

44th India Fellowship Seminar

Date: 26th & 27th June 2025

Group - 6 Cyber Insurance

Presented By :

- 1. Anshul Bohara**
- 2. Harshvardhan Gupta**
- 3. Rishabh R Jain**
- 4. Swargesh Kant Tripathi**



Case study

InsuraPeak, a major Indian insurer, plans to launch a Cyber Insurance product covering: Business interruption, ransomware, forensic investigation, legal fees, and third-party liability.

Internal strategy discussions focus on pricing, underwriting, distribution, claims handling, and capital needs.

One month before launch, E-Tech Innovations suffered a major cyber-attack:

- DDoS + Ransomware attack led to 48+ hours of service outage.
- Customer data encrypted; INR 2 crore ransom demanded.
- 100+ clients are affected, revenue and reputation severely impacted.

Incident triggered a reassessment of InsuraPeak's pricing, coverage inclusions, and product features. The presentation explores:

- (a) Challenges in pricing, channels, claims, and underwriting.
- (b) Claims evaluation and incident resolution complexity.
- (c) Reinsurance role in capital requirement planning.
- (d) Use of AI for cyber risk scoring and client assessment.
- (e) Strategic product features to manage risk and align with risk tolerance.
- (f) Risk mitigation strategies vs. traditional insurance models.

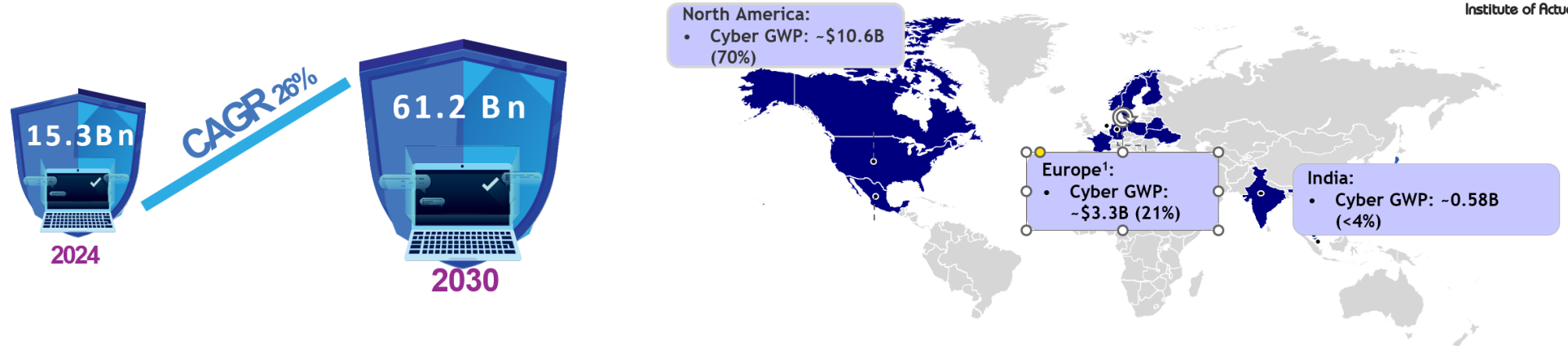
WHAT IS CYBER INSURANCE

Cyber insurance provides financial protection and incident response support for businesses/individuals against losses arising from cyber events, such as:

- Cyber extortion
- Virus Damage
- Theft of Data
- Data Breaches
- Regulatory penalties
- Reputation damage
- Network outages



