CYBERSECURITY - BUILDING A RELIABLE CHAIN

ISACA Round Table Eindhoven, 16 November 2016

Sandra Konings, Partner BDO Advisory - Cybersecurity
Chair Eindhoven Cyber Security Group

BDO

Supply chain security risks

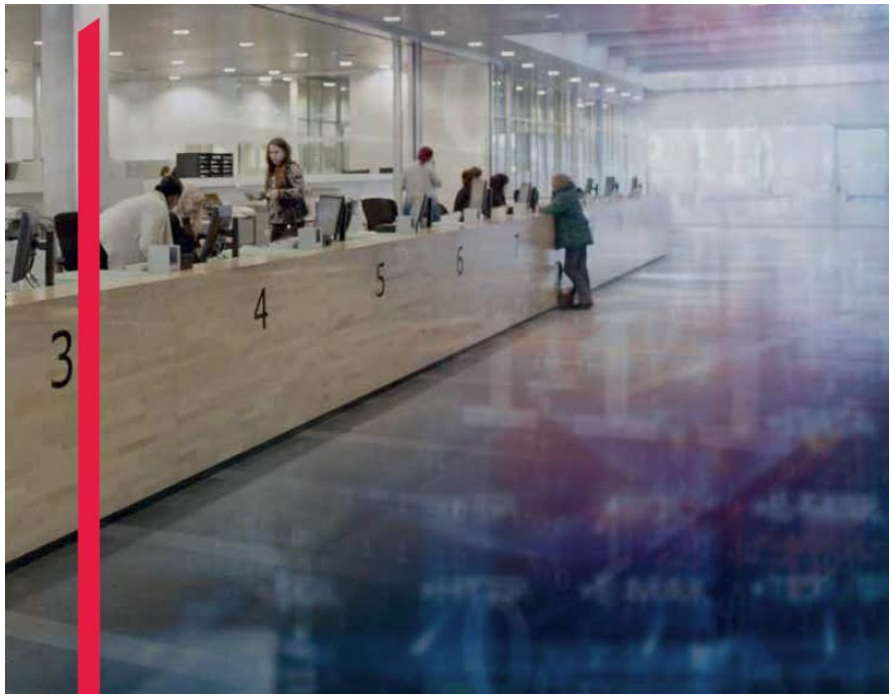
Data protection risks

- Leakage of sensitive customer/supplier information
- Leakage of your sensitive information, like
  - Privacy sensitive information
  - Intellectual Property
  - Financial figures before press release

BDO Investigation local government / cities

Recent developments

- Cities buy healthcare for citizens
- Cities need data to proof legality of bought healthcare
- Many cities request too much data to ensure proper control -> *privacy issues!*
- Cities and healthcare companies have to formalize their information exchange in Data Processing Agreements

