CYBER SECURITY KNOWLEDGE CENTRE

Cyber Security

Vanuit een veranderkundig perspectief

Rob Broersen MBA

Cyber Security Knowledge Centre
Industrieel platform Cyber Security (NEN)
Integere Haven Rotterdam

Intro

Hot item:

The "cyber threat is one of the most serious economic and national security challenges we face as a nation… America's economic prosperity in the 21st century will depend on cyber security."

Er wordt meestal op risico's ingegaan
"Wat er allemaal mis kan gaan …"

Cyber Security als enabler voor diensten.
Geen kostenpost maar opbrengsten !!

MVO wordt al helemaal niet in verband gebracht met Cyber Security.

Hoe in de gehele organisatie met Cyber Security om te gaan …
bedrijfsprocessen … werkwijzen … mensenwerk >>> cultuur

Toch wat voorbeelden

Uit recent onderzoek van Symantec blijkt dat er een stijgend aantal aanvalspogingen van cybercriminelen gericht blijft op de energiesector.
De energiesector behoort wereldwijd nu zelfs tot de top 5 van sectoren waar regelmatig aanvallen op gepleegd worden.

Ambtenaren verlekkeren zich aan gevoelige privégegevens van bekende Nederlanders. Ruim 140 keer vergaapten medewerkers van 13 gemeentelijke sociale diensten zich aan de alimentatiebetalingen, schulden, villa's en wagenparken van voetballers en filmsterren.

"We hadden recentelijk een klein probleem", volgens JPMorgan directeur Jamie Dimon. De banktopman liet verder weten dat de security-uitgaven de komende vijf jaar van 250 miljoen dollar naar 500 miljoen dollar zullen worden verdubbeld. "Het gaat om firewallbescherming, het gaat om interne beveiliging, het gaat om leverancier bescherming, het gaat om alles dat verbinding met je maakt"

Toch wat voorbeelden

NSA Chief Warns Chinese Cyber Attacks Could Shut U.S. Infrastructure

China and "probably one or two" other countries have the ability to invade and possibly shut down computer systems of U.S. power utilities, aviation networks and financial companies, Admiral Mike Rogers, the director of the U.S. National Security Agency, said.

Onderzoekers van de cyber security firma Infracritical hebben bijna twee jaar lang gezocht naar industriële controlesystemen op het internet. Ze vonden miljoenen systemen die direct aan het internet zijn verbonden waardoor de veiligheid van kritieke infrastructuur wordt bedreigd (Internet of Things)

Techniek en mensen

Al tientallen jaren viruscontrole, firewalls, etc ..

Nog steeds diverse kleine en grote incidenten.

30% - 40% techniek

60% - 70% mensenwerk

Bestanden even kopiëren …..
Geen idee waar het over gaat ….
Instellingen niet veranderen tijdens installatie ….
Geen tijd voor onderzoek …..

Trends

Cybersecuritybeeld Nederland
CSBN-2

" De grote afhankelijkheid van ICT voor onze maatschappelijke en persoonlijke veiligheid betekent dat een cyberverstoring of cyberaanval (in potentie) grote impact heeft op zowel de maatschappelijke als de persoonlijke veiligheid." (*Cybersecuritybeeld Nederland / NCSC*)

De ontwikkeling dat steeds meer apparatuur (waaronder medische apparatuur, voertuigen, industriële- en huishoudelijke apparaten) aan internet verbonden is, zal doorzetten. De software in deze apparatuur zal altijd beveiligingslekken bevatten.

Trends

Internet of Things - big data analyse - privacy !

Malware blijft stijgen:

- Botnets worden beter verhuld, ingezet voor zwaardere DDoS aanvallen (onbereikbaarheid)
- Mobiele malware neemt toe (nog niet in NL)
- Gerichte spearphishing (diefstal persoonlijke gegevens)
- Ransomware agressiever (gijzelingen)
- Opkomst cryptoware besmettingen (versleutelde gijzeling)

Geen IT aansprakelijkheid

Cyber security is geen aangelegenheid voor de IT-afdeling of de CIO alleen. Aangezien het gaat om de continuïteit van bedrijfsprocessen, reputatie, kosten en aansprakelijkheid of bescherming van klant- of persoonsgegevens en risicomanagement, raakt het de kern van de organisatie en daarmee alle medewerkers.