Cyber Global Market and Trends



KEY SECTORS

- BFSI
- IT/ITES, Telecom
- Healthcare
- Manufacturing
- Government Bodies

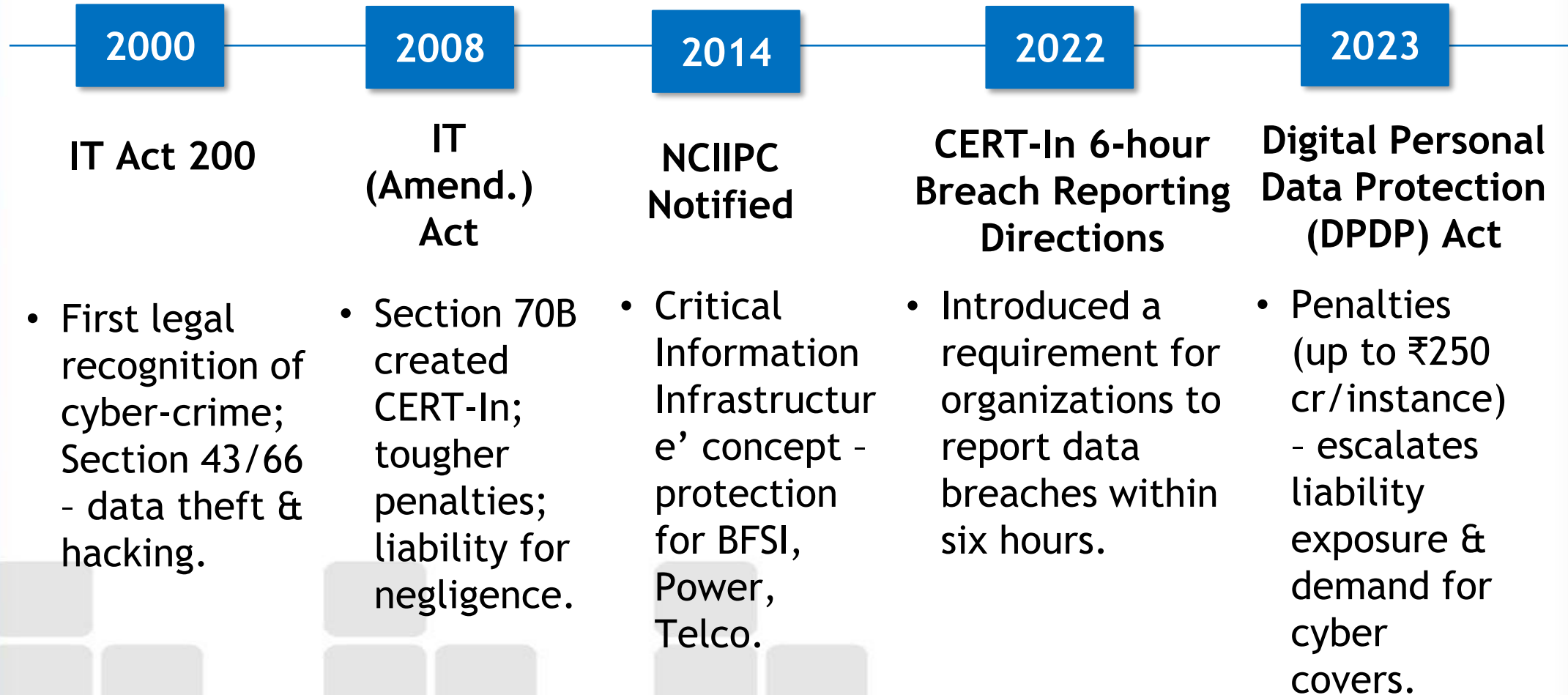
TOP DRIVERS

- Increased Cyber Attacks
- Digital Transformation
- Increased Litigation
- Business Interruption
- Emerging Technologies
- Increased awareness
- Automation of manufacturing

CYBER ATTACK TRENDS

- Increase in Ransomware Attacks
- Phishing and social engineering
- Emergence of AI Driven Attacks
- Supply chain vulnerabilities

Key Policy & Regulatory Milestones - India



Cyber Insurance product in Indian market: Key Challenges



Cyber Insurance product in Indian market

- Key Challenges

- Underwriting
- Pricing
- Distribution
- Other Considerations



Underwriting Challenges (1/3)

Difficulty in Risk Profiling

Cyber risks are non-standardized. Unlike other traditional insurance, cyber underwriting involves assessing multiple areas as shown below -

IT Infrastructure & Security Posture Evaluation

- Firewall, Antivirus, MFA, IT Maturity
- Data encryption standards, Backup practices & patching frequency

Third-Party / Vendor Risk Exposure

- Vendor access controls; Use of cloud services (e.g., SaaS)
- Reliance on managed service providers and their security

Human Factor

- Employee awareness, phishing resilience, internal policy effectiveness

Business Profile Analysis

- Industry type, revenue scale, data volume & sensitivity, global exposure

Expertise

- Underwriting expertise is required for risk profiling for cyber risks, such as Cyber specialists, Tech specialists etc.

