Cyber Risk Underwriting Thematic Review Results

December 2022

SOUTH AFRICAN RESERVE BANK
Prudential Authority

Content

1. Background
2. Outcomes
- General
- Affirmative Cyber
- Not writing cyber
- Prudential Supervision
3. Conclusions

1. Background

Background

- Growing digitisation, connections, big data, cyber threats
- Cyber insurance potentially significant - attracted supervisory attention of regulators
- Result - Cyber Risk Underwriting Thematic Review
- Relevant emerging risk, warrants further investigation:
  - IAIS 2019 Supervisory Stocktake and IAIS 2020-2024 Strategic Plan
  - PA flavour of the year “Impact of new technologies on financial institutions”
  - Cyber risk underwriting is central to industry discussions

Scope

- Includes insurers that underwrite affirmative cyber risk
- Includes exposures to non-affirmative cyber
- Excludes operational cyber risk faced by insurers

Objectives

Better understanding of status quo, specifically cyber risk:

- Underwriting strategy and insurance products
- Underwriting exposures and potential aggregation
- Challenges faced

- Key themes:
  - Overview of cyber risk underwriting market
  - Size of affirmative cyber risk insurance market
  - Risk appetite to provide affirmative cyber risk cover / not
  - Main affirmative cyber insurance products
  - Key classes / sub-classes of business underwritten
  - Underwriting processes followed / pricing methods used
  - Challenges faced
  - Risk management / mitigation strategies
  - Expected contribution of PA

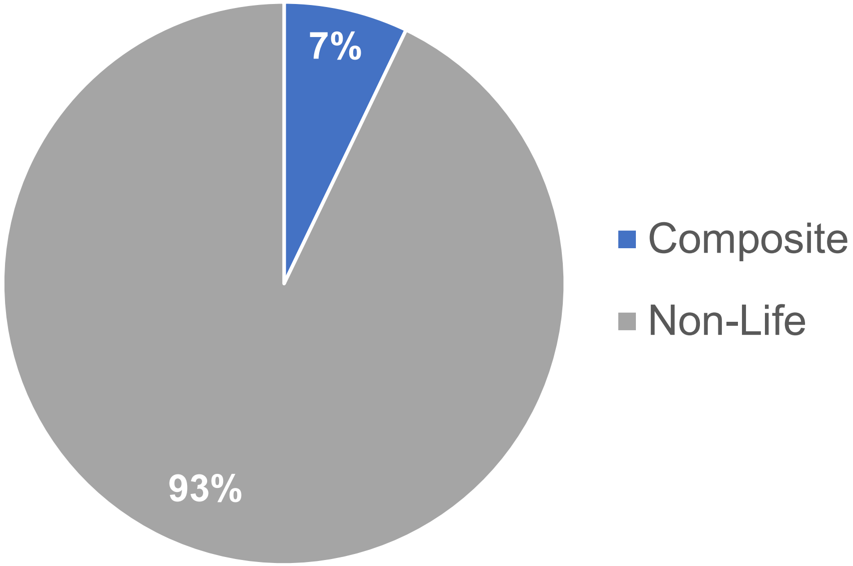
Outcome - General

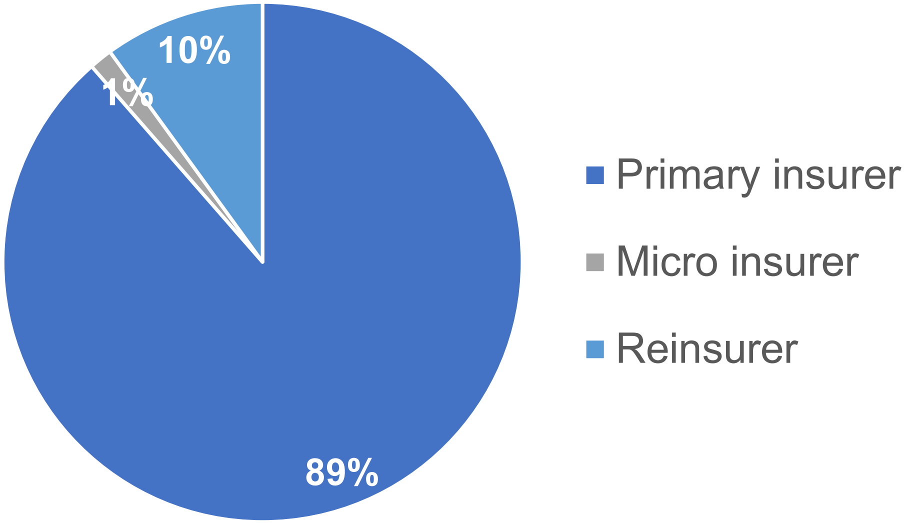
Affirmative vs Non-affirmative cyber risk

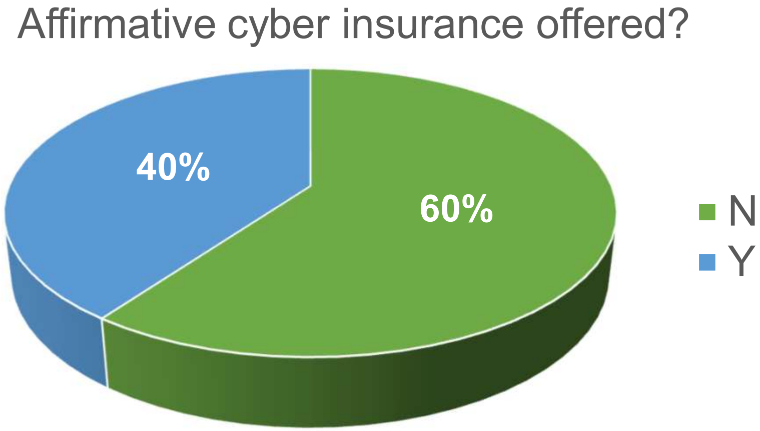
- Affirmative cyber risk
  - Policies explicitly include cover for cyber-related losses
  - Example: Data restoration insurance policy which covers professional restoration of data loss due to cyber event.

- Non-affirmative cyber risk (silent cyber)
  - Policies **do not** explicitly include or exclude cover for cyber related losses
  - Example: Malware attack scrambles the controlling system of a factory, resulting in fire or machinery breakdown.