Cyber security is ‘business as usual’. Cyber security mag geen belemmering zijn voor innovatie, gebruiksgemak of efficiënter werken en daar horen praktische oplossingen voor security bij. Het gaat niet alleen om technologische oplossingen, maar ook om bewustzijn van het management en medewerkers m.b.t. relatie bedrijfsprocessen.

Definitie Cyber Security

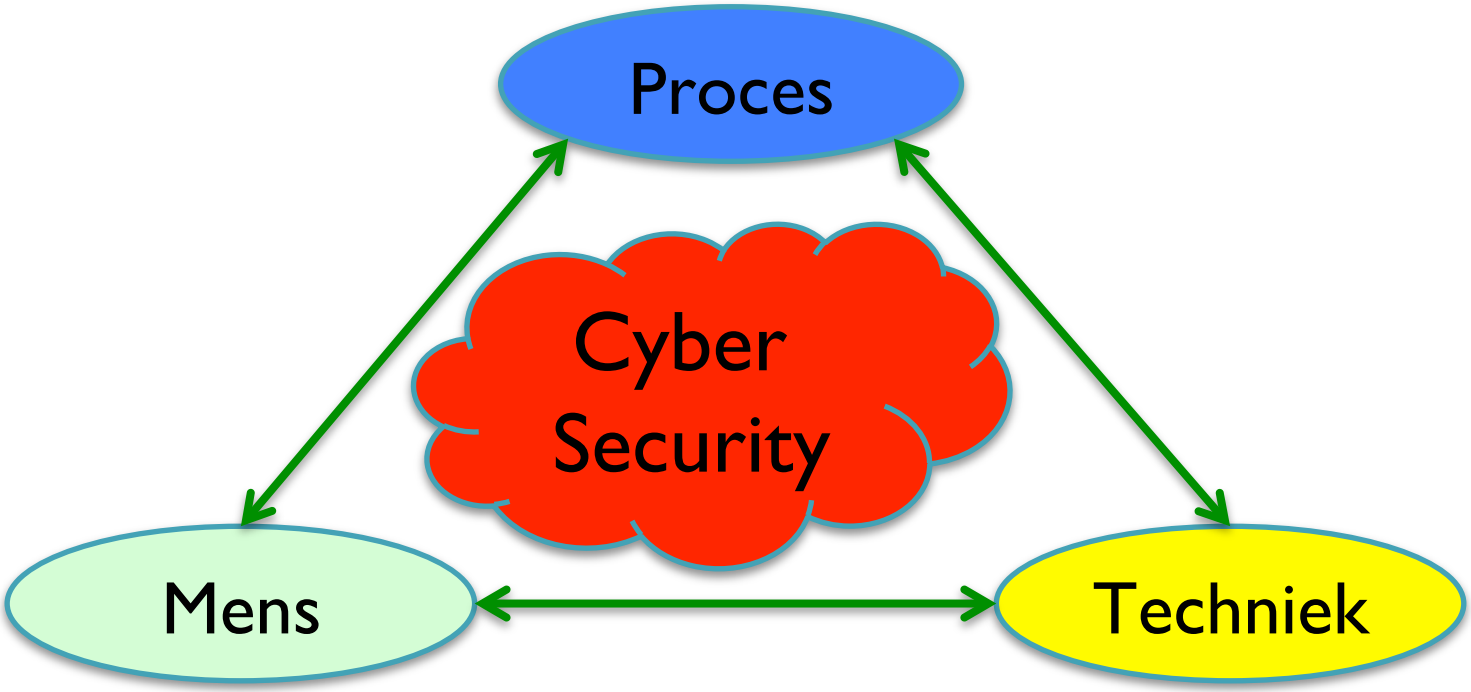
Cyber security is het vrij zijn van gevaar of schade, veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijk-heid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.

NCSC

Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.
Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

NIST

Proces – techniek – mens




FOKKE & SUKKE
MAKEN ALTIJD EEN STRAKKE
PROJECTPLANNING
EN DE CULTUUR-
OMSLAG ?
DIE IS DONDERDAG
DE 17E OM HALF VIER.
RGVT

Verandermanagement

Combinatie van: personeel, competenties, cultuur, structuur, processen, systemen en managementstijl.

Europees onderzoek: 380 Westeuropese bedrijven - in NL 40% onvoldoende succesvolle veranderingen

Onderzoek in NL: kostenreductie 80% slaagkans / kwaliteitsverbetering 65% / strategie-implementatie 58% / cultuurverandering 20% slaagkans !!

Projecten falen veelvuldig door gebrek aan kennis betreffende verandermanagement !

"Verander strategieën"

Veranderen als implementeren
(de verzorgde reis)
Veranderen als proces van co-creatie
(de trektocht)

Veranderen: **niet** ontwikkelen nieuwe ideeën,
wel ontsnappen aan verouderde ideeën.

!! Het denken over organiseren en veranderen laat zich te veel sturen door geaccepteerde denkkaders. **!!**

"Trektocht"

Veranderproces als "trektocht" ingaan -> co-creatie.

Hiervan is echter de uitkomst onzeker.
Nu is de inrichting van en hoe te handelen met cyber security redelijk directief.

Werelden Business en ICT met elkaar in overeenstemming brengen (alignment).

Indien er geen overeenstemming komt dan zal er eerder binnen de organisatie onvrede en weerstanden ontstaan.
De business ziet het snel als een ICT feestje.

Verandermanagement

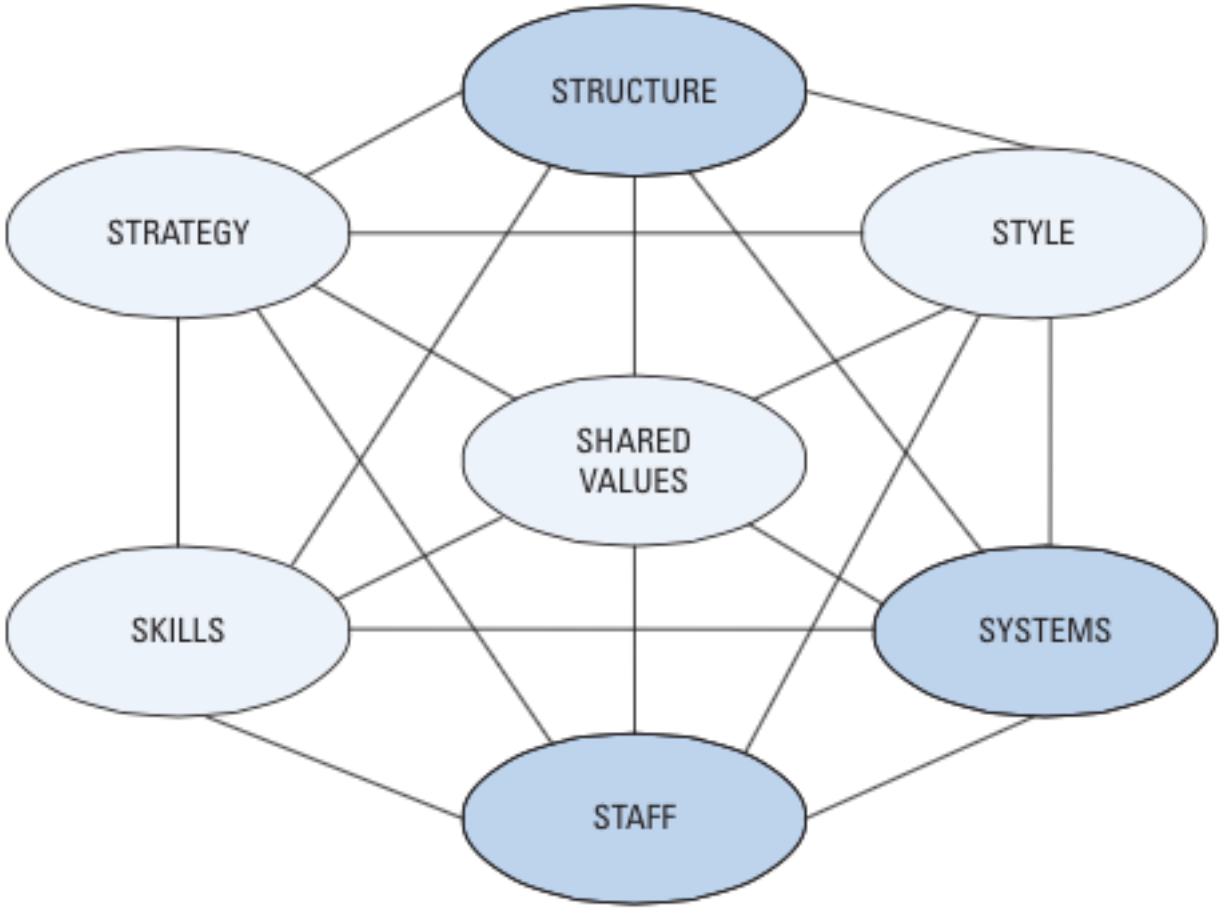
- Kurt Lewin (1951)
  - Unfreeze – Change – Refreeze
- Léon de Caluwé en Hans Vermaak
  - 5 veranderingsperspectieven – kleurdenken
- Jaap Boonstra
  - 5 strategieën
- Andre Wierdsma
  - Co-Creatie
- Thijs Homan
  - "On-stage" - "Off-stage" / betekeniswolken
- ADKAR
  - Benodigde stappen voor verandering per individu

