- Information sharing-

Does it really work?

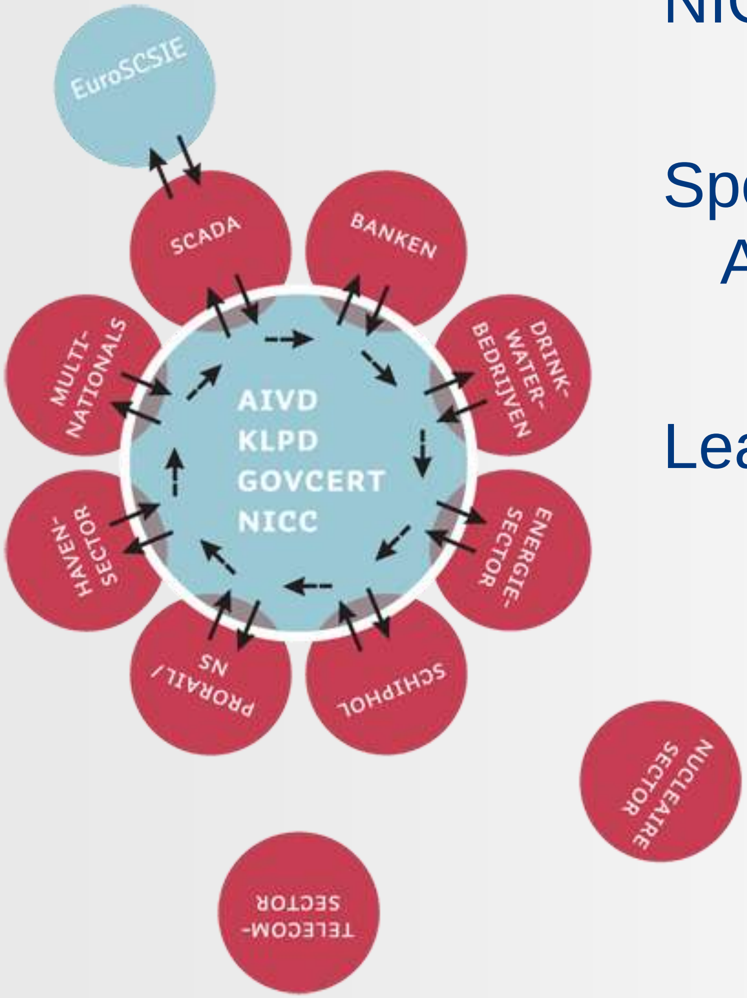
Amsterdam 17 March 2010

Dr. Wim Hafkamp CISSP LL.M. (Chair FI-ISAC)

Agenda

- FI-ISAC.NL
  - Participants
  - Operational framework
  - Deliverables
- Stakeholder issues related to information sharing
  - The formal world vs informal world
  - Different goals
- Threats and Trends
- FI-ISAC Europe, next steps

NICC



NICC = National Infrastructure (against) CyberCrime

Sponsored by Dpt. of Economic Affairs

Learning by doing

- Key factors:
- Trust
- Value

Operational framework

- 8 meetings a year
  - Open and closed sessions
- Max. 2 participants per member (senior IT security/ fraud experts)
- NICC guidelines
  - Proven effort
  - Non disclosure agreement
  - Traffic light model
- Information Exchange via e-mail, factsheets and during meetings
- Additional services
  - Threat monitor, Malware monitoring service (CMIS++)

TLP

- Red: on going incidents, information with potential PI-damage, information from secret services
  - Verbal, not recorded during meetings
- Yellow: information that is meant for further distribution within the bank or the (ICT) service provider
  - Confidential, not top secret
  - Anonymized
  - Distributed via closed FI-ISAC listserver
- Green: no rules for disclosure

FI-ISAC.NL

Members:

ABN AMRO

ING

Fortis

Rabobank

SNS Reaal

BNG

Van Lanschot Bankiers

Achmea Staalbankiers

Friesland Bank

Financial Sector (core infrastructure):

NVB (NL Bankers' Association)

Equens

Swift

DNB (not as supervisor)

Currence

Government:

