TeliaSonera CERT CC
(TS-CERT CC)

Jimmy Arvidsson
TeliaSonera - in brief

• Result of a merger of the Swedish incumbent Telia AB and Finnish incumbent Sonera Corporation in December 2002
• 2008 net sales USD 15.7 billion
• Approx. 32,000 employees
• Market capitalization approx. USD 21 billion*
• Largest shareholders - Swedish state (37.3%) and Finnish state (13.7%)

• More than 453 million population
  Total number of subscriptions almost 128 million
  – of which ~40 million in the majority-owned operations
  – and ~88 in the associated companies

* As of February 10, 2009
Corporate Security Governance

External influences

- Legal requirements
- Regulatory demands
- Social responsibility

Internal influences

- Vision & Values
- Business strategies
- Customer requirements

Corporate Security Policies, Standards and Guidelines

Setting the rules
Facilitate compliance
Monitor and correct

Policy and process owner

Compliance and control

- Fraud Management
- Products & offerings security
- Network & Technology Security
- Corporate Safety & Security
- Security Incident Handling
- Risk & Crisis Management

Facilitating role

Security Centers

Common Service Portfolio
Group common delivery in Sweden, Finland, Norway, Denmark and Lithuania

TS-CERT

HO CSO

Head SD

Mobility

Head SD

Broadband

Head SD

Eurasia

subCERTs
Security areas

Security Incident Management
Risk Management
Crisis Management

Products & Offerings Security
Fraud Management

Corporate Safety & Security

Network & Technology Security
SIH Area Steering Documents (Internal Control)

Corporate Security Policy

Corporate Information Security Policy

Information Security Classification Model

Corporate Security Guideline Security Incident Management

Appendix: Security Incident Organization

Supporting Security Control in Security Incident Handling: Operational Level Agreement of SubCERT

SubCERT only

Appendix: Accreditation of Investigation Teams

Code-of-Ethics (CoE)

CSIRT Code-of-Practice (CCoP)

Instructions: Handling Security Incidents

Instructions: Security Incident Handling

Instructions: Post-Mortem Analysis
Security Delegation Agreement

SDA structure for incident management

- CSO
- Steering of incident handling
- C&C
- Security Centre
- CERT function
- Local agreements with BA
- SDA 1
- SDA 2
- SDA 3
- Policy
- Guideline
- Instructions
- CSIRT Sweden
- CSIRT Finland
- CSIRT Denmark
- CSIRT Norway
- Incident handling system HITS

Microsoft Word Document
Guideline Security Incident Handling

- Targets all Investigation Teams
  - IT-security (TS-CERT, subCERTs and abuse teams)
  - Fraud investigation teams
  - Information security investigators
  - External investigators as national police, insurance companies and approved 3rd party

- Sets the rules on team members, team leaders and team owners via OLA

- Accreditation of Investigation teams and members

- Follow up annually
Pre-requisites for SubCERT in TeliaSonera

- **OLA agreement**
  - Purpose and goal (formally decided by management)
  - Constituency (field of operations) and Demarcations
  - Roles and responsibilities
  - Reporting
  - Staffing and financing
  - Co-operation

- **Signing Code-of-Ethics and CSIRT Code-of Practice**

- **Procedures**
  - Triage
    - Taxonomy (talking about the same things)
    - Definition of Severity Levels
    - First Actions (stop and contain, dead/live system?)
  - Escalation Procedures
  - Incident Tracking System
  - E-mail templates, Report templates, Incident Flows

- **Training**
- **Follow up**
Contact Information:
Jimmy Arvidsson
TeliaSonera AB
Corporate Security
TS-CERT CC
SE-123 86 Farsta
Sweden

E-mail: jimmy.arvidsson@teliasonera.com
Phone: +46-8-504 52889
PGP Keyid: