Corus Information Security Group

Risk Assessment in practice
Presentation at the TU-Twente (2007-05-29)
Peter van Boxtel

The Corus Way
Value in steel
Introduction

The situation 40 years ago:

- Risk assessment was not an issue
- Only in the chemical labs, regarding explosions
- The first lecture had to do about explosions

- Students like to try it out
Introduction

Development in the threats:
From:
• Fun
• Challenge

To:
• Professional use
• Criminal
Introduction

Computer developments:
In 1967
• The era of computers was approaching
• Big legacy systems (IBM, salary, banks etc)
• Process control (design HSM-2, PDP)
• Computer threats were related to trust, fraud and physical threats

To now:
• Modern use
• Networks
• Computer threats are a wide scope of issues, especially regarding networks and access
Corus is an international metals group that manufactures, processes and distributes metal products and provides related services in design, technology and consultancy.

Corus has manufacturing operations in many countries with major plants located in the UK, the Netherlands, Germany, France, Norway and the USA.

Corus also has sales offices and service centres all over the world.

Corus is organised into four divisions and employs about 45,000 people.

Corus is part of the TATA steel division.
Company Profile

Steel producers (1 - 10)

- Mittal (Global)
- Nippon Stel (Japan)
- POSCO (South Korea)
- JFE (Japan)
- Tata Steel (India)
- SBGC (China)
- USS (USA)
- Nucor (USA)
- RIVA Group (Europe)
- ThyssenKrupp (Germany)
Company Profile

Key markets

- Construction: 32%
- Automotive: 19%
- Manufactured goods: 22%
- Packaging: 13%
- Other: 14%
Company Profile

Employees by Region

- UK: 54%
- NL: 25%
- GE: 10%
- USA: 2%
- BE: 2%
- FR: 3%
- Other: 4%
AND DON'T BE BACK TOO LATE. ROMANS CAN WAIT, BUT ROAST BOAR CAN'T.
Risk Assessment

Fundamentals:

• Business is leading
• Business Impact is related to the business processes
• IT systems and networks are supporting business processes
• Security controls in balance with impact regarding the supported business processes
Risk Assessment

Information Security is about:

• Confidentiality
• Integrity
• Availability
Of
• Information
• Information systems
• Networks
• Applications
• Operational processes
Risk Assessment

Steps in Risk Assessment:
• Business Impact assessment
• Continuation?
• Threat and vulnerability assessment
• Control assessment
• Action plan
Risk Assessment

Business Impact assessment

• Evaluate with a questionnaire which impact a breach in security will have regarding:
  • Confidentiality
  • Integrity
  • Availability
• Questionnaire is based on a general document but sometimes dedicated for a special topic.
• If no issues are detected the assessment can be stopped and no special measures have to be taken
• If any security issues is detected next steps are to be performed.
• The results will be documented.
Risk Assessment

Threat and vulnerability assessment

- Evaluate with a questionnaire which threats and vulnerabilities can be detected for the process, application, system etc. regarding:
  - Confidentiality
  - Integrity
  - Availability
- Questionnaire is based on a general document but often we make it dedicated to a special topic.
- Dependent on the probability of the threats the controls have to be defined.
- The results will be documented.
Risk Assessment

Control assessment

• Evaluate with a questionnaire which controls are required to mitigate the threats and vulnerabilities.

• Controls are selected on base of internal and external best practices, general standards (ISO 17799, ISF Standard of Good Practice)

• The importance of the controls is based on a weighing between the probability and the impact of possible breaches.

• When evaluating an existing environment the existing controls are evaluated.

• When evaluating a new environment the defined controls are evaluated.

• For the control implementation a balance will be made of the risk and the costs of implementation of the controls.

• The results will be documented.
Risk Assessment

When to use this (1)? ISRAC

- For a complete system in a design phase we use an automated tool: ISRAC for the organisation InfoSecure
- Tool is based on the SPRINT (ISF) structure with a BIA, TVA and a LOC
- The controls are based on the ISO 17799
- Detailing the controls is evaluated in the process.
- The systems documents and reports.

