De bullshit bingo van cyber security en compliancy

Joris den Bruinen

Security Congres, 7 oktober 2025

HSD
securitydelta.nl

1. Context of growing cyber threats: 2020

HSD
securitydelta.nl

Context van groeiende cyber dreigingen

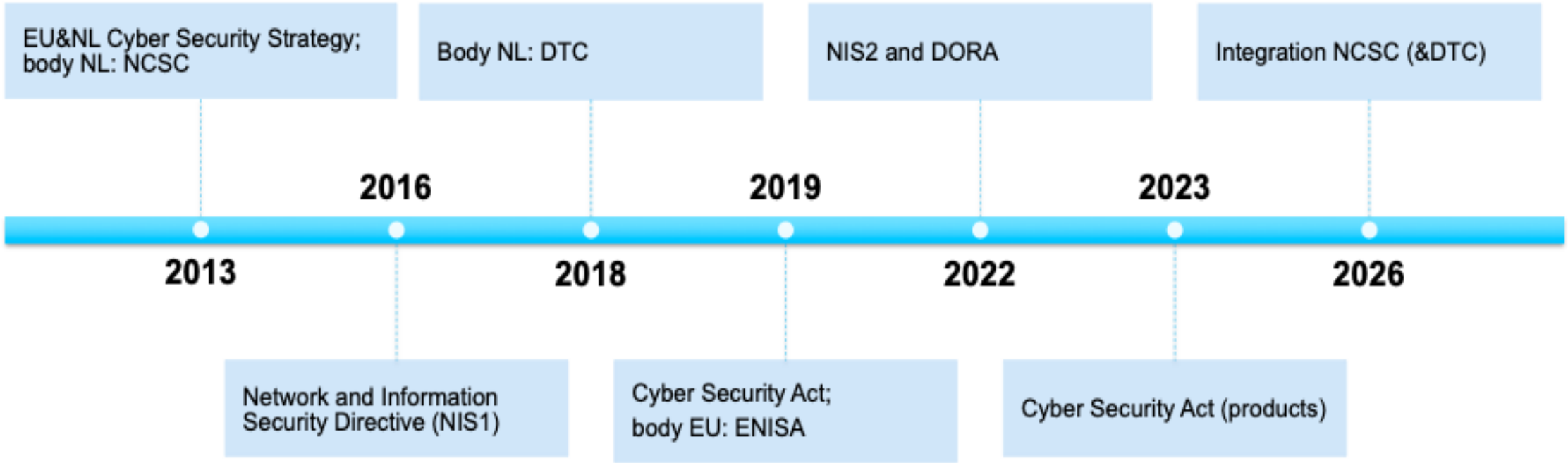
Verwacht het onverwachte - dreigingslandschap

- Situaties in Oekraine, Israel, China, Taiwan VS -> staat gerelateerde aanvallen
- Attractief business model voor criminelen:
  - Ransomware betaling wereldwijd boven de 1 miljard
  - 84% verhoging in 2023 en verwachting verdriedubbeling naar 2030
- Technologische dreigingen:
  - Verhoging van aanvalsvlakte door kwetsbaarheden in de keten, IT/OT
  - Misbruik via AI, bijvoorbeeld genAI maakt phising makkelijker en beter

Top cyber incidenten in Nederland: gamechangers

1. DigiNotar: valse uitgifte certificaten websites wereldwijd, bedrijf failliet
2. KPN Hack: verouderde software, 17 jarige jongen veroordeeld
3. Mearsk – APM terminals: 1/3 Rotterdamse haven plat
4. ASML attack/insider threat: mogelijk verlies intellectueel eigendom
5. Ransomware attack VDL familie bedrijf maakindustrie
6. Log4j software vunerability: open source software als stukje in andere software
7. Bakker Logistics attack: keten consequentie -> help: geen kaas!
8. Hof van Twente: aansprakelijkheid eindgebruiker vs IT leverancier
9. Crowdstike beveiligingssoftware update fout, gevolgen op systemen en fysieke wereld
10. Defensie netwerk ligt plat: kwetsbaarheid en ketenafhankelijkheid
11. Politie hack: gegevens CRM en politieagenten incl ondercovers liggen op straat
12. OM: kantoor automatisering en IT systemen liggen al maanden gedeeltelijk plat
13. Clinical Diagnostics: gevoelige data 750.000 vrouwen bevolkingsonderzoek op het darkweb

New EU/NLs legislation
Milestones in the evoluation of EU CyberSecurity law



The answer of legislation: EU Digital Decade Strategy

Strategy for data:	• Data Act • Data governance act • Regulation on the free flow of non personal data • e-Evidence Regulation
Digital Privacy:	• GDPR • e-Privacy Regulation
Digital Services Package:	• Digital Services Act • Digital Markets Act
AI Strategy:	• AI Regulation • Product Liability Directive • Machinery Regulation

EU Digital Decade Strategy

Cyber Security Strategy:

- Security of Network and Information Systems Directive (NIS2)
- Digital Operational Resilience for the Financial Sector (DORA)
- Cyber Security Act (CSA)
- Cyber Resilience Act (CRA)

