Virtual Meeting

CASUALTY ACTUARIAL AND STATISTICAL (C) TASK FORCE
Tuesday, May 7, 2024
11:00 a.m. – 12:30 p.m. PT / 12:00 – 1:30 p.m. MT / 1:00 – 2:30 p.m. CT / 2:00 – 3:30 p.m. ET

ROLL CALL

D.J. Bettencourt, Chair	New Hampshire	Anita G. Fox	Michigan
Chlora Lindley-Myers, Vice Chair	Missouri	Grace Arnold	Minnesota
Mark Fowler	Alabama	Eric Dunning	Nebraska
Lori K. Wing-Heier	Alaska	Justin Zimmerman	New Jersey
Barbara D. Richardson	Arizona	Alice Kane	New Mexico
Ricardo Lara	California	Judith L. French	Ohio
Andrew N. Mais	Connecticut	Glen Mulready	Oklahoma
Karima M. Woods	District of Columbia	Andrew R. Stolfi	Oregon
Michael Yaworsky	Florida	Michael Humphreys	Pennsylvania
Gordon I. Ito	Hawaii	Alexander Adams Vega	Puerto Rico
Amy L. Beard	Indiana	Michael Wise	South Carolina
Doug Ommen	Iowa	Cassie Brown	Texas
Vicki Schmidt	Kansas	Kevin Gaffney	Vermont
Timothy J. Temple	Louisiana	Mike Kreidler	Washington
Robert Carey	Maine	Allan L. McVey	West Virginia
Kathleen A. Birrane	Maryland		

NAIC Support Staff: Kris DeFrain, Roberto Perez

AGENDA

1. Consider Adoption of its Working Group Reports:
   A. Actuarial Opinion (C) Working Group—*Miriam Fisk (TX)*
   B. Statistical Data (C) Working Group—*Sandra Darby (ME)*

2. Hear a Presentation about Reserving Analytics for Regulators—*Charlie Stone and Cat Drummond (InsurSight)*

3. Present the American Academy of Actuaries' Cyber Risk Toolkit—*Christian Citarella (NH), Julie Lederer (MO), Sandra Darby (ME), Kris DeFrain (NAIC), Travis Grassel (IA), Arthur Schwartz (LA)*

4. Discuss Any Other Matters Brought Before the Task Force—*Christian Citarella (NH)*
   - Regulator-to-Regulator, May 21, 1pm Central: Discuss Rate Filing Issues. Submit agenda items to Kris DeFrain (NAIC).
   - Book Club, May 28, 1pm Central

5. Adjournment

Supporting effective regulatory oversight

Extracting maximum insight from insurers' reporting

MAY 2024

Introductions

Cat Drummond, FIA
Partner and Appointed Actuary
+44 (0)20 7432 0637
cat.drummond@lcp.uk.com

Charlie Stone, FIA
Partner and Head of Insurance Analytics
+44 (0)20 3922 1315
charlie.stone@lcp.uk.com

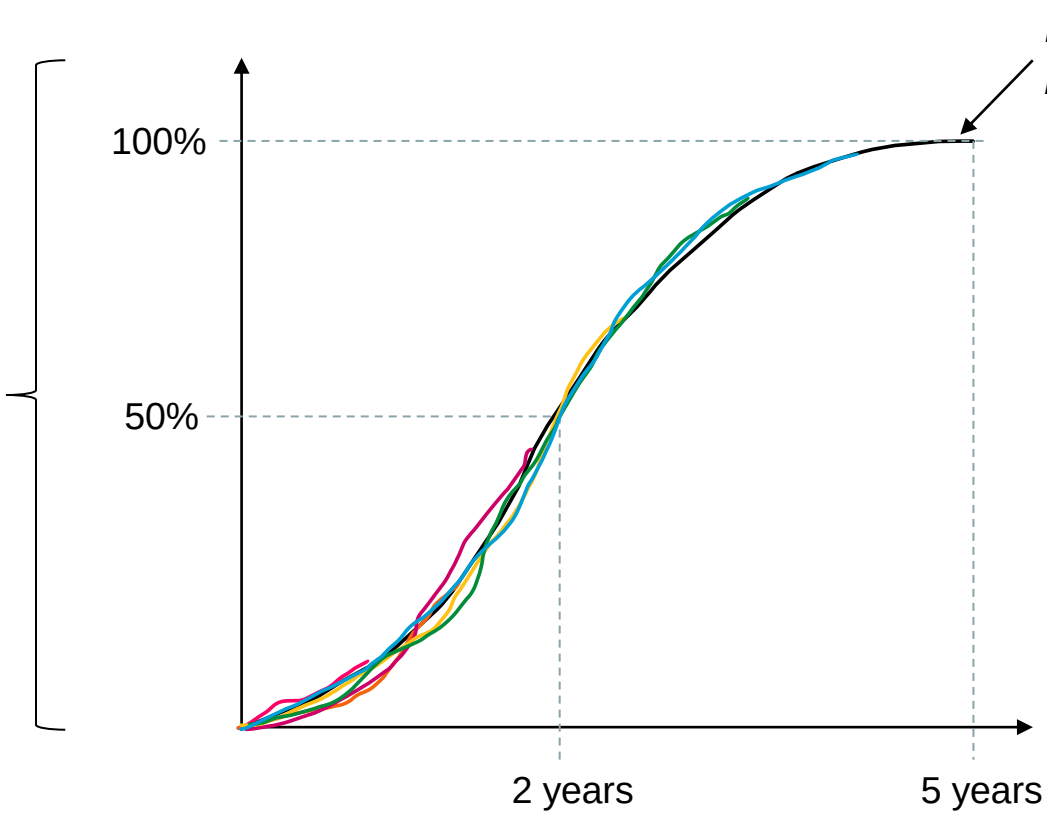
Some scene setting…

- Insurers around the world submit a lot of regulatory data each year
- Some of this is publicly available
- Analyse data ➔ unlock more insights
- Useful for regulators, insurers and actuaries, but:
  - How can we spot trends?
  - How useful are they?
  - How can we automate this?

Spotting trends

Claims (now) as a % of total ultimate claims (how quickly are claims emerging?)

$$\frac{\textit{Reported (or paid) claims}}{\textit{Total ultimate claims}}$$



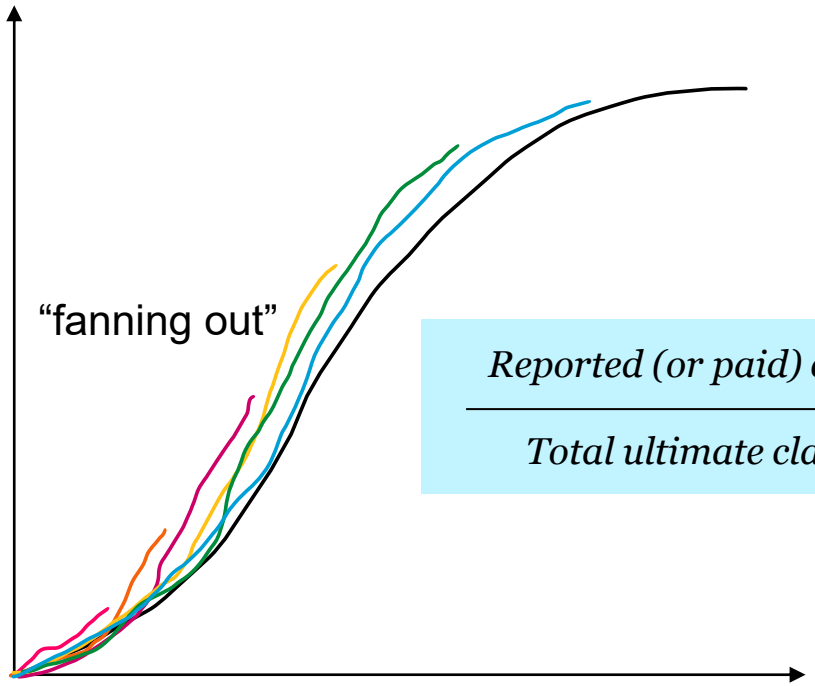
Black line = expected development, based on past experience