- Some screen-prints following:
Imagine that an employee leaves to join a competitor and takes business information with him. Or because of an error everyone (including people outside the organisation) has free access to our data. The following questions focus on the consequences of problems regarding the confidentiality of data.

- C.1 Competitive disadvantage
- C.2 Direct loss of business
- C.3 Public confidence
  - If information is disclosed, what damage could there be to customer confidence, public image, or shareholder or supplier loyalty?
- C.5 Staff morale
- C.6 Fraud
- C.7 Additional costs
The availability of data may be very vital for the processes and the organisation. But there are several threats for the organisation to degrade availability. The following questions focus on the possible threats regarding the availability of data in the process or the organisation. Decide to what extent this could be possible in the organisation. Consider the situation without any specific measures. The controls are to mitigate these threats. If it is daily practice or frequent situation use “probably”, if it is impossible use “impossible”. Else choose a level between.

<table>
<thead>
<tr>
<th>Question</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1 Major disasters</td>
<td></td>
</tr>
<tr>
<td>A.2 Inadequate IT contingency arrangements</td>
<td></td>
</tr>
<tr>
<td>A.3 Inadequate business continuity plans</td>
<td></td>
</tr>
<tr>
<td>A.4 Day-to-day system outages and systems threats</td>
<td></td>
</tr>
<tr>
<td>A.5 Unforeseen demand/volume</td>
<td></td>
</tr>
<tr>
<td>A.6 Denial of Service</td>
<td></td>
</tr>
<tr>
<td>A.7 Back-office failure, transaction delays</td>
<td></td>
</tr>
</tbody>
</table>

In many cases where a newly built web-application is integrated with legacy back-office applications, the availability rate of the web-part is far higher than that of the back-office link. In some circumstances, this may result in users entering transactions on the website, that are not processed correctly by the back-office.
Risk Assessment

Assessment - NewCo \ Business Unit 1 \ Department 1 \ Logistics (business risk assessment) ...

11.1 Business requirement for access control

Objective:
To control access to information.

Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements.

Access control rules should take account of policies for information dissemination and authorization.

11.2 User access management

Objective:

<table>
<thead>
<tr>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>? 11.1.1 Access control policy</td>
</tr>
<tr>
<td>? 11.2.1 User registration</td>
</tr>
<tr>
<td>? 11.2.2 Privilege management</td>
</tr>
<tr>
<td>? 11.2.3 User password management</td>
</tr>
<tr>
<td>? 11.2.4 Review of user access rights</td>
</tr>
<tr>
<td>? 11.3.1 Password use</td>
</tr>
<tr>
<td>? 11.3.2 Unattended user equipment</td>
</tr>
<tr>
<td>? 11.3.3 Clear desk and clear screen policy</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
</tbody>
</table>

**Overall score:** 5.44
# Risk Assessment

## 11. Access control

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Weight</th>
<th>Control Presence</th>
<th>Control Score</th>
<th>Evidence</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control policy</td>
<td>401.00</td>
<td>45%</td>
<td>180.45</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User registration</td>
<td>236.00</td>
<td>55%</td>
<td>129.80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privilege management</td>
<td>85.00</td>
<td>45%</td>
<td>38.25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User password management</td>
<td>202.00</td>
<td>45%</td>
<td>90.90</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review of user access rights</td>
<td>227.00</td>
<td>55%</td>
<td>124.85</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password use</td>
<td>224.00</td>
<td>45%</td>
<td>100.80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unattended user equipment</td>
<td>157.00</td>
<td>45%</td>
<td>70.65</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear desk and clear screen policy</td>
<td>31.00</td>
<td>65%</td>
<td>20.15</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>User authentication for external connections</td>
<td>11.00</td>
<td>55%</td>
<td>6.05</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of system utilities</td>
<td>28.00</td>
<td>55%</td>
<td>16.28</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Session time-out</td>
<td>12.00</td>
<td>55%</td>
<td>6.60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limitation of connection time</td>
<td>12.00</td>
<td>55%</td>
<td>6.60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information access restriction</td>
<td>59.00</td>
<td>55%</td>
<td>32.35</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Teleworking</td>
<td>279.00</td>
<td>65%</td>
<td>181.38</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Total weight:</strong></td>
<td>1961.00</td>
<td><strong>Total:</strong></td>
<td>1011.05</td>
<td>29%</td>
<td></td>
</tr>
</tbody>
</table>

