NVB Nederlandse Vereniging van Banken



National Infrastructure against Cybercrime
A public private partnership

Dr. Wim Hafkamp CISSP LL.M.

Rabobank / Chair FI-ISAC.NL

NVB Nederlandse Vereniging van Banken

Cybercrime Information Exchange



NICC = National Infrastructure (against) CyberCrime

Sponsored by Dpt. of Economic Affairs

Learning by doing

- Key factors:
- Trust
- Value

NVB Nederlandse Vereniging van Banken

Trust is key

- Trust and value grow together but need investment
- Flourishes in small groups, same members. It is personal
- Participation is voluntary, but not free of obligations
- Strict information sharing protocol (TLP) is important to build trust

Building trust takes time!

NVB Nederlandse Vereniging van Banken

Key success factors

- The Network works
- Raising awareness (information)security, also on management level
- Added value for all participants
- Only successful if all participants contribute
- No contribution = no participation
- Voluntary but not without obligations
- Trust as foundation for information sharing
- Flywheel necessary to keep the network going. Permanent input of content is needed!

NVB Nederlandse Vereniging van Banken

Summary

The success factors of the Information Exchange

- Trusted environment
- Continuity
- Impartiality
- Driven by the demands and needs of the sectors
- Government as facilitator
- Secure ICT infrastructure
- Value for every party involved
- Flexibility in its implementation
- Contribution of information from governmental organizations
- Focus on cybercrime and ICT security
- Specification and streamlining of the analysis function
- Acts as the flywheel
- Cross-sector exchange
- International network

NVB Nederlandse Vereniging van Banken

Operational framework FI-ISAC

- 8 meetings a year
  - Open and closed sessions
- Max. 2 participants per member (senior IT security 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++)

NVB Nederlandse Vereniging van Banken

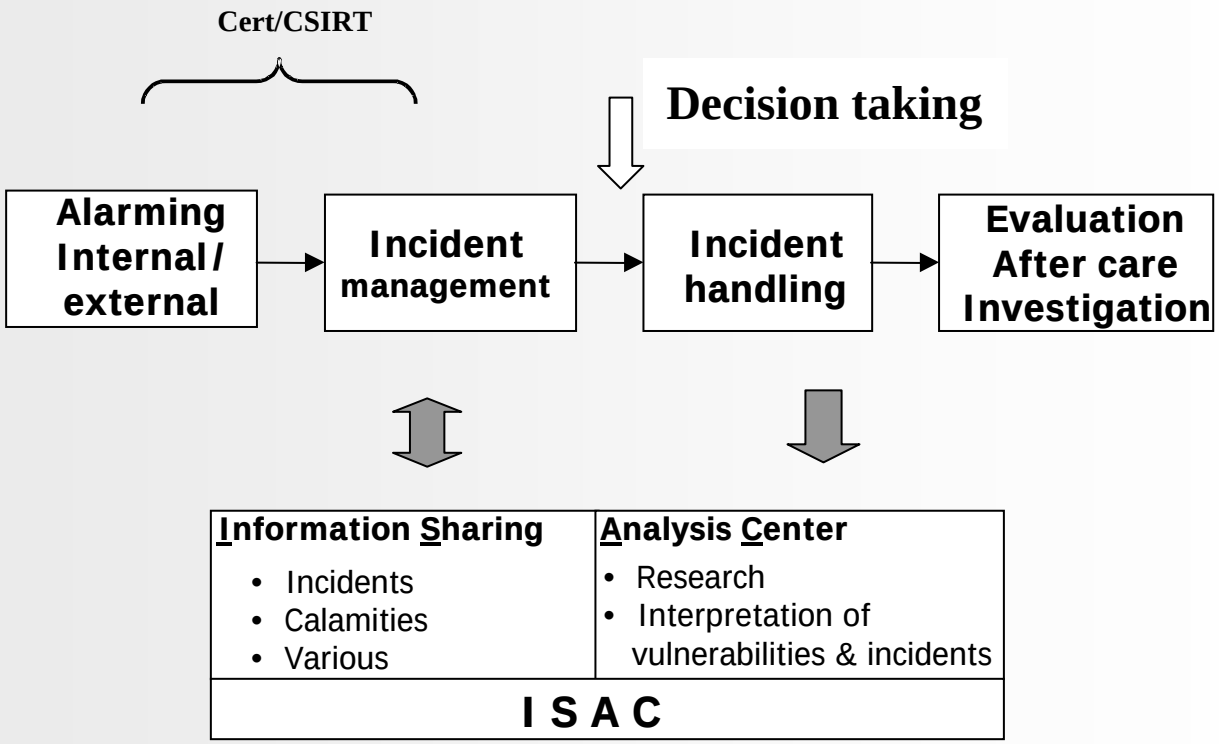
Traffic light model

- 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



NVB Nederlandse Vereniging van Banken

ISAC ≠ CERT



NVB Nederlandse Vereniging van Banken

FI-ISAC

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

DNB (IT)