Conclusion

➔ Consistent claims development (each cohort follows similar pattern, aligned with past experience)

Spotting trends (2)

BUT, what if development is not consistent?



$$\frac{\textit{Reported (or paid) claims}}{\textit{Total ultimate claims}}$$

➔ Each cohort appears to be following different pattern, with younger cohorts (ie shorter lines) being higher than older cohorts (longer lines))

Could be indicating:

1. Claims are genuinely coming in (or being paid) more quickly than in the past (and therefore will be fully settled more quickly), **OR**
2. Ultimate claims are too low (under-reserved)
   ➔ future reserve deteriorations

Some follow-on questions

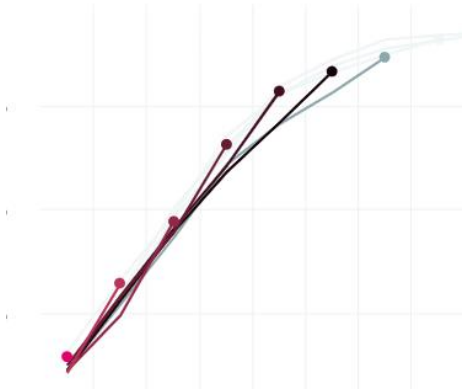
- Are there other metrics that are useful to help us spot trends and/or understand if reserves are too low?
- Can we back-test this on historical data to check our theory?
- Can we use machine learning to help us spot these trends quickly across large datasets?
- Can we automate reporting to help regulators see quickly where to focus efforts?

Answer: YES! Let's see how…

Other useful metrics to spot under-reserving

Development triangle based diagnostics

Incurred / ultimate	Paid / ultimate
Incurred % / yr 1 incurred %	Paid % / yr 1 paid %
Incurred loss ratio	Paid / incurred



Trend identification converts each diagnostic into:

- Trend confidence (0% - 100%).
- Direction (+ve increasing or –ve decreasing).

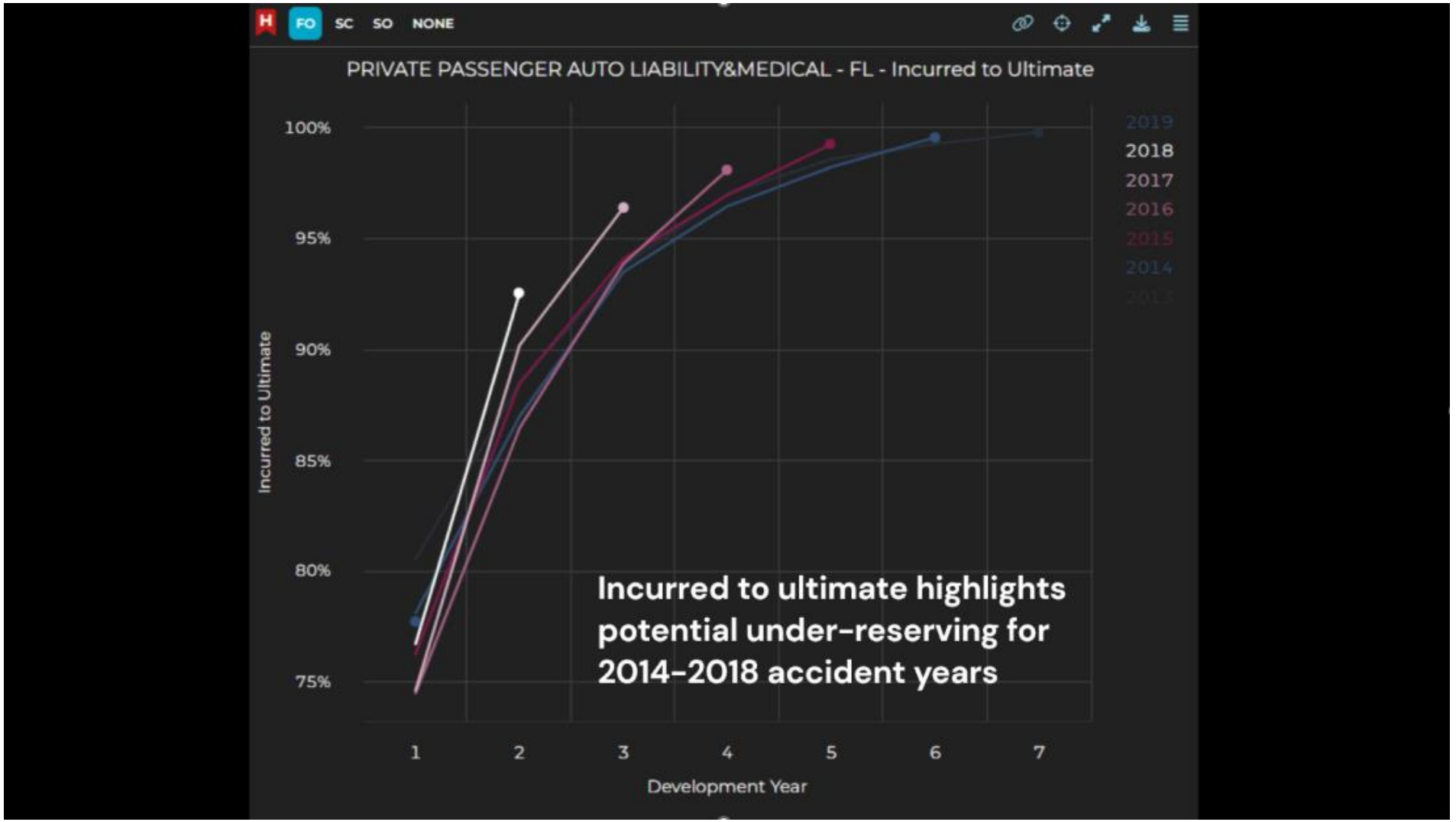
Across three trends (fanning out, step change, sticking out)