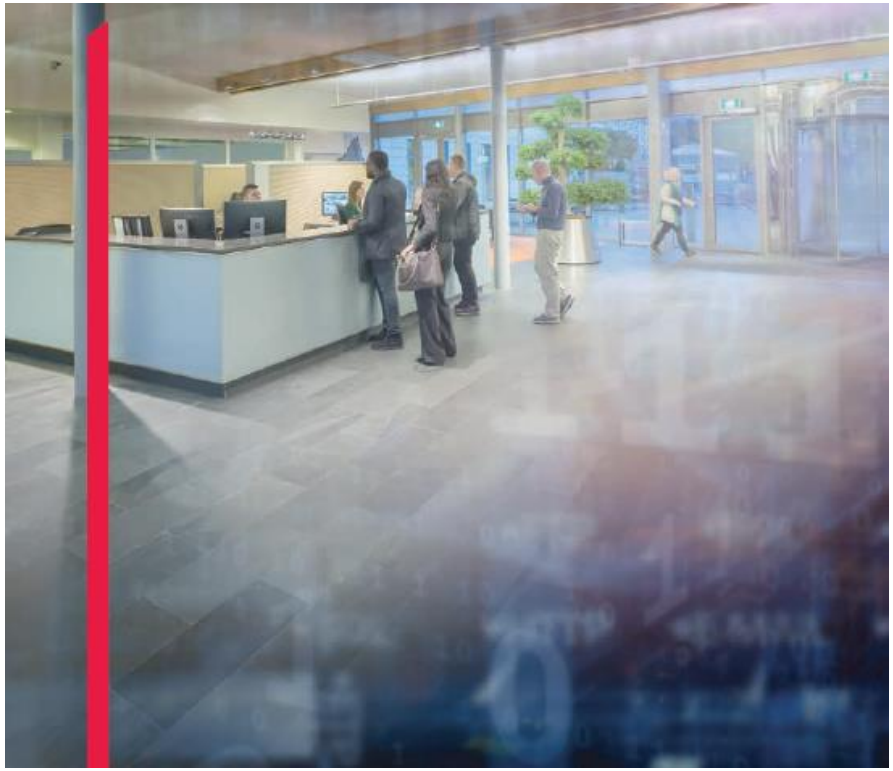


This report can be downloaded from https://www.bdo.nl/nl-nl/branches/lokale-overheid/informatiebeveiliging

BDO Investigation housing corporations

Recent developments

- Housing corporations receive an increasing number of data from their tenants
- Many do not know how the responsibility for data protection has been arranged within the organization and with external parties



This report can be downloaded from https://www.bdo.nl/nl-nl/branches/woningcorporaties/informatiebeveiliging

Supply chain security risks

Data protection risks

- Leakage of sensitive customer/supplier information
- Leakage of your sensitive information, like
  - Privacy sensitive information
  - Intellectual Property
  - Financial figures before press release

Denial of Service risks

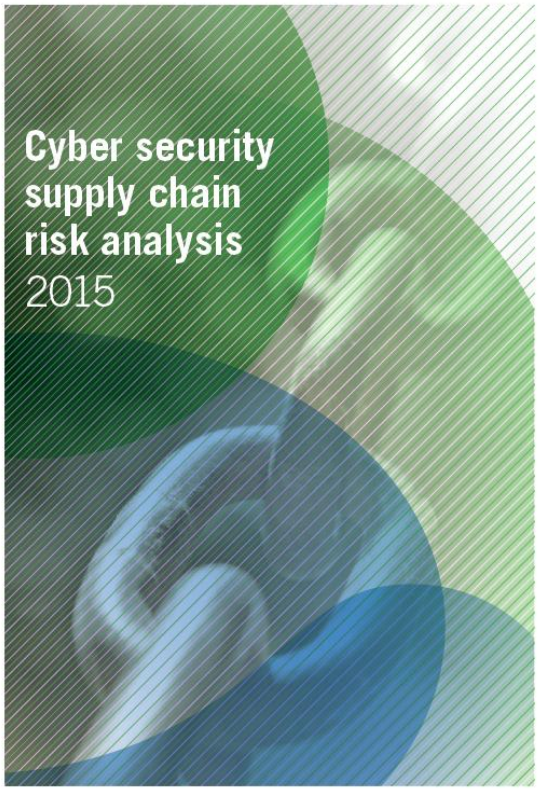
- Denial of service key IT systems
- Factory downtime leading to delayed delivery

Cybersecurity supply chain risk analysis

Developed in 2015 by
Shelll, Gasunie, Nuon, TenneT and Alliander
With NCSC and ‘Cyber Security Raad’

Key objectives:

- Define cybersecurity risks for energy supply
- Define method re-usable for other industries



https://www.cybersecurityraad.nl/010_Actueel/digitale-ketenveiligheid-krijgt-veel-te-weinig-aandacht.aspx

Supply chain security risks

Data protection risks

- Leakage of sensitive customer/supplier information
- Leakage of your sensitive information, like
  - Privacy sensitive information
  - Intellectual Property
  - Financial figures before press release

