40th Indian Fellowship Seminar

Date: 14th-15th December 2023

Group 4: Charting A Course for Cyber Insurance

Guide : Sabyasachi Das

Presented By :

1. Hemant Malani
2. Vaishnavi Kaushik
3. Naga Teja Mariyala
4. Shreya Goel

Institute of Actuaries of India

About our guide: Sabyasachi Das

Sabyasachi Das, Corporate Actuary and Head of Risks Life and Health, MunichRe India Branch.

Sabyasachi has more than 18 years of Actuarial Experience and has worked in the areas of Life and Health Reinsurance, Life Insurance and UK Pensions. He is a key member of the **Life and Health** Leadership Team at MunichRe India Branch and is responsible for the Valuation and Monitoring of the **LH** Business, Business Planning and Statutory and Shareholder Reporting.

Sabyasachi is a Fellow of the Institute of Actuaries of India (IAI) and the Institute and Faculty of Actuaries, UK (IFoA).

Agenda

- Introduction
- Case Study Overview
- Cyber Risk Landscape
- Product Features
- Data Sources and Modelling Techniques
- Reinsurance, Regulatory and Legislative Framework
- Pricing Strategy and Projected Business Plan

Agenda

- Introduction
- **Case Study Overview**
- Cyber Risk Landscape
- Product Features
- Data Sources and Modelling Techniques
- Reinsurance, Regulatory and Legislative Framework
- Pricing Strategy and Projected Business Plan

Case Study Overview

- **Company:**
  - Small-sized GI company
  - Planning to launch a new Cyber Insurance product in a highly competitive market

- **Product Coverage:**
  - Loss due to Cyber frauds or digital risks
  - Legal expenses and financial loss due to data breach and fraudulent transactions

- **Develop a Pricing Strategy while considering:**
  - Key challenges in pricing the product accurately
  - Data sources and modelling techniques that can be used
  - Impact of regulatory changes on pricing and profitability
  - Reinsurance arrangements
  - Balance between competitive pricing and sustainable profitability
  - Business plan to ensure that Cyber insurance grows 3x in premium volumes in the coming 5 years.

Agenda

- Introduction
- Case Study Overview
- **Cyber Risk Landscape**
- Product Features
- Data Sources and Modelling Techniques
- Reinsurance, Regulatory and Legislative Framework
- Pricing Strategy and Projected Business Plan

Introduction - Cyber Risk Landscape- Worldwide

Opportunities

- The global cyber insurance market size was valued at $13.83 bn in 2022. Over the next 7 years it is projected to grow at a CAGR of 25.7% to $63.62 bn in 2029 (Fortune Business Insights)
- IBM estimates that about 90% of the data in the world today has been created in the last 2 years. (IBM Big Data Success)

Risks

- Global cyber attacks increased by 38% from 2021 to 2022 according to 2023 Cyber Security Report by Checkpoint.

High Profile Data Breaches	Amount (US $ millions)
Equifax	575
Deutsche Telekom - T Mobile	350
Home Depot	200
Capital One	190
Uber	148

Introduction - Cyber Risk Landscape- India

Opportunities

- Ministry of Electronics & IT forecasted that the digital economy of India has the potential to grow from US $200bn in 2019 to US $1 trillion by 2025.
- Deloitte estimated that the cyber insurance market size in India in October 2023 is US$ 50–60mn . The market has been consistently growing at a CAGR of 27–30 percent over the past three years. It is expected to maintain the growth rate over the next 3–5 years with increasing awareness levels.