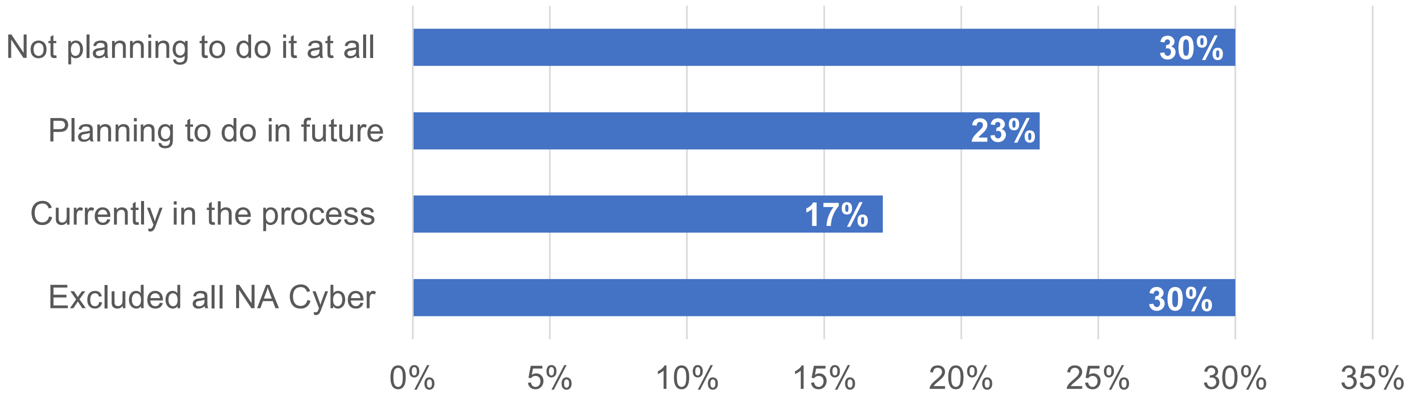
Submission Information







Exclude non-affirmative cyber risk exposures



Rewording of policy documents

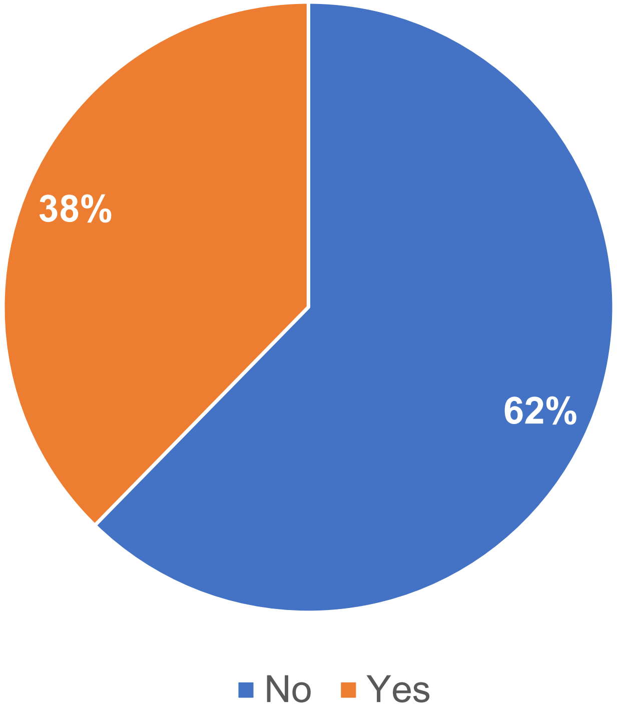
Analyse traditional business lines

Improve underwriting processes

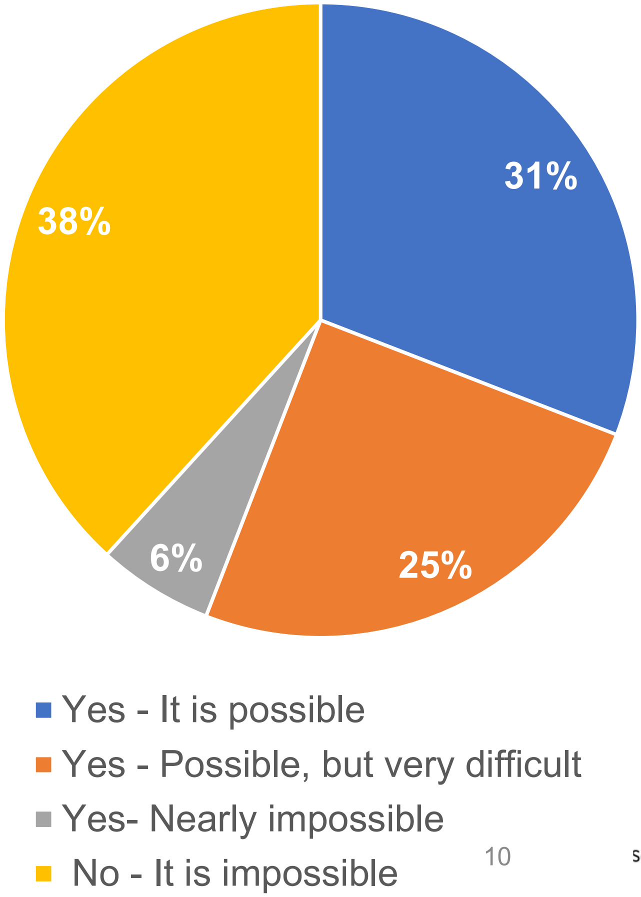
South African Reserve Bank
Prudential Authority

