HSD
The Hague Security Delta

Rabobank

barents
krans

Programma Cybersecurity: een zaak van de directie!

- 15.30 Ontvangst

- 16.00 Welkom door Dennis Werkman, Directeur Grootbedrijf Rabobank Den Haag en omgeving & Michiel Martin, bestuursvoorzitter BarentsKrans

- 16.05 Introductie door Ida Haisma, directeur The Hague Security Delta

- 16.10-17.00 10-minuten presentaties:
- **De Nederlandse visie op Cybersecurity** *Gerben Klein Baltink - secretaris Nationale Cyber Security Raad*
- **De visie van een hacker** *Rickey Gevers - Digital Investigations*
- **Hoe gaat een bank om met cybersecurity?** *Frans Szabo - Manager Security Virtuele kanalen, Rabobank*
- **Hoe bereid ik me voor als ondernemer?** *Roel van Rijsewijk - Partner Deloitte, expert Cybercrime*
- **Aansprakelijkheid van de directie** *Martijn van Maanen - partner BarentsKrans*

- 17.05-18.00 5 ronde tafelgesprekken met als moderators Ida Haisma, Gerben Klein Baltink, Rickey Gevers, Frans Szabo en Roel van Rijsewijk

- 18.00-18.15 Plenair: samenvatting en conclusies ronde tafelgesprekken (Ida Haisma)

- 18.15-19.00 Borrel + snack

Ida Haisma

Directeur The Hague Security Delta

The Hague **Security Delta**

TITEL

Ida Haisma Director HSD

Tcyber: een zaak van de directie

10 april 2014

www.thehaguesecuritydelta.com

@HSD_NL

HSD
The Hague Security Delta

Europa's grootste veiligheidscluster

- Nederlands veiligheidscluster met kern in Den Haag
  - Bedrijven, kennisinstellingen, Ministerie van Veiligheid & Justitie
  - Boegbeeldproject in Topsector High Tech Systems & Materials
- Sterke banden met (internationale) innovatieregio's & Europese instellingen
- Gezamenlijke ambitie: economische ontwikkeling en innovatie in veiligheid

Economische ontwikkeling en innovatie in veiligheid

Feiten en cijfers over de Nederlandse veiligheidsindustrie (2012)	
Bedrijven	▪ 3.100 veiligheidsbedrijven (400 in regio Den Haag) ▪ Regio Den Haag vooral sterk in niet-traditionele, innovatieve veiligheid (Cyber)
Omzet (€)	▪ 6 miljard (1,7 miljard in regio Den Haag) ▪ 4.1% jaarlijkse groei (2006-2010) ondanks economische crisis ▪ 50% groei (verwachting 2020) ▪ Forensisch en cyber veiligheid grootste groeisectoren
Jobs	▪ 61.500 banen(13.400 in regio Den Haag) ▪ 25% groei (verwachting 2020)

HSD
The Hague Security Delta

Nieuwe risico's vragen nieuwe oplossingen

Noodzaak voor bedrijven, overheid en kennisinstituten om samen te werken

- Vraag en aanbod beter op elkaar aansluiten
- Radicale innovatie op basis van (bewezen en nieuwe) technologie
- Synergie en schaalvoordelen realiseren; innovatiebudgetten afstemmen
- Aanbod geschoold en gekwalificeerd personeel en afstudeerders vergroten

HSD
The Hague Security Delta

Gezamenlijke initiatieven

- Innovatie in veiligheid stimuleren
- Toegepast veiligheidsonderzoek en onderwijs
- Uitbreiden & versterken veiligheidsnetwerk
- Internationale marketing en acquisitie
- Gezamenlijke innovatieprogramma's en -projecten
- Stimuleren vraagbundeling binnen Nederlandse overheid

- Innovatieprogramma's
- HSD Campus, landelijk innovatiecentrum
- Living labs
- Stimuleringsfonds
- Cyber Security Academy
- Kennisontwikkeling
- Matchmaking
- Events
- Handelsmissies
- Marketing & PR
- Internationale & overheidsrelaties

HSD
The Hague Security Delta

The Hague Security Delta Campus

Landelijk innovatiecentrum voor veiligheid

- Cyber security
- National security
- Urban security
- Forensics
- Critical infrastructure

HSD
The Hague Security Delta

Met grote stappen vooruit

2012

- Start The Hague Security Delta

2013

- Start HSD Stimuleringsfonds –*co-financiering innovatie*
- The Hague Security Delta Stichting opgericht
- NFI ondertekent contract om CSI Capetown (SA) te bouwen -*export forensische innovaties*
- European Cyber Crime Centre gevestigd in Den Haag
- Ned. Cyber Security Centrum gevestigd in Den Haag

2014

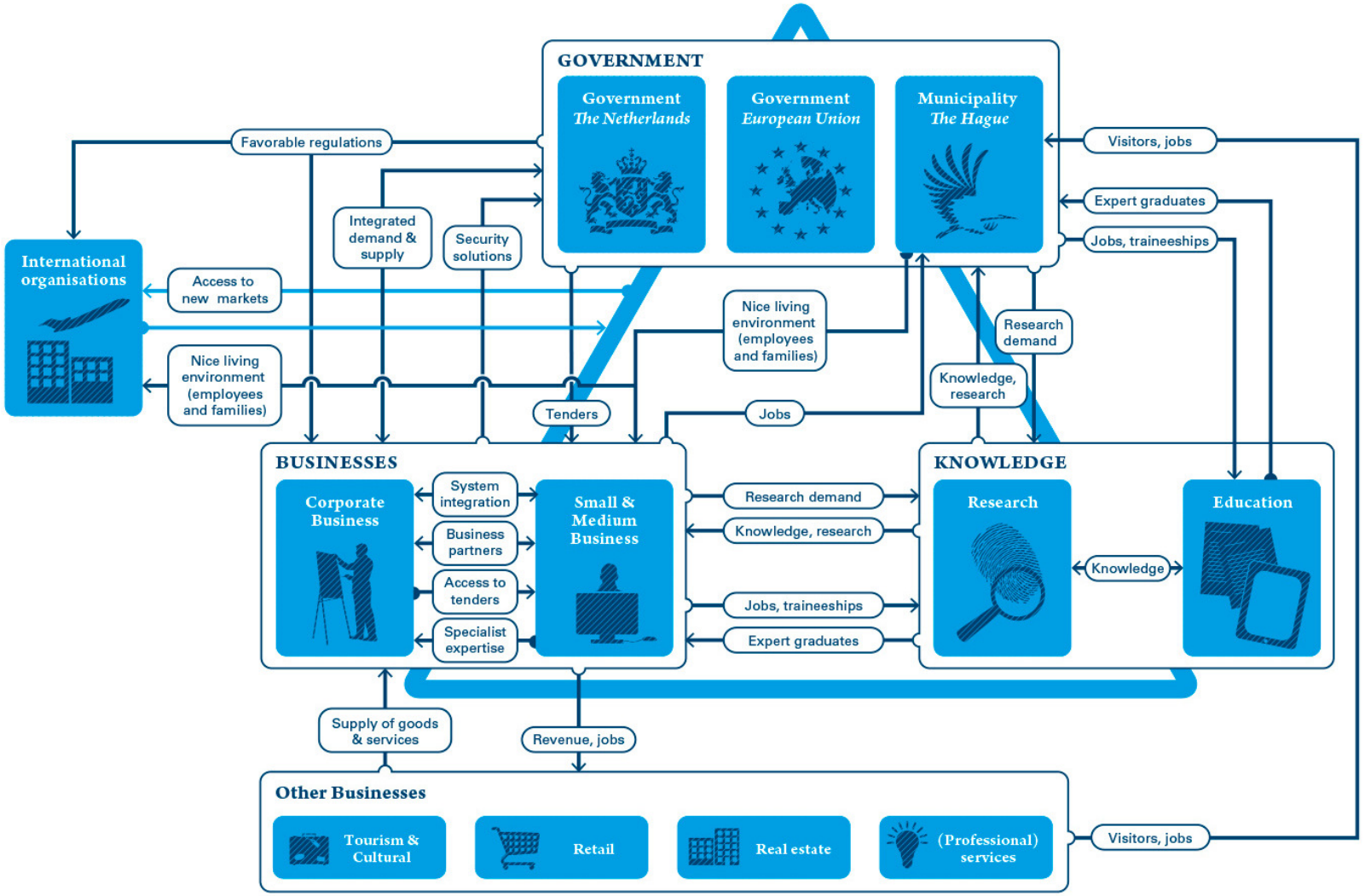
- HSD Campus - *nationaal innovatiecentrum veiligheid*
- Cyber Security Academy opgericht in Den Haag
- World Nuclear Security Summit in Den Haag
- ASIS Europe 2014 conferentie in Den Haag
- Start van 8+ innovatieprogramma's & projecten

