Changing Landscape of Liability Risks and Insurance
GIC Re & Howden India Conference, Shimla 2013

Changing Nature of Operational Risks in Technology firms

Nithyanandan Radhakrishnan
Senior Vice President & General Counsel, Infosys Ltd.

The IT Services Industry

- Low Cost Staff Augmentation to Full Service Provider – Y2K, Staff Augmentation, ADM, System Integration, Product Development, BPO, Turnkey IT Service provider, Consulting, SaaS, Transformational IT

- Sophistication in seller behavior – investing in deal pursuit teams, risk management, in-house legal teams, insurance advisors… resulting in multi-year, multi-billion transactions

- Marketplace is both commoditized and specialized ADM services are not distinguishable; transformational IT, big data, analytics, KPO are highly specialized;

- Buyer Advisory market has matured – Industry Analysts, law firms, security audit firms, industry bodies have educated and influenced the outsourcing market demand and behavior

Conflict Behavior

- Conflict and Risk behavior of all players is changing;
  - relationship management is not a salve;
  - contractual terms are imposed!
    - Step-in rights
    - benchmarking
    - set-offs
    - vendor replacement costs
    - data security breach notices
  - no-claim history is history
  - regulatory risks are real: employment, immigration, data security and privacy, fraud, financial propriety, whistleblower, reputation
  - Litigation costs are spiraling – e-discovery costs hurt; document retention practices are poor;

Outsourcing of Risk along with Outsourcing of IT

Risk Management

- Risk management has transformed from ‘checkbox’ coverage to threat evaluation, vulnerability preparedness and asset protection;
  - market availability is changing from ‘anywhere’ to locally-admitted
  - New threats mean tighter coverage; differentiation in offerings
  - Claim incidence is refining pricing
  - Higher deductible/lower deductible dilemma continues
  - Insistence on choice of counsel/ legal services pricing control

And of all of this resulted in…?

- A careful assessment of the IT Assets (data, software, hardware, people, facilities..)
- An appreciation of the vulnerabilities (security, error, malfeasance..)
- Threat scenario forecasting (loss, availability, reputation, confidentiality..)
- Driving risk transfer behavior (vendor obligation, loss definitions, indemnification obligations, third party accountability, non-contributory, primary cover, additional insured, named)
- Pursuing coverage gaps (capacity and quantum, exclusions and definitions, jurisdiction, trigger of loss event are changing from ‘point-in-time exposure’, ‘injury-in-fact’ to…?

- …..Higher Operational Risks, Financial Exposure, complicated life!....leading to….

Clients: Successful risk planning will result in successful blame transfer as well

Operational Risks

Basel Committee: “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.” (excludes strategy, reputation, systemic risk, but includes legal risk)

- Internal Fraud – Fidelity/Crime covers
- External Fraud/Acts – Computer Crime/Cyber/Data Security covers
- Employment Practices and Workplace Safety – EPLI/WorkersComp/D&O
- Damage to Physical Assets - Property
- Business Disruption, System Failures – Property/BI/CGL
- Clients, Products and Business Practices – IP and PI
- Execution, Delivery and Process Management - PI

- But the Hassle Committee in board’s of tech firms say “make it easy for Sales to win business but cover risks including strategy and reputation” really?

Operational Risks Sound Practices

- Clear strategies and oversight by the board of directors and senior management
- An appropriately robust internal control and reporting culture
    - Business units and Quality Control
    - Finance
    - Compliance/general counsel/internal audit or other relevant control and oversight functions within the organization.
- Effective planning, policies and processes
    - Operational procedures, SQM manuals, documentation
    - Change control
    - IT/IS management – incidents, resolutions
    - Segregation of duties – check and balance
    - Capacity planning and monitoring
    - Housekeeping - Policies, standards, guidelines, and procedures
    - Compliance

Traditional Risk Offerings

First Party
Property, including Computer Property
Business Interruption

Third Party
PI, Directors' and Officers' Liability
General Liability
Excess Casualty/Umbrella

Typical Coverage Gaps or Issues with Traditional Coverage

- A disgruntled employee programs a logic bomb into the client payroll system, programming it to destroy data two weeks after his or her name is removed from the system.