Awareness and Quantification of NA cyber risk exposure

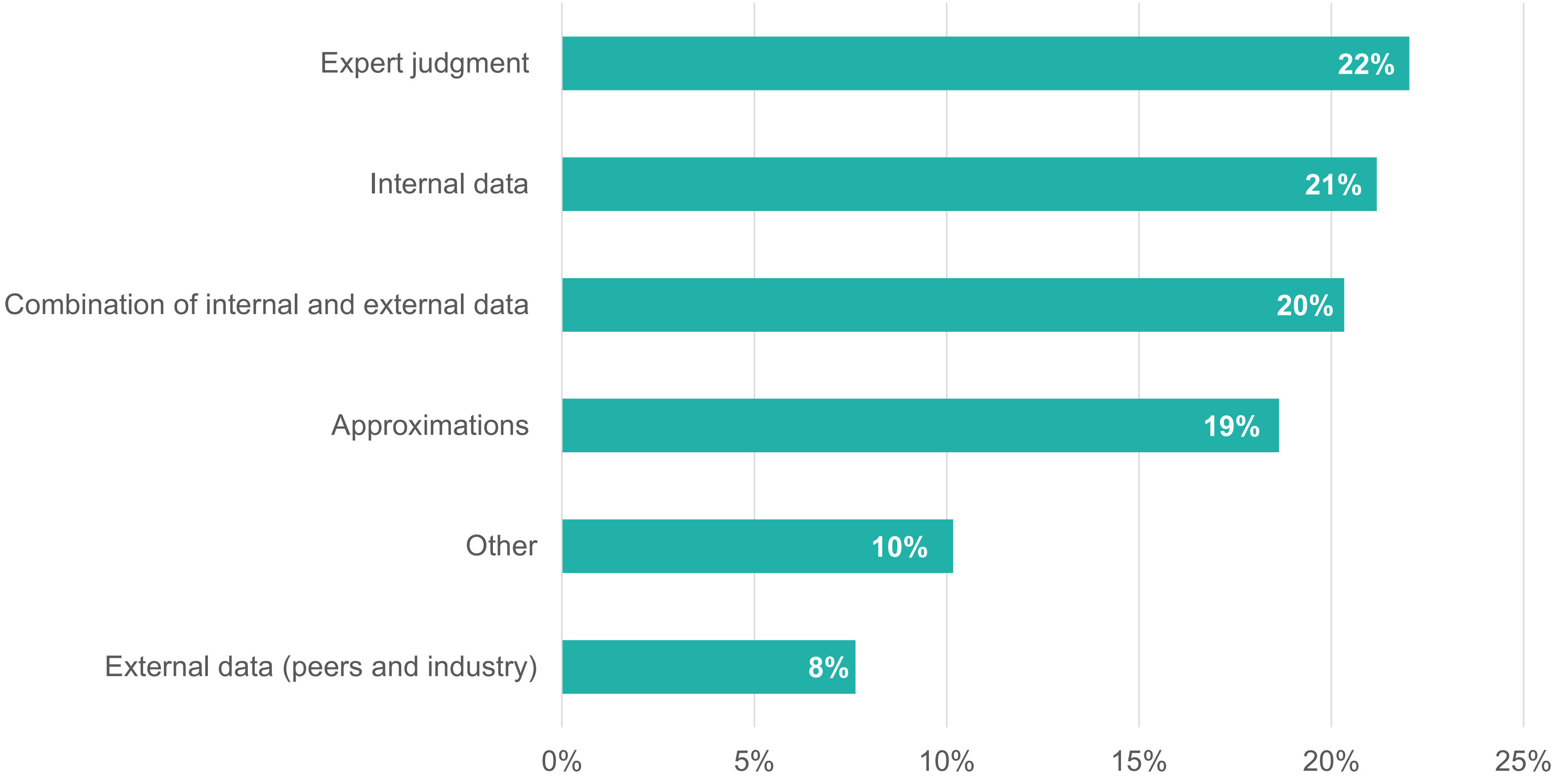
Are insurers aware if they inadvertently offer cyber risk cover on a non-affirmative basis?



Are insurers able to adequately quantify and assess non-affirmative exposures?

