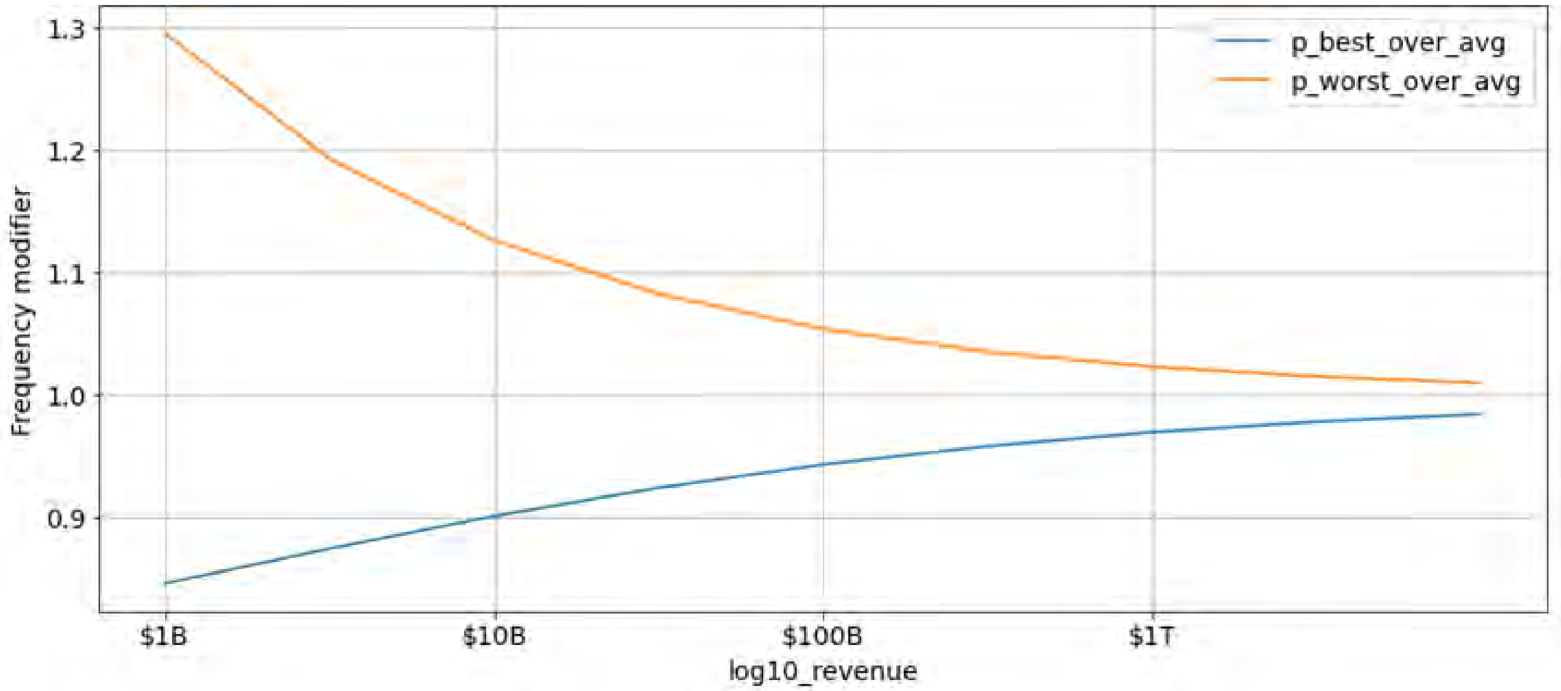
Outside-In Data Efficacy



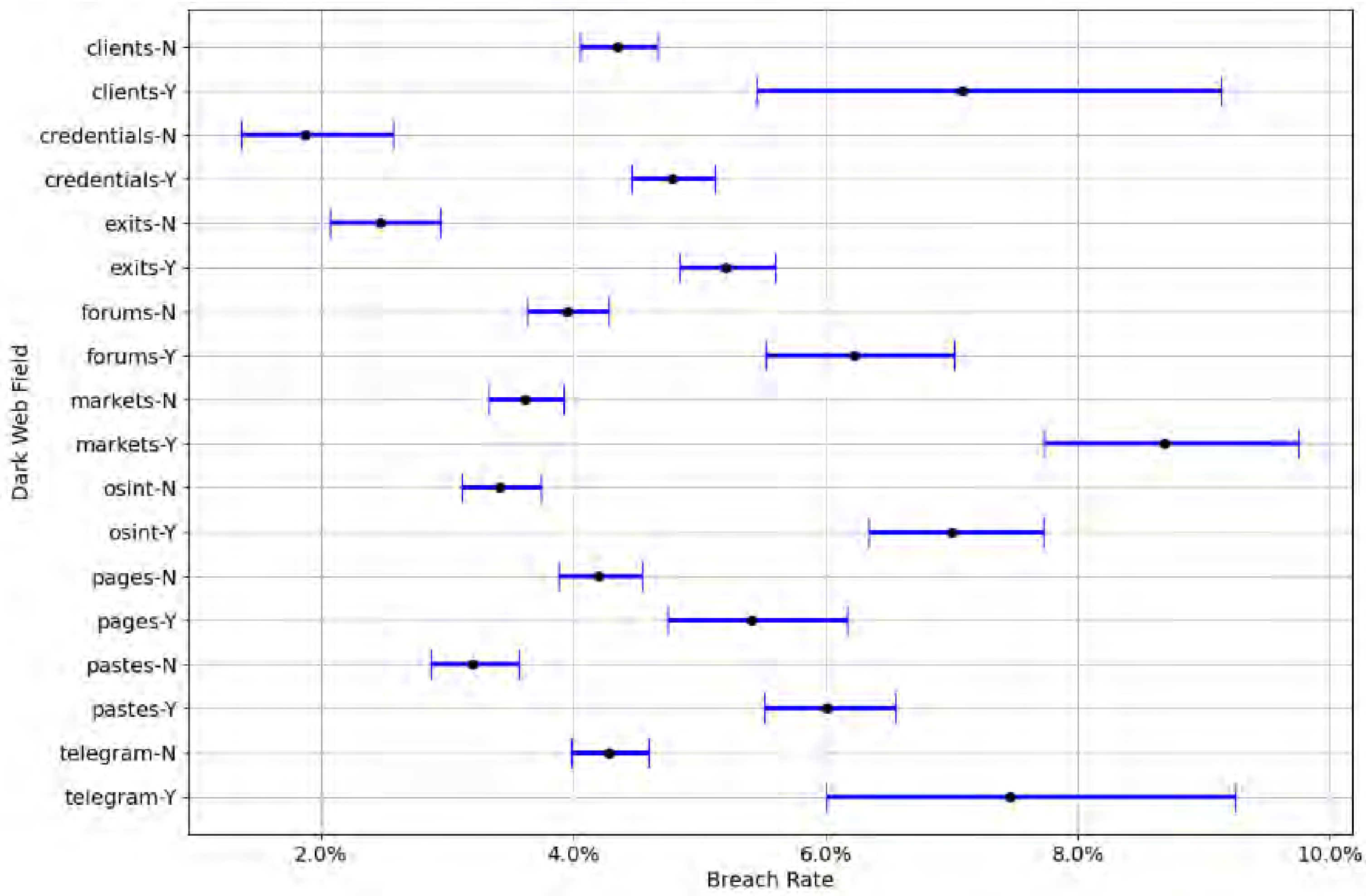


Outside-In Loss Impact

Increase/decrease in cyber incident frequency for the very best and worst scores for one example industry for various revenue companies