Underwriting Challenges (2/3)

High setup Costs

- Costs involved in assessing cyber risk with expertise, such as,
 - Cyber security experts, Cyber Risk underwriters
 - Underwriting tools
 - Time constraints

Reinsurance arrangements

Cyber risks are heavily reinsured, and underwriting decisions are made in alignment with reinsurance arrangements. Challenges include -

- Availability of reinsurances for cyber risks at required terms and conditions such as treaty capacity, facultative arrangements,
- Cost of available reinsurances
- Standalone individual RI may not be available

Adverse Selection

Organizations with poor cyber hygiene are more likely to purchase cyber insurance, skewing the risk pool.

Underwriting Challenges (3/3)



Lack of industry-wide standardized cyber risk benchmarking or scoring mechanism

- Lack of universal cyber risk score
- Underwriters rely on subjective assessments and Internal evaluation.
- Some frameworks and certifications offer guidance, but require contextual adaptation:
 - CERT-In guidelines
 - ISO 27001 Certification
 - NIST Cybersecurity Framework
 - i4C Cyber Hygiene Practices

Individually underwritten

- As cyber risks are non-standardized, therefore, written on case to case basis

Cross-border Data Flow and Jurisdictional Risks

Underwriters must understand regulatory liabilities for multinational clients storing data in foreign jurisdictions, under global laws such as DPDP and GDPR

Cyber Insurance product in Indian market

- Key Challenges

- Underwriting
- Pricing
- Distribution
- Other Considerations



Pricing Challenges (1 / 3)

Experience/Exposure based pricing

- **Lack of Historical Data**
 - Insufficient long-term loss trends to model pricing accurately
 - Underreporting of Breaches to avoid reputational damage
 - There are some information available through sources like:
 - IIB, however, the data are limited due to the low penetration and Cyber insurance being in infancy stage in India
 - CERT-In, however, there are sharing limitations and lack of granularity
- **Issues in Frequency and severity estimation**
 - Low frequency - further exacerbated by limited data and under and delayed reporting of cyber breaches
 - Volatile losses - losses can vary from small to very large losses
 - Frequency and Severity vary significantly by industry, type of attack etc.

Pricing Challenges (2/3)

Experience/Exposure based pricing

- **Dynamic and evolving risk area:**
 - Past data may not predict future risks due to new attack vectors (e.g., AI-driven phishing, zero-day exploits)
 - Difficult to incorporate changing environment
 - Requirement of frequently updating pricing models
- **Aggregation of Risk and Systemic Events:**
 - Single events (e.g., cloud provider breaches) can trigger multiple claims.
 - Modeling and underwriting catastrophic cyber risk (so-called “cyber CAT”) is an evolving area

Pricing Challenges (3/3)

Benchmarks - Reinsurers and Global

- Benchmarks from reinsurers and global or industry sources can inform pricing, however they come with key challenges, such as—
 - Policies are not standardized
 - Coverage alignment needs to be ensured
 - Adaptability of Assumptions and Methodology employed by the reinsurer or globally in the Indian market context

Challenges in maintaining competitive pricing

- Cyber risks are increasing over time with emergence of new attacks
- The direct and indirect costs involved in incident resolution is increasing which will attract higher expense loadings into the premiums
- The reinsurance costs can be more volatile given the global developments around the cyber risk

Cyber Insurance product in Indian market

- Key Challenges

- Underwriting
- Pricing
- **Distribution**
- Other Considerations



Distribution Challenges (1 / 2)

Segment	Challenges
Large corporates • Corporate Broking –driven by Large brokers • Direct Sales	• Entering into existing cyber programme • Maintaining Pricing adequacy due to negotiations
SMEs/Individuals • Direct Sales • Agency • Banca • Digital Platforms • Embedded Partnerships	• Complexity of Product & Jargon Barrier • Limited Product knowledge • Sales • Advisors • Lack of Digital Partner Ecosystems, especially with SaaS, cloud providers, or cybersecurity platforms

Distribution Challenges (2/2)

Other distribution challenges:

Challenges	Description
Low Awareness	• Many SMEs and individuals lack understanding on cyber risk or insurance benefits. • Need education-heavy sales process.
Price Sensitivity in SME Sector	• MSMEs often reluctant to pay unless tied to contracts or compliance.
Lack of Standard Product Structure	• Wide variation in terms and exclusions makes it hard to compare or bundle online.
Long Sales Cycle in B2B & Onboarding and Underwriting Delay	• Corporates take time to assess, compare, and get internal approvals before first time buy • Requirement of cyber risk questionnaires, Underwriting assessments delays quick issuance.