Underlying principal of cyber regulations = risk management

Understanding:

- Threats & vulnerabilities
- Organisational goals
- Crown jewels
- Impact (IT & OT and business)
- Confidentiality, integrity and availability

Proof working on:

- Cyber Hygiene
  -> technical, proces, people
- Incident response and Resilience
- Board responsibilty
- Raise cyber security maturity level
- by Plan Do Act Evaluate -> planning&control cycli

Security Delta (HSD)

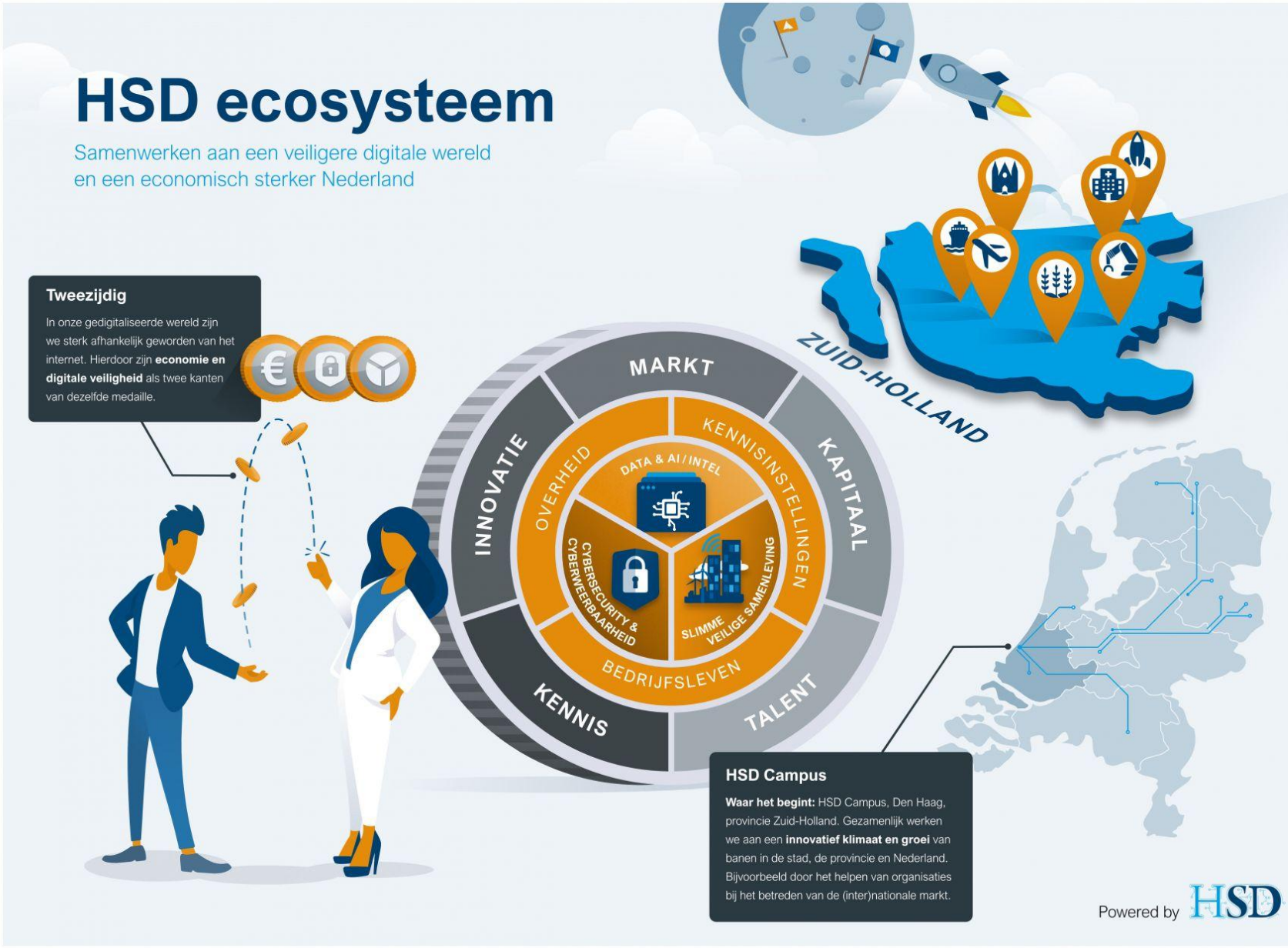
- The Dutch Security Cluster
- Community with 300+ businesses, governments & knowledge institutions
- Non-profit organisation, founded in 2013
- HSD Campus in The Hague