Denial of Service risks

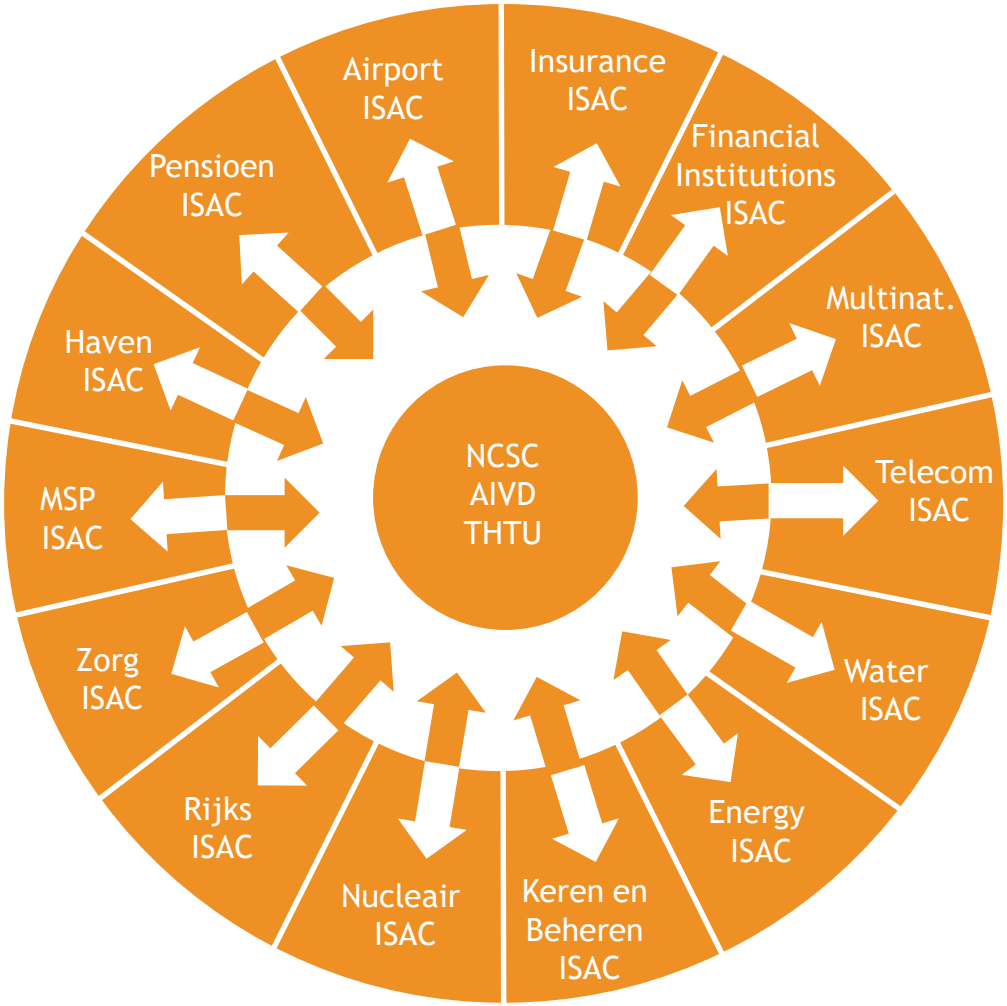
- Denial of service key IT systems
- Factory downtime leading to delayed delivery

Malware infection risks

- Inherited malware

Cooperation initiatives

Information Sharing & Analysis Centres (ISACs)