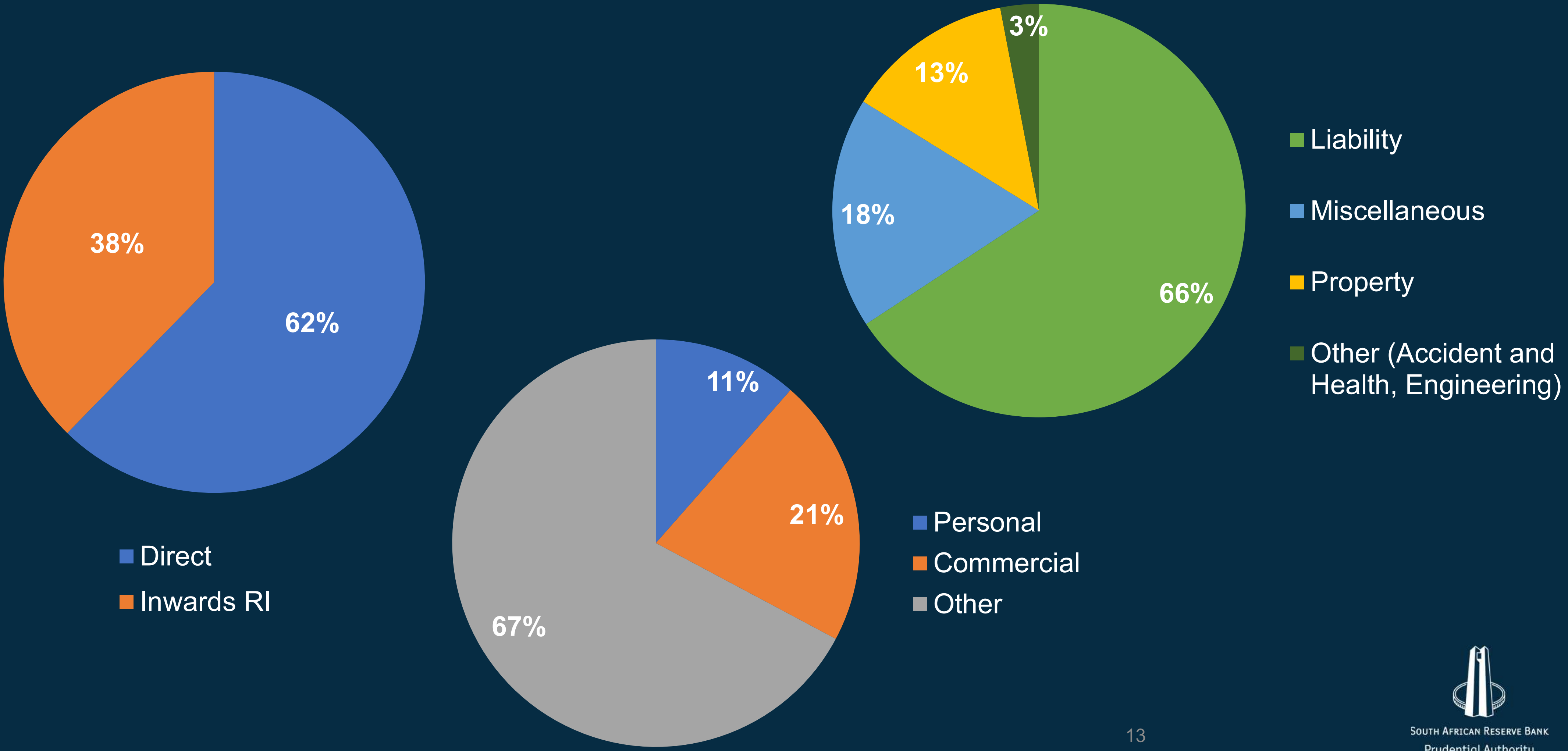


Quantification methods of NA cyber risk exposure

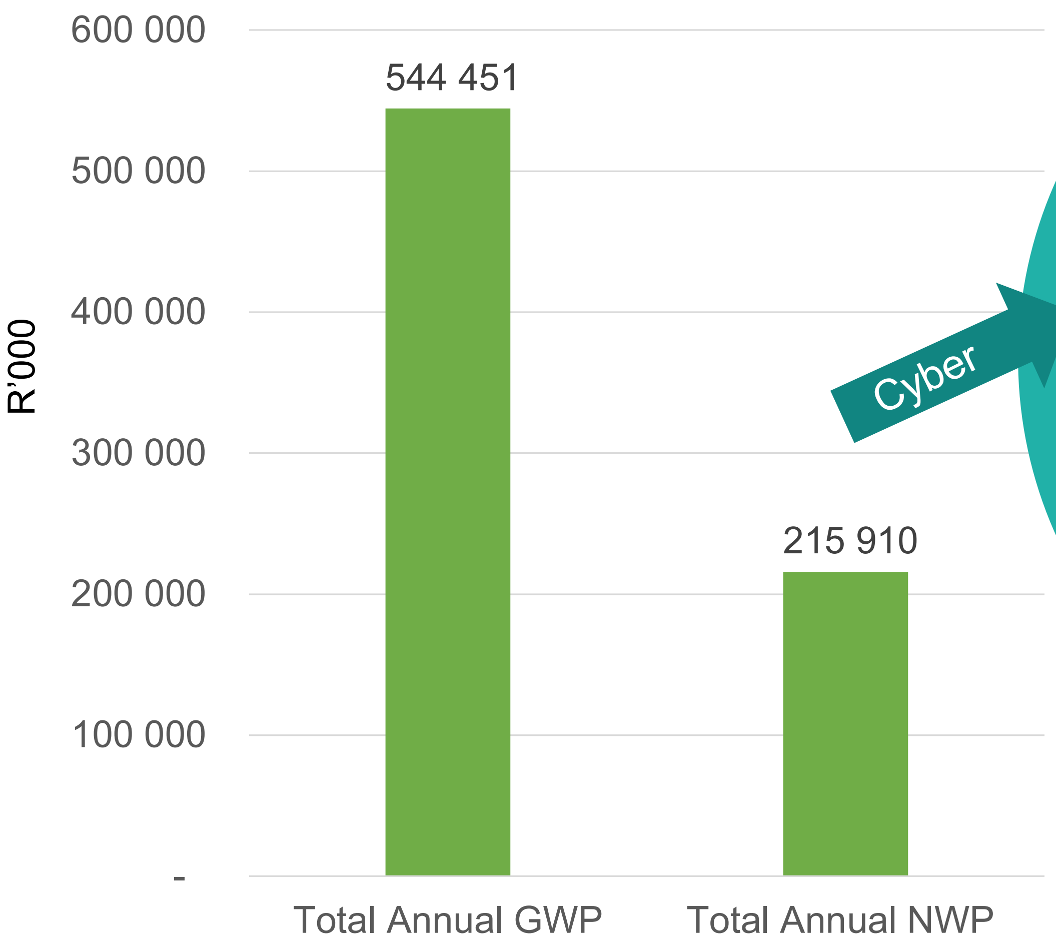


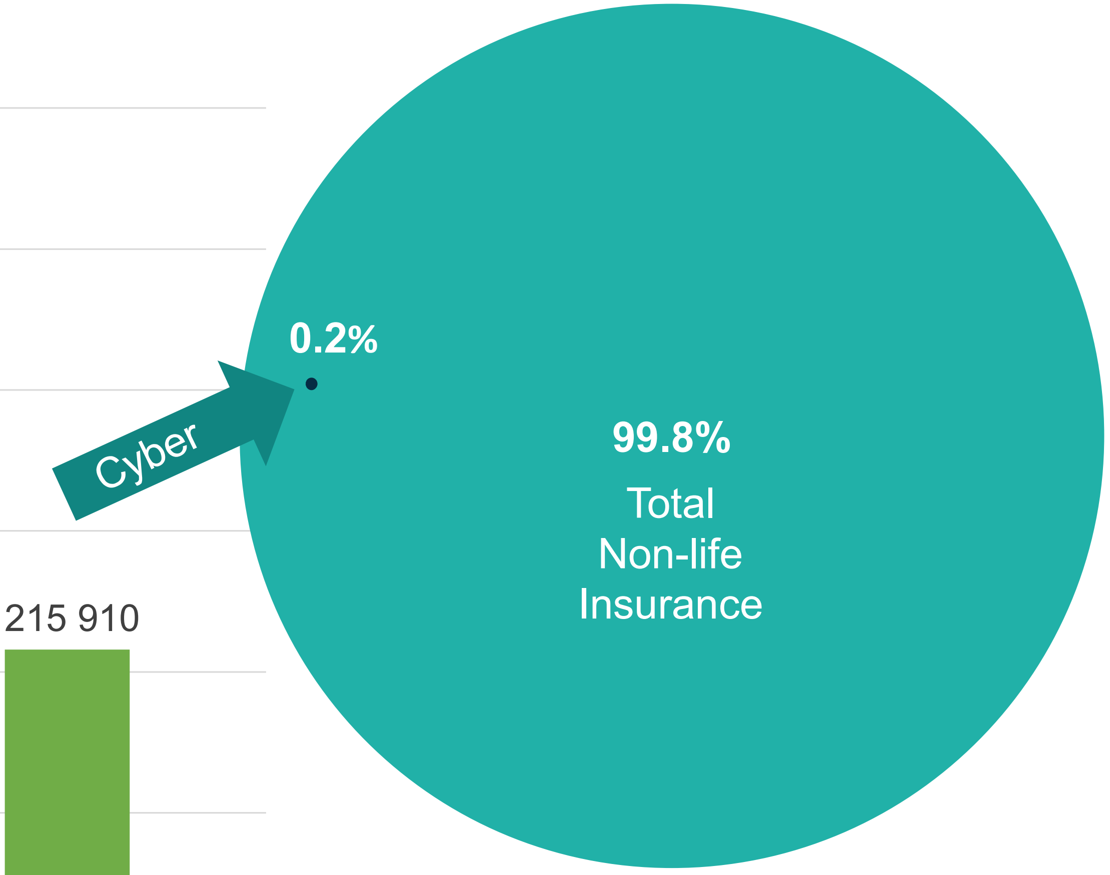
Outcome - Affirmative Cyber

Affirmative Cyber Composition Overview



Total Cyber Premiums and Policies

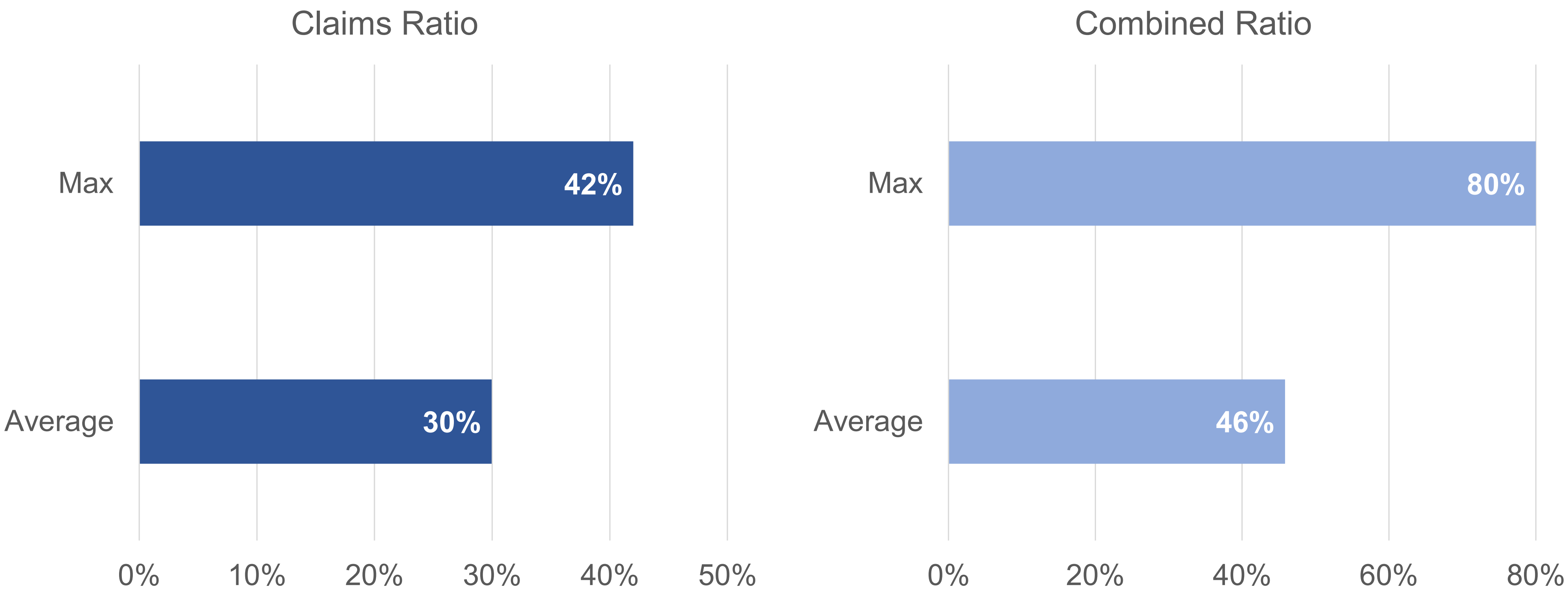