Together we Secure the Future

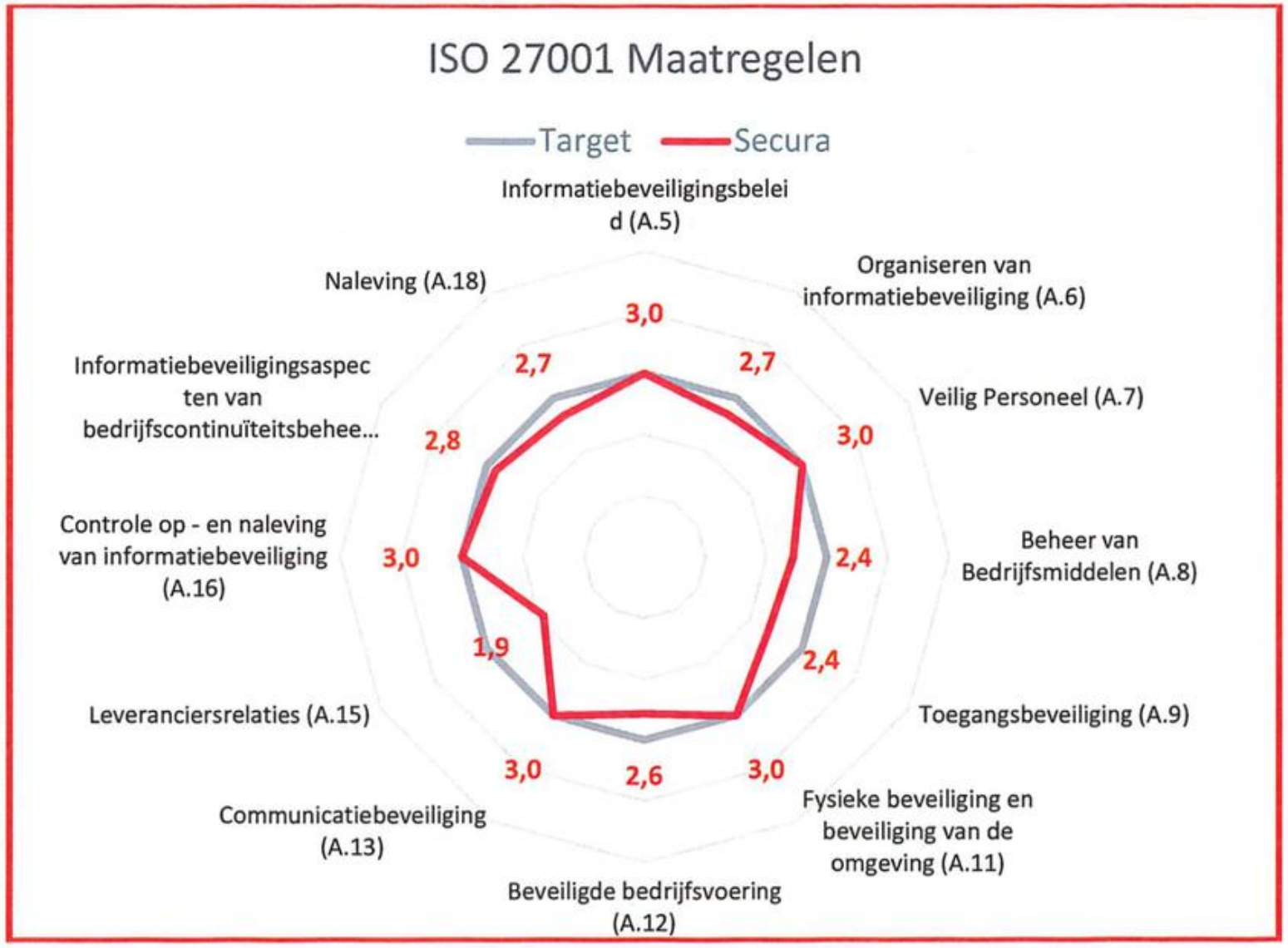
300+ partners: business, government, knowledge & education

HSD ecosysteem

Samenwerken aan een veiligere digitale wereld
en een economisch sterker Nederland