Risks

- According to CERT-IN 1.39mn cyber security incidents happened in India in 2022.
- India reported 1,787 cyber attacks per week from Sept 2022 to Feb 2023 in comparison to global average of 983. (Checkpoint)

Agenda

- Introduction
- Case Study Overview
- Cyber Risk Landscape
- **Product Features**
- Data Sources and Modelling Techniques
- Reinsurance, Regulatory and Legislative Framework
- Pricing Strategy and Projected Business Plan

Product Features

- **Product Category:**
  - Commercial Product
- **Perils Covered:**
  - Virus Damage
  - Hacker Attack
  - Theft of Corporate data
  - Business Interruption due to cyber frauds
  - Losses relating to breaches or actions by suppliers and business partners
  - Ransomware
  - Legal expenses
- **Benefits:**
  - **Base Product:**
    - Assistance with incident management and minimizing reputational damage
    - Payment to cover:
      - System rebuilds, equipment repair and replacement
      - Restoration of data
      - Business Interruption

Product Features

- Onward virus transmission
- Legal & PR costs
- Regulatory fines [subject to specified limits]
- Ransom demands [subject to specified limits]
- Costs of investigation
- Compensation demands for customers

- **Add-on Product:**
  - Extended Policy Period
  - Advancement of Defense Cost
  - New Subsidiary [subject to limit on revenue and professional services]
  - Network Interruptions [subject to waiting hours period]

Product Features

- **Exclusions:**
  - Anti-Trust
  - Bodily Injury and Property Damage
  - Deliberate, reckless or negligent actions by the policyholder
  - Claims relating to download of inappropriate material
  - Intellectual Property Rights
  - Trading losses
  - Unauthorized trading
  - Pollution
  - Damage caused by employees
  - War/Terrorism

Agenda

- Introduction
- Case Study Overview
- Cyber Risk Landscape
- Product Features
- **Data Sources and Modelling Techniques**
- Reinsurance, Regulatory and Legislative Framework
- Pricing Strategy and Projected Business Plan

Data Requirements & Challenges

Institute of Actuaries of India

Data Requirements for Pricing >> Policy Data | Claims Data

Why there are data challenges with Cyber Insurance ??

- Difficulty in Quantifying Cyber Risk
- Underreporting of Cyber incidents
- Heterogeneity of Cyber Risks
- Dynamic and Rapidly Evolving Threat Landscape
- Data Privacy Concerns
- Global nature of cyber threats

Need of the hour:

1. Breaking the “vicious circle” of data-related obstacles in cyber insurance!
2. Facilitating anonymous data sharing mechanism for the benefit of the entire market. Collaboration between researchers, insurance companies, IT firms and regulators.
3. Data collection and analysis to be adaptive due to non stationarity.
4. Relevance of historical information will most likely decrease over time. Important to combine expert opinions supported by advanced modelling techniques with the statistical evaluation of data.

Other Uses of Data

- Claims Management
- Marketing
- Reinsurance
- Demand Modelling
- Fraud Detection

Data Sources

Evaluating Alternative Data Sources

Pricing Considerations

Measure of Exposure

- Volume of customer records held
- Company Revenue

Claims Characteristics

- Number of Claims, Claims Cost
- Claims Inflation
- Delay Patterns
- Both Short tailed and Long tailed
- Accumulations
- Moral Hazard

Risk Factors and Rating Factors

- Scale, Scope and Type of Insured's operations
- Nature of data held by the insured and the security framework around it
- Technology framework of the insured: Level of interconnected ness and related vulnerabilities
- Crisis management and Resilience plans
- Past Incidents and Claims History

Underwriting Factors

- Presence of a comprehensive cybersecurity program and regular employee training.
- Leadership commitment to security culture
- Organization's relationships with third-party vendors
- Industry Reputation
- Regulatory Compliance

- The goal is to tailor insurance coverage and pricing to accurately reflect the unique characteristics and risks of each insured entity in the rapidly evolving landscape of cyber threats.