Other metrics

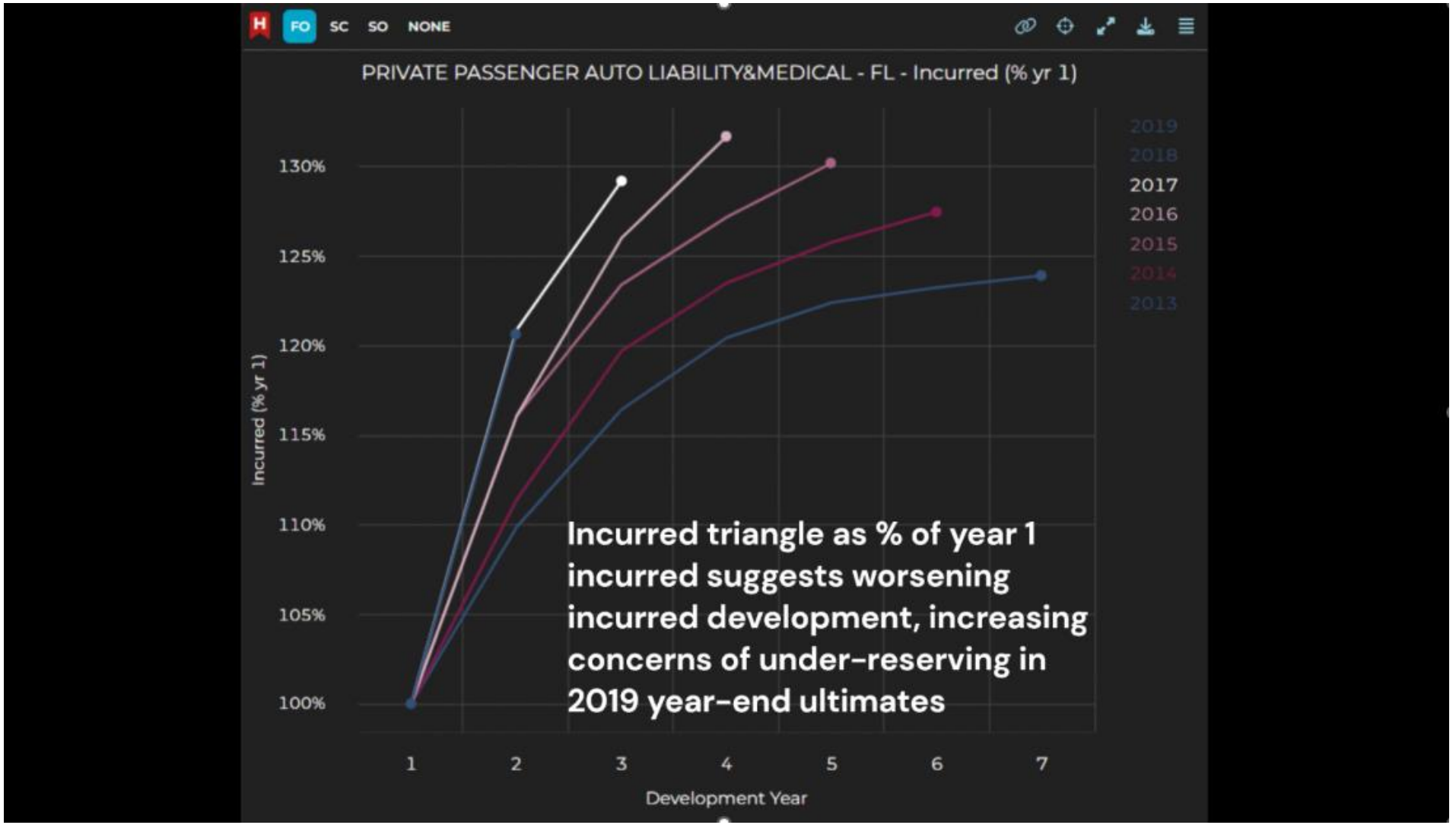
- Avg past deterioration
- Premium growth
- CoB reserves / total company reserves