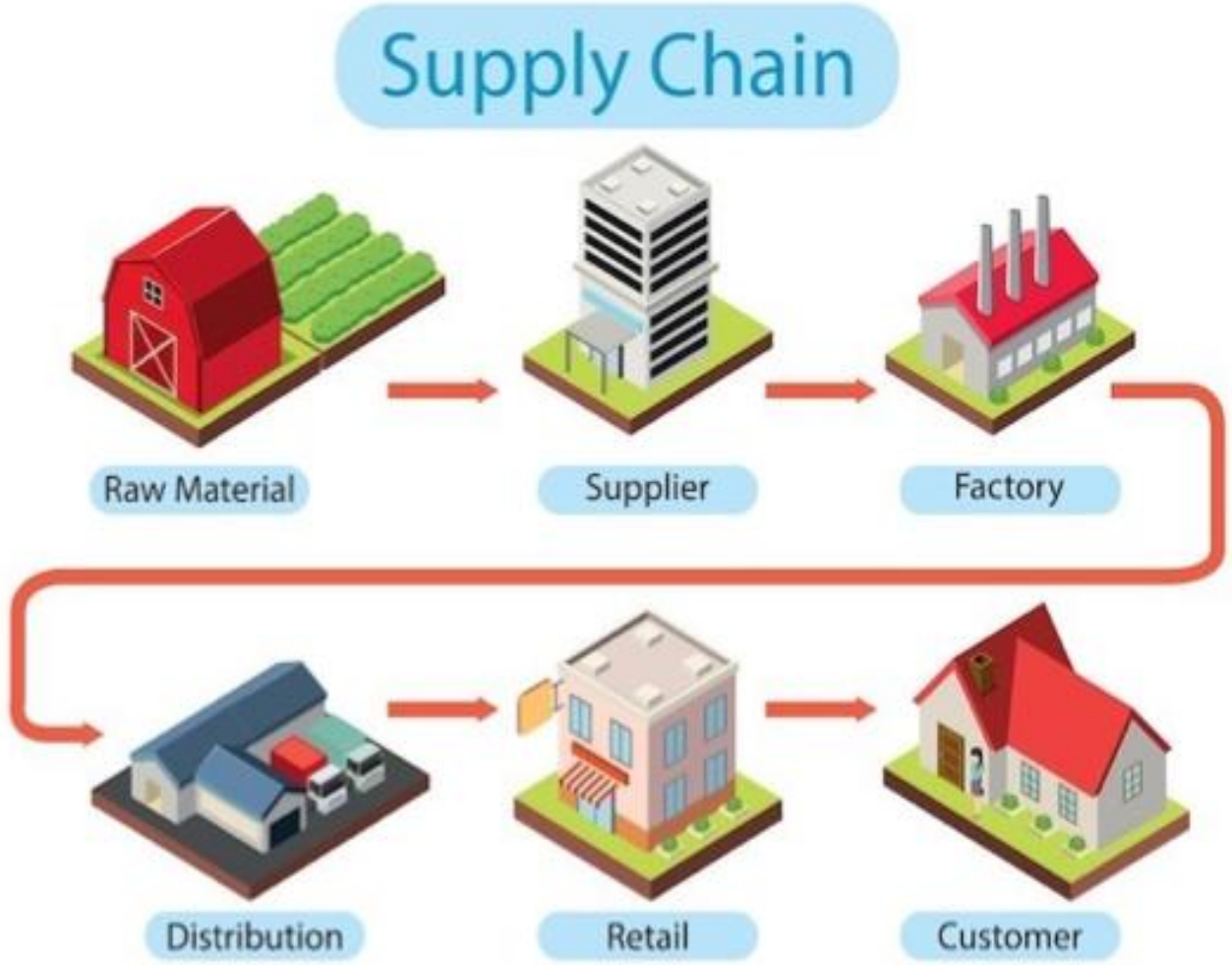
HSD
securitydelta.nl


ISO 27001 Maatregelen
Target
Secura
Informatiebeveiligingsbelei d (A.5)
Organiseren van informatiebeveiliging (A.6)
Veilig Personeel (A.7)
Beheer van Bedrijfsmiddelen (A.8)
Toegangsbeveiliging (A.9)
Fysieke beveiliging en beveiliging van de omgeving (A.11)
Beveiligde bedrijfsvoering (A.12)
Communicatiebeveiliging (A.13)
Leveranciersrelaties (A.15)
Controle op - en naleving van informatiebeveiliging (A.16)
Informatiebeveiligingsaspec ten van bedrijfscontinuïteitsbehee...
Naleving (A.18)
3,0
2,7
3,0
2,4
2,4
3,0
2,6
3,0
1,9
3,0
2,8
2,7

Control Area	Omschrijving	Score Secure	Target Score	Bevinding(en)	Aanbeveling
A.6	Organiseren van informatiebeveiliging	2.7	3	Verantwoordelijkheden aangaande IB/ security voor de Financial controller zijn onvoldoende vastgelegd en herleidbaar.	Definieer wat de IB-verantwoordelijkheden zijn voor de Financial Controller inclusief de verwachtingen van deze rol
A.8	Beheer van bedrijfs-middelen	2.4	3	HSO Office heeft een effectief AVG beleid en uitvoering gerealiseerd. Een overzicht waarin een dataclassificatie van HSO-Office is vastgesteld ontbreekt. De verwachting dat UNO hierin een verantwoordelijkheid heeft is onjuist. HSO Office is verantwoordelijk om deze classificatie vast te stellen. De mobiel, laptop en tablet zijn beveiligd op de hoogst mogelijke standaard. Welke	Creëer een praktische Informatieclassificatie (bijv. Uitvoorbeeld public, intern, vertrouwd etc.) onder verantwoording van de IB verantwoordelijke zodat de relatie van genomen beveiligingsmaatregelen voor de bedrijfsmiddelen, authenticatie en toegangsrechten in verhouding en herleidbaar zijn.
A.12	Beveiligde Bedrijfs-voering	2.6	3	Medewerkers hebben Admin. rechten op de laptops/ Macbooks en kunnen hier software op installeren. Informatiebeveiligingsbeleid is hier niet expliciet in.	Stel zeker dat het risico voor gebruik van admin. rechten op de laptop/ Macbooks acceptabel is met de vastgestelde beveiligingseisen
A.15	Leveranciers-relaties	1.9	3	Er is bij HSO Office geen effectief proces vastgesteld HSO Office haar specifieke IB eisen stelt aan zijn van leveranciers (UNO, HSO Campus ...) is opgenomen. Er is geen ondertekende SLA met UNO herleidbaar. Tevens is er een SLA versie van januari 2021 van UNO die niet in lijn is met de SLA die HSO Office in bezit heeft. De 24/7 verwachting van HSO is formeel geen onderdeel van de services Er is een SLA rapportage van UNO van januari 2022. De Financial controller is hier niet van op de hoogte. En heeft	HSO Office zal een striktere leveranciers rapportage moeten inrichten waarbij de IB eisen helder zijn vastgesteld en afgestemd met de leveranciers. Contracten/ SLA dienen te worden ondertekend waarbij verwachtingen, verantwoordelijkheden en rapportages duidelijk worden gecommuniceerd. Advies is om de meest recente security Baseline van O365 te implementeren zodat de mitigatie