Modelling Techniques

Pricing Approaches (1/2)

Pricing Approaches

- **Underwriting Practices**
  - **Case Basis Underwriting**
    - Evaluation through Underwriting Practices. Assess cyber exposures for each insured on a case specific basis.
    - Rating Factors, Underwriting Factors, Judgement.
    - Adopt a segmentation approach to underwriting.
    - Critical to have good Tracking & Monitoring models in place.
  - **Pricing Additional Coverages**
    - For legal expenses, the rating is normally based on the sum insured.
    - Regulatory fines to vary by jurisdiction and framework (subject to change).
- **Further Assessment Measures**
  - Insurer can also undertake further assessment measures like Cyber scanning tools and reports that offer a view of potential cyber vulnerabilities of the Insured and cyber risk grading.
  - Detailed security risk assessment through in-house or third-party cyber security agencies.
  - Tabletop discussion with the Insured to get an in-depth view from the Insured.

Modelling Techniques

Pricing Approaches (2/2)

Pricing Approaches

Other Modelling Techniques

Pricing with Limited data:

- Apply large loadings for uncertainty, apply more conservative assumptions than usual (may not be possible due to high market competition)
- Use of ILFs for higher layers (once lower layer premiums estimated)
- CAT Cyber Models can be applied to active exposures in order to understand overall impact. Can be used to formulate sales, underwriting strategy and reinsurance capacity. (But limited availability, still in early stages of development)
- Can seek help and advice from IAI, if uncertain

Practical Considerations

- Market Competition
- Business objective
- Reinsurance capacity
- Method of sale
- Experience rating

APS 21

- Appropriate Premium Rates is a probability statement.
- Must exercise judgement based on sound techniques.
- Other considerations - Type of product, Claim costs and expenses, Adequacy of the provisions for acquisition costs and other expenses, Impact of future inflation and legislations
- Claim experience
- Industry experience
- Capital requirements

Recommendation: Focus on producing a “risk-informed model” instead of “definitive predictive model” in shifting threat landscape at present. Monitor product performance over time.