# Cyber policies: ± 26 000

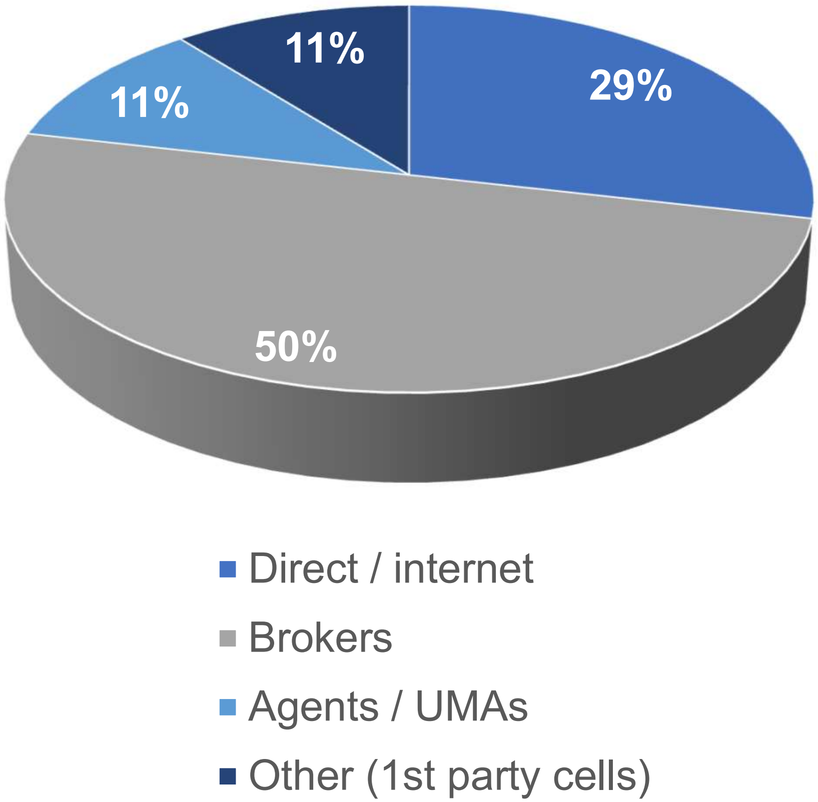
South African Reserve Bank
Prudential Authority

Affirmative Cyber Claims and Combined Ratios



Claims ratio = Net incurred claims (NIC) / Net Earned Premium (NEP)
Combined ratio = (NIC + net expenses + net commissions) / NEP

