Legal Risk Management

Stanley Greenstein
Stanley.greenstein@juridicum.su.se

A little about myself

- Stanley Greenstein
- BA, LLB Degrees from the University of Cape Town, South Africa.
- Master in Law and Information Technology, Stockholm University.
- Working at the Swedish Law and Informatics Research Institute.
- Presently a Junior Lecturer and Doctoral candidate in law and informatics. Department of Law, Stockholm University.

Plan for today

- Legal Risk Management
  - Theoretical issues
  - In practice – outsourcing/off-shoring contract
  - e.g. Information security
  - Concluding remarks
Why law?

• Avoiding danger
• Humans come into conflict
• Balancing of interests
• Predictability
• Handle change
• Trust
• Modern technology

There is a need to deal with risks
(Need to deal with problems)

Traditional legal strategy

• Reactive/repairing
  – Sanctions e.g. if you do X then your punishment will be Y
  – Restoring e.g. damages, starting point is that something has already happened

Why not avoid instead?

Other sectors
  e.g. transport, medicine, economy, construction

Proactivity

• "Clients prefer to have a fence at the top of a cliff rather than an ambulance at the bottom"

Richard Suskind, "The End of Lawyers"
Risk?

- Some kind of threat or insecurity
- All types of activities
- Can one eliminate a risk?

  - Practice: Minimize or control
  - Which risks can one afford to control
    - Is it worth the price tag?

Risk (cont.)

- International Standards Organization (ISO)
- ISO 31000: 2009
- Principles and guidance on risk management
- Other area specific standards
  - Eg. information security
- “effect of uncertainty on objectives”
- Positive, negative, deviation from the expected
- Event, change in circumstances, consequence

Legal risk?

- Risk is the way to measure the potential or theoretical loss of rights, such as legal proceedings, or unforeseeable acts affected by, inter alia, parties to an agreement or transaction, third parties or by force majeure.
- Risk is the possibility of a future event producing certain negative results, which are not desired by any party which is involved in, e.g., a transaction, contract, carrying on of business, project or legal proceeding. Risk as such can affect the whole or just a part of the object. Such loss might also be a result of changes in applicable legislation, negligence, technical failure or a failure to somehow protect the rights, resources or assets in an adequate manner.

- The law student perspective
Models of identification/classification

- Physical, logical & organizational
- General, processes & information
- Person perspective
- Intentional versus unintentional
- Documentation, legal uncertainty, political

Concept of risk?

- Relative to other concepts

Protection can be described as the process of eliminating risks or minimizing their effects should they occur.

Effect, frequency, cost

<table>
<thead>
<tr>
<th>Effect</th>
<th>Frequency</th>
<th>Cost of repairing damage/avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophy</td>
<td>Very often</td>
<td>Unreasonable</td>
</tr>
<tr>
<td>Critical damage</td>
<td>Quite usual</td>
<td>High</td>
</tr>
<tr>
<td>Considerable damage</td>
<td>Sometimes occurs</td>
<td>Reasonable</td>
</tr>
<tr>
<td>Marginal damage</td>
<td>Very seldom</td>
<td>Low</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Very unusual</td>
<td>Insignificant</td>
</tr>
</tbody>
</table>
Differing environments

- Risks differ depending on the activity
  - Computer programming, security, business administration, government authority etc etc.
- Differ from case to case
- Subjective
  - IT Manager vs Board of Directors
  - Who identifies the risks?
- Intentional risks
  - Business world
  - Law suits

The Risk Analysis

- Good risks – “manufactured/dynamic”
  - Chinese “Dangerous opportunity”
  - may have negative consequences but may also lead to opportunities
  - Should not be avoided
- What is at risk?
  - Property, capital, personnel, data
- What is the risk?
- Is there a need for action?
- Not always size

Calculation

1 Cost of Insurance
2 Administrative cost
3 Cost of prevention
4 Cost of repair
5 TOTAL COST
Legal environment

- Legal work can be described as a process of identifying and handling risks
  - E.g. contract law
  - Established set of rules ensure a risk-free environment
  - Laws foresee a certain degree of risk analysis e.g. "negligence"
  - Ignoring the law is itself a risk
- Public law and Private law
- Law therefore a source of risk and risk control

Some examples

- Some activities require that a multitude of laws be followed
- Secrecy law
- Environmental law
- Family Law
- Criminal law
  - Contravention Arms Act (Blawblaw)
  - sentencing
- Public Authorities
  - ... must identify all possible risks and the cost that this can have to the state
- Contract
  - Sale of Goods Act
  - Purchase a house

Family Law

- Innan ändringen stod det i 6 kap. 2 a § FB att rekvisiten som skulle beaktas när man bedömde barnets bästa var att barnet inte skulle utsättas för övergrepp och att barnet skulle ha en nära och god kontakt med båda föräldrar. Ordalydelsen i nuvarande lagstiftning är att risken för att barnet utsätts för övergrepp måste utredas.

  "...the risk that the child will be abused must be investigated"
Legal environment (cont)

- Proactivity of lawyers
  - Legal risk assessment (identifying the risks)
  - Legal risk control (managing the risks)

Richard Suskind, "The Future of Law"

Methods of identifying risks

- Statistical
- Graphical
- Scenario
- Checklists
- Matrices
- Flow Charts

Statistics/quantitative

😊 Flexible, works in most situations, can get a numerical value, can compare similar activities, delegation possible, generally accepted

😢 Severe risks may have a low frequency and be underestimated, manipulation, psychology, ethics
Graphical

- Several persons within an organization can work with it at the same time, can be developed step by step.
- Difficult to find consensus, difficult to focus, psychology

Graphical cont.