Cyber Insurance product in Indian market

- Underwriting
- Pricing
- Distribution
- Other Considerations



Other Considerations

- **Legal & Regulatory Variability**
 - New regulations (e.g. DPDP Act)-products need to adapt to legal shifts, liability and fines, altering risk exposure
 - Other evolving regulations in future may create underwriting and pricing challenges
- **Insured's dissatisfaction due to limiting product coverages**
- **Practice Standards** : Actuary should consider the APS during product launch and continuously to ensure sound, compliant practices.

APS Duty	Application to Case Study
<i>Ensure premium rates are fair, adequate, and sustainable</i>	Pricing should reflect the underlying risk exposure especially tail-risk events
<i>Assess capital required for new product launch</i>	The AA must ensure adequate capital support and solvency, given catastrophic potential
<i>Maintain IBN(E)R and PDR reserves reflecting cyber claim patterns</i>	• Initial estimate may be very low • High claim volatility

Evaluating Cyber Claims and incident resolutions

Evaluating Cyber Claims (1/2)

- **Incident Verification:**
 - Assessing policy coverage - coverage triggers, limits, sublimits etc.
 - Nature - Ransomware, DDoS, phishing, insider breach, etc.
 - Timing - Regulatory timeliness of notification
 - Scope of breach - Data loss, downtime, financial theft, reputational damage.
- **Forensic Investigation:** Technical evidence to support the claim - to verify occurrence, timeline, and impact of breach or attack.
- **Documentation Provided:** Logs, IT reports, PR/communication records, emails, legal correspondence—all relevant to verifying claim validity.
- **Cost Documentation:** Legal, PR, recovery, and customer notification costs

Evaluating Cyber Claims (2/2)

- Loss assessment considerations
 - **Business Interruption:** Downtime duration, lost income, fixed cost cover, evidence of financial data.
 - **Ransom Payments:** Legitimacy, negotiation documentation, payment method.
 - **Regulatory Compliance:** DPDP/IT Act penalties and legal exposures, US/Europe Exposure, any legal limitations on what's claimable
 - **Third-Party Liability:** Breach origin tracing and client contracts - legal liabilities to customers, partners, or regulatory penalties

Cyber claim challenges (1/2)

- Insured

- **Forensic Gaps:** Limited cybersecurity infrastructure, IT Hygiene and IT documentation among clients
- **Reputation vs Reporting:** Insureds hesitate to disclose breaches.
- **Delayed Reporting:** Late breach notifications reduces evidence reliability.
- **Third-Party Complications:** Vendor breaches, unclear contractual liability.
- **Unnotified Ransom Payments:** May breach insurer or regulatory protocol.
- **Inflated or Fraudulent Claims:** Difficulty verifying intangible losses.

- Legal

- **Privacy and Data Protection Laws:** DPDP Act adds compliance obligations, legal risk of disclosed or leaked data.
- **Jurisdictional Complexity:** Cross-border systems or customer data raise questions of jurisdiction—especially for SaaS firms.
- **Coordination with CERT-In:** Enforcement and data-sharing bottlenecks.
- **Lack of Precedents:** Limited case law under DPDP or IT Act.

Cyber claim challenges (2/2)

- Coverages

- **Ambiguous Policy Triggers:** Disputes over coverage definitions (e.g., downtime vs cyberattack).
- **Coverage Overlap and silent cyber:** Ambiguity between cyber and property or liability policies.

- Evaluation

- **Loss Quantification Issues:** Business interruption losses and data breach costs are difficult to quantify.
- **Multiple Stakeholders:** Involves IT teams, lawyers, PR, brokers, insurers, and forensic vendors. Coordination and timelines become hard to manage
- **Multiple Events/One Claim:** Complex causality and event aggregation, example vendor breach

Claims Case study

- **Background**
 - In late July 2024, across small cooperative banks, thousands of UPI and IMPS transactions started failing.
 - NPCI immediately blocked these banks from the UPI/IMPS network.
- **Claim process**
 - Bank's cyber insurers triggered a coordinated response.
 - Forensic investigation team reviewed system logs and breach and concluded - root cause was a failure at the common vendor
- **Settlement**
 - Banks first-party cyber insurance covered temporary operational disruptions and forensic expenses.
 - But the main liability fell on C-Edge and their E&O policy paid for
 - Claims from affected banks,
 - Costs of containment
 - Ransomware-related expenses.