Currence

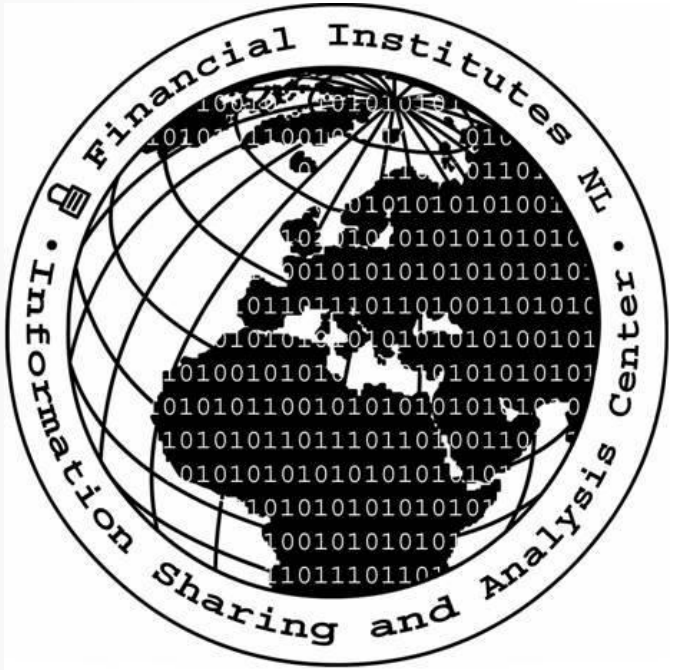
Government:

KLPD

AIVD

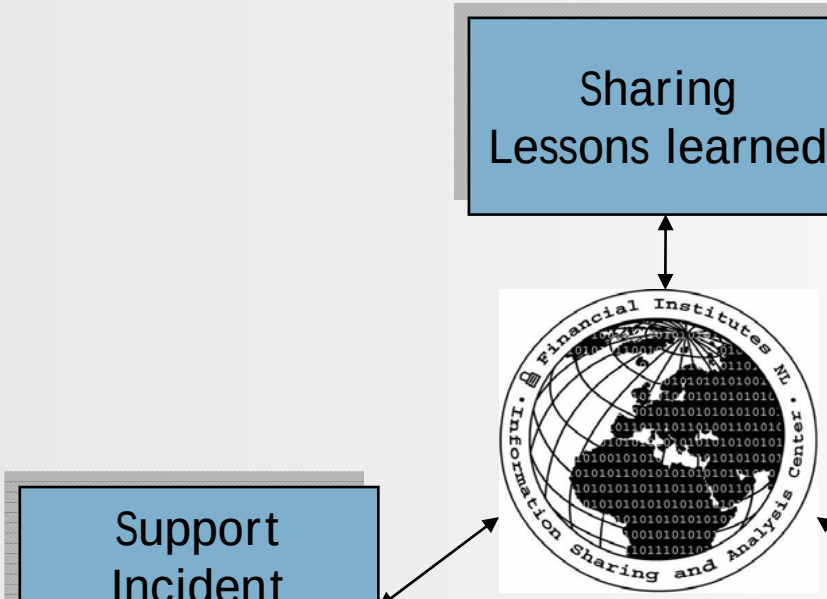
GOVCERT.NL

NICC



NVB Nederlandse Vereniging van Banken

3 pillars



Factsheets
Exchange during meetings
Presentations

- Notice-and-Takedown
- AUSCert listserver

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

NVB Nederlandse Vereniging van Banken

Factsheets

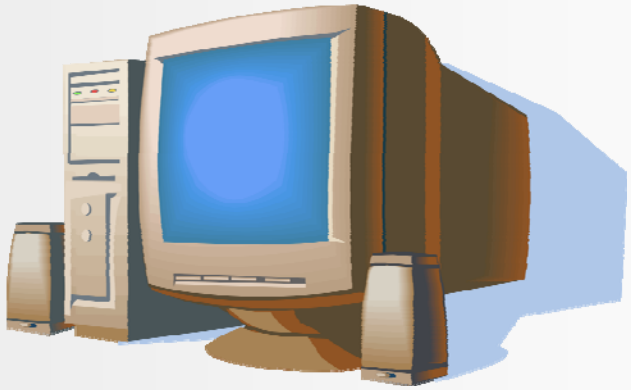
MIFARE CLASSIC VULNERABILITY

MIM ATTACK (FIREFOX)

Two factor identification/ authentication

PHISHING

MALICIOUS CODE & SPYWARE



DNS-spoofing

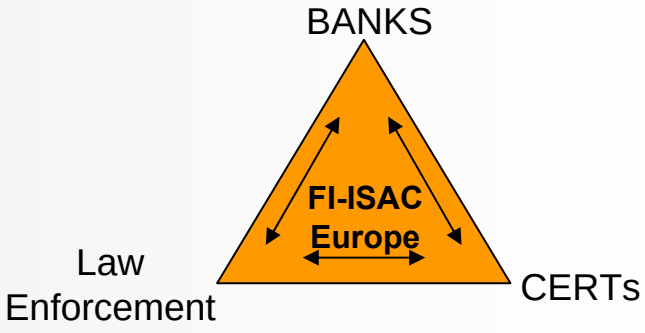
DDOS-attacks

CROSS SITE SCRIPTING

NVB Nederlandse Vereniging van Banken

Expanding the FI-ISAC IE outreach

- Towards a European FI-ISAC
  - November 2008 first meeting together with CERT-Hungary, Switzerland and some twelve other countries
  - Sponsored by ENISA
  - 20-21 April 2nd meeting in Amsterdam
  - 3rd meeting planned for November (in Bern)
  - Model more or less the same 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

Questions