Cyber
Weerbaarheidscentrum
Greenport

HSD
securitydelta.nl


Supply Chain
Raw Material
Supplier
Factory
Distribution
Retail
Customer

Learning 1:

If you want to go fast go alone, if you want to go far go together.

Cyber Weerbaarheidscentrum Greenport

HSD
securitydelta.nl

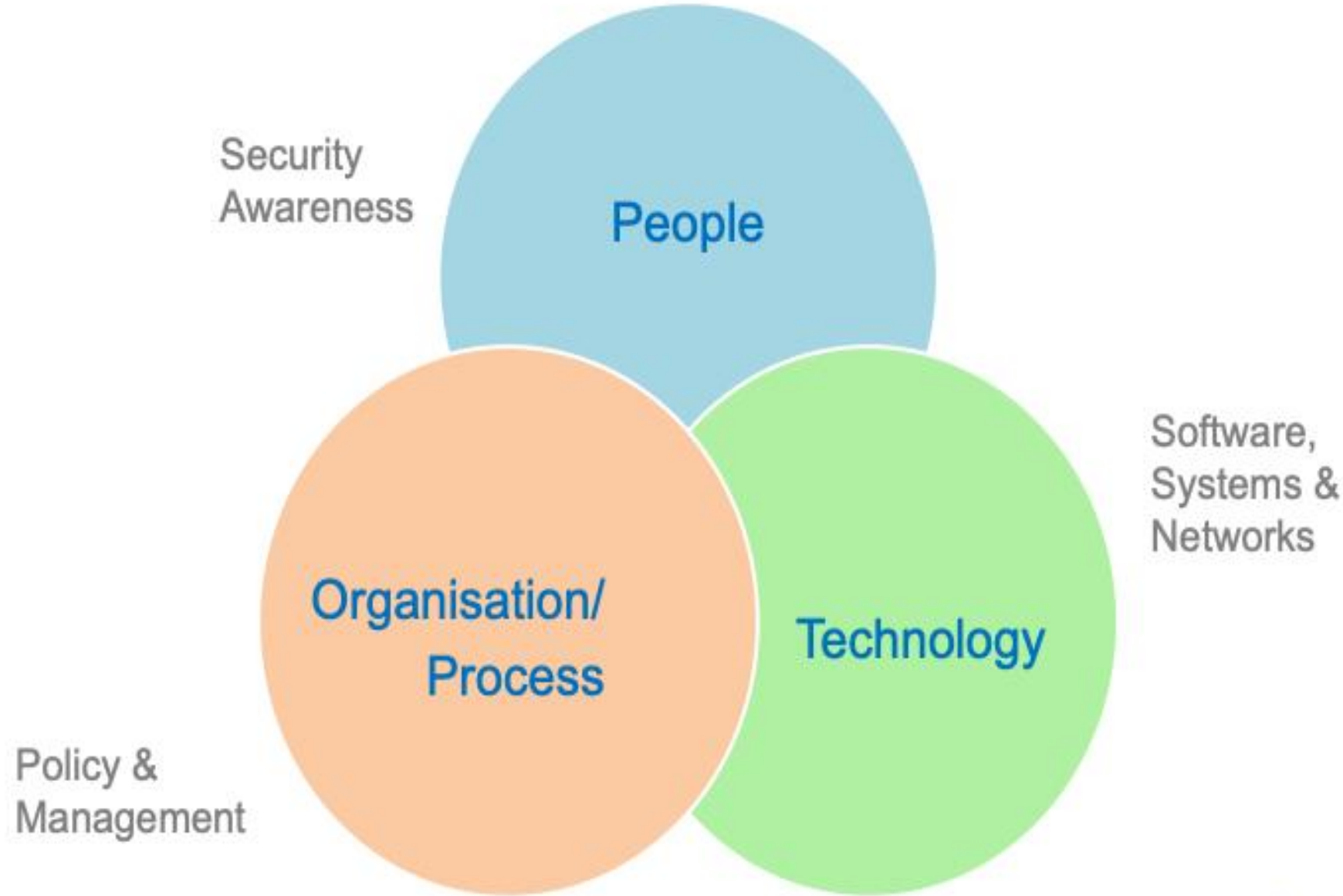

Cyber
Weerbaarheidscentrum
Greenport
Royal Flora Holland
Delphy
Dutch Fresh Port
GREENPORT West-Holland
Interpolis
Anthura
unlimited in varieties
hoogendoorn
growth management
HSD
securitydelta.nl
Glastuinbouw Nederland
DE HAAGSE HOGESCHOOL
provincie Zuid-Holland
digital trust center.