## 12. Information systems acquisition, development and maintenance

- Sector score: 5.16
- Sector weight: 1.00
Risk Assessment

When to use this (2)? ISF Survey

- For periodical evaluation of the Corus Security level we participate in the ISF biannual survey
- This survey that follows the ISF SOGP is done for:
  - Security Management
  - Critical Business Applications
  - Computer Installations
  - Networks
  - Systems Development
  - End User Environment
- It is a benchmark with other organisations
- It gives a clear view of the quality of the security status and the related risks.
- The results are reported by ISF.
## Status: Received

**Overall Security Rating: 2.81**

Warning: All Security Ratings are calculated at question level. Consequently, the rating for an Area is an average rating for all questions in that Area rather than an average of all Sections in that particular Area.

<table>
<thead>
<tr>
<th>Area or Section</th>
<th>Security Rating</th>
<th>All questions answered?</th>
</tr>
</thead>
<tbody>
<tr>
<td>AREA UE1 LOCAL SECURITY MANAGEMENT</td>
<td>2.33</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE11 Roles and responsibilities</td>
<td>2.47</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE12 Security Awareness</td>
<td>2.82</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE13 User Training</td>
<td>2.17</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE14 Local Security Co-ordination</td>
<td>2.88</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE15 Information Classification</td>
<td>1.10</td>
<td>Yes</td>
</tr>
<tr>
<td>AREA UE2 CORPORATE BUSINESS APPLICATIONS</td>
<td>3.47</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE21 Access Control</td>
<td>2.87</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE22 Application Sign-on</td>
<td>3.22</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE23 Change Management</td>
<td>3.96</td>
<td>Yes</td>
</tr>
<tr>
<td>AREA UE3 DESKTOP APPLICATIONS</td>
<td>3.73</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE31 Inventory of Desktop Applications</td>
<td>3.73</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE32 Protection of Spreadsheets</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Section UE33 Protection of Databases</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Section UE34 Desktop Application Development</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>AREA UE4 COMPUTING DEVICES</td>
<td>2.64</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE41 Workstations</td>
<td>3.36</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE42 Hand-held Devices</td>
<td>3.45</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE43 Portable Storage Devices</td>
<td>1.69</td>
<td>Yes</td>
</tr>
<tr>
<td>AREA UE5 ELECTRONIC COMMUNICATIONS</td>
<td>2.48</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE51 General Controls</td>
<td>2.67</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE52 Email</td>
<td>2.19</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE53 Instant Messaging</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Section UE54 Internet Access</td>
<td>3.80</td>
<td>Yes</td>
</tr>
<tr>
<td>Section UE55 Use of Voice over IP (VoIP)</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Section UE56 Wireless Access</td>
<td>1.27</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Risk Assessment

When to use this (3)? All kind of specials

• Evaluate the level of trust with third parties
  • A small business Impact questionnaire
  • A third party questionnaire about required controls for their access

• Evaluate the need for improvement actions in applications
  • A small business Impact questionnaire
  • Ranking of the urgency for repairs

• Evaluate the need for business continuity and Disaster recovery requirements
  • A small business Impact questionnaire
  • Ranking of the urgency for DRP measures
Risk Assessment

Conclusions

- A very practical approach
- Adapt the questionnaires if possible
- Make questionnaires not bigger than necessary: people get bored
- Give guidance: see if staff is completing it seriously and does not stick in details
- Give feedback
- Evaluate always in relation to the business consequences: don’t start a discussion about some Euro’s in the process of the mills