Using simple diagnostics to spot issues

Using simple diagnostics to spot issues

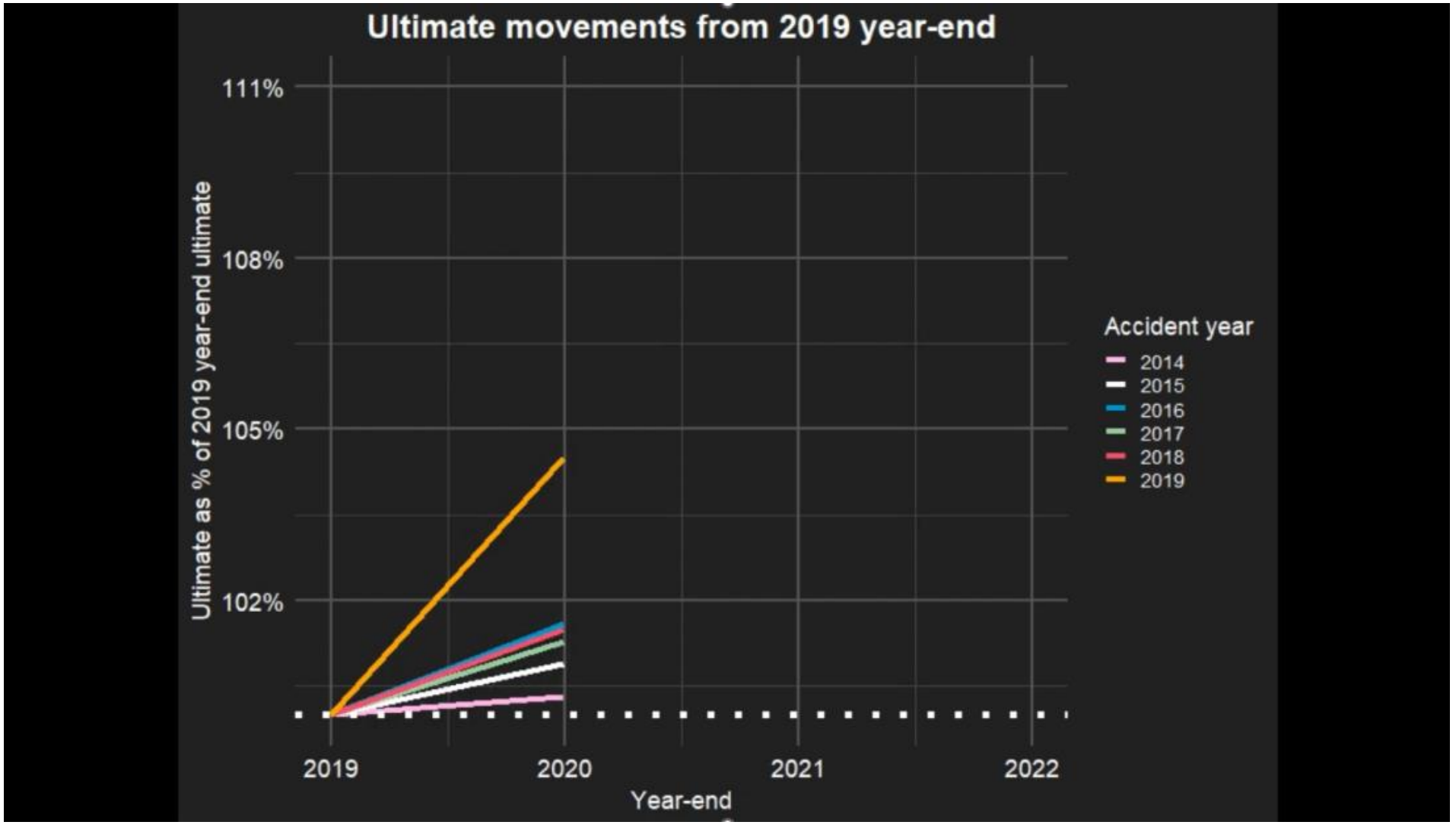


Using simple diagnostics to spot issues

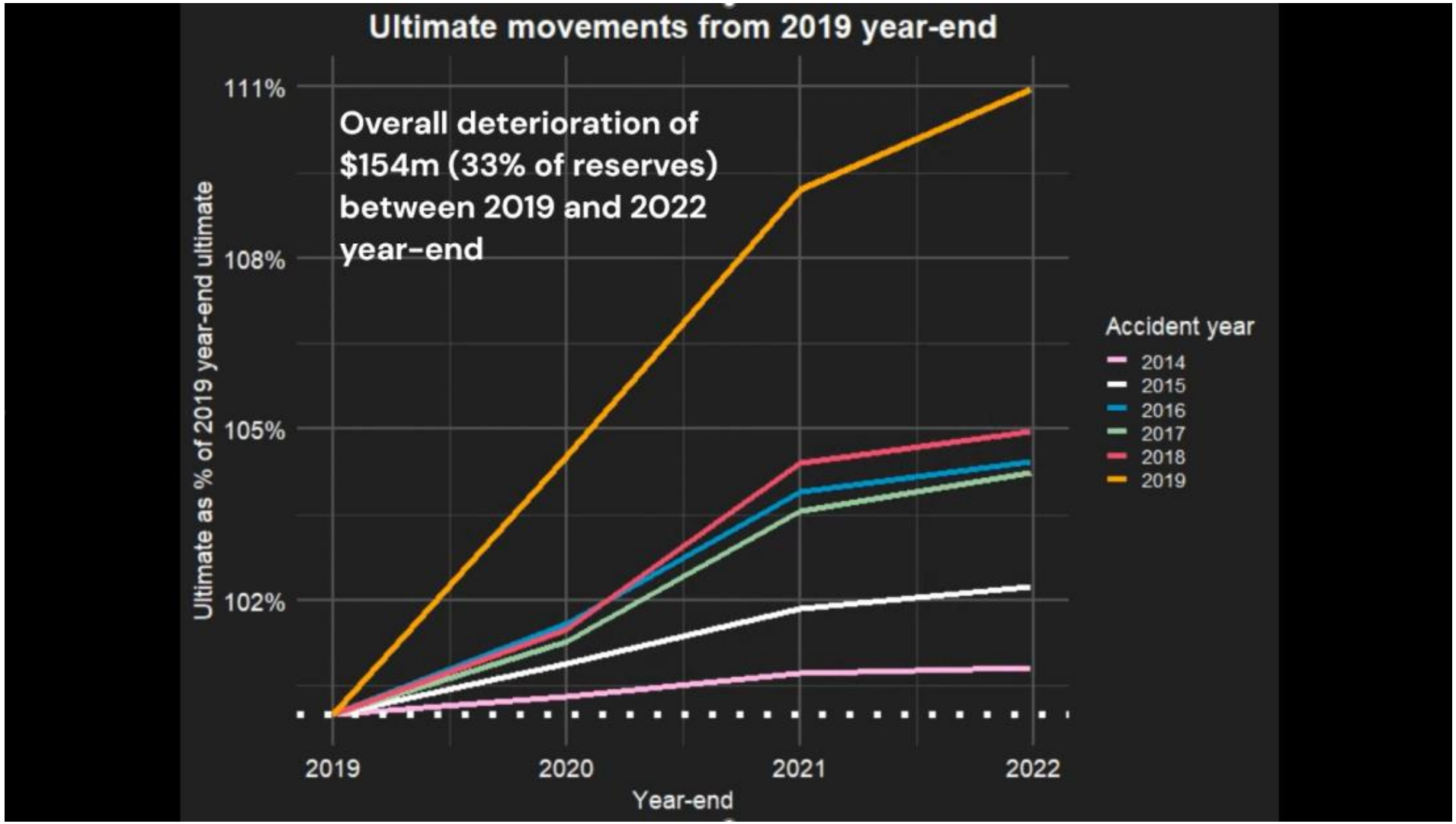


Using simple diagnostics to spot issues

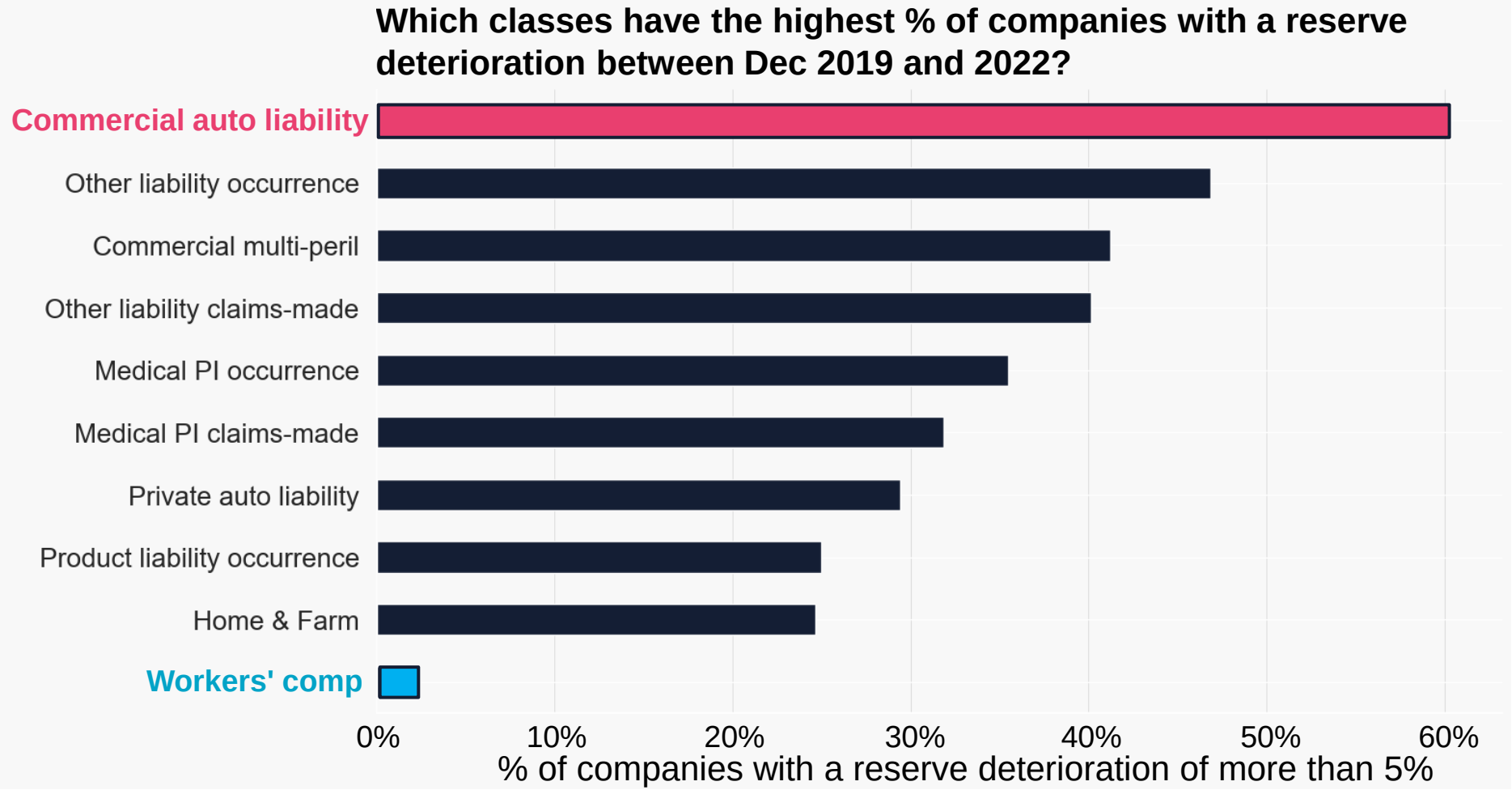
Using simple diagnostics to spot issues



Using simple diagnostics to spot issues



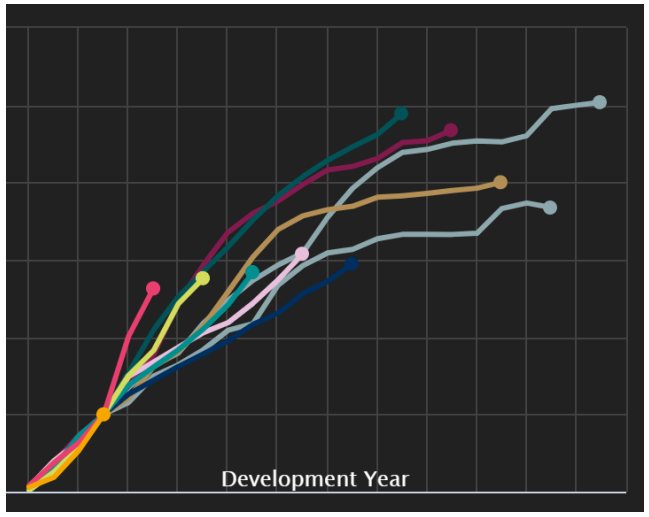
Deteriorations in the US market: 2019 to 2022

