The CORAS method for security risk analysis

ESSCaSS 2008
NODES Tutorial

28/8-08

Heidi E. I. Dahl
SINTEF
Norwegian research group with 2000 employees from 55 different countries

More than 90 percent of our earnings come from contracts for industry and the public sector, and from project grants from the Research Council of Norway

Research divisions

- Health Research
- Technology and Society
- ICT
- Materials and Chemistry
- Building and Infrastructure
- Marine
- Petroleum and Energy

SINTEF Foundation

Limited companies
SINTEF ICT
> Cooperative and Trusted Systems
> Quality and Security Technology

- Model based security analysis
- Model driven security architecture
- Trust management
- Tools for analysis and documentation
- Empirical research on methods and tools to build secure systems

- Security risk analysis – CORAS
  - Method
  - Language (textual syntax, semantics, calculus)
  - Usability and Security
Outline

- Security risk analysis
- An example driven introduction to the CORAS method
- CORAS resources
The example

- A PhD student is worried about losing the work she has done on her thesis.
- The Big Corporation funding her work is worried that sensitive business information will reach its competitors.
- They decide to do a security risk analysis to determine whether the risk level is acceptable.
Why do we analyse security risks?

- Asset, something of value
- Vulnerability
- Threat
- Reduced risk level

Constitutes a security risk

We need to introduce security mechanisms
75 % of all sensitive data losses are caused by human error

Taking Action to Protect Sensitive Data,
IT Policy Compliance Group, 2007
Deliberate threat → Risk → Asset

Analyst

Decision maker

Security expert
System developer

BC security expert

SINTEF researcher

BC thesis advisor

Ann

System user

SINTEF researcher

Ann

Decision maker

Security expert
System developer

BC security expert
The CORAS method

Model based method for security risk analysis that provides

- a customized graphical language for threat and risk modelling
- a diagram editor
- detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis

CORAS

- has been developed through both empirical investigations and a series of industrial field studies (projects financed by the Norwegian Research Council and the EU)
- is based on international standards for risk management (e.g. AS/NZS 4360:2004)
The standard analysis process

from the Australian Risk Management Standard
AS/NZS 4360:2004
Elements of the analysis

Analysis context

Vulnerability

Threat

Unwanted incident

Asset

Target

Risk

Treatment

Likelihood

Consequence
The CORAS method

1. Introduction
2. High level analysis
3. Approval
4. Risk identification
5. Risk estimation
6. Risk evaluation
7. Risk treatment
Introductory meeting

→ Introduce the analysis method
→ Gather information from the client about the target of analysis and the desired focus and scope.

→ Decision makers
→ Technical expertise (optional)
Introductory meeting – Agenda

- A short introduction to CORAS
- The client presents the target of analysis
- A discussion of the focus and scope of the analysis
Client’s presentation of target

- Ann Onymous
- PhD student in Computer Science
- Uses data from Big Corporation (BC)
- Works in her office at the university and at home

At the university
- Shares an office with another PhD student
- Works on laptop in docking station
- Wired internet

At home
- Lives with her boyfriend
- Brings her laptop home with her or uses shared computer
- Wireless internet
Focus and scope

The focus of the analysis is data security, in terms of business sensitive data from BC and the PhD thesis itself.

The scope is data security at home and at work. We do not consider risks involved in transporting the data.
Output from the introductory meeting

- Informal description of the target
- Necessary system documentation
  - Contract between Ann and BC
  - IT security guidelines at the university
  - Security measures in place at home and at the university
  - A sketch of Ann’s work habits
- A short statement of the focus and scope of the analysis
High-level analysis

→ Ensure that the analysts and the client have a common understanding of the target of analysis
→ Determine the assets that will focus the analysis
→ Get an overview of the client’s initial concerns

→ Decision makers
→ Technical expertise
High-level analysis – Agenda

- The analysts present a description of the target of analysis
- The client corrects errors and misunderstandings
- Asset identification
- High-level analysis
System description