2015

- 4e internationale conferentie over Cyberspace in NL
- NATO Cyber Security diensten gevestigd in Den Haag

HSD
The Hague Security Delta

Samenwerking in de gouden driehoek



HSD
The Hague Security Delta

Integrale aanpak veiligheid

Samenwerken in gouden driehoek

Kennis ontwikkelen en ontsluiten

Talent aantrekken en opleiden

High-profile innovatie-projecten

‘Leader firms’ (rolmodellen) verbinden

Kapitaal aantrekken

Vestiging in HSD aantrekkelijk maken

Internationaal op de kaart zetten

Optimale condities creëren voor cluster

HSD
The Hague Security Delta

CYBER SECURITY

- RISICO: KANS **X** EFFECT **X** KWETSBAARHEID
- EFFECT: IMPACT OP:
    - PEOPLE
    - ASSETS
    - KEY PROCESSES
    - STAKEHOLDERS (SHAREHOLDERS/CUSTOMERS)
- INDIRECT: IMAGO
- KWETSBAARHEID: INVLOED VAN CYBER (POSITIEF EN NEGATIEF)

CRISISMANAGEMENT

- FACTOREN VOOR ONTSTAAN CRISIS:
  - NIET INTEGERE CULTUUR
  - SLECHTE KWALITEIT MANAGEMENT
  - IT SYSTEMEN

Gerben Klein Baltink

Secretaris

Nationale Cyber Security Raad

CYBER SECURITY RAAD

Cyber Security in Nederland

Op weg naar een open, veilige en betrouwbare digitale samenleving

CSR, Den Haag, 10 april 2014

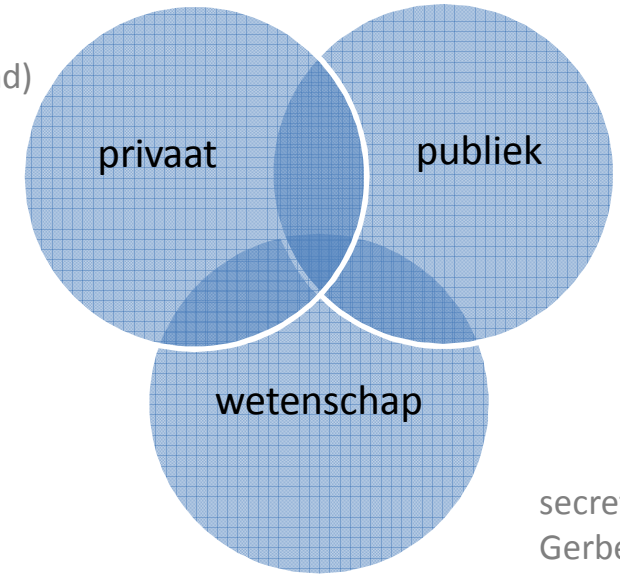
De Cyber Security Raad: onafhankelijk advies

De Cyber Security Raad bestaat uit vertegenwoordigers van publiek, privaat en wetenschap en verbindt verschillende werelden en inzichten op strategisch niveau.

co-voorzitters

Eelco Blok

Dick Schoof



Eelco Blok (VNO-NCW/MKB-Nederland)
Bart Hogendoorn (Nederland ICT)
René Steenvoorden (CIO Platform)
Ben Voorhorst (vitale infrastructuur)
Tineke Netelenbos (ECP)
Jan van Bekkum (Multinationals)

Dick Schoof (min. Veiligheid & Justitie)
Mark Dierikx (min. Economische Zaken)
Rob Bauer (min. Defensie)
Jannine van den Berg (Politie)
Marc van Nimwegen (Openbaar Ministerie)
Rob Bertholee (AIVD)

secretaris
Gerben Klein Baltink

prof. Bart Jacobs (Radboud Universiteit)
prof. Corien Prins (Universiteit Tilburg)
prof. Michel van Eeten (TU Delft)

Rollen voor de Raad

- Toezien op de uitvoering van de strategie
- Gevraagd en ongevraagd advies aan het kabinet
- Verbinden van publiek-privaat-wetenschap
- Uitdragen van bewustwording cyber security
- Lessen leren uit incidenten

Leren van incidenten

Diefstal en misbruik van Diginotar certificaten

KPN hack, met gelekte data van een webwinkel

BABY-DUMP
ALLES VOOR JE BABY TEGEN DUMPPRIJZEN

DIGITAL Investigation

Pobelka-botnet, met 750GB gestolen data ...

CyberBunker

SPAMHAUS

Rabobank

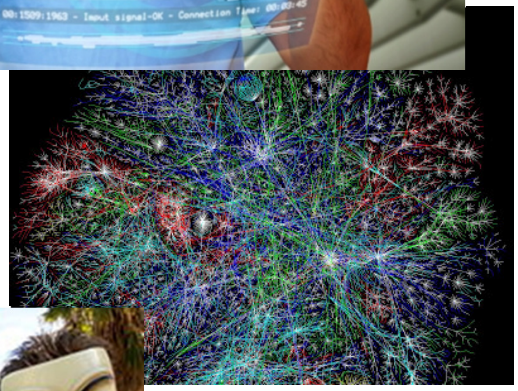
DDOS aanvallen Spamhaus en op de NL banken

Strategische lessen uit deze incidenten

1. Incidenten en crises zien als zegening: ‘wake-up call’ en start van nieuwe dialogen
2. Meer vertrouwen ontstaat door dialogen en ervaren van samenwerking, vertrouwen wordt versterkt door reputatie
3. Taboes worden bespreekbaar binnen organisaties en in de samenleving: strategische top betrokken, security centraler in (inkoop)beleid, toezicht opnieuw bekeken
4. Incidenten worden (toch wel) publiek: zorg voor openheid, dat verhoogt reputatie
5. Cyber security = economie: vertaal cyber security naar economische belangen
6. Goede beveiliging alleen niet genoeg, ICT is niet feilloos (faaltolerantie moet fors omhoog): zorg ook voor focus op detectie en (multi-disciplinaire) respons
7. Leren van incidenten belangrijk: bespreek/vertel de geleerde lessen op vele podia, binnen en buiten de cyber security community
8. Zorg ook voor ‘pijn’ als het moet en benadruk het ‘moreel kapitaal’ bij maatregelen

Dilemma´s in het Digitale Domein

- Governance
- Privacy
- Bewustwording
- The Internet of Things
- Internationale samenwerking



Werkprogramma CSR 2014

- Bewustwording
- Standaarden (zoals WEF Principles, PAS555, ISO 27000-serie)
- Keteneffecten ICT in de vitale infrastructuur
- Zorgplicht
- Risico's van *legacy* systemen
- Onderwijs: zowel voor de basis als voor experts
- De burger in controle over zijn eigen data

Gerben Klein Baltink
g.d.klein.baltink@nctv.minvenj.nl
06-46891841

Rickey Gevers

Digital Investigations

Frans Szabo

Manager Security Virtuele kanalen,
Rabobank Nederland

Rabobank

Cybercrime en de Rabobank

Hoe gaat een bank om met cybersecurity?