Reinsurance and Capital

Reinsurance (1 / 2)

Type	Application	Relevance
Quota Share Treaty	Insurer cedes fixed percentage of every risk.	• Useful for capacity building, especially in initial product phase. • Overall product support • Product wordings • Pricing/underwriting • Claims support • Higher QS allows InsuraPeak to scale without assuming full volatility
Surplus Treaty	Cede risk exceeding retention per risk.	• Useful where risk profiles are highly variable • May not be available with appropriate commission • Not frequently used for liability LOBs

Reinsurance (2/2)

Type	Application	Relevance
Excess of Loss (XoL)	Insurer retains loss up to attachment point	• This can be useful where the company is planning to write larger risks • Helps in reducing impact of large losses on Balance Sheet
CAT XL	Insurer retains aggregate losses upto attachment point	• Ideal for protection against catastrophic events • Helps in controlling risk aggregation
Facultative Reinsurance	Case-by-case basis.	• For large risks where treaty limits are breached • For risks, which are not covered the treaty

Impact on Capital requirements (1/2)

- Current Capital Regime is factor based
 - Reinsurance reduces capital requirements; maximum benefit of reinsurance is capped at 25% for Cyber LOB
 - Non proportional doesn't reduce capital requirement to the extent of reduction in portfolio risk.
- Under future RBC regime, capital calculation will be based on aggregation of
 - Net Insurance risk - capital relief broadly in line with retention
 - Reinsurance credit risk including concentration risk
 - Other risks etc.

However, risk charge may not reflect the true risk exposure

Impact on Capital requirements (2/2)

- Cyber risks have:
 - High tail risk
 - Aggregation risk
 - Unmodelled exposure risk
 - Volatile and evolving risk

As a result, InsuraPeak may hold additional internal capital beyond the regulatory solvency requirement until credible claims experience is developed and purchase adequate Reinsurance Basis Company's risk appetite rather than capital requirement.

AI Use in Cyber Risk Evaluation and Client Capabilities



Use of AI in Risk Evaluation (1/4)

Evaluation Techniques

- AI tools powered by NLP can
 - review client responses to security questionnaires.
 - analyze submitted cyber security reports, vulnerability scans, risk assessments, incident logs.
- Benefits
 - Automates extraction of critical insights.
 - Ensures insurers get a comprehensive, real-time view of client security postures.
 - Reduction in underwriting TAT and still helps case to case underwriting

Case in Point: *Coalition*, a U.S. cyber insurer, uses AI to validate and enrich questionnaire data, drastically cutting down manual review time.

Use of AI in Risk Evaluation (2/4)

Cyber Risk Scoring Methods

Cyber Hygiene Scoring

- Platforms like BitSight continuously monitor patch status, open ports, SSL configurations.
- They assign hygiene scores used to inform underwriting.

Case in point: *Marsh* integrates BitSight scores into its application process, offering preferred pricing for higher-scoring applicants.

Automated Security Posture Evaluation

- AI-driven scans and document reviews assess patch management, endpoint protection, MFA implementation, incident response readiness

Case in point: *Beazley's Cyber Services* platform identifies gaps that may result in premium surcharges or coverage exclusions.

Use of AI in Risk Evaluation (3/4)

Assessing Client Cybersecurity Capabilities

Behavioral Analytics for Insider Threat Detection

- AI-driven behavioral analytics tools monitor user activities within a client's network to identify anomalous behavior that may indicate insider threats or compromised accounts

Case in point: Darktrace uses AI to analyze user behavior on networks, detecting unusual patterns like accessing sensitive data at odd hours or downloading large volumes.

Simulated Attacks via AI

- AI simulates cyberattacks—like social engineering or DDoS—on client systems (with consent).
- Reveals vulnerabilities and provides actionable insights.

Case in point: *Hiscox* partners with cybersecurity firms to conduct AI-powered automated pen testing, adjusting deductibles and coverage based on findings.