Learning 2:

Cybersecurity is more than IT

Cyber
Weerbaarheidscentrum
Greenport

HSD
securitydelta.nl



HSD

Cyber
Weerbaarheidscentrum
Greenport

Cyber
Weerbaarheidscentrum
Greenport

HSD
securitydelta.nl

Learning 3:

Digitization should be safe, otherwise risks will be too hard to manage.

Cyber Weerbaarheidscentrum Greenport

HSD
securitydelta.nl

HSD
securitydelta.nl

Risicomanagement

NIS2, DSA & CRA

Inzicht in dreiging

Awareness

Kennis & vaardigheden

Leverancier management

Cyber Weerbaarheidscentrum
Maakindustrie Zuid-Holland

Cyber Weerbaarheidscentrum Maakindustrie Zuid-Holland

Initiatiefnemers:

BOERS&CO PRECISION SOLUTIONS

hitech

batenburg techniek

LELY

koninklijke metaalunie

FME

HSD securitydelta.nl

HiDelta! magneet voor duurzame groei

Innovation Quarter

In samenwerking met:

Cyber Weerbaarheidscentrum BRAINPORT

Centrum voor Veiligheid en Digitalisering

CYBER NETWERK DRECHTSTEDEN

DE HAAGSE HOGESCHOOL

Digitalzh

MRDH METROPOOLREGIO ROTTERDAM DEN HAAG

digital trust center.