Frans Szabó, Manager Security Virtuele Kanalen, Rabobank Nederland

Wat is “top of mind” voor een bank vanuit klantperspectief ?

Cybervandalism

Storingen iDeal en ING kwamen door ddos-aanval - update

Door Arnoud Wokke en Joost Schellevis, vrijdag 5 april 2013 20:42, views: 66.819 • Feedback
Submitter: Worsteneter

De storingen vrijdag bij iDeal en ING kwamen door een ddos-aanval op banken. Dat meldt de Nederlandse Vereniging van Banken. Eerder vrijdag bleek al dat Amerikaanse banken met ddos-aanvallen worden bestookt; onduidelijk is of er een relatie is.

Het is onduidelijk wie er achter de ddos-aanval zit. De ddos-aanval lijkt specifiek gericht op betalingsverkeer, aangezien naast ING ook de dienst iDeal plat ging. Door de ddos-aanval was het urenlang niet mogelijk om internetbankieren, mobiel bankieren en de site van ING te gebruiken, schrijft de NVB in een verklaring die op de site van ING is geplaatst. Bij andere banken waren alleen iDeal-betalingen getroffen, al

Cyberfraude

Nieuws

11.000 slachtoffers fraude internetbankieren

Woensdag, 13:25 door Redactie

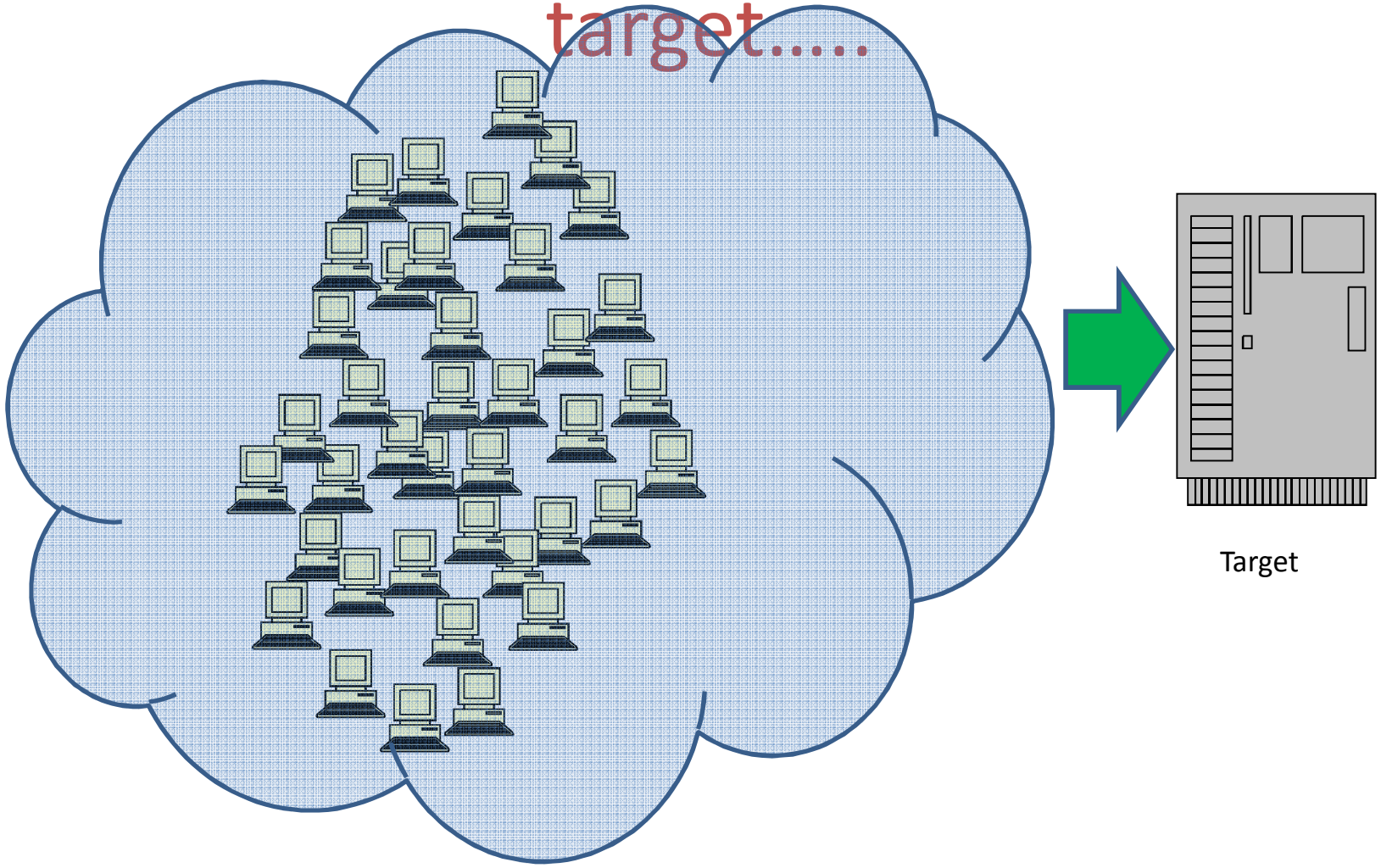
Het aantal Nederlanders waarbij criminelen middels malware en phishing toegang tot de bankrekening kregen is vorig jaar explosief gestegen ten opzichte van 2011. Ging het in 2011 nog om 7600 slachtoffers, vorig jaar werden 10900 Nederlanders de dupe van malware en phishing. Een toename van 35%. Gisteren publiceerde de Nederlandse Vereniging van Banken de schadecijfers van 2012.

Werd er in 2011 nog 35 miljoen euro door cybercriminelen gestolen, vorig jaar bedroeg het 34,8 miljoen euro. Daardoor is het gemiddelde gestolen bedrag per slachtoffer wel gedaald. In 2011 raakten slachtoffers gemiddeld 4.600 euro kwijt, in 2012 was dat gemiddeld 3.200 euro.

Criminelen zouden steeds vaker malware in plaats van phishing gebruiken om toegang tot de bankrekening van slachtoffers te krijgen.

Cyber-vandalisme

Hoe het er normaal uitziet voor het target.....



Hoe het er uitziet voor het target bij een DDOS…..