Use of AI in Risk Evaluation (4/4)

Risk modelling

Predictive Analytics

- ML models can be used to analyze historical claims data to identify risk patterns and predict the likelihood and severity of future cyber incidents.

Case in point: Munich Re uses AI to predict ransomware losses, tailoring coverage for high-risk clients

Systemic Risk Modeling

- AI helps model large-scale, cross-portfolio events: Cloud outages, Supply chain hacks, Simultaneous ransomware attacks
- Analyzes interdependencies to prevent catastrophic concentration risk.

Case in point: *Lloyd's of London* uses AI to stress-test its entire cyber portfolio, proactively identifying systemic vulnerabilities.

Strategic Coverage Features for Cyber Insurance

Strategic Coverage features (1/3)

Sub-limits

Purpose:- Cap exposure on high-cost modules (e.g., ransomware, BI)

Risk Impact:- ↓ Claim severity

Deductibles & Waiting Periods

Purpose:-

- Introduce retentions or time excesses for specific risk types (e.g. BI)
- Aligns with self-insurance principles for frequent but low-impact events

Risk Impact:- ↓ Claim Frequency

Coinsurance (co-pay)

Purpose:- Reduce moral hazard, Share Claims

Risk Impact:- Reduces Claim Frequency and Severity

Strategic Coverage features (2/3)

Modular Coverage or Tiered Product Structure

Purpose:-

- Customizes cover offering to control risk.

Risk Impact:- Controls exposure aggregation & Improves underwriting granularity

Exclusions

Purpose:-

- War, terrorism,
- Bodily Injury, Death
- Trade Secrets and Intellectual Property
- Design Failure and Use of untested/unlicensed softwares
- Prior Claims and Circumstances notified to prior policies or known before the insurance period.
- Contractual Liability

Risk Impact:- Removes Non-Insurable losses , perils covered elsewhere, Reduces anti selection and moral hazard

Strategic Coverage features (3/3)

Warrantties

Warranty Type	Purpose
MFA & Access Controls	Prevent unauthorized Access
Data Backup & Encryption	Ensure data recovery and protection post-ransomware.
Patch Management	Reduce exposure to known software vulnerabilities.
Email Security Controls	Reduce phishing risks—a common ransomware entry point.
Incident Response Plan	Ensure readiness for breach containment and timely notification.

Risk Impact:- Reduces Claim Frequency and Severity

Discovery Period

Purpose:- Limits reporting window for incidents that occurred during the policy term but discovered later

Risk Impact:-

- Reduces reporting delay, frequency and latent claims

Cyber Risk Mitigation Strategies: A Proactive & Differentiated Approach



Risk Mitigation Strategies (1/2)

Strict Underwriting & Cyber Assessments

- Use of real-time vulnerability scans (Shodan, BitSight) to assess risk.
- Use AI to generate risk scores basis proposal form and associated reports.

Differs from traditional: Analyze real-time posture vs. static methodology in traditional products

Pre-Breach Risk Services for Clients

- Provide value-added services:
 - Phishing simulations, patch advice, cyber hygiene checkups
 - Incident Response planning, employee cyber training
 - Can bundle or provide low-cost cyber security suite for SMEs

Encourage secure behavior before any breach.

Differs from traditional: Other lines offer minimal loss-prevention; cyber demands active involvement to control claims frequency and severity.

Risk Mitigation Strategies (2/2)

Post-Breach Incident Response Capabilities

- Partner with digital forensics, Data Recovery teams, PR & Legal firms
- Provide 24/7 breach response hotline.
- Actively manage reputational damage and regulatory requirements

Differs from traditional: Traditional insurers generally pay post-loss; cyber insurers actively involve to contain damage.

Portfolio Management

- Track capacity, aggregation by
 - Sector/Industry mix (e.g., IT, retail, finance)
 - Common Vendor dependencies (like AWS, Azure),
 - Software ecosystems and vulnerabilities (e.g., Log4j, SolarWinds)
 - Layer participation (Primary vs XS)
 - Reinsurer
- Cyber CAT modelling - to manage portfolio aggregations
- Use Reinsurance to balance portfolio and reduce volatility

Differs from traditional: Proactive measures necessary as compared to other traditional lines due to aggregation prone

Thank You!
Any questions?