Home computer

- Check email
- Internet browsing
- Trying new software
- File sharing
- Writing PhD thesis

Ann

Boyfriend

High level analysis
Asset identification

We use an asset diagram to model the parties involved in the analysis, which assets they want to protect, and whether harm to one asset may cause harm to any of the others.
## High-level analysis

<table>
<thead>
<tr>
<th>Who/what is the cause?</th>
<th>How? What may happen? What does it harm?</th>
<th>What makes this possible?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ann</td>
<td>Deletes the thesis by mistake</td>
<td>No backup</td>
</tr>
<tr>
<td>Laptop</td>
<td>Crashes and the last hours’ work is lost</td>
<td>Old laptop</td>
</tr>
<tr>
<td>Hacker</td>
<td>Gains access to business sensitive information and sells it to competitor</td>
<td>Lack of security at home</td>
</tr>
</tbody>
</table>
Output from the high-level analysis meeting

- Asset diagram
- Preliminary list of unwanted incidents
Approval

→ Arrive at an approved target description
→ Decide which risk levels are acceptable for each asset
→ Decision makers (important)
→ Technical expertise
Approval – Agenda

- The target description and assets are approved by the client
- Consequence scales
- Likelihood scale
- Risk evaluation criteria
## Likelihood scale

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>rarely</td>
</tr>
<tr>
<td>2</td>
<td>sometimes</td>
</tr>
<tr>
<td>3</td>
<td>regularly</td>
</tr>
<tr>
<td>4</td>
<td>often</td>
</tr>
</tbody>
</table>
# Consequence scale

Consequence
(PhD thesis and Business sensitive information)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>harmless</td>
</tr>
<tr>
<td>2</td>
<td>moderate</td>
</tr>
<tr>
<td>3</td>
<td>serious</td>
</tr>
<tr>
<td>4</td>
<td>catastrophic</td>
</tr>
</tbody>
</table>
Risk matrix

<table>
<thead>
<tr>
<th></th>
<th>rarely</th>
<th>sometimes</th>
<th>regularly</th>
<th>often</th>
</tr>
</thead>
<tbody>
<tr>
<td>harmless</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>moderate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>serious</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>catastrophic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(PhD thesis and Business sensitive information)
Output from the approval meeting

- Approved target description
- Likelihood and consequence scales
- Risk matrices
Risk identification

→ Create an overview of the risk picture, i.e. how threats may exploit vulnerabilities to cause unwanted incidents that cause damage to the assets.

→ Technical expertise
→ Users
Risk identification – Agenda

→ Model risks in threat diagrams
Modelling risks in threat diagrams

We use threat diagrams to model threats, what we fear they may do to our assets, how it happens and which vulnerabilities makes this possible.
What are the threats?

- Hacker
- Ann
- Home computer
- Business sensitive information
- PhD thesis
What do we fear will happen?

- Competitor uses business sensitive information strategically
  - Business sensitive information is published in national newspaper
    - All work on thesis is lost
      - A day’s worth of work on the thesis is lost
  - Business sensitive information
    - PhD thesis
    - A day’s worth of work on the thesis is lost

Hacker
Ann
Home computer
How does it happen?

- Boyfriend runs file sharing application on home computer
- Boyfriend shares folder with business sensitive information
- Hacker gains access to Ann’s laptop
- Hacker copies all data from laptop
- Hacker deletes all files in “My documents”
- Spyware crashes computer
- Computer components fail
- Competitor uses business sensitive information strategically
- Business sensitive information is published in national newspaper
- All work on thesis is lost
- A day’s worth of work on the thesis is lost
- PhD thesis
- Business sensitive information
- $
Which vulnerabilities makes this possible?
Risk estimation

- Estimate the current risk level
- Decision makers
- Technical expertise
- Users
Risk estimation – Agenda

→ Assign likelihoods to each unwanted incident
→ Assign consequences to each impact relation
Assigning likelihoods and consequences

Competitor uses business sensitive information strategically [rarely]

Business sensitive information is published in national newspaper [rarely]

Risk estimation
Assigning likelihoods and consequences

- Hacker deletes all files in "My documents" [rarely]
- Spyware crashes computer [sometimes]
- Computer components fails [rarely]

All work on thesis is lost [sometimes]
A day's worth of work on the thesis is lost [sometimes]

Risk estimation
Risk evaluation

→ Evaluating which risks are acceptable and which are not.
→ Give an overview of the risks.