Cyber-fraude

Cyberfraude toegelicht

rtl Nieuws

Do 7° | 14°

Home | Binnenland | Buitenland | Economie | Sport | Boulevard | Opmerkelijk

Uitgelicht: Special troonswisseling | Rusland: kritiek versus belangen | In beeld: Sabia, nieuwe vl

RTL Nieuws | 02 april 2013, 19:24

Meer mensen slachtoffer van cyberfraude

Cyberfraude is geen voorbijgaand verschijnsel.....

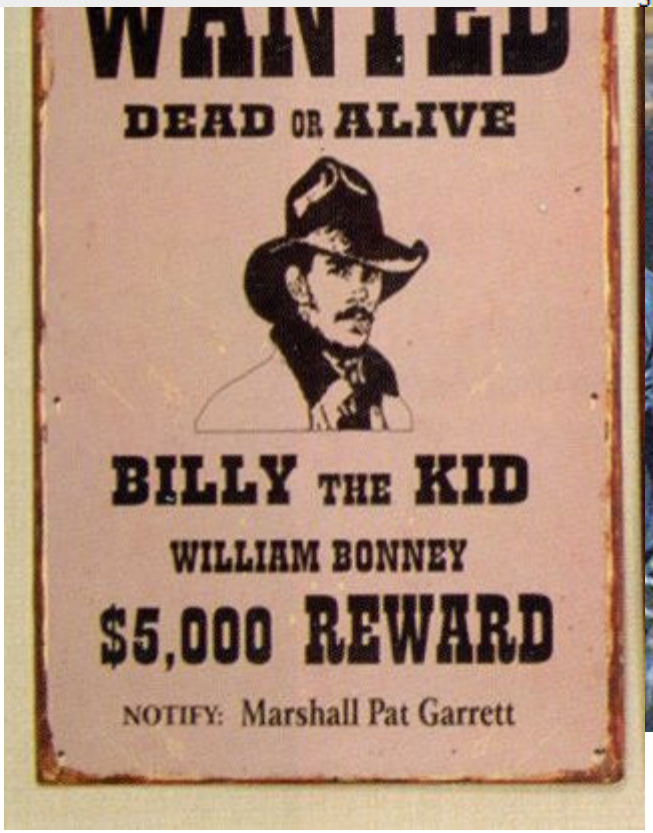
Overval pinautomaat Zeist

Foto: RTV Utrecht

Maandagavond 19 maart pinnen een man en een vrouw bij een pinapparaat bij het winkelcentrum onder één van de flats aan de Laan van Vollenhove in Zeist. Uit het niets duikt er een man achter hen op. Hij heeft een vuurwapen bij zich en wil geld van
een jogger voorbij. Hij
pinautomaat. De man
te trekken, maar tever
dreigt de overvaller no
vuurwapen en dan bes
pint een geldbedrag e
is goed te zien op bew

Signalement:

kieren?



erheid

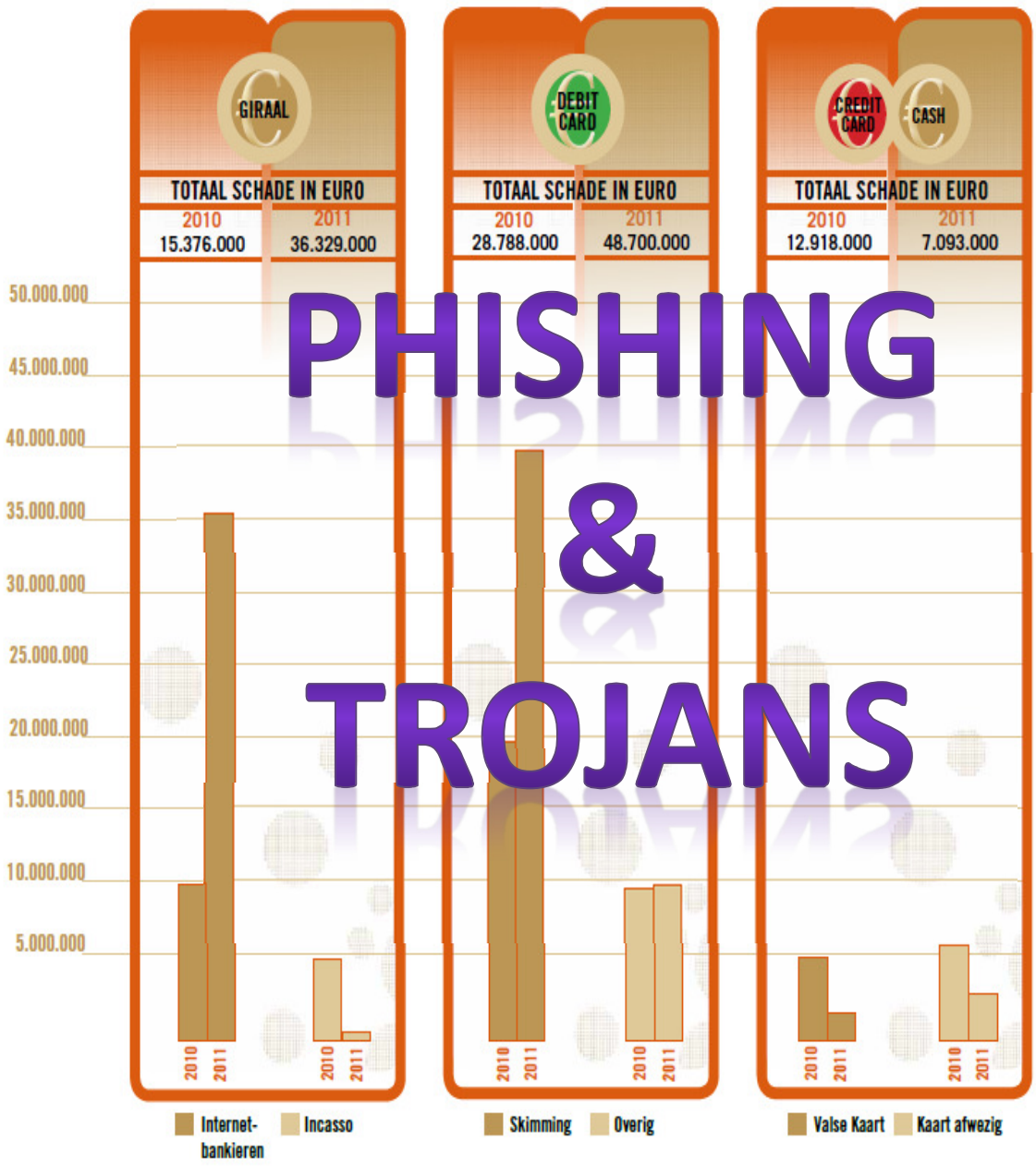
Waarom zoveel focus op Internet Bankieren ?

Geld en spullen zijn anoniem op iedere willekeurige plek te krijgen, pakkans nihil….