- Traditional Coverage: Property Insurance (Commercial Property or Computer Property policy)? Crime?

- Coverage may not include intangible data; Coverage may not include intentional acts of employees.

Typical Coverage Gaps or Issues with Traditional Coverage

- A denial-of-service attack is launched against the client's systems, causing a severe degradation of service to their online investment application. End-customers file lawsuits claiming missed opportunities. Let's say owernship of the application and the system is complicated (ASP, leased, in-testing and not accepted)

- Will Client's policies cover it? Will IT Service Provider's Property Insurance (Commercial Property or Computer Property policy) or CGL cover?

- General Liability Coverage may only apply to only those systems within direct ownership or control, or a direct attack against the insured.

Typical Coverage Gaps or Issues with Traditional Coverage

- A professional identity-theft ring hacks into your system and steals customer information and records. Loss of customer confidence combined with possible lawsuits. Cost to notify clients' customers and attendant costs of credit score monitoring.

- Will Client's policies cover it?
- Coverage does not extend to nonproprietary systems and networks?

- Will IT Service Provider's Computer Crime policy cover?
- Coverage applies only to direct financial loss of property?

Typical Coverage Gaps or Issues with Traditional Coverage

- A professional identity-theft ring hacks into your system and steals customer information and records. Loss of customer confidence combined with possible lawsuits. Cost to notify clients' customers and attendant costs of credit score monitoring.

- Will Client's policies cover it?
- Coverage does not extend to nonproprietary systems and networks?

- Will IT Service Provider's Computer Crime policy cover?
- Coverage applies only to direct financial loss of property?

Typical Coverage Gaps or Issues with Traditional Coverage

- A recent worm outbreak infects your entire back office systems, spreading through your network after being introduced via a network connection to the Internet.. Costs to restore network. Possible loss of customer data.

- Will IT Service Provider's Computer Crime policy cover?
- The definition of virus may not include 'machine-to-machine propagation' but rather only covers loss due to the physical introduction or placing of a virus into a system.
- Will contractual terms protect?

Typical Coverage Gaps or Issues with Traditional Coverage

- Customer contracts requires you to provide all supporting IT Applications (pre-existing service provider IP) for free; the software application you designed to offer free online bill presentment and payment service on behalf of your top commercial customers is flawed and fails to execute automatic payment amounts.
- Potential customer lawsuits; loss of customers

- Will IT Service Provider's E&O policy cover?
- Coverage is traditionally only afforded to those services offered for a fee.

- Will contractual terms protect?

Typical Coverage Gaps or Issues with Traditional Coverage

- Regulatory examiners cite violations to prescriptive Gramm-Leach-Bliley security and privacy provisions and file suit against the client's board of directors for failure to fulfill responsibilities as required under the regulation..

- Potential customer lawsuit; indemnification obligations

- Will IT Service Provider's E&O policy cover?
- Regulatory suits and actions may be excluded..

- Will contractual terms protect?

Typical Coverage Gaps or Issues with Traditional Coverage

- You decompile a third party proprietary software that your client asks you maintain and re-engineer. The 3PPS owner joins you in the decompilation or gives client the right to decompile. You buy a competitor of the 3PPS much later.

- 3PPS sues client and you for trade secret misappropriation; indemnification obligations to client

- Will IT Service Provider's E&O policy cover?
- TSM is an excluded risk; Is decompilation 'misappropriation'?
- If 3PPS provides client the right to decompile is the proprietary software a trade secret? Is it valuable?
- Is it a breach of confidentiality (a covered risk in E&O)?
- Can you sue the re-insurer in India?
- Will contractual terms protect?

Typical Coverage Gaps or Issues with Traditional Coverage

- You provide accounting and book-keeping KPO services. You follow your client's instructions but have a catch-all indemnification for compliance with laws applicable to your services and the client's business

- Client is investigated by the tax authority for accounting malpractice and asks you to indemnify for failure to comply with laws

- Will IT Service Provider's E&O policy cover cost of investigation and failure to comply with laws?

Issues for consideration

- An open market – can we buy our liability cover where we like to cover our liability?
- Can we have a foreign choice of law in the policy?
- Can we go past ‘privity of contract’ when the cover is ultimately managed by the foreign re-insurer?