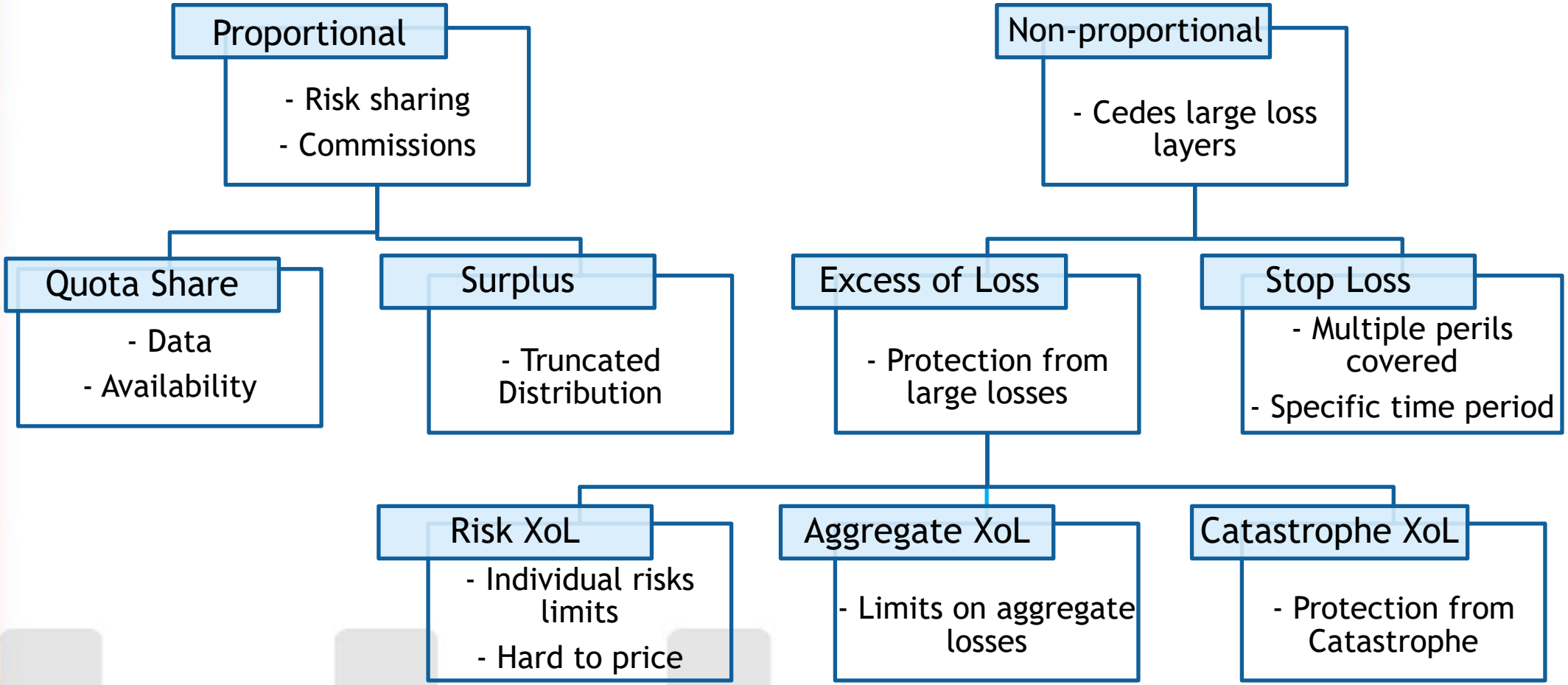
Agenda

- Introduction
- Case Study Overview
- Cyber Risk Landscape
- Product Features
- Data Sources and Modelling Techniques
- **Reinsurance, Regulatory and Legislative Framework**
- Pricing Strategy and Projected Business Plan

Reinsurance

- Data
- Expertise
- Capital requirements
- Claims smoothening
- Add-on Coverages
- Regulation
- Portfolio Diversification
- Large loss protection

Reinsurance



Reinsurance

Quota Share + Stop Loss

- Available in the market
- Write larger business
- Portfolio diversification
- Protection from Large losses
- Simple administration for QS

IRDAI Initiatives in the Cyber Insurance

- Task Force to examine the implications of the DPDP Act, 2023 on the insurance sector. – 24/11/2023
- Observing National Cyber Security Awareness Month (NCSAM)- October 2023 – 19/10/2023
- Constitution of Inter-Disciplinary Standing Committee on Cyber Security – 14/09/2023
- Circular on Reporting of Cyber Security Incident – 13/06/2023
- IRDAI Information and Cyber Security Guidelines, 2023 – 24/04/2023
- Guidance Document on product structure for Cyber Insurance – 08/09/2021
- Report of the Working Group (WG) to Study Cyber Liability Insurance. – 20/01/2021
- Guidelines on Information and Cyber Security for insurers – 07/04/2017
- Cyber security framework for insurers – 31/10/2016

Source: https://irdai.gov.in/

Regulatory Governance Framework

- IRDAI (Appointed Actuary) Regulations, 2022.
  - Rendering actuarial advice to the management of the insurer, in particular in the areas of product design and pricing, insurance contract wording, investments and reinsurance
- APS 21 –Appointed Actuary
  - Ensuring that overall pricing policy of the insurer is in line with the overall underwriting and claims management policy of the insurer
  - Ensuring adequacy of reinsurance arrangements
- APS 34 –General Actuarial Practice
  - Data quality, Assumptions & methodology
  - Model Governance
  - Process Management
  - Peer Review
  - Documentation
- Professional Conduct Standards

Sources:
https://irdai.gov.in/ https://www.actuariesindia.org/

Laws & Regulations – Cyber Security

- Information Technology Act, 2000
  - Granting legal recognition to all transactions done through electronic data exchange
  - Legal recognition of books of accounts in electronic form
  - Addressing Computer-related crimes and cyber offenses
  - Protecting privacy and sensitive personal data
- Digital Personal Data Protection (DPDP) Act, 2023
  - the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes.
- Digital India Act 2023 (Proposed)
  - will focus on key elements such as online safety, trust, and accountability, and evolving digital landscape. It is to address emerging technologies and to be made future proof.
  - Replaces IT Act 2000 and work in conjunction to DPDP Act 2023, National DGP and IPS Amendments for Cybercrimes.