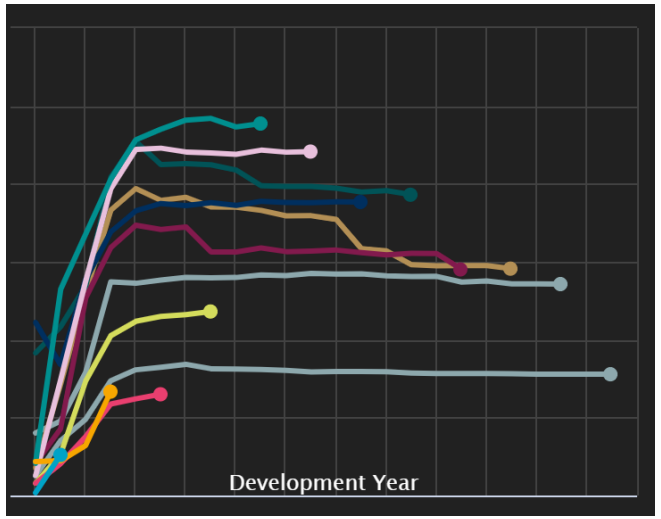


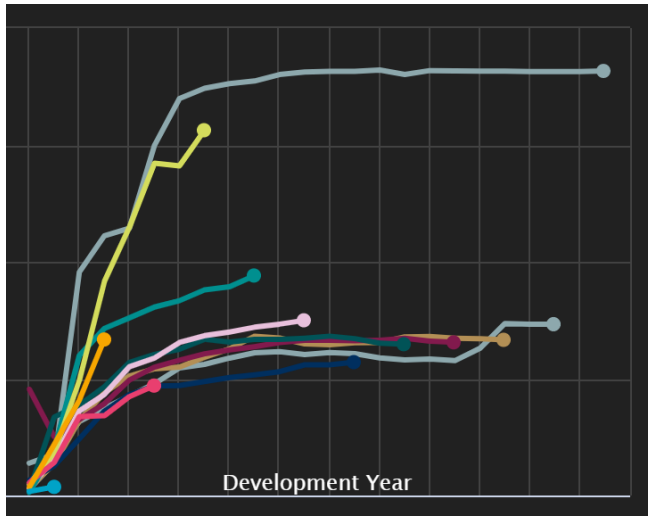
Scale
1,829 company and class of business segments with reserves above $10m.

Materiality
Total reserve deterioration of $28.6bn on those segments with a deterioration of more than 5%.

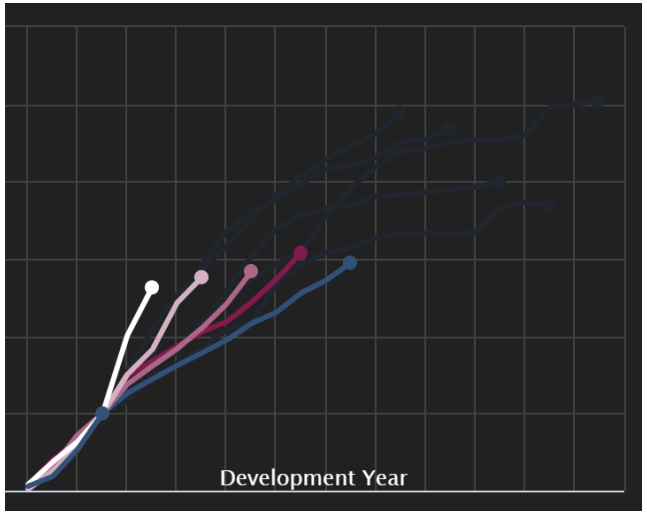
How do we quickly pick out these trends?

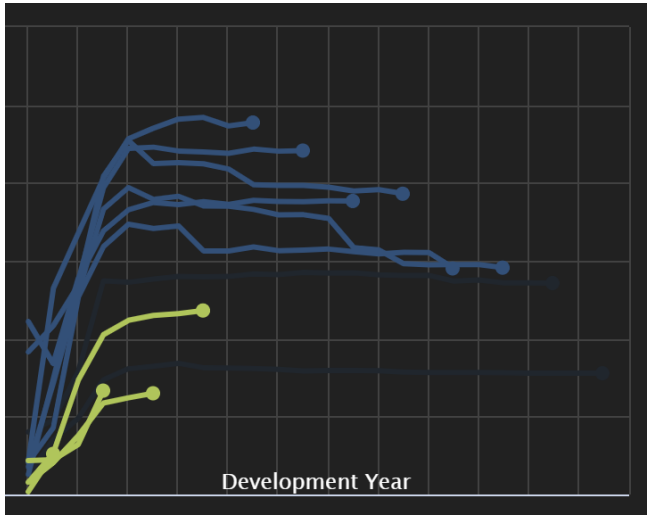


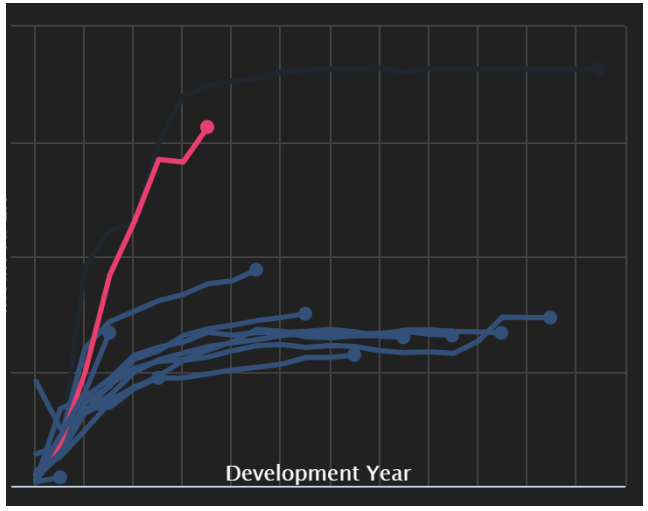




Automated trend identification







How well can we predict deteriorations?

Pretty well! More detail below.

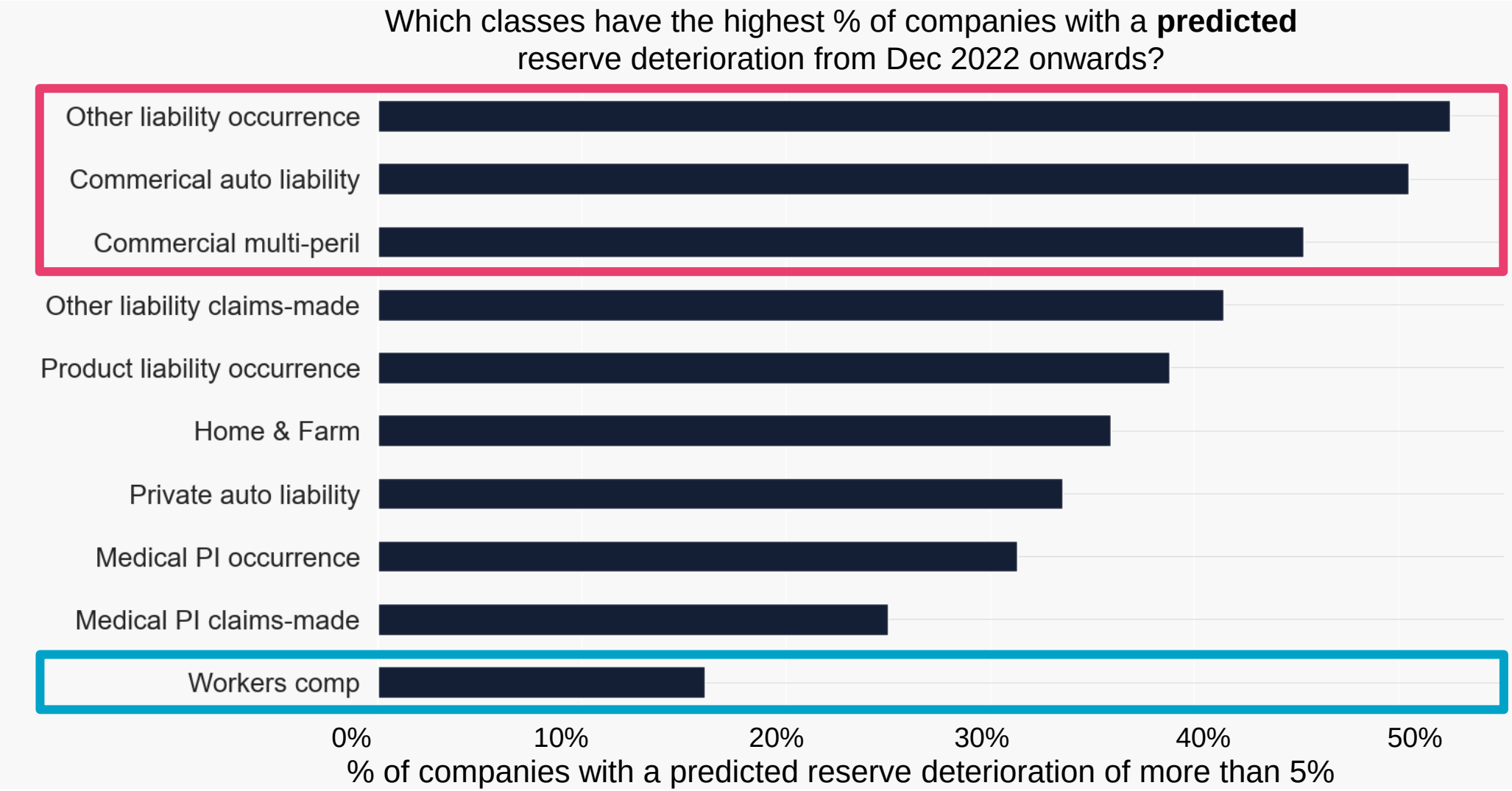
71% of deteriorations correctly predicted