FERM Rotterdam Port Cyber Resilience Platform

Cyber Weerbaarheidscentrum Greenport

CYBER WEERBAAR NL

provincie Zuid-Holland

Rijksdienst voor Ondernemend Nederland

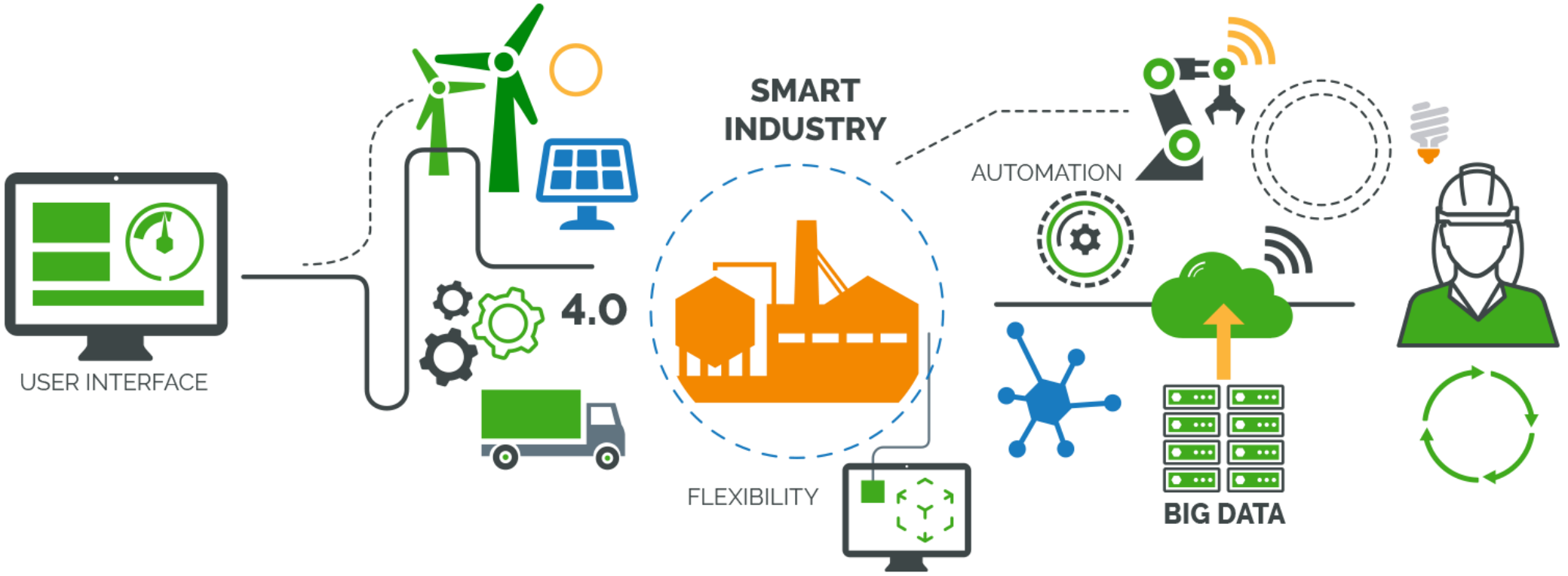
#1

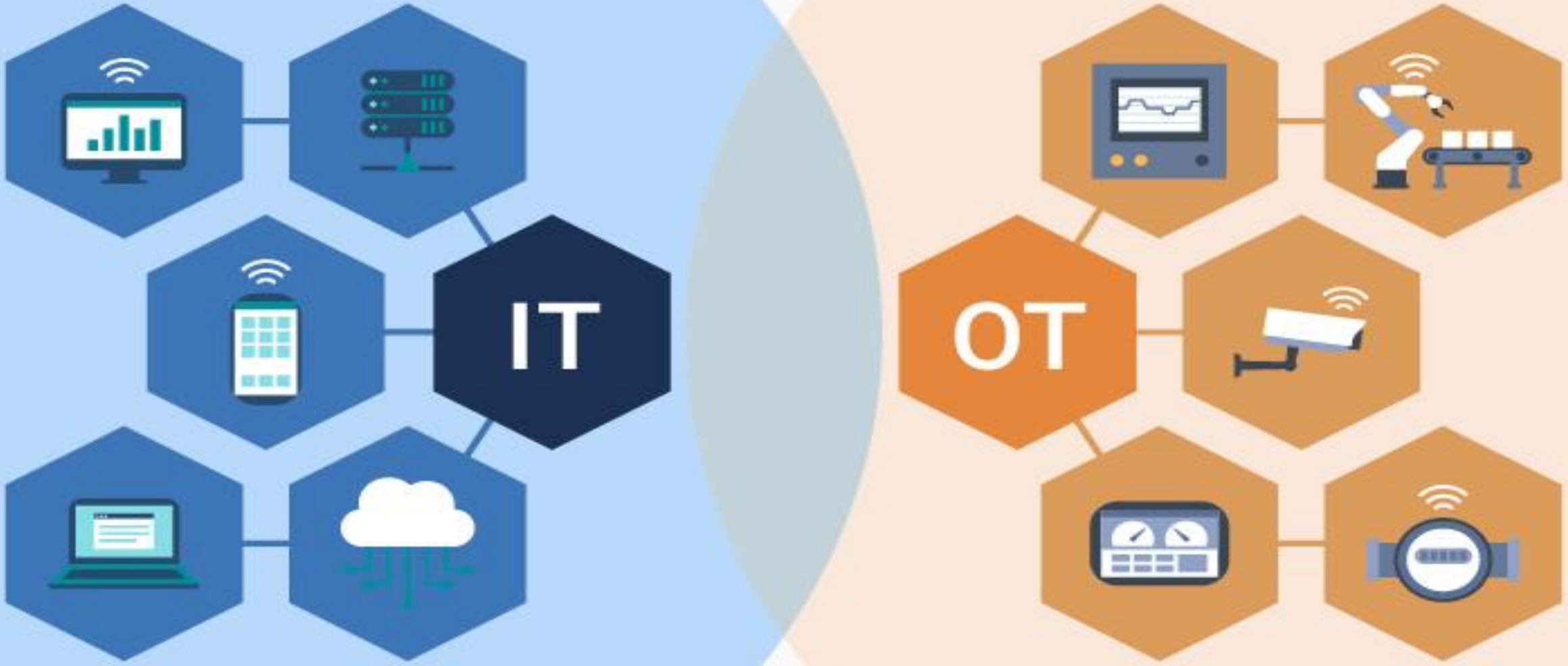
MANUFACTURING REPLACED FINANCIAL SERVICES AS THE TOP ATTACKED INDUSTRY

33%

INCREASE IN THE NUMBER OF INCIDENT FROM 2020 TO 2021

Cyber Weerbaarheidscentrum
Maakindustrie Zuid-Holland


USER INTERFACE
4.0
SMART
INDUSTRY
FLEXIBILITY
AUTOMATION
BIG DATA



Cyber
Weerbaarheidscentrum
Maakindustrie Zuid-Holland

Aan de slag met IT- en OT-security

- Concrete handvatten en tools
- Praktische begeleiding
- Beveiligingsadvies
- Nul-meting en stappenplan
- Dreigingsinformatie
- Hulp van experts
- ISAC Overleggen
- Kennisuitwisseling