Distribution Channels and Underwriting Obstacles



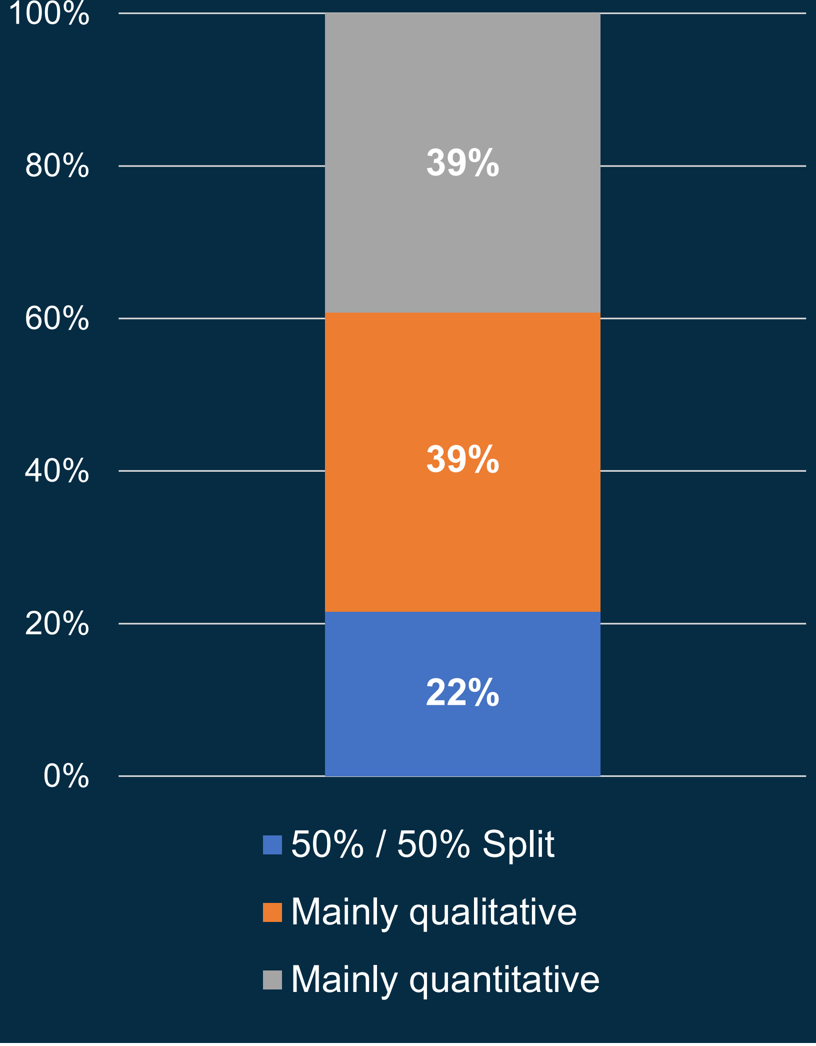
Lack of data

Lack of cyber expertise

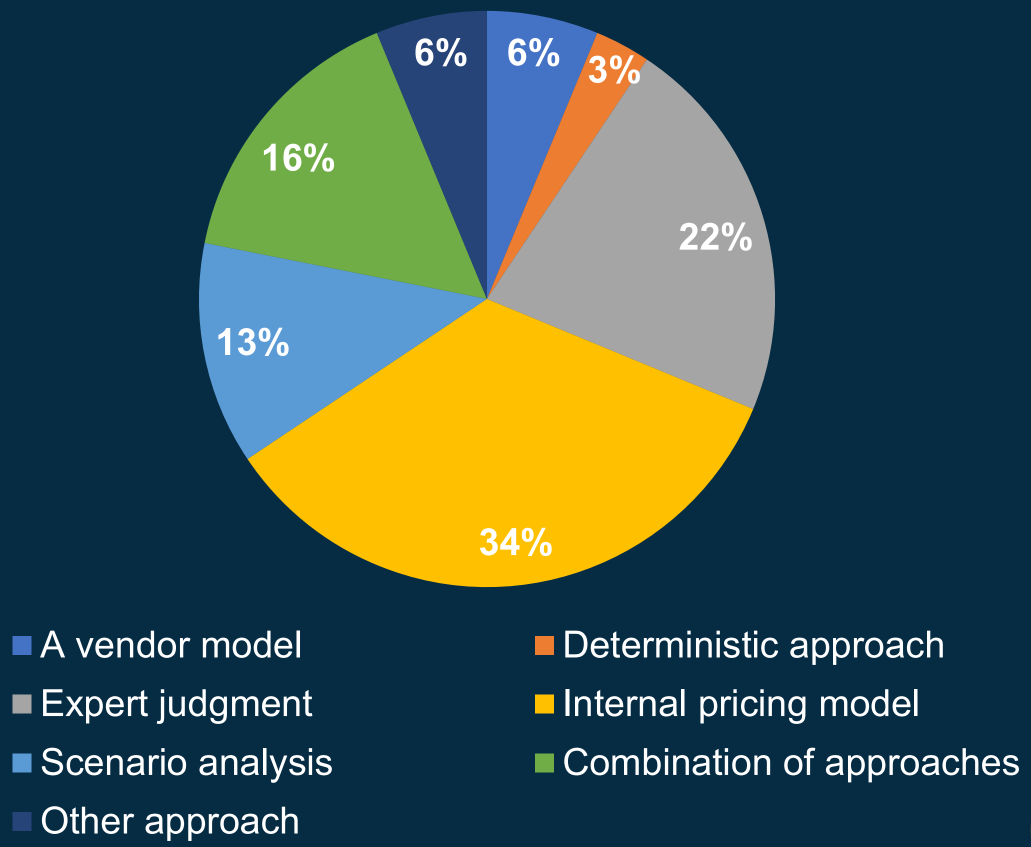
Costly / detailed underwriting process

Risk of over / under pricing

Qualitative vs. Quantitative Underwriting Data



Approaches used to underwrite cyber risk:



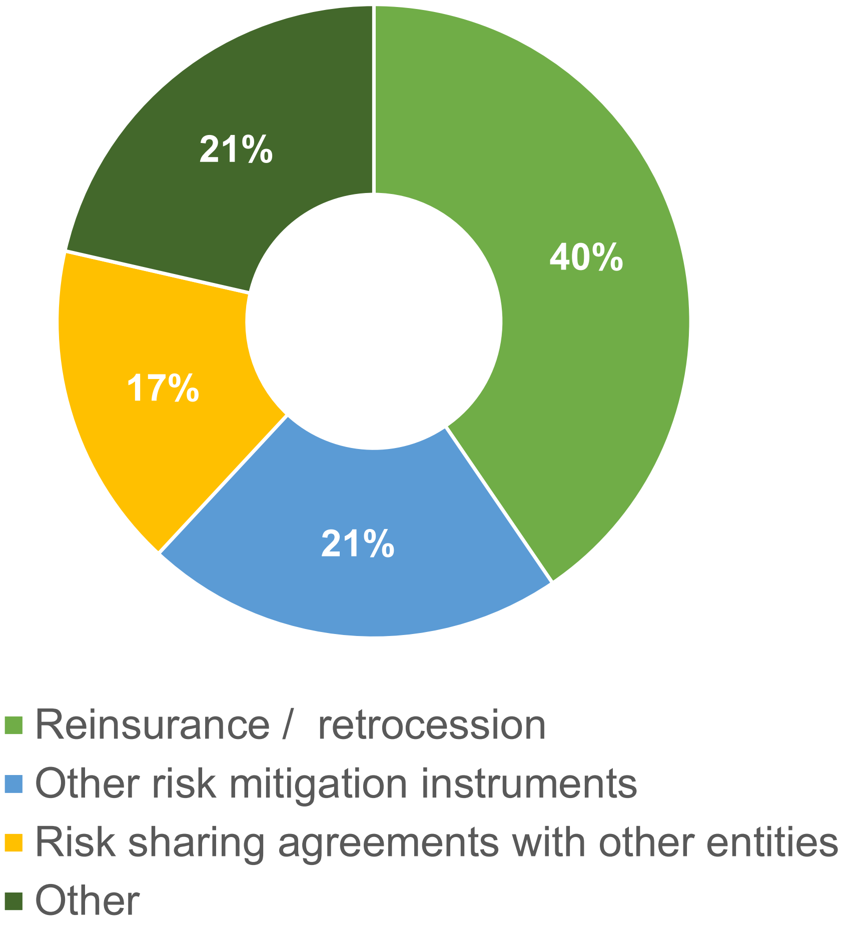
Challenges and Trends

1. Systemic nature of potential events
2. Lack of historical data to quantify risks
3. Broadness of coverage
4. Risk of underpricing
5. Lack of specialised underwriters / reinsurance coverage
6. Dynamic and constantly evolving environment