78% of non-deteriorations correctly predicted

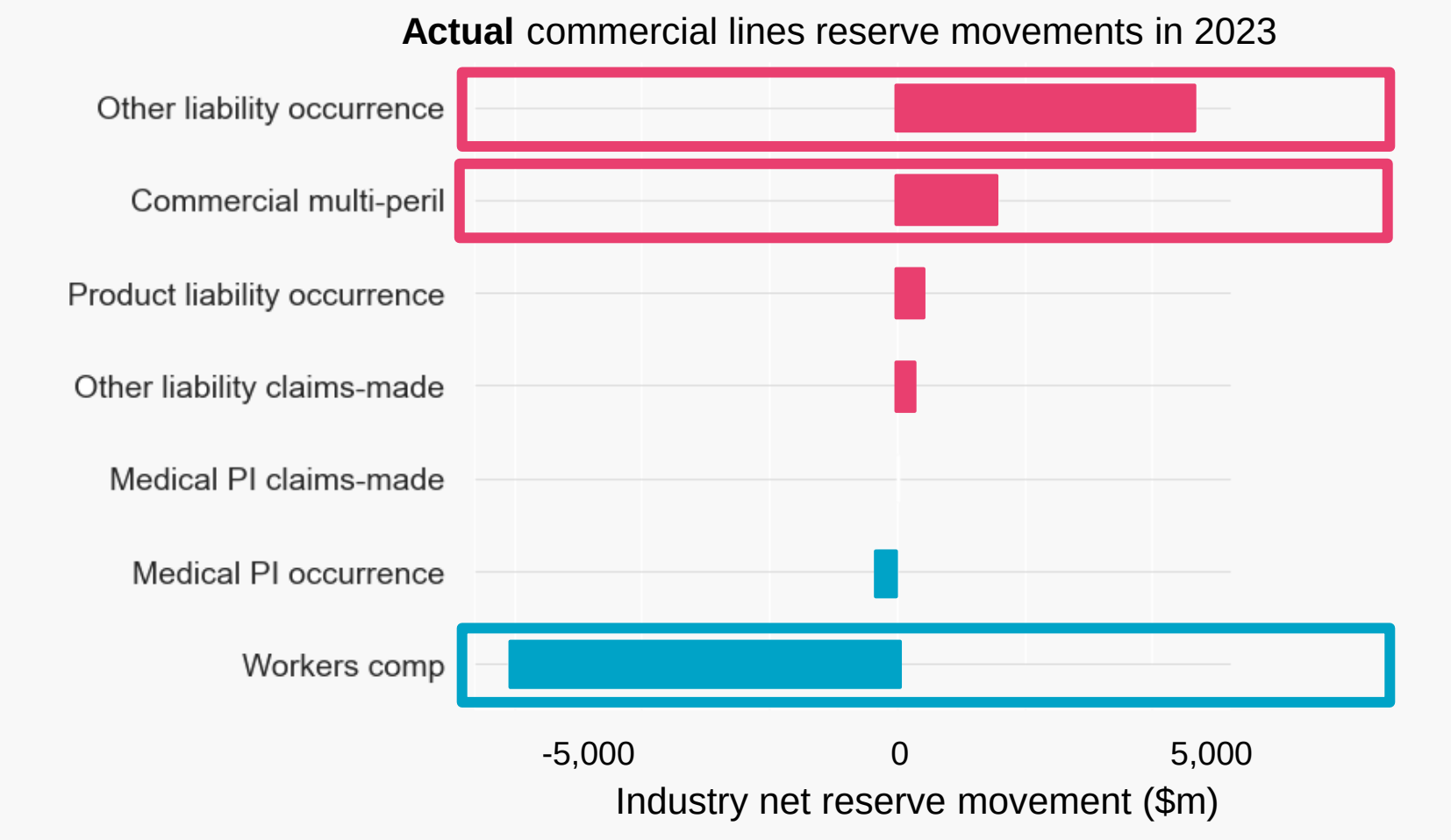
AUC of 82% (averaged over 5-fold cross validation)

What's next?

Predicted deteriorations in the US market from Dec 2022 onwards



Back to the future!



Source: S&P Capital IQ, Insurance Insider US - LinkedIn

Identifying firms for regulatory focus

Company	Class of business	Reserves	Deterioration risk score
A	Other liability occurrence	$134m	92%
A	Commercial multi-peril	$354m	65%
B	Other liability claims-made	$45m	75%
B	Medical PI Occurrence	$123m	32%
C	Commercial auto liability	$843m	84%
C	Workers' comp	$231m	13%
C	Medical PI claims-made	$32m	22%

- Assess entire market efficiently.
- Use diagnostics like incurred to ultimate and overall deterioration risk score to pin-point firms and classes of business for regulatory focus.

Live demo of theory working in practice…

Key takeaways

- Simple diagnostics can (and did) spot issues resulting in recent reserve deteriorations
- Machine learning can pick out trends in multiple triangle diagnostics and combine these into an overall deterioration risk score
- This overall deterioration risk score can be used to understand those companies with the highest risk of reserve deterioration for further review

Cat Drummond, FIA
Partner and Appointed Actuary
+44 (0)20 7432 0637
cat.drummond@lcp.uk.com

Charlie Stone, FIA
Partner and Head of Insurance Analytics
+44 (0)20 3922 1315
charlie.stone@lcp.uk.com

Cyber Risk Toolkit

Casualty Actuarial and Statistical (C) Task Force

May 7, 2024

NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

“An Introduction to Cyber”

The cyber market is relatively new, immature, and growing.

- Per a 2021 study, only 47% of all U.S. companies purchase coverage, either stand-alone or packaged policies.
- Some of the policy coverages, exclusions, conditions, and terminology are not as uniform as they are for other mature and developed lines of business.
- The cyber insurance market is still relatively young, and its true claim cost is still uncertain since we have yet to observe a global market-wide catastrophic insurance loss.
- Cyber premiums more than doubled between 2019 and 2021.
  - Excluding surplus lines cybersecurity policies, both the stand-alone and packaged policies combined to a $4.6 billion U.S. market in 2021. Cyber made up 0.6% of the total direct premiums written in the U.S. P&C market.
- Loss ratio performance has been favorable compared to the overall P&C market, but the recent increase in cyberattacks and ransomware demands has increased the loss ratio. The growth in the Internet of Things and the expansion of virtual work/educational environments could put further pressure on the loss ratio.
- Commercial insurance across all lines had an average rate increase of 6% overall during the first quarter of 2022, but cyber insurance rates increased 19.75% on average.
  - Cyber insurers are increasing prices and reducing coverage by increasing retentions, reducing overall policy limits, incorporating new coinsurance provisions and introducing other exclusions.
    - For each cyber insurance policy, there is generally a maximum policy aggregate that caps all insurance loss payouts, in addition to each coverage's limits.
  - Cyber insurers are also requiring greater cyber security from their policyholders and are providing pre-breach services to aid insureds to identify, mitigate, and reduce cyber losses.