„On stage”

Gaat het zo goedkomen?

„Off stage”

7S model McKinsey



Samenhang

- **Strategie** → **Bestuur**: Leiderschap
- **Verandering** → **Business**: Competenties, personeel, stijl, cultuur (ADKAR aanpak)
- **Project** → **ICT**: Structuur en systemen

Leiderschap

Leiderschap houdt zich bezig met organisatieverandering door het ontwikkelen van een visie met bijbehorende strategie, het communiceren van die visie en het inspireren en motiveren van medewerkers door die visie.

Visie en strategie m.b.t. Cyber Security zijn niet geheel vrijblijvend. Kaders dienen in dit geval helder geschetst te worden. Dit vraagt om een bepaald type leiderschap.

Situationeel leiderschap !

Leiderschap

Tendens: Bedrijven moeten in hun jaarverslag aangeven welke inspanning zij verrichten t.a.v. digitale veiligheid.

Vragen voor de "Board":

- "Kroonjuwelen" van het bedrijf ?
- Toewijzing van resources o.b.v. risico analyse en strategische assets ?
- Welke technische voorziening om real-time verstoringen te detecteren ?
- Hoe vaak wordt de "board" geïnformeerd over digitale dreigingen ?
- Plan om te reageren op verstoringen / aanvallen ?
- Relatie met derden om effectief te reageren op Cybercrime ?

Verandering

ADKAR

- Organisaties veranderen niet – mensen binnen organisaties veranderen.
- Basis hulpmiddel om het “hoe, waarom en wanneer” te snappen.
- Projectmatige aanpak met ruimte voor verschillende interventies.

ADKAR

Awareness		de noodzaak van de verandering
Desire		deelname en ondersteuning van de verandering
Knowledge		hoe te veranderen
Ability		gebruik maken van benodigde skills en gedrag
Reinforcement		versterken van de verandering

Awareness

Enorm werkgebied om bewustzijn Cyber Security te verbeteren.

Je kunt simpelweg niet genoeg doen !

Echter niet alles zal door medewerkers, partners of klanten begrepen worden.

In het algemeen is het totale plaatje Cyber Security te complex en continue aan vernieuwing onderhevig.

Accepteer: niet alles is te verbeteren.

Awareness

Focus: meetbare veranderingen doorvoeren.

Succesvol “awareness programma”: alleen hoogste prioriteiten.