Scenario

- Simulate an incident and its consequences, learn from experience, focus on certain aspects
- Not every situation will be the same
Checklists

 Forces the study of a business activity, forces one to think about the actions to take should a risk occur, flexible, can combine with practical actions, standardization within information security – comprises checklists, easy to understand, all situations

 Presupposes an initial in-depth analysis, tedious

Matrix

several aspects can be combined, beneficial in a situation where there are many suppliers, contractors, regular contracts with many actors

 Time consuming, rigid

Matrix (cont.)

<table>
<thead>
<tr>
<th>Legal person</th>
<th>Authorization</th>
<th>Delay</th>
<th>Error</th>
<th>Pay</th>
<th>Secrecy</th>
<th>Dispute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use org.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supp1</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supp2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supp3</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consult1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consult2</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pub Auth1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pub Auth2</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>client1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>client2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Matrix (cont.)

<table>
<thead>
<tr>
<th>Legal person</th>
<th>Authorization</th>
<th>Delay Error</th>
<th>Pay</th>
<th>Secrecy</th>
<th>Dispute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Own org.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supp1</td>
<td>△</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supp2</td>
<td>△</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supp3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consult1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consult2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pub Auth1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pub Auth2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Method: Risk Matrix

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Very Likely</th>
<th>Likely</th>
<th>Possible</th>
<th>Unlikely</th>
<th>Rare</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insignificant</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>Minor</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Moderate</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Major</td>
<td>VERY HIGH</td>
<td>VERY HIGH</td>
<td>VERY HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>VERY HIGH</td>
<td>VERY HIGH</td>
<td>VERY HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

A practical example: outsourcing

Outsourcing contract

Outsourced services
- India Services
  > back-office
  > customer calls
- "Staywarm" program
  > special type of customer accounts
  > for elderly people and vulnerable customers
Inadequate customer support

V does not provide adequate customer service
P loses customers
P not cooperating with us (V)

Continued loss of customers

Profit

V to provide adequate customer service

Failure to collect debts: “Stay Warm”

V has a different interpretation of Stay Warm responsibilities
V fails to collect debts from Stay Warm customers

Uncollected debts not recoverable (pending change in law)

"Stay Warm"

£11 million loss due to unrecoverable debts

Profit

V to collect debts from Stay Warm customers

Law suit

P terminates outsourcing contract
V sues Powergen

P cannot act based on termination
P has additional costs due to trial

Either party shall take any legal action against the other

P叁lachaeu to seek interim injunction in court

Profit

P cannot act based on termination

Parties allowed to seek interim injunction in court

Profit
Alleged unauthorized data processing in India

Customers learn about this

Loss of customers

Reputation

Profit

V to comply with all legal obligations

Issues

• “Breakdown in the relationship”
  - “P has lost confidence in V”
  - Several (disputed) details of material breach
  - Alleged non-compliance with data protection law
• “It is perfectly possible that the SLAs permit a level of performance which is, objectively, unsatisfactory”
  - “SLAs silent in relation to important aspects of the Staywarm function”
  - “India Services SLA fails to provide the yardstick against which […] performance can be measured”
• Deficient exit strategy?

A practical example: outsourcing/offshoring

Outsourcing contract

Stay warm debt

Unlawful Data processing

"good industry practice"

P’s duties

“Stay warm” Customers
A practical example: outsourcing/off-shoring

Customers

Outsourcing contract

P’s duties

"Stay warm"

Risk matrix

Legal risk analysis

- ...in the context of information security
Data protection

- DIRECTIVE 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Article 17
- Security of processing
- 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
- Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Critical Infrastructure

- Directive 2008/114/EC
- Identification and designation of critical infrastructures and the assessment of the need to improve their protection
- “risk analysis”: consideration of relevant threat scenarios in order to assess the vulnerability and the potential impact or disruption or destruction of critical infrastructure (article 2(c))
  - Communication mechanism to report identified risks (article 5(4))
  - Member State shall report every two years to the Commission generic data on a summary basis on the types of risks, threats and vulnerabilities encountered (article 7.2)
  - Common methodological guidelines for carrying out risk analyses in respect of ECIs may be developed by the Commission in cooperation with the Member States (article 7.4)
  - conduct a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact (Annex II)

Privacy Impact Assessment (PIA)

- General Data Protection Regulation (draft)
- Article 33:
  - Introduces the obligation of controllers and processors to carry out a data protection impact assessment prior to risky processing operations
PIA cont.

- Risks: competitors, natural disasters, cyber attacks, environmental contamination, reputation etc...
- Privacy now poses a risk
- To be addressed within the broader context of risk management
- At an early stage (effectivity)
- Building into design
  - Article 23: Data protection by design and by default, technical standards

PIA cont.

- "Privacy risks"?
- Collection, storage, use and disclosure of personal data
- 2 types of risks:
  - Risks to the individual and risks to the organization
- Identifying privacy solutions
  - Accept the risk, impacts or liabilities (id, document)
  - Avoid the risk (e.g. exclude a technology)
  - Mitigate the risk (destruction of data as soon as possible)

Concluding Remarks

- What is in need of protection?/What is your core competence?
  - R&D, Personal information, Client information, Contracts, Pricing, Etc etc...
- How do we protect these assets?
  - Who are you asking?
  - It costs money
  - Do we even know?
  - Process for process
  - How is the company structured?
  - Transaction intense?
  - IT environment?
  - Structure to take care of incidents?
- The biggest threat is usually from within
  - Who has access to what information
- The threat from outside is increasing
Concluding remarks (cont.)

- Outsourcing contract
- Company
- Cloud computing
- Off-shoring

Further reading...

- "Juridisk Riskanalys"
  - Mot en säkrare juridisk metod
  - Professor Peter Wahlgren, Jure AB, Stockholm, 2003