<u>Other government initiatives</u>

- The Indian Cyber Crime Coordination Centre (I4C)
- Cyber Swachhta Kendra
- National Critical Information Infrastructure Protection Centre (**NCIIPC**)

Source: https://www.meity.gov.in/

Impact of DPDP Act 2023 on Pricing Strategy

- Increase in demand
  - Operational challenges
- Coverage
  - Allowed legally? Yes, in India
  - Which penalties? To what extent?
  - Regulatory fines up to INR 250 Cr.
- Changes in risk profile
  - More risk controls in place
  - Anti-selection
  - Moral Hazard
- Internal Expenses
  - Compliance expenses
  - Consent mechanism revamping
  - Data management infrastructure
- Commissions
  - Intermediaries

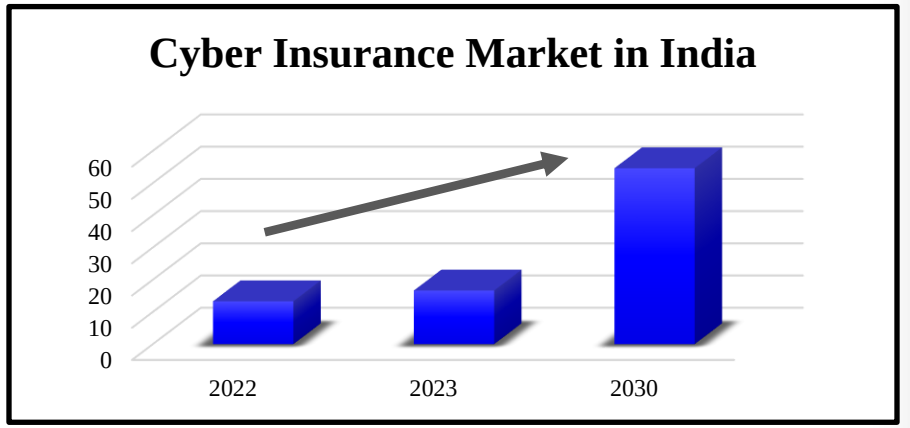
Agenda

- Introduction
- Case Study Overview
- Cyber Risk Landscape
- Product Features
- Data Sources and Modelling Techniques
- Reinsurance, Regulatory and Legislative Framework
- Pricing Strategy and Projected Business Plan

Achieving Business Plan – 3X Growth

OPPORTUNITIES

1. Digital Personal Data Protection Act 2023
2. Growing Potential with large share of the market untapped
3. Increased Regulatory Reforms by IRDAI and Guidance Structure
4. Increased Customer Awareness
    - Awareness campaigns
    - Conference and Events
    - Media coverages
    - Social Media



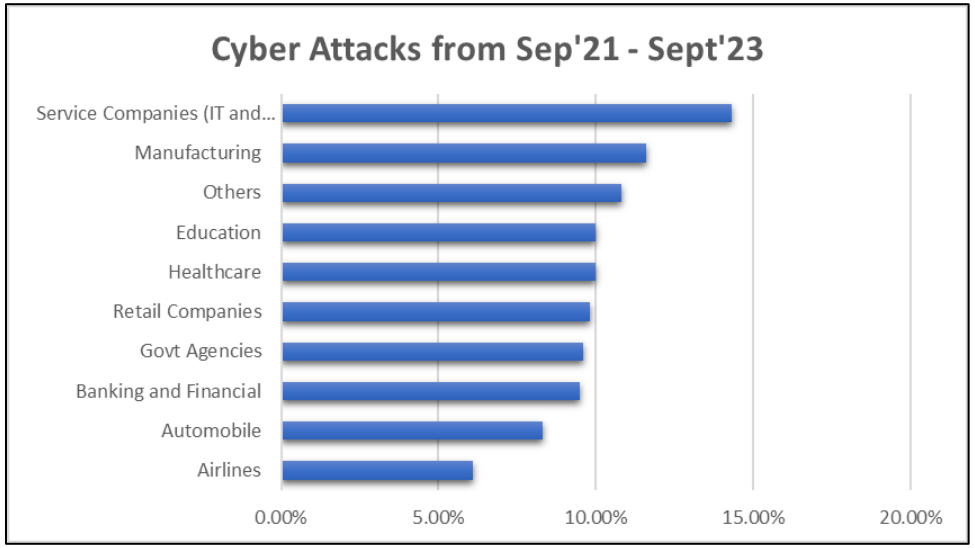
According to a report by Deloitte – "The market has been consistently growing at a CAGR of 27–30 percent over the past three years. It is expected to maintain the growth rate over the next 3–5 years with increasing awareness levels."