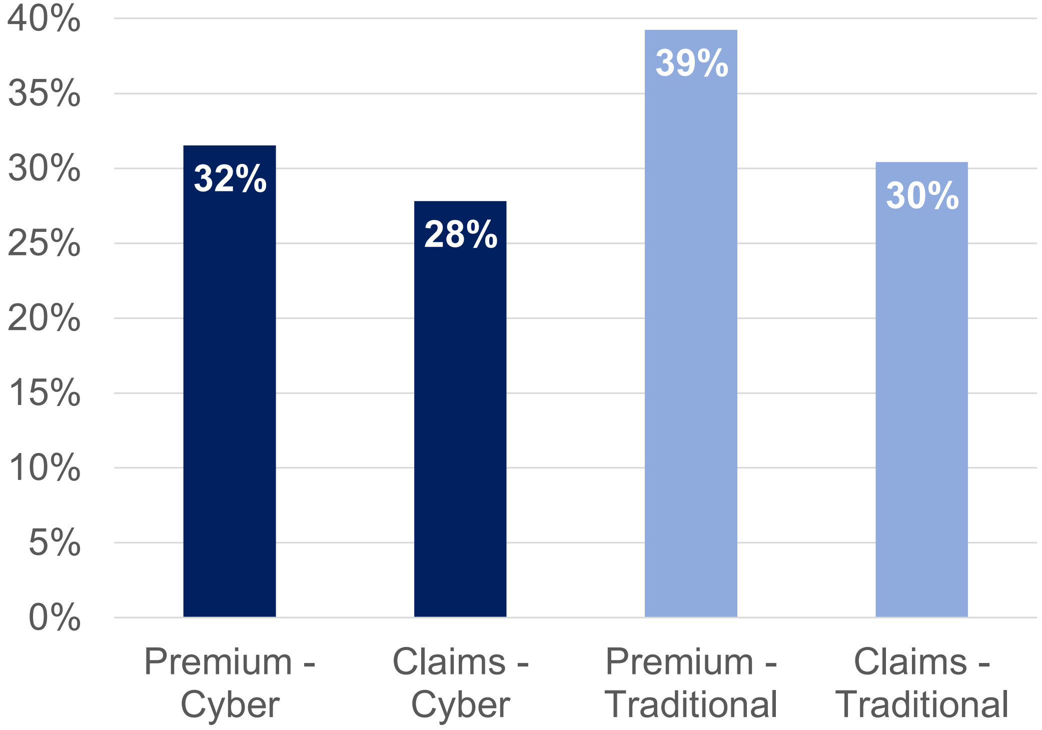
1. More spent on cyber security than insurance
2. Premiums charged are increasing rapidly
3. There are more new buyers
4. Higher limit options are sought