Start niet met slogans

Start met onderzoek

Kennis – houding – gedrag

(nulmeting: tijdens de verandering meten wat goed werkt en wat niet)

Kennis – houding – gedrag

Vraag de juiste vragen

1. Vragen om kennis en bewustzijn CS te meten;
2. Vragen om attitude en perceptie t.o.v. CS-management te achterhalen;
3. Vragen in hoeverre staf en klant gedrag bijdraagt in het uitdragen van CS-verantwoordelijkheden.

Awareness

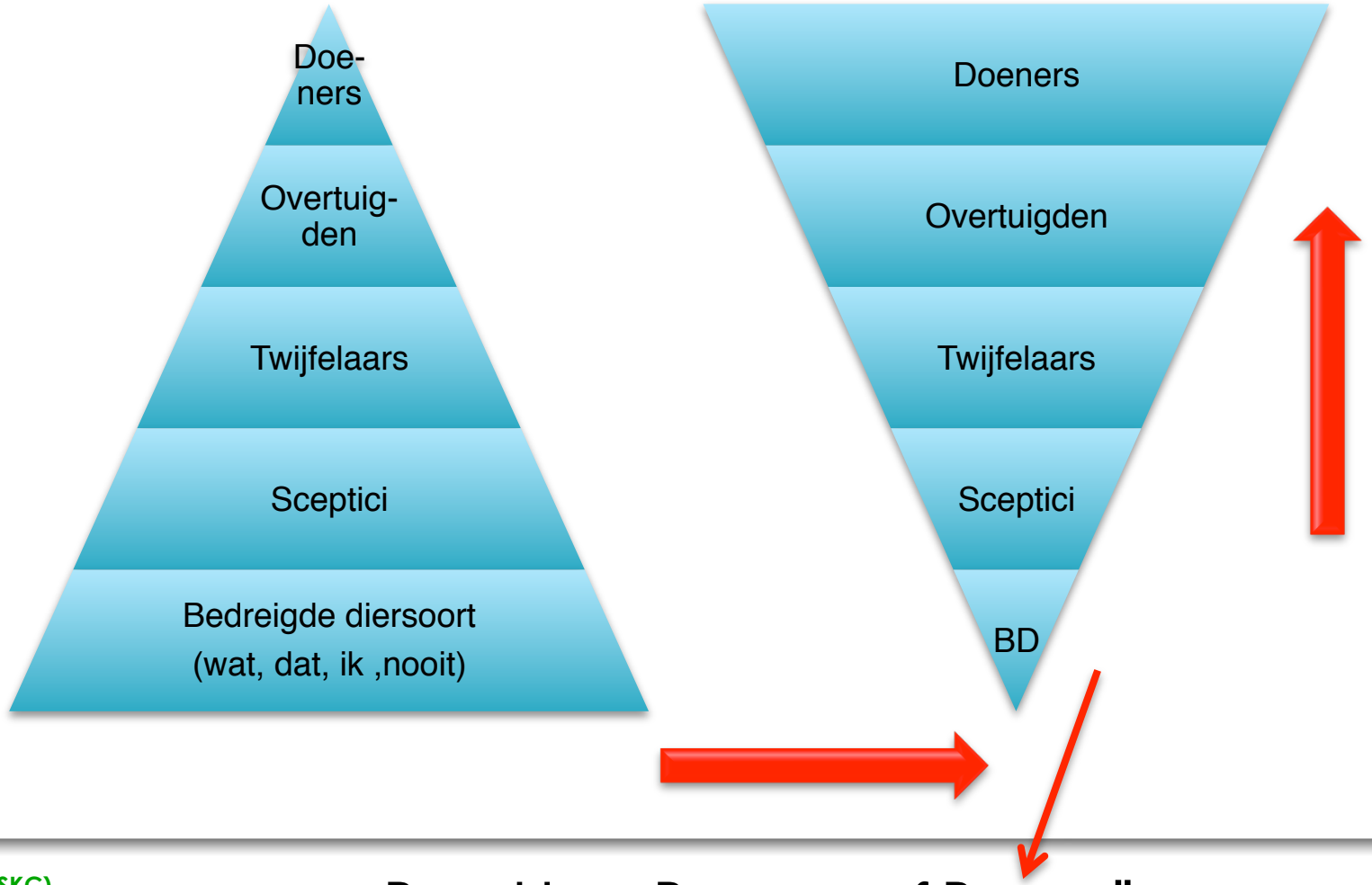
Inschakelen:

Interne communicatie afdeling
Marketing (merk)
Media
Workshops
.....