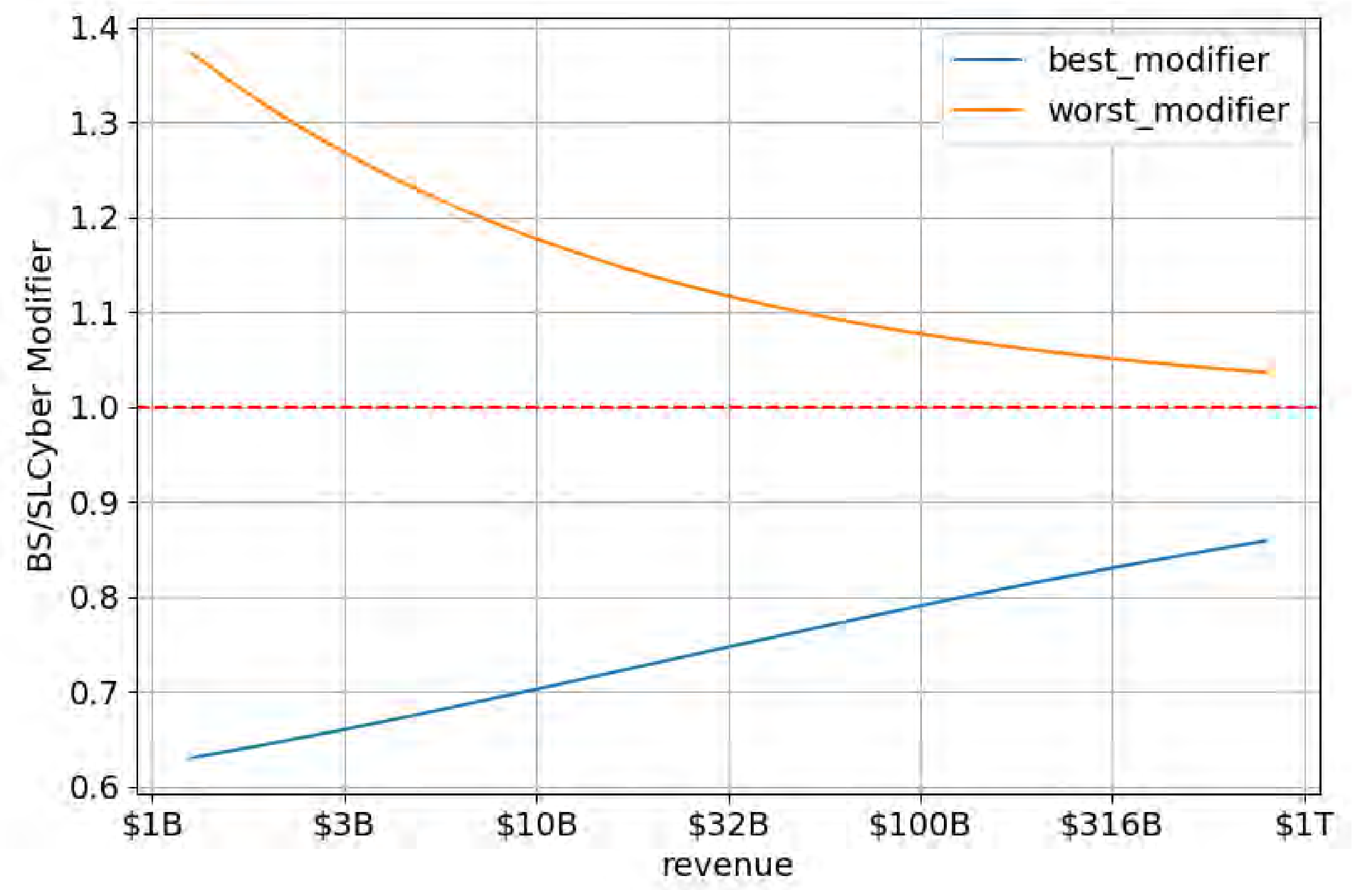


Dark Web Data Efficacy



Field	Has Finding?	Insurance loss rate	Sample Size
clients	Y	7.08%	749
clients	N	4.35%	1,718
credentials	Y	4.78%	15,960
credentials	N	1.87%	1,977
exits	Y	5.21%	13,038
exits	N	2.47%	4,899
forums	Y	6.23%	4,028
forums	N	3.95%	13,909
markets	Y	8.69%	2,992
markets	N	3.61%	14,945
osint	Y	7.00%	5,227
osint	N	3.41%	12,710
pages	Y	5.42%	3,878
pages	N	4.20%	14,059
pastes	Y	6.01%	8,053
pastes	N	3.20%	9,884
telegram	Y	7.47%	1,018
telegram	N	4.28%	16,919

Combined Dark Web & Outside-In Impact



Top Cybersecurity Controls For Insurability

The key to insurability, mitigation, and resilience

Marsh recommendations for the underwriting process:

1. Start early! Evaluate your cybersecurity maturity and be prepared for carrier questions around key categories of interest. Lack of key controls may put availability of coverage at risk.
2. Expect detailed cybersecurity questions from underwriters, including specific to evolving “hot topics” like AI/Copyright, third party aggregation, etc.
3. “Maturity” is dynamic – explain your organization’s risk philosophy, how your controls complement one another to fill in potential gaps, and future enhancements planned or ongoing.

- Multifactor authentication for remote access and admin/privileged controls
- Endpoint Detection and Response (EDR)
- Secured, encrypted, and tested backups
- Privileged Access Management (PAM)
- Email filtering and web security
- Patch management and vulnerability management
- Cyber incident response planning and testing
- Cybersecurity awareness training and phishing testing
- Hardening techniques, including Remote Desktop Protocol (RDP) mitigation
- Logging and monitoring/network protections
- End-of-life systems replaced or protected
- Vendor/digital supply chain risk management

Note: Each insurance carrier has their own specific control requirements that may differ by company revenue size & industry class. For more on the Cyber hygiene see: [Cyber hygiene controls critical as cyber threats intensify (marsh.com)]

Stay in Touch – Want a Copy of our Studies?

Connect to me on LinkedIn, or use this QR code to get a copy of our slides or have us present to your team directly!

Marsh

The information contained in this document is confidential, may be privileged, and is intended for the use of the individual or entity named above. If you are not the addressee, please do not read, copy, forward, use, or store this document or any of the information contained herein.

A business of Marsh McLennan