PostNL lanceert innovatieve pakketautomaat in Almere

Zelf tijd en plaats bepalen voor ophalen en wegbrengen pakket

PHISHING & TROJANS



TOTAAL 2010:
- giraal
- debit card
- credit card
- cash

57.082.000

TOTAAL 2011:
- giraal
- debit card
- credit card
- cash

92.122.000

Phishing


AmericanBank.net
Enter your SSN:

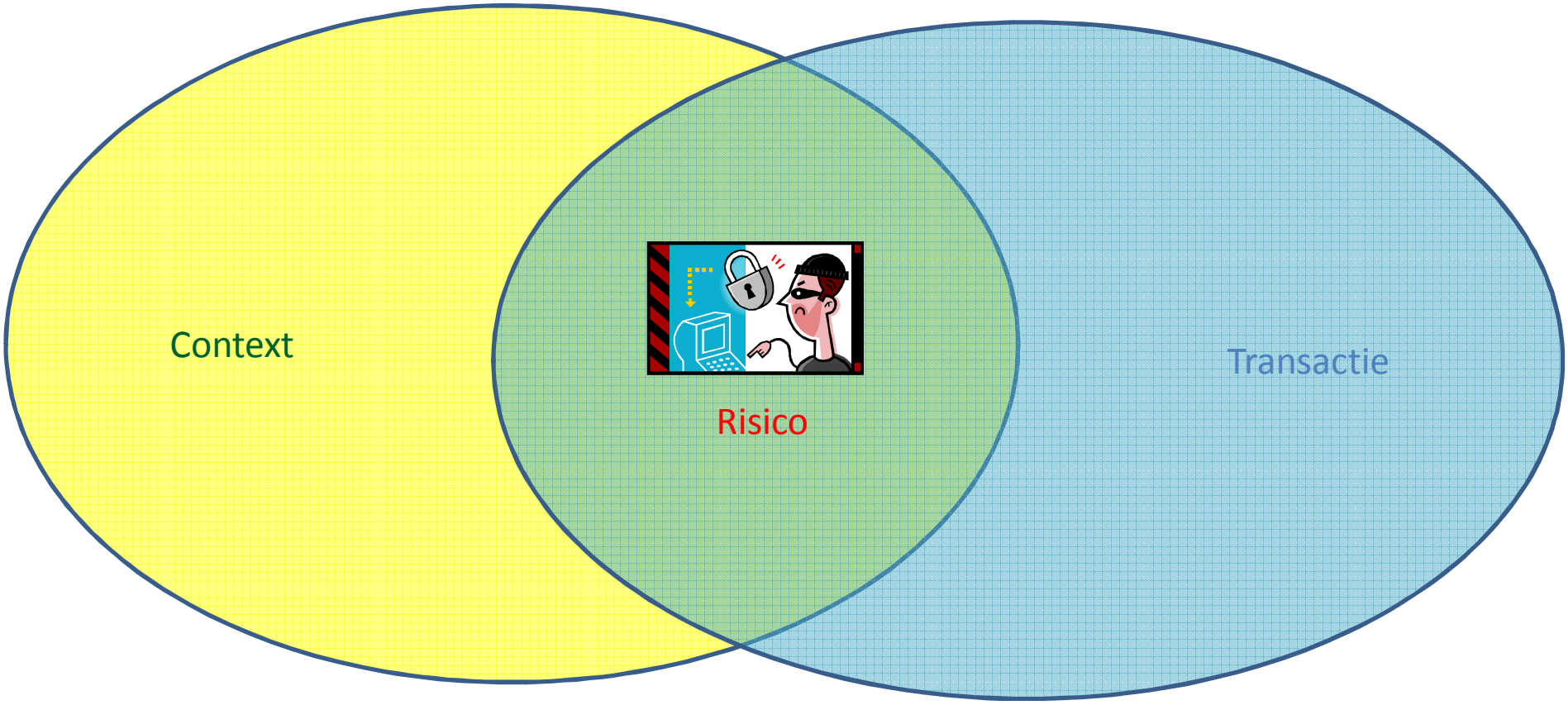

We need to verify your credit card number.
Don't take the bait. Protect your financial information.

Malware na virusbesmetting..

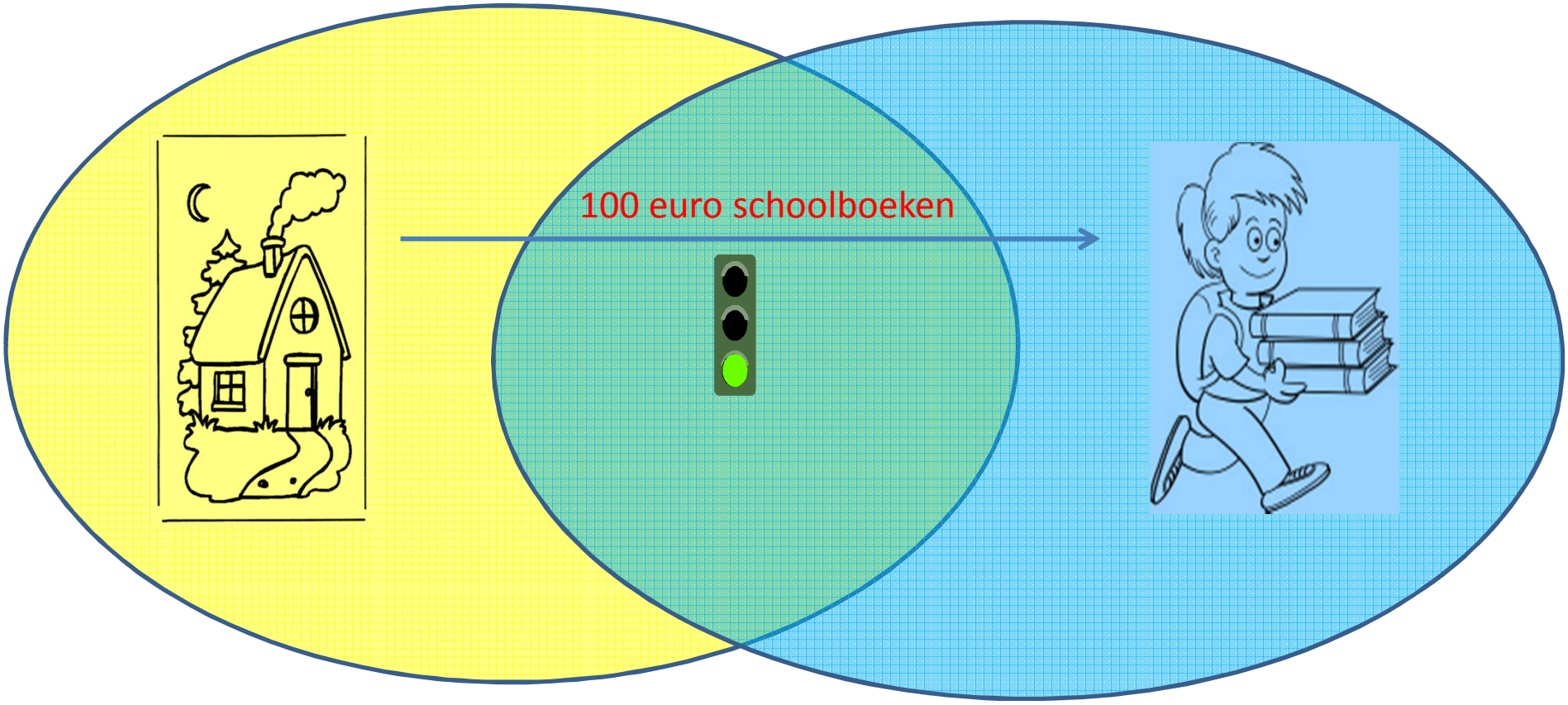
Wat doet de Rabobank om veiligheid van internetbankieren te waarborgen?

- De Rabobank zorgt voor een beveiligde verbinding en systemen.
- Random Reader.
- Instellen van betaallimieten.
- Communicatie naar klanten / pers.
- Signaleren van verdachte situaties: monitoring en detectie in de keten.