According to a report by Cyfirma a cybersecurity firm it was reported that India had been the most targeted country in 2022 .It was reported that 13.7 per cent of the cyberattacks are happening in India, and it is followed by the United States with 9.6 per cent, Indonesia with 9.3 per cent and China with 4.5 per cent of attacks noted. Source

Achieving Business Plan – 3X Growth Contd…

STRATEGY

- Marketing
- Competitive Prices
- Simple policy wordings
- Customer Service
- Leverage data available over time.
- Providing tailored coverages
- Target certain specific industries
- Tie ups with Cyber Security companies
- Use the existing customer base to cross sell
- Leverage the existing distribution channels
- Launch a Personal Cyber Insurance



Source - Times of India

Achieving Business Plan – 3X Growth Contd…

CHALLENGES

- Conflict between investment in Cyber Security and Insurance for the insureds
- Limited understanding of Cyber Insurance and Coverages
- Lack of data
- Increasing Frequency and Severity of claims
- Loose Policy Wordings – Cover wider than priced for
- Lack of Reinsurance coverages
- Ambiguity in payouts
- Lack of Expertise
- Court Settlements
- Accumulation of Risk
- Comparative benefits to larger player
- Operational Challenges
- Moral Hazard

Rate Increase

According to a report – "Cyber premiums in India have also been rising from 2019-20. Premium for a Rs. 50 Crore SI commercial cyber policy rose nearly 20% and costs around Rs. 30 lakhs. The average premium increase for cyber policies has been in the 15%-20%, higher claims and consequent higher reinsurance costs are driving this increase in India, just as with other markets" - Source

Achieving Sustainable Profitability

Institute of Actuaries of India

- Tight Policy wordings
- Good Underwriting →
  - Industry
  - Territory
  - Jurisdiction
  - Company Turnover
  - Does the company perform employee verification
  - The existing cyber security systems in place
  - Does it have a separate Business Interruption Plan
  - History of any cyber attacks
  - Any data collections or other activities outsourced
  - Can critical information be retrieved in case of a cyber attack/ Data breach
  - Does the company invest in training it employees against cyber risks
  - Laptop protection and browser restrictions imposed on employees
- Claims Management and Loss Prevention →
  - Develop incident response plans
  - Partner with Specialized Vendors
  - Promote Cyber Hygiene
  - Share best practices
  - Invest in Data Analytics
  - Implement AI and Machine Learning
  - Invest in Cyber Security

Achieving Sustainable Profitability Contd…

- Expense Management
- Limit the coverages for specific threats
- Deductible
- Incentives like NCB
- Increase Customer Awareness and Marketing to increase market share to benefit from economies of scale
  - Better than Price cuts work on differentiating the product from the competitor
  - Strict underwriting can help capture good risks and larger market by offering lower prices
  - Offer broader coverage with lesser exclusions
- Better Reinsurance Protections and Coinsurance
- Since the business plan covers 5 years, basis experience in initial years strategy can be concentrated on better portfolio of risks
- Purchase higher Reinsurance Protection in initial years and then adjust as per experience
- Regular assessment of Portfolio Profitability
- Avoid Risk Accumulations
- Avoid Long Term product

Institute of Actuaries of India

Questions?

Institute of Actuaries of India

Thank You