Security risk management in a business context
Erik Wisløff, CISA, CISM
Group Risk, Telenor ASA

1st Dutch Workshop in Information Risk Management
University of Twente - 31st June 2007

Roadmap

1. Context:
   - About Telenor

2. Perspective:
   - Business and security risk management

3. Case:
   - An IS-division’s approach to risk management

Voiced opinions are mine, not necessarily those of Telenor
123 million mobile subscriptions

Subscription figures in millions - 100% figures for all companies

Telenor’s mobile world

Norway
Telenor 100%

Denmark
Sonofon 100%

Sweden
Telenor 100%

Hungary
Pannon 100%

Montenegro
Promonte 100%

Serbia
Telenor 100%

Austria
One 17.5%

Ukraine
Rykyltar 56.5%

Russia
VimpelCom 29.9%

Pakistan
Telenor Pakistan 100%

Bangladesh
GrameenPhone 62.0%

Thailand
DTAC 73.2% (*)

Malaysia
Digi 61.0%

*Economic exposure
Social responsibility

- Customers shall be confident that the Group conducts business in an ethically responsible manner
- Investors expecting high standards of social commitment shall prefer Telenor
- Employees shall be proud of the way in which the Group manages its social responsibilities

A commercial business creates value

Value creation = (profit * growth) @ risk
Security should support value creation

- Defend value creation, e.g.
  - Safeguard assets, protect against crime
  - Protect against loss of reputation by security incidents

- Bolster the business model, e.g.
  - Trusted systems as default
  - Trustworthy systems when required
  - Be socially responsible

---

Risk is two-sided.
Security and business managers are not.

Risk

- The chance of something happening that will have an impact on objectives.

Risk Management

- Culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.
Business driven security risk management

Value creation = (profit * growth) @ risk

Security risk management *is* difficult

- **Utility:**
  - Who foots the bill?
  - Who reaps the benefits?
  - Who shares what with whom?

- **Time line:**
  - Who decides the time line?

- **Responsibility:**
  - Who treats the risk?
  - Who owns the risk?
Achieving business driven security is “easy”

- Business determines system objectives
  - Business model
  - Security policy
- Perform system wide security risk management
  - Risk assessment during system development
  - Risk treatment according to policy
- Aggregate across all business areas/divisions
- Assess risk exposure in context of external environment
- Iterate...

Can you standardize security risk management?

- What is "the system"?
- When is security required?
- Where to apply security?
- Why bother?
- Who cares?
- How to implement policy?
- Is it profitable to all?
You can standardize (some) concepts

- "Risk" as a **negative** concept, e.g.
  - Risk is the chance of a loss or a negative experience

- "Risk" as a **neutral** concept, e.g.
  - Risk = probability * consequence

- "Risk" as a **positive** concept, e.g.
  - Risk is the chance of a gain or a positive experience

You **can’t** standardize risk perception

- Some parameters that determine how I perceive risk
  - Have I chosen to undertake the risk?
  - Do I have prior experience with the risk?
  - Am I in control?
  - Are children involved?
  - What’s in it for me?
  - Is my primal brain in control?
You can standardize simple models

- Risk = f(event, probability, impact)
  - Impact is a non-zero value
  - 0 < probability < 1
  - Functions: additive, multiplicative

You can’t standardize complex models

- Risk = f(event, probability, impact, perception, time, actor)
  - Associative functions
  - Communicating the risk defines the risk
  - My opportunity is your threat
  - A threat today → an opportunity tomorrow
A particular standard for a particular model

Telenor’s Risk Management Process is a generic process based on AS/NZS 4360:2004

State your goals Assess risks Decide risk strategy Implement strategy Monitor the results

Communicate throughout
Risk assessment is a generic *activity* within the risk management process

Security risk management in a business context

- Security management requires input
  - Business goals
  - Security policy
  - Actor perspectives, perceptions and objectives
  - System description, timeframe

- Risk assessments are crucial
  - Understanding risk exposure
  - Treatment suggestions
  - Fostering action → dynamics
Desired risk assessment output 1:  
*Risk map*

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high gain</td>
<td>O2</td>
</tr>
<tr>
<td>High gain</td>
<td></td>
</tr>
<tr>
<td>Medium gain</td>
<td>O1, O3</td>
</tr>
<tr>
<td>Moderate gain</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td>T2, T7</td>
</tr>
<tr>
<td>Occasional</td>
<td>T1, T8, T3, T6</td>
</tr>
<tr>
<td>Intermittent</td>
<td></td>
</tr>
<tr>
<td>Frequent</td>
<td>T4</td>
</tr>
</tbody>
</table>

Desired risk assessment output 2:  
*Recommended treatments*

<table>
<thead>
<tr>
<th>ID</th>
<th>Recommended / planned treatment</th>
<th>Target effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Desired risk assessment output 3: 

**Foster action**

Action = f(motivation, commitment, anticipation)

Collate security risk from all areas
Consider objectives and environment

“The business”

- Operations
- Sales
- Human resources
- Information systems
- External environment

Treat risk and/or update security policies

“The business”

- Operations
- Sales
- Human resources
- Information systems
- External environment
Case: IS division of Telenor Nordic

Security risk management embedded in a business driven change management process
Update risk registers

Aggregate
Example: summary portfolio risk report

Portfolio xyz

<table>
<thead>
<tr>
<th>Assessment themes</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Specific assessment pr theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology – access control</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Regulatory – Contracts</td>
<td>☑</td>
<td>NA</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Personnel – Management/Organization</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Finance – Market/Customers</td>
<td>☑</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Total per system</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>

Some learning points

- Understand how value is created and costs are shared
- “Good enough” is better than perfect in a business setting
- Timing and perspective does matter
- Risk communication is crucial
  - Don’t be a scare monger; be factual, speak in plain language
  - Visualize risk exposure
  - Recommend a course of action – but the decision maker decides
Static vs. dynamic security risk management

- Risks are a threat ↔ Risks are opportunities
- Do things the right way ↔ Do the right thing
- Make a secure system ↔ Make a profitable system

A business focussed security risk manager

- Understands the business
  - Customers: what are their needs
  - Business model: Sharing costs and gains
  - Dynamics: timing, actors, objectives

- Understands the value chain
  - Assets: Protect that which needs protection
  - Actors: Perspectives, needs, mental models

- Understands the system
  - Goal: Trusted or trustworthy
  - Policy: Static or dynamic
Security isn’t about risk avoidance, it’s about risk management

(Microsoft techNet, November 2000)

Thank you

Erik Wisløff, CISA, CISM
Telenor ASA, Group Risk
erik:wisloff () telenor;com

No aspirations → no risk
No risk → no security requirements