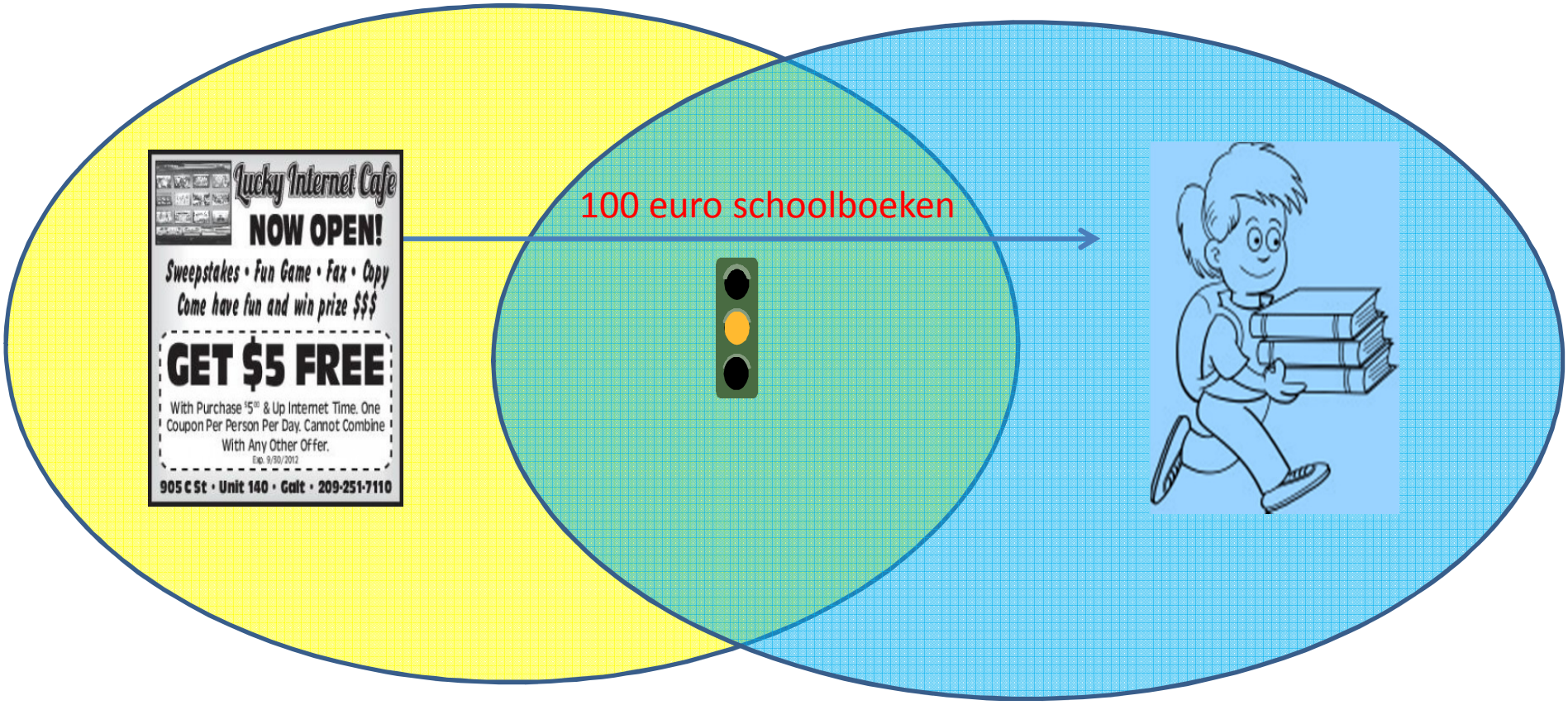
Waarop is Monitoring en Detectie gebaseerd ?



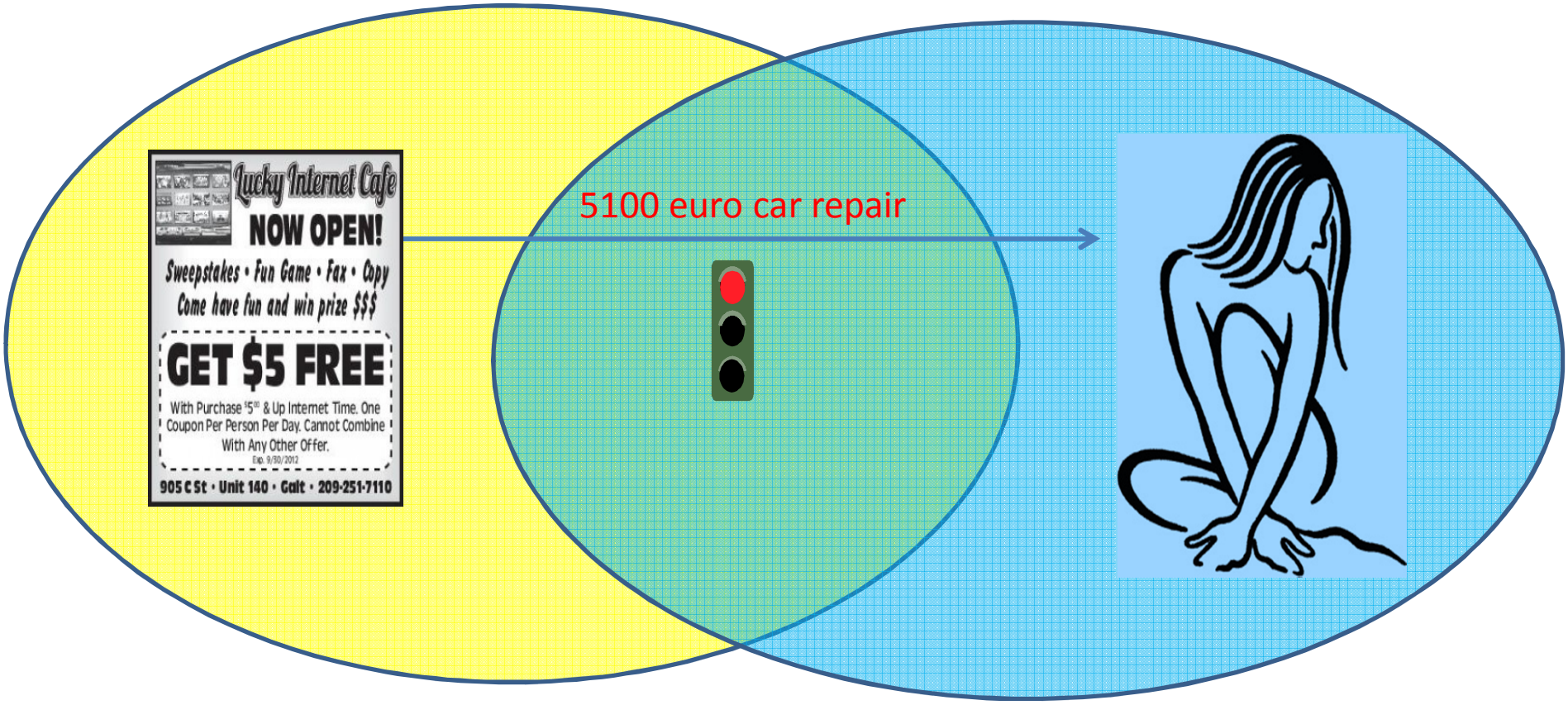
Waarop is Monitoring en Detectie gebaseerd ?



Waarop is Monitoring en Detectie gebaseerd ?



Waarop is Monitoring en Detectie gebaseerd ?



Wat is de uitdaging bij Monitoring en ie ?