Affirmative^ cyber coverage typically offers first- and third-party coverage.

First party coverages:

- Business interruption*
- Property damage*
- Privacy breach response services
- Computer attack and cyber extortion
- Computer and funds transfer fraud
- Identity recovery

** Often include a time retention whereby actual coverage will trigger after the designated period has elapsed (like a deductible, but stated in terms of hours instead of dollars)*

Third party coverages:

- Electronic media liability
- Regulatory defense and penalties
- Payment card industry fines and penalties
- Information security and privacy liability
- Network security liability

^ Non-affirmative coverage, more commonly known as “silent cyber,” is triggered when cyber perils are not explicitly included or excluded in the policy wording. Silent cyber can cause insurers to pay losses from cyberattacks on policies that were not intended to offer cyber coverage. Insurers are dealing with silent cyber by explicitly including or excluding coverage for some aspects of cyber-related losses.

Cyber insurance premiums are typically rated based on traditional actuarial ratemaking using schedule rating modifications.

- A simplified example of a rating plan: Premiums = Base Rate x Increased Limits Factors x Deductible Factor x Cyber-specific Rating Factors x Schedule Modifications
- The most common exposure base for cyber insurance policies is revenue, but insurers are considering other exposure bases that might be a better measure of an insured's risk level, like number of connected devices, number of records, IT spend, or number of employees. Some carriers account for these elements instead in schedule rating.
- Other characteristics commonly used in schedule rating:
  - Loss history
  - Type and nature of sensitive information
  - Dependency on network
  - Merger-acquisition activity
  - Age of company
  - Financial condition
  - Data encryption and security patch processes
  - Privacy and security control procedures, including awareness training
  - Business continuity and disaster recovery plan
  - Use of third-party vendor management
- Common variable in cyber coverage: Hazard group that differentiates the riskiness of industries. Businesses that store and utilize numerous PII or sensitive information such as the healthcare and professional services industry will be classified as higher risk hazard groups over others.

Cyber Threat Landscape

Due to heavy reliance on computer systems, businesses are susceptible to significant risks when those systems are unavailable or corrupted:

- Business Interruption
- Competition
- Liability
- Direct Loss

Cyber Threat Landscape

Threat Vectors:

- Phishing
- Software Vulnerability
  - Misconfiguration or bugs
  - Lack of regular patches or system updates
  - Inside Jobs
- Simple/Weak Passwords
  - Brute force programs can solve short and simple passwords
  - Credential stuffing

“Silent Cyber”

Silent cyber can trigger unexpected payouts.

- Silent cyber coverage: coverage for cyber risk that the insurer did not consider and/or did not price
  - Most typical under traditional insurance policies (general liability, property, etc.) but can also occur in policies that provide affirmative coverage of cyber perils
- Drivers of silent cyber:
  - The wording of policy terms has not evolved as rapidly as technology; ambiguous language may make cyber coverage available under policies that were not originally designed for this exposure.
    - Ambiguous language is typically viewed in favor of the insured. The insured may expect that cyber coverage exists in traditional lines policies that do not explicitly include or exclude cyber risks.
  - Cyberattacks are rapidly evolving beyond what was anticipated when the insurance policy forms were written.
  - If a policy does not have named perils coverage, there is a potential for coverage for anything that is not explicitly excluded.
  - Businesses, infrastructure systems, cars, and homes have increased their dependence on technology, so silent cyber is becoming prevalent in virtually every type of insurance coverage.

Insurers face challenges when trying to manage silent cyber.

Ways to manage silent cyber exposure:

- Explicitly exclude cyber risk from standard policies.
- Grant affirmative cyber coverage for an additional premium via a standalone cyber policy or endorsement; implement sublimits on cyber exposure.
- Try to quantify silent cyber exposure by determining the range of potential exposures from a cyber event and overlaying these exposures with the existing portfolio.

Challenges in managing cyber exposure:

- Rapid expansion and evolution of cyber risk makes it hard to predict what future claims may look like and to keep cyber models up to date.
- Data needed for cyber risk assessment (e.g., an insured's supply chain dependencies and cybersecurity protocols) may not be collected in traditional P&C exposure datasets.
- Historical data is limited and therefore not sufficient for pricing.
- Losses that were cyber-related may not have been coded as such, so there's no reliable database of silent cyber events.
- It's not clear how the legal system will treat non-affirmative policy wordings.

CYBER DATA

Cyber Risk Toolkit

ACTUARY.ORG

CYBER DATA - AVAILABILITY

- Limited data
- Exposure is evolving
- Not all events are insured
- Growing amounts of data due to digitization which helps
- Historical events do not always predict future ones
- Knowledge of the common software makes threats change
- New laws surrounding cyber security and data privacy

CYBER DATA - CHALLENGES

- New market so insurers hesitant to underwrite risk they do not understand
- Coverage structured with narrow terms and conditions
- Similar evolution as with other lines as time goes on insurers broaden coverage
- Concern over organizations understanding of cyber insurance coverage leading to lack up take in coverage and data
- Lack of data leads to supplementing with third party data
- Historical claim data not keeping up with evolving nature of cyber polices

CYBER DATA

- Enhanced Data Collection
  - Third Party vendors
- Which Data Elements Should be collected and why
  - Inconsistent data collection results in issues while evaluating risk
  - Ways to over come challenges
    - Expand sources and collection of data
    - Receive input from a variety of subject matter experts
    - Obtain and understanding of the industry and its exposure to risk
    - Leverage third-party cyber vendors information
  - Technology firms

CYBER RISK ACCUMULATION

Cyber Risk Toolkit

ACTUARY.ORG

CYBER RISK ACCUMULATION

- Accumulation risk in insurance, also known as aggregation risk, refers to the likelihood of a greater than-anticipated accumulation of claim costs due to multiple exposures being tied to the same event or a related event.
  - Example: Web services disruption that spreads to multiple businesses
- Modeling can be difficult as it's challenging to identify all the dependencies of the risks
  - Reliance on Cyber Experts
- Although, Statistical data can be derived from past cyber incidents the ever-changing environment new threats develop
  - Example: Significant increase in working from home during pandemic

CYBER RISK ACCUMULATION-MODELING

- Deterministic
  - Simple approach using market share. If 20% of market than similar exposure to cyber threats.
  - Alternatively gather data on technology providers so exposure can be linked to aggregation points. More accurate but more effort
- Probabilistic
  - Losses are modeled using distributions.
  - Need to be continually reviewed for changes in cyber environment

CYBER RISK ACCUMULATION

- Emerging issues
  - Various models to help manage cyber accumulation
  - Gap in understanding of motivations for attacks
  - Technological vulnerability alone not an adequate predictor of cyber risk
  - Manmade risk, Cyber events much less random than they seem
- Vendor Models
  - Traditional catastrophe insurance modelers expanding into cyber risk
  - Newer Cyber risk Service providers moving into insurance

Cyber Risk and Reinsurance

Because of uncertainty in the Cyber Risk primary market a larger portion of the risk is reinsured relative to more traditional lines of business.