SOUTH AFRICAN RESERVE BANK
Prudential Authority

Risk Mitigation



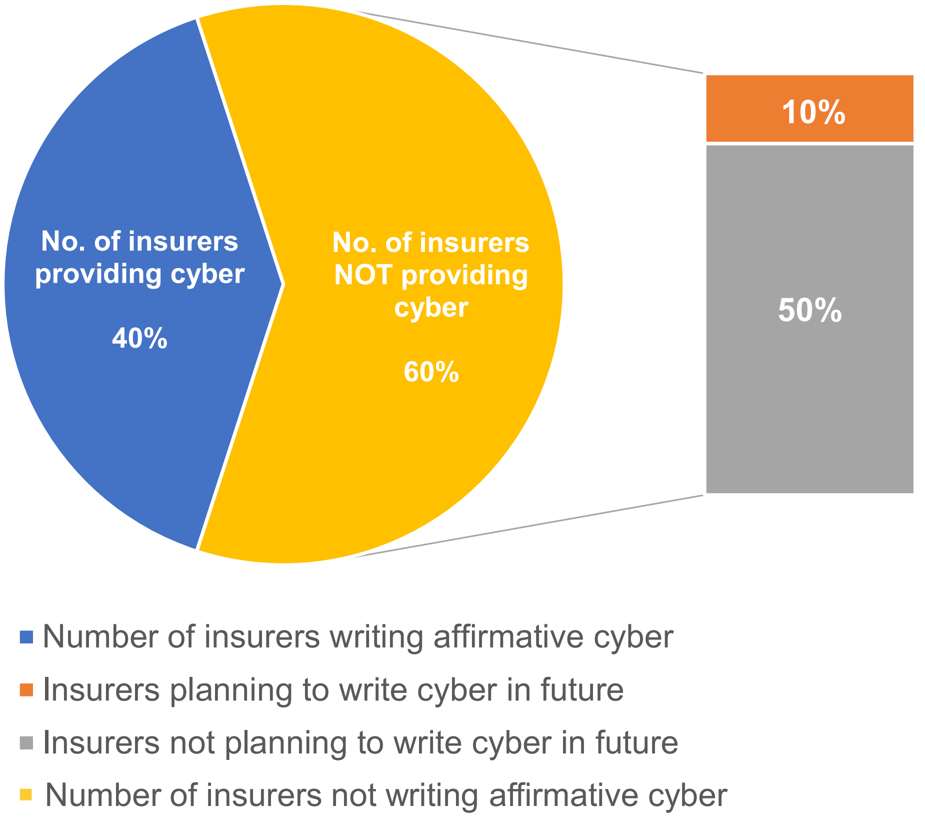
Premium and Claim Retention Ratios

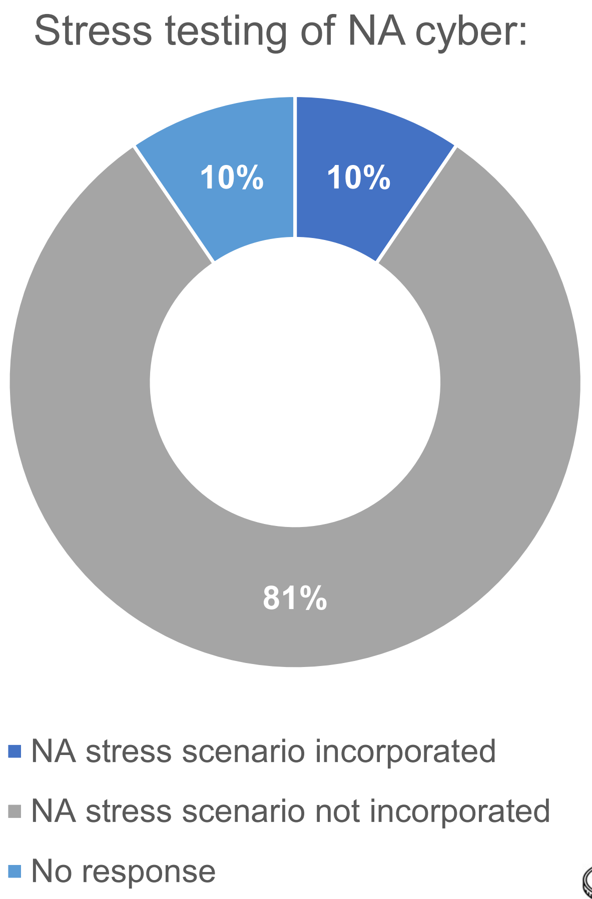


Retention ratio = net / gross

Outcome - Not Writing Affirmative Cyber

Insurers planning to provide affirmative cyber





South African Reserve Bank
Prudential Authority

Outcome - Prudential Supervision

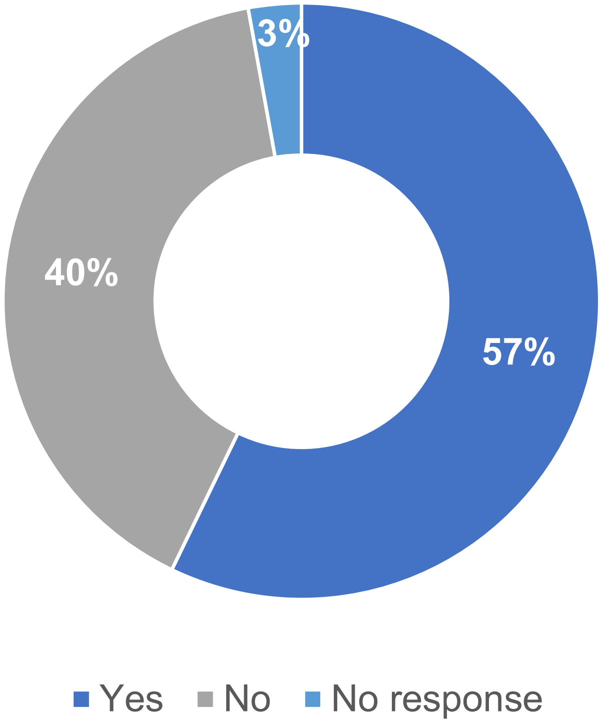
Obstacles and Expected Contributions

- Regulatory business classes / SF do not cater for cyber insurance
- Costly, cumbersome, and lengthy regulatory processes.
- Lack of cyber specific supervisory guidance and standards
- Inability of supervisory framework to adapt to fast paced cyber insurance industry

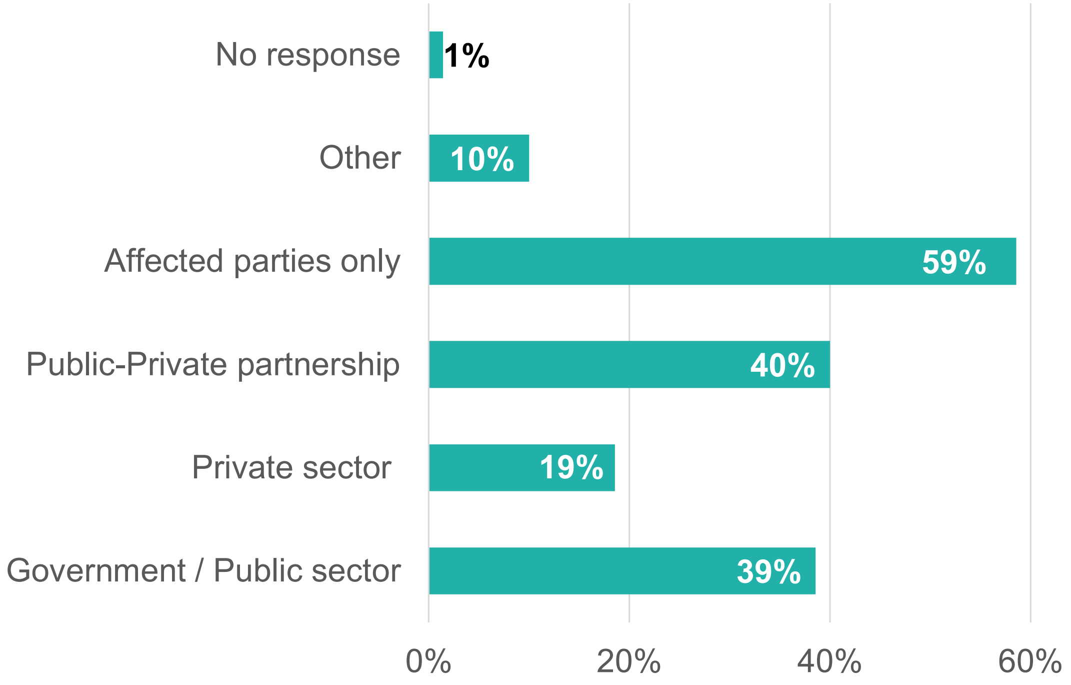
- Develop clear and concise cyber standards and guidance notes
- Provide support:
  - Education, training, knowledge sharing
  - Increase awareness / understanding of cyber insurance
- Setting industry standards and provide monitoring / oversight

Industry Participation

Participate in anonymous industry data sharing?



Parties responsible for uninsured losses in an extreme cyber risk event?



3. Conclusions

Conclusions

- Quantitative data is of poor quality or lacking
- Size of affirmative cyber risk insurance market is very small
- Limited risk appetite to provide affirmative cyber risk
- Cyber mainly written in the Liability class
- Mainly annual standalone cyber policies sold via brokers
- Underwriting methods used - internal + expert judgement
- Challenges faced - lack of data and cyber expertise
- Main risk management strategy is reinsurance
- Industry view - expected contribution of PA as regulator
- Refine on-going supervision via insurer discussions and stress tests in ORSAs