Er zijn heel veel plekken waar je kunt bankieren met heel veel devices…

Wat voor de ene klant bijzonder is, is voor de andere klant gewoon

Miljarden bankrekeningen en webshops wereldwijd

5100 euro car repair

Wat zegt dan het begrip risico ?

Hoe effectief werkt dat bij de Rabobank ?

Rabobank monitort alle verdachte transacties

Vandaag, 07:48 door Redactie

De Rabobank zegt dat het alle verdachte transacties monitort en zodoende **X = 99%** fraudepogingen via internetbankieren voorkomt. "We monitoren al geruime tijd al het verdachte internetverkeer en alle verdachte transacties. We grijpen vervolgens in waar nodig", zegt Mark Bergevoet, manager Service & Support van Rabobank.

De bank installeert hiervoor geen software op de pc van de klant, die monitoring daarnaast ook niet zou opmerken. "De klant kan dus anyplace veilig internetbankieren, ook op andere pc's. Veiligheid hoeft niet ten koste te gaan van gemak, integendeel", stelt Bergevoet.

Hij merkt op dat de bank geen 100% bescherming kan garanderen. "Maar we zijn op de goede weg." De Rabobank zou een dalende trend zien, zowel voor malware als voor phishing.

Vragen ?

Roel van Rijsewijk

Partner Deloitte; expert cybercrime

Deloitte.

Rabobank Den Haag en omgeving / BarentsKrans

Cyber Security

- Assume you will be hacked, prepare for the worst

Lange Voorhout

Trends

That grow the need for cyber

Society & Economy

1. Dependence on technology is growing.
2. Connectivity increases exponentially.
3. Disruptions in technology are a clear and present danger to business continuity.

Cloud computing, Social Media, mobile computing, BYO, remote working, always online, digital-supply-chain, online shopping, online banking, etc.

Cyber Threats

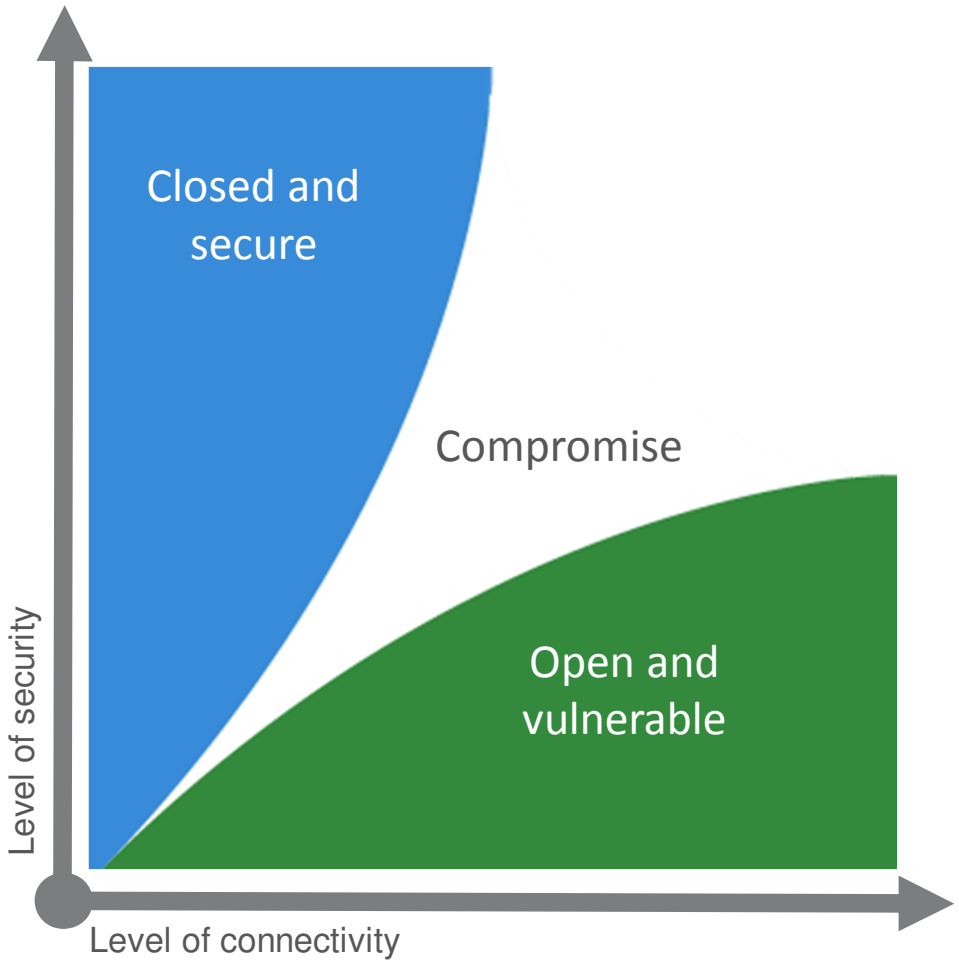
1. Increased digital exposure.
2. Cybercrime is professionalizing.
3. Increase in other factors and motivations.

DDoS, Skimming, SPAM, Phishing, Spear-phishing, Internet banking hack, Credit card data theft, Identity theft, Password cracking, Disclosure confidential data, hacking Social Media, hacking parking terminals, disruption manufacturing systems, etc.

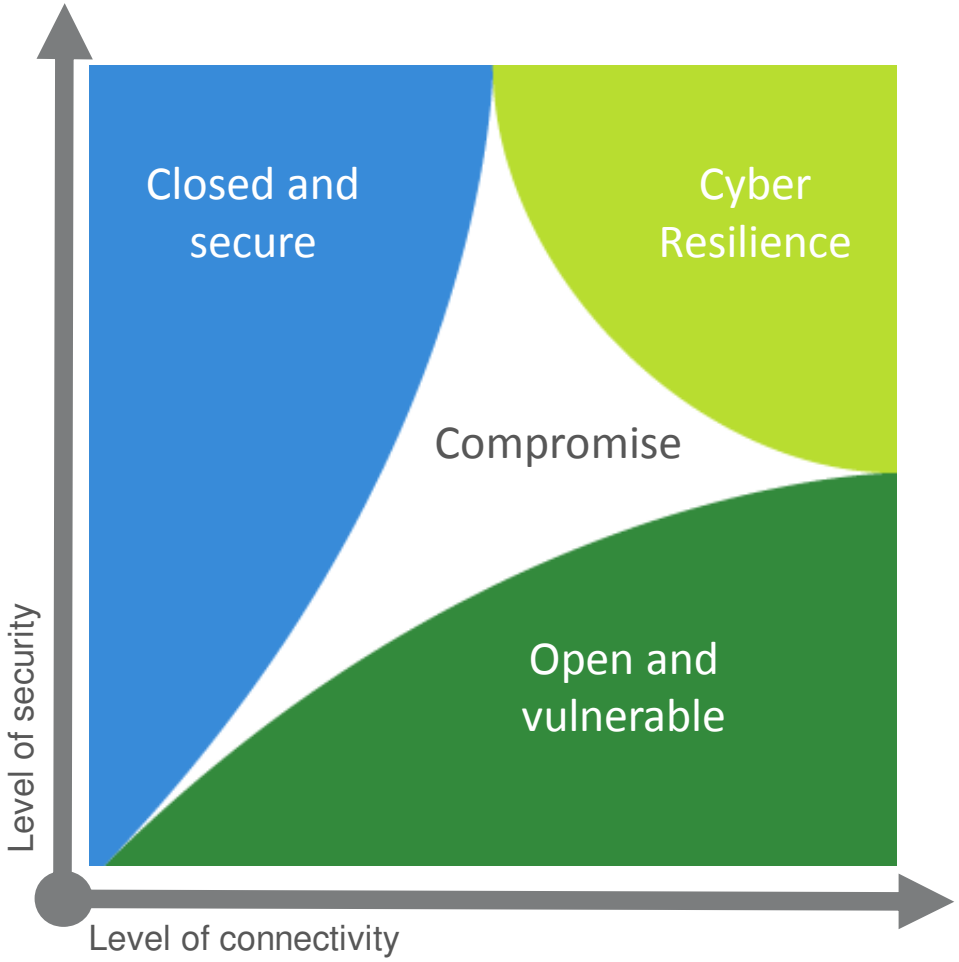
“They Couldn’t Hit an Elephant at that Distance.”