→ Decision makers
Risk evaluation – Agenda

- Enter the risks in the risk matrix
- Summarize the risk picture in risk diagrams
## Are the risks acceptable?

### Risk matrix (PhD thesis and Business sensitive information)

<table>
<thead>
<tr>
<th></th>
<th>rarely</th>
<th>sometimes</th>
<th>regularly</th>
<th>often</th>
</tr>
</thead>
<tbody>
<tr>
<td>harmless</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>moderate</td>
<td></td>
<td></td>
<td>A day’s worth of work on the thesis is lost</td>
<td></td>
</tr>
<tr>
<td>serious</td>
<td></td>
<td>BS info is published in national newspaper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>catastrophic</td>
<td>Competitor uses BS info strategically</td>
<td>All work on thesis is lost</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Summarizing the risk picture

- We use risk diagrams to show how threats pose risks to the assets.

Risk estimation

<table>
<thead>
<tr>
<th>Threat</th>
<th>Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>(deliberate)</td>
<td></td>
</tr>
<tr>
<td>(accidental)</td>
<td></td>
</tr>
<tr>
<td>(non-human)</td>
<td></td>
</tr>
</tbody>
</table>

Risk
Risk diagrams

- R1: Competitor uses business sensitive information strategically
- R2: Business sensitive information is published in national newspaper
- R3: All work on thesis is lost
- R4: A day’s worth of work on the thesis is lost

Risk estimation

- Business sensitive information
- PhD thesis
Risk treatment

→ Getting an overview of potential treatments of the unacceptable risks.

→ Decision makers
→ Technical expertise
→ Users
Risk treatment – Agenda

→ Add treatments to the threat diagrams
→ Add treatments to risk diagrams
Adding treatments to the threat diagrams
What can we do to reduce the risks to an acceptable level?

- Boyfriend runs file sharing application on home computer
  - Complicated file sharing preferences

- Hacker gains access to Ann’s laptop
  - Hacker deletes all files in "My documents" [rarely]
  - Ann installs software that contains spyware on her laptop

- Computer components fail [rarely]
  - Spyware awareness course
  - Old components

- Spyware crashes computer [sometimes]
  - No backup of thesis files

- Business sensitive information is published in national newspaper [rarely]
  - Restrict sharing on home computer

- All work on thesis is lost [sometimes]
  - Do regular backups of thesis files

- Business sensitive information
  - Install firewall
  - Ann
  - Hacker

- Ann’s boyfriend
  - Home computer
  - ICT
Risk treatment

R1: Competitor uses business sensitive information strategically

- Ann's boyfriend
- Hacker

R3: All work on thesis is lost

- Ann
- Home computer
- Spyware awareness course

Do regular backups of thesis files

Restrict sharing on home computer

Business sensitive information

PhD thesis

Install firewall

Restructuring overview diagram

Treatment overview diagram

ICT
Executive summary

- The focus of the security risk analysis is data security, in terms of business sensitive data from BC and the PhD thesis itself.
- The scope is data security at home and at work. We do not consider risks involved in transporting the data.
- The unacceptable risks that were uncovered were
  - R1: Competitor uses business sensitive information strategically
  - R3: All work on thesis is lost
- In order to reduce the risks to an acceptable level, the following treatments were suggested:
  - Restrict sharing on home computer
  - Install firewall
  - Spyware awareness course
  - Do regular backups of thesis files
Resources: http://coras.sourceforge.net/

**Downloads**
- The CORAS diagram editor
- The CORAS icons (Visio stencil, PNG, SVG)

**Publications:**
Questions?

Heidi E. I. Dahl
heidi.dahl@sintef.no