- 40% of cyber coverage premium is ceded
- 10-15% for Property and Liability LOBs

Underwriting remains a challenge

- Chicken and egg problem
- Risk aggregation and Silent Cyber
- TRIA does provide a backstop

Cyber Risk and Reinsurance

Alternative Risk Transfer

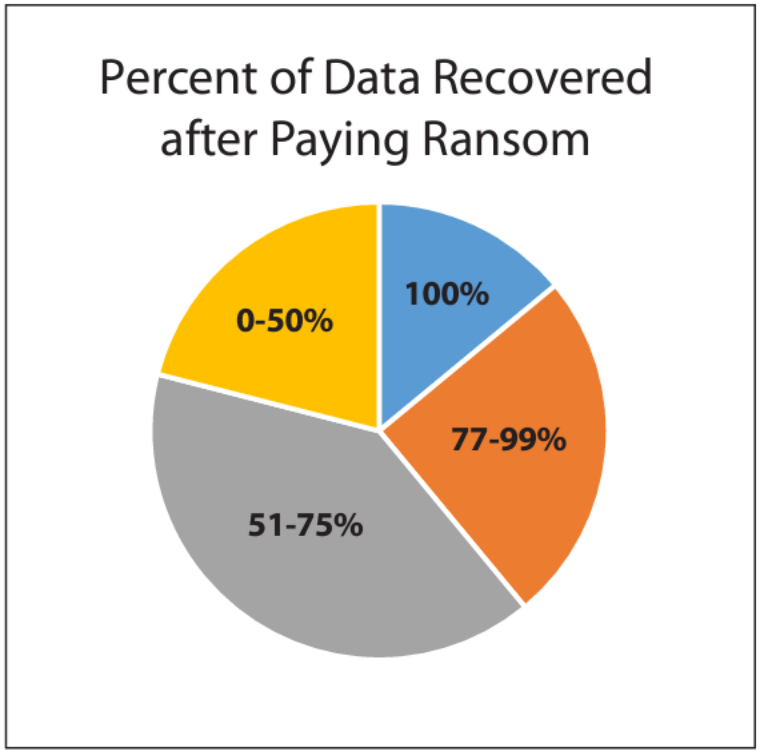
- Insurance Linked Securities might be a possibility because they are looking to expand beyond natural catastrophe risks but lack of quality loss models in cyber is a deterrent.
- Cat-Bond Structure
- Contingency Capital
- Loss Warranty Arrangements

Ransomware

https://www.actuary.org/sites/default/files/2023-02/7Ransomware.pdf

- Data loss, operational shutdown, hardware inoperable
- Double: release of data
- Triple: threaten customers

Choice: pay the ransom or invest the cost and time in repairing the infected system.



"Organizations are Better Prepared to Fight Ransomware but Gaps Remain", Tech Republic, April 12, 2022.

NAIC Casualty Actuarial & Statistical Task Force (CASTF) Meeting Tuesday May 7, 2024 Cyber Risk Tool Kit Presentation

War, Cyberterrorism, and Cyber Insurance

American Academy of Actuaries February 2022 Publication

IOWA Department of Insurance and Financial Services

Cyber insurance coverage continues to evolve and grow in application

Increasing concern among policyholders whether policies will cover them when cyber incidents impacting them are tied to cyber and technology disruptions stemming from attacks that may be supported by nation-states and state-backed military units.

Gray areas exist due to:

- No existence of publicly known denial of a cyber incident corresponding to the War Exclusion under a cyber insurance policy.
- Attribution (who was behind the attack) may take time to identify as well as difficult to achieve and prove.

IOWA™ | Department of Insurance and Financial Services

Within Cyber Insurance Policies are War Exclusions with Cyberterrorism Endorsements

Most, if not all, cyber insurance policies include an explicit exclusion to losses arising out of or attributable to war and military actions.

War Exclusion (AIG & AXIS combo): Insurer not liable for losses from war, invasion, hostilities/warlike operations/military action – declared or not, strike, lock-out, riot, civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against any of these events.

Cyberterrorism as defined by AIG: Premeditated use of disruptive activities against any computer system or network by an individual or group of individuals, or the explicit threat by an individual or group of individuals to use such activities, with the intention to harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

Endorsements to the War Exclusion and Defining Cyberterrorism

1. The definition of the War Exclusion is amended such that it does not apply to acts of Cyberterrorism.
2. The coverage sections are amended such that acts of Cyberterrorism are included within the coverage.
3. The term Cyberterrorism is defined accordingly.

Ambiguity may still exist and may create uncertainty for policy issuers, policyholders, and regulators. Attorneys will likely continue to be heavily involved! Other insurance professionals, such as actuaries, will have credible and valuable input as well as this coverage continues to evolve from larger data sets.

Actuarial Responsibilities

1. Gain familiarity with coverage clauses and endorsements to understand what they say may or may not be covered.
2. Understand that the impact of potential systemic, war-related, and military-related cyber incidents will influence both the pricing and reserving of losses falling under cyber policies.
3. Realize that unique events that cross the line from cyberterrorism to acts of war and invoke exclusions under the policy will likely be litigated in court (similar to 9/11 and COVID-19 claims/events).
4. Uncertainty around payouts from litigated coverage cases will add complexity to the overall reserving process.
5. Greater clarity will come with time - awareness of nuances and uncertainties is very important until that time comes.

Autonomous Vehicles and Cyber Risk

Three key cyber risks:

- Stealing a car
- Car is driven to commit crimes
- Data in the car is stolen: personal data or data on trips

Digital Assets and their Current Roles within Cybercrime

https://www.actuary.org/sites/default/files/2023-07/DigitalAssetCYBER.pdf

- Cryptocurrency
- Drop in $ in 2022 from

  1) decrease in willingness to pay
  2) not finding the criminals' changed addresses
  3) insurance companies incentivize insureds to strengthen controls and backup measures
  4) increase in sanctions from governmental entities

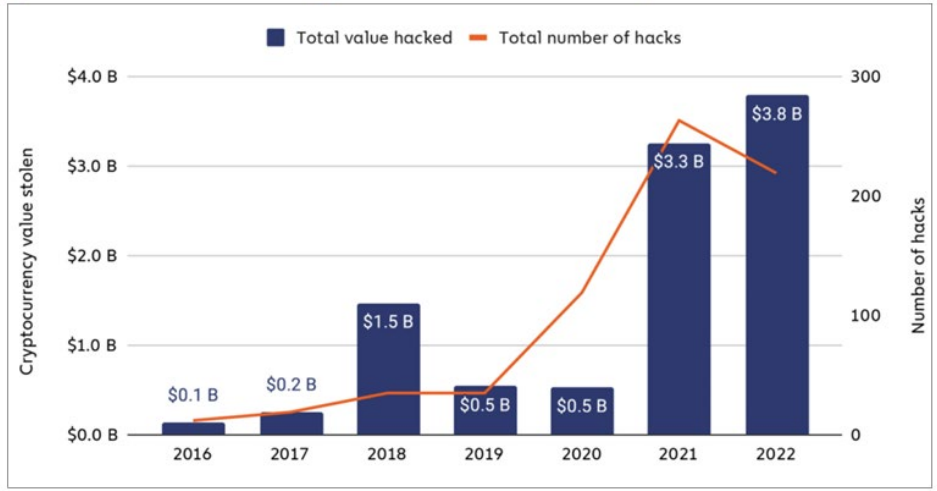
- Direct theft of digital asset from exchanges and DeFi platforms.

Table 2. Share of Companies That Paid a Ransom[4]

Year	Paid Ransom	Did Not Pay
2019	76%	24%
2020	70%	30%
2021	50%	50%
2022	41%	59%

Coveware

Chart 4. Total Value Stolen in Crypto Hacks and Number of Hacks, 2016–2022[12]



Chainalysis

Protect yourself from Personal Cyber Attacks

- Create strong passwords and change them often
- Two factor authentication means that a password PLUS access to a phone is required to access a website
- Copy important documents and photos to an external drive, and update that weekly
- If sending money, send a small amount first, then check if received by a phone call
- Add a Cyber endorsement to a home insurance policy