Topics like

Sharing Incidents/ best practices

Legal aspects of Cyber

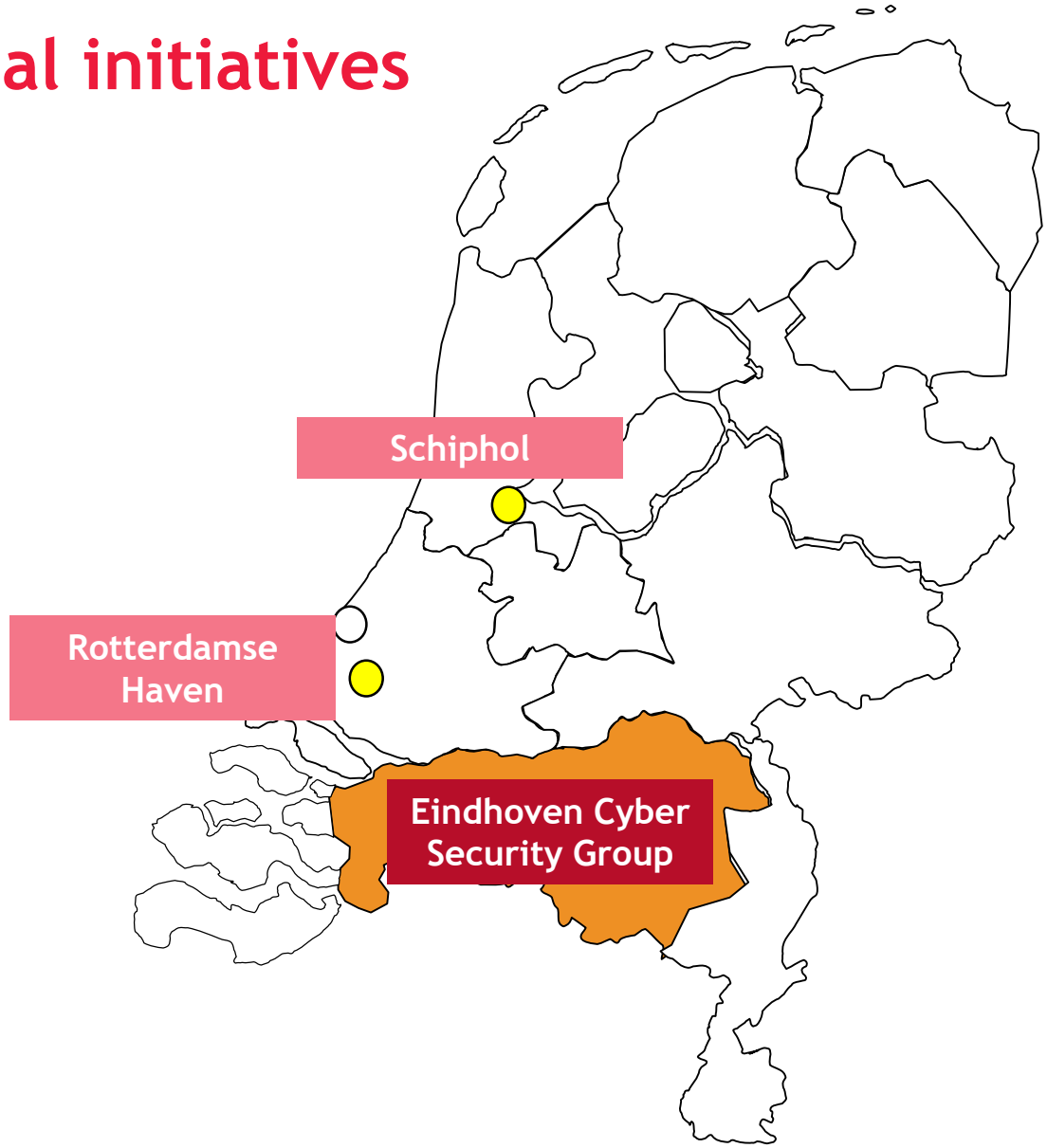
IP Protection, IAM

SOC, SIEM, Threat Intelligence

Cyber Insurance

Awareness

Local initiatives



EU Directive on security of network and information systems

Directive on security of network and information systems(NIS)

European Commission

This Directive was adopted by the European Parliament in July 2016
It is in force since August 2016

Key objectives

- Increasing cybersecurity capabilities and cooperation
- Making the EU a strong player in cyber security
- Mainstreaming cyber security in EU policies

Purpose of NIS: Legal measures to boost the overall level of cybersecurity in the EU

1. Member States must be prepared via
   - Computer Security Incident Response Team (CSIRT)
   - Competent national NIS authority

2. Member States must co-operate via
   - Cooperation groups
   - A CSIRT Network

3. Sectors which are vital for our economy and society and rely heavily on ICT must create a culture of security
   - Such as energy, transport, water, banking, financial market infrastructures, healthcare, digital infrastructure, and digital service providers (search engines, cloud computing services and online marketplaces)
   - Operators of essential services must take appropriate security measures to notify serious incidents to the relevant national authority

NIS Directive – Next steps

This Directive is in force since August 2016

Member States have

- 21 months to transpose the Directive into their national laws, and
- 6 months more to identify operators of essential service

Translation to Dutch law

- The House of Representatives ('Tweede kamer') has adopted the law about cybersecurity on 27-Oct-2016
  - Critical sectors have to report severe security incidents to NCSC
  - Critical sectors are: electricity, gas, nucleair, drinking water, telecom, transport (mainports Rotterdam and Schiphol), finance and government
- Currently waiting for approval by Senate ('Eerste kamer')


For more information and support

Cybersecurity – Building a reliable chain
More information and support

Sandra Konings
Partner BDO Advisory – Cyber Security
Chair Eindhoven Cyber Security Group

Email: sandra.konings@bdo.nl
Phone: +31 (0)30 284 9960