www.cwmaakindustrie.nl

Cyber
Weerbaarheidscentrum
Maakindustrie Zuid-Holland

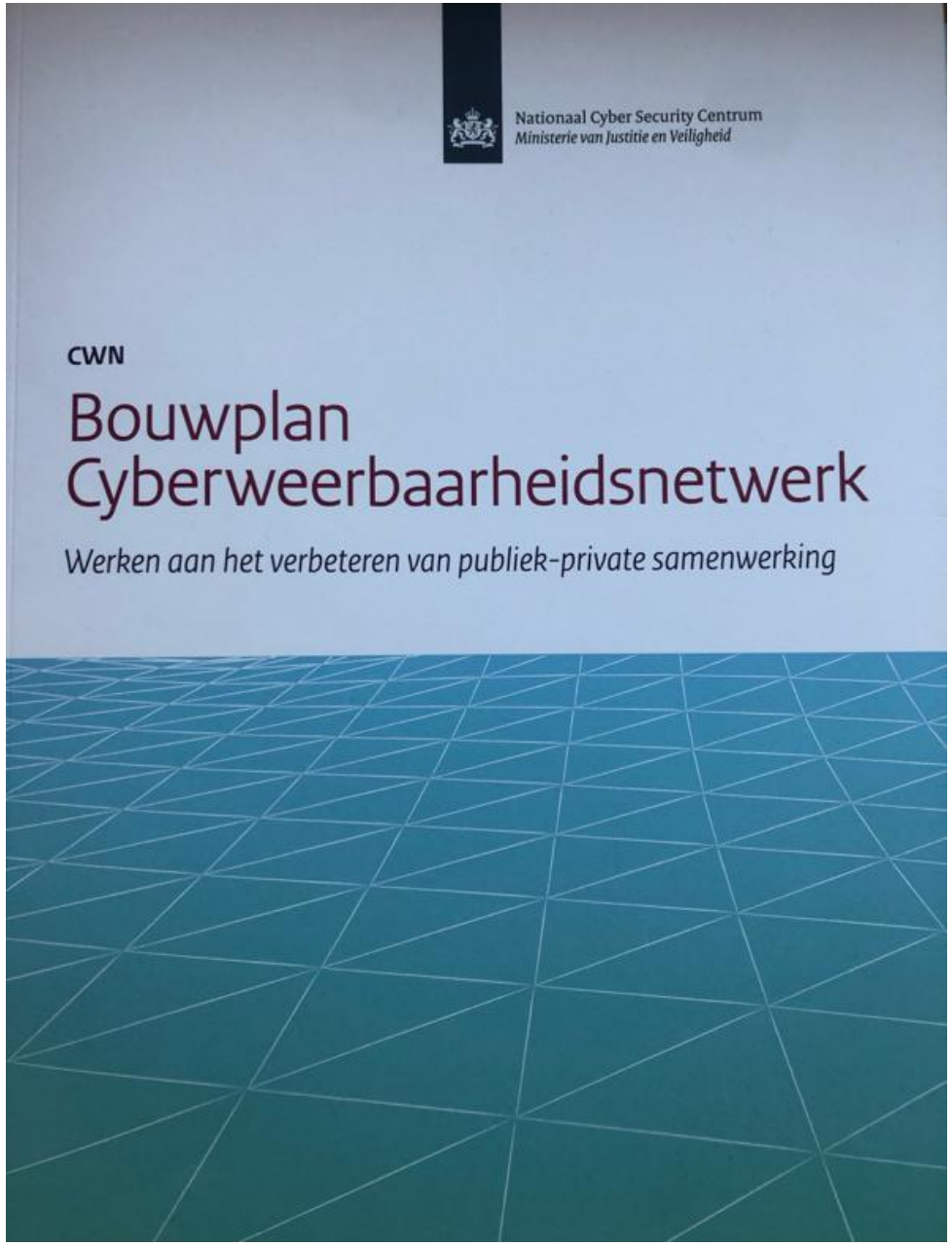
De 8 basismaatregelen voor Cyber Veiligheid NCSC

- Installeer updates
- Zorg voor voldoende loginformatie
- Pas multifactorauthenticatie toe
- Maak regelmatig back-ups en test ze
- Segmenteer netwerken
- Bepaal wie toegang heeft tot data en diensten
- Versleutel opslagmedia met gevoelige bedrijfsinformatie
- Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze

Alleen ga je sneller, samen kom je verder

Naar een landelijke dekkend stelsel 2.0, bouwplan cyberweerbaarheidsnetwerk:

- NCSC (incl DTC)
- Cyberweerbaarheidscentra Greenport en Maakindustrie ZH, powered by HSD
- Nationale Cyber Campus/"House of Cyber"
- Cyberweerbaarheidscentrum Brainport, House of Cyber Brabant i.o.
- FERM (havencomplex)
- MKB Cybercampus Noord NL
- Centrum voor Digitalisering&Veiligheid (CVD) Oost NL
- CyberweerbaarNL
- Centrum Criminaliteitspreventie en Veiligheid (CCV)
- Platform Veiligheid & Ondernemen (PVO)
- Connect2Trust
- Samen Digitaal Veilig (MKB Nederland)
- Diverse brancheverenigingen
- CISO community NL
- ISACA, PvIB, IT auditors, accountants, privacy officers, IT/OT security experts
- U en wij



- Waarom negeren bestuurders vaak risico's en adviezen over cyberveiligheid?

- De **Shift-Right stroming** in risicomanagement blijft onverminderd populair binnen de Nederlandse directiekamers. (Erik de Jong) Het gaat goed zolang het niet fout gaat, beveiligingsmaatregelen en bijbehorende kosten worden uitgesteld, tenzij onvermijdelijk na incident of regulering.
- **Shift Right**, waarom? Je kunt er lang mee weg komen. Ook risico accepteren is ook valide in risicomanagement als mitigeren meer kost dan nu verantwoord is en als andere prio op grotere risico's aan de orde zijn
- **Shift-Left**, waarom? Secure by design, persoonlijke aansprakelijkheid in de wet, keten verantwoordelijke dwingt af, maak de businesscase: voorkomen en/of snel up&running is beter dan genezen zonder actieplan, spreek andere taal, ook in de gehele P&C cyclus en vanuit Audit & Accountancy en Toezichthouders

HSD

securitydelta.nl

www.securitydelta.nl

@HSD_NL