Desire


IK DOE NIET MEE!
BLAH BLAH BLAH...
VERANDER ZELF MAAR!
LET OP MANNEN! VOLGENS PLAN VERANDEREN WE ALLEMAAL IN FASE 2!
IMPLEMENTATIE
FASE 1
FASE 2
FASE 3

Herkenning



Betrekken, Bewegen of Be-out."

Weerstandreductieplan

BEZIEN VANUIT DE MEDEWERKER:

1. Gebrek aan bewustzijn of waarom verandering nodig is
2. Impact op huidige werk en functie
3. Prestatie-verleden van verandering in de organisatie
4. Het ontbreken van zichtbare steun en inzet van managers

Knowledge

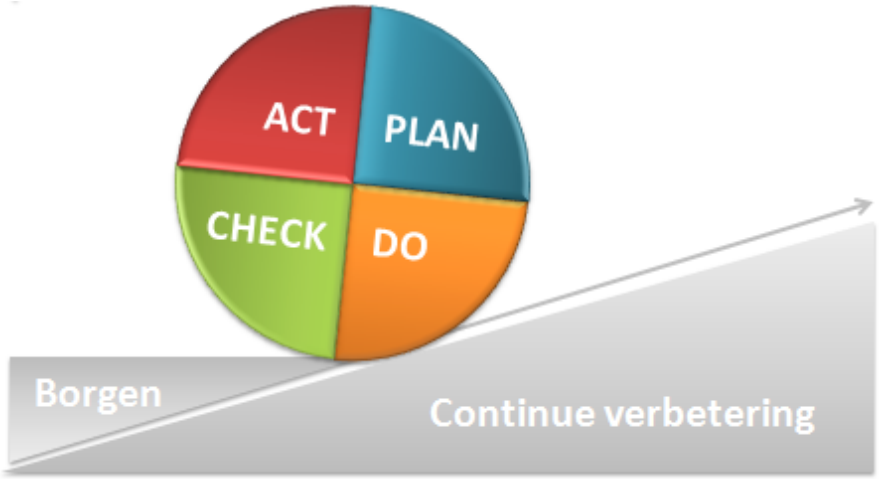
- Standaarden toepassen
- Praktische uitwerkingen beleid
- Opleiding afgestemd op functies en verantwoordelijkheden
- Inzicht verschaffen: koppeling bedrijfsproces met CS

- Workshops: “Hoe ga je om met ..”

Ability

- De kans krijgen om effectief je werk te kunnen doen, niet gehinderd door CS maatregelen.
- Aandacht op veel verschillende zaken (CS complex speelveld), fouten sluipen erin.
- Selectie personeel: kunde korte termijn geheugen snel laten landen in lange termijn geheugen (handelingen automatiseren)
- CS voor 1 organisatie monitoren is inefficiënt: leer van andere organisaties en gebruik kennis die er al is.

Reinforcement



Lering uit incidenten (feedback loops)

Monitoring – integreer in organisatie

Informatievoorziening bestuurders

Cyber Security Management

- Volwassenheidsniveau
- SABSA (Security Architecture)
- Code voor Informatiebeveiliging
- ISO 27001 certificering
- ISO 27K standaarden
- ISA99 (standaard voor *Industrial Automation and Control Systems (IACS) Security)*
- *NIST (National Institute of Standards and Technology)*

CS als enabler …

Geen kostenpost maar enabler voor digitale transformaties !

- Social-trend: organisatie – omgeving door social media
- Mobile-trend: BYOD – 24/7 anywhere
- BIG-Data: dienstverlening verbeteren / veiligheid
- Cloud: flexibiliteit

Cyber Security thema voor directiekamers !

www.cskc.eu
rob.broersen@cskc.eu
06-42237288