KLPD

AIVD

GOVCERT.NL

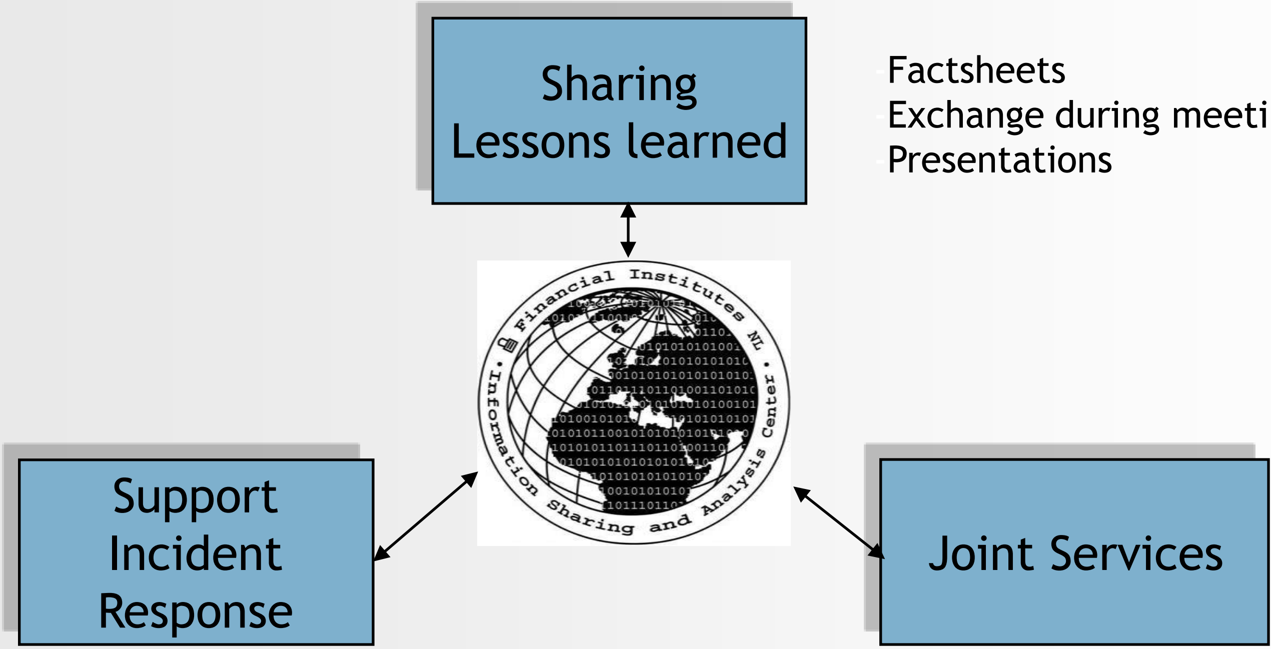
NICC

NVB Nederlandse Vereniging van Banken

3 pillars

Rabobank

Goal: learning from others



Sharing Lessons learned
Financial Institutes NL
Information Sharing and Analysis Center
Support Incident Response
Joint Services

- Factsheets
- Exchange during meetings
- Presentations

- Risk Analysis
- Notice-and-Takedown
- AUSCert listserver

- Cybercrime monitor and Investigation Service ++
- Information Threat Monitor

ISAC ≠ CERT

Why we do not want to share information !

- Sharing of operational data is ‘not done’

  ➔ Chain of evidence

  ➔ Privacy data
- How reliable is the information?
- Can I trust the information receiver?
- What happens with my information after the distribution?

  ➔ Company reputation!
- Is it our duty to exchange information?

Why we have to share information !

- Get after or scare the criminals➔ AA2007-casus
- Sharing modus operandi really prevents incidents from happening
- One voice to the outside world (‘3Xkloppen’campaign) ➔ reputational profit !
- Helps to set priorities and…….
- ….. It saves money (CMIS++)

enisa European Network and Information Security Agency

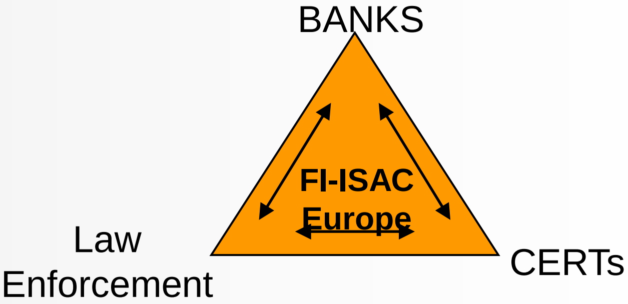
Information sharing good practice guide

Upcoming threats

- Organized High Tech Crime
  - Sophisticated attacks on internal infrastructures?
  - Physical attacks on internetbanking customers?
  - Malware, malware, malware….will it ever stop?
- Data Leakage
  - Cloud computing?
  - Teleworking?
  - Social media?
- Attacks on mobile banking apps?
- EMV-related exploits?
- Other threats……?

Expanding the FI-ISAC IE outreach

- Towards a European FI-ISAC
  - November 2008 first meeting in Budapest
  - Spring 2009 2nd meeting in Amsterdam
  - 3rd meeting in November that year in Bern
  - Next meeting is scheduled for spring 2010 in Helsinki
  - Sponsored by ENISA
  - Model more or less the same model as in NL
    - However situation varies per country
    - Politics play a role and of course the level of trust….
  - Main question: who wil co-ordinate/facilitate this European initiative?



NVB Nederlandse Vereniging van Banken

Q & A

Rabobank

w.h.m.hafkamp@rn.rabobank.nl