John Sedgwick
May 9, 1864

Digital Dilemma



Digital Dilemma



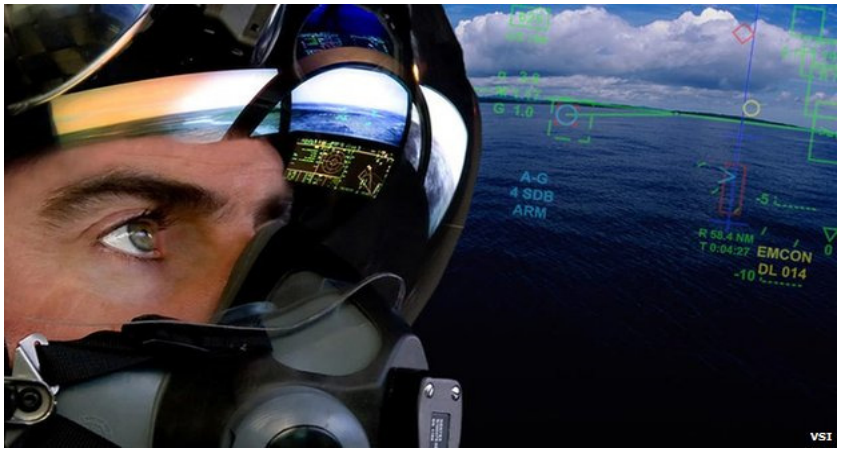
Paradigm shift in Security

Reactive

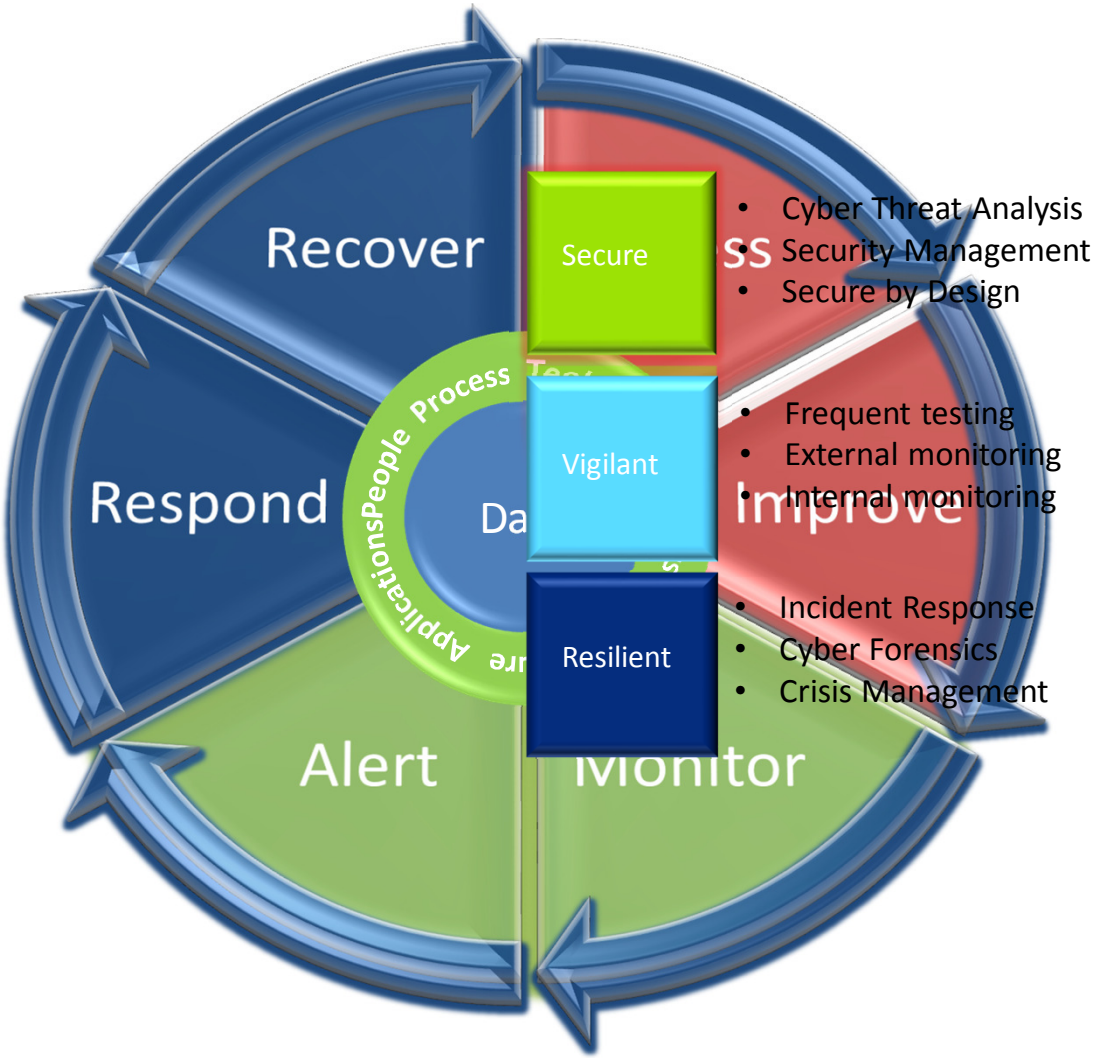
- Static
- Perimeter
- Keep out

Proactive

- Dynamic
- Open & connected
- Detect and respond

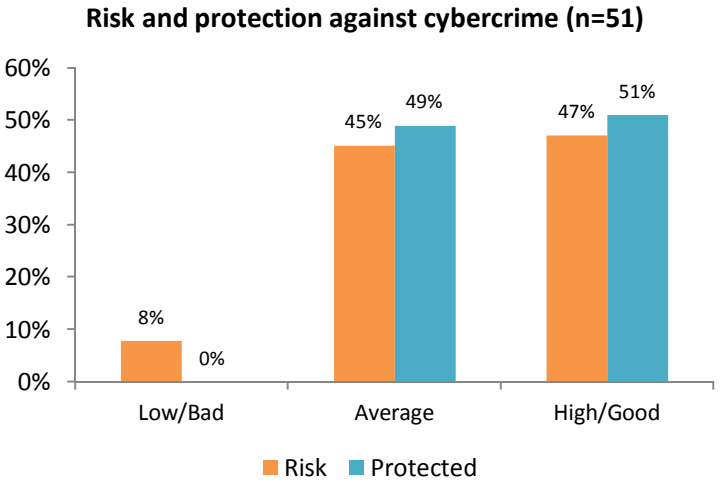


What do you need to do?

