Cyber risk quantification and insurance
CSP - Risk Assessment and Cyber Insurance Workshop

Brussels, April 2015
Contents:
1. Quantification model
2. Company perspective
3. Insurance perspective
4. Society perspective
High level overview cyber risk quantification model

Collection of models jointly determines parameters for probability model

Requirements for quantification model:

**Generic applicability** – allows for comparability and additivity

**Ease of interpretation** – allows for expert judgment

**Based on measurable events** – full data available in principle

**Scalability and fractality** – possibility to make explicit outside relations

**Modular building blocks** – multiple components each easier to solve

**Causal and logical** – reduced dependency on historic data

The quantification model developed by Deloitte under the World Economic Forum contains the components depicted on the right:

**Probability model** – determines breach rates per hacker-company pair

**Global threat model** – outside-in cyber threat intelligence

**Hacker model** – behavior and activity per hacker type

**Attack model** – identifies attack types and characteristics

**Asset & Loss model** – expected loss given successful attack

**Security model** – identifies resilience per attack type and surface

**Company model** – identifies company attractiveness
Probability model – process structure
Attractiveness and resilience determine breach probability distribution

Model structure below is mapped to a stochastic model to allow for quantification on a probabilistic basis

Description of states (1) in probability model
1. Hackers arrive in non-criminal assessment
2. First initial foothold / breach furthers assessment
3. Upon detection, security response enabled
4. If hacker has sufficient control, attack ensues
5. Detected attacks trigger response capabilities

Hacker entry point description (→)
1. Cyber threat determines hacker arrival rate
2. "Sleeper" hackers may by-pass entry barriers
3. Attacks directly from outside bypass barriers
Hacker model – behavioral model for hackers

In order to have a model that is the more comprehensive and general as possible, and to be able to take into account any kind of threat, we aim to describe the most common hacker types by introducing 4 main dimension or attributes:

Goal: main goal that hacker aims for, determines attack types and timescales
- **Theft** ↔ **Disruption**

Determination: uniqueness of the targeted asset to hacker, sets hacker perseverance
- **Opportunistic** ↔ **Targeted**

Skill: quality and types of attack to breach and circumvent resilience, determines detection rates and loss rates
- **Simplistic** ↔ **Sophisticated**

Organization: level of hacker organization and coordination, scaling skill and time
- **Individual** ↔ **Coordinated**

For each of the dimensions introduced above, there is a monotonic link to the parameters in the probability model. In addition, the hacker model combined with the Attack model determines:

- Asset type(s) targeted per Hacker type
- Attack type(s) used per Hacker type
- Capacity to assess vulnerabilities per Attack type for a given company
High level process flow of Asset & Loss model

1. Vulnerabilities uncovered
2. Access resulting from vulnerabilities
3. Expected loss given successful attack

- Assessment time
- Attack type
- Existing vulnerabilities
- Segmentation
- Asset size per type
- Asset type targeted

- Hacker model
- Security model
- Company model

© 2014 Deloitte The Netherlands
Asset & Loss model

Vulnerabilities uncovered determine acquired level of access to assets and loss

- For the purpose of the model, we distinguish three types of assets
  - Tangible assets (e.g. money in electronic bank accounts, control over physical assets)
  - Intangible assets (e.g. intellectual property, intelligence)

- The loss distribution for each asset type is modelled in four steps
  1. Vulnerabilities uncovered by hacker
  2. Access provided through vulnerabilities
  3. Expected loss given successful attack
  4. Expected loss given hacker behavior (based on the probability model)

- Given the resulting probability distribution per hacker type the total exposure for a given company can be estimated, including implications from changes in relevant trends
## Data model

High level description of resulting (complex) data model

<table>
<thead>
<tr>
<th>Value</th>
<th>Cyber resilience</th>
<th>Cyber threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Business value</td>
<td>- Prevention</td>
<td>- Warfare</td>
</tr>
<tr>
<td>- Recovery</td>
<td>- Detection</td>
<td>- Terrorism</td>
</tr>
<tr>
<td>- Insurance</td>
<td>- Response</td>
<td>- Espionage</td>
</tr>
<tr>
<td>- Compliance</td>
<td></td>
<td>- Criminality</td>
</tr>
<tr>
<td>- Legal X</td>
<td>X</td>
<td>- Activism</td>
</tr>
<tr>
<td>- Data</td>
<td>- People</td>
<td>- Target</td>
</tr>
<tr>
<td>- Devices</td>
<td>- Process</td>
<td>- Speed</td>
</tr>
<tr>
<td>- Applications</td>
<td>- Systems</td>
<td>- Sophistication</td>
</tr>
<tr>
<td>- Services</td>
<td></td>
<td>- Scale</td>
</tr>
<tr>
<td>- Structure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Traffic X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Contents:
1. Quantification model
2. Company perspective
3. Insurance perspective
4. Society perspective
Cyber risk dashboard context

State of the art dashboard requires state of art components

Deloitte dashboard components

Cyber threat intelligence (CTI)

Cyber risk dashboard displays:
- Exposure to cyber risks based on
  - Cyber risk threat levels
  - Cyber security levels
  - Plotted against Risk Appetite
  - Resulting in cyber Value at Risk

Cyber risk framework

Cyber security analytics

Cyber risk quant model

Company input

- Cyber risk vision
- Cyber risk appetite
- Threat scenarios
- Cyber risk control data
- Incident data

Result

- Cyber ecology secure
- Cyber security efficient
- Cyber security effective
- Cyber risk managed

© 2015 Deloitte The Netherlands
Schematic overview cyber risk dashboard

Value at Risk depends on combination of resilience and threat levels

Conceptual components cyber risk dashboard
(see appendix for sample dashboards)
Contents:
1. Quantification model
2. Company perspective
3. **Insurance perspective**
4. Society perspective
Cyber insurance model
The outside-in perspective

- **Total cyber exposure**
  - Portfolio cyber risk model
  - **Correlated scenarios / value chain analysis**
    - Threat scenarios including correlated scenarios
  - CTI

- **Company cyber exposure**
  - Company cyber risk model
  - **Questionnaire**
    - Assessment
    - Scaling parameters
  - Cyber threat
    - Company incident data (optional)
  - **Cyber value**
    - Ins. cover
    - Cyber assets
  - **Cyber resilience**
    - Questionnaire
    - Assessment
    - Scaling parameters
  - **Cyber assets**
  - **Cyber liabilities**
Diversification is key ingredient for insurance.

Independence is source of diversification (in probabilistic sense).

Benefit from diversification shared between insurer and insured.

Cost (operational and capital) may not outweigh benefit!

For cyber risk this independence is threatened by:
- Scaling of threat medium combined with
- Behavior of threat actors (alignment) and
- Interdependence of underlying value chains

Resulting high correlations and heavy tails (catastrophe risk) extremely hard to predict (no data).

Business case for insurance may be at risk requiring countermeasures:
- Exclusion of tails from terms and conditions (hard to define and not competitive)
- Information sharing (ISAC), integrated security and emergency responses (CERT)
- Collaboration with other business (expertise) and government (conditions)
Contents:
1. Quantification model
2. Company perspective
3. Insurance perspective
4. Society perspective
Cost impact to society from cyber threats

Cyber threats stemming from, criminals, nations, terrorists, activists, etc. are undesired by-effect of scalability ICT solutions.

Key components of cost to society:
• Frictional costs resulting from delayed investments, diminished trust, increased governmental interference, etc.
• Resources spend on cyber resilience
• Direct losses resulting from attacks
• Indirect costs resulting from attacks (loss competitive advantage, reputational damage, etc.)
• Recovery costs after an attack
• Potential future losses (prob x impact / capital buffers)

Emerging innovations like “internet of things”, artificial intelligence, etc. may be limited by prohibitive costs of cyber security. Security needs to become embedded in design while layers of protection would break undesired by-effect of scaling for cyber threats.

Based on Coase theorem we may expect to collectively deal with these negative externatilities, even without central regulator.
However, also paradigm shift taking place on the role of information and conditions to allow for information assymmetry.
Value of insurance to society

Intrinsic scaling

Potential for insurance against cyber risk is great, however:
- Only US market sizable – primarily given legal system
- European market knows friction from privacy controls
- Risks still largely unquantified, with little reliable data available
- Insurers may be buying market share at expense of future insolvency / defaults in case of cyber catastrophe

What we need is
- Breaking of scaling of threats by multi-layered protection (involving public, business and government)
- Further development of cyber resilience approaches
- Maturing cyber risk management approaches
- Common threat intelligence sharing platforms
- Cyber insurance for diversification of residual risk to optimize business climate
Maarten van Wieren PhD.
Senior Manager
Risk Services
Email: mvanwieren@deloitte.nl
Phone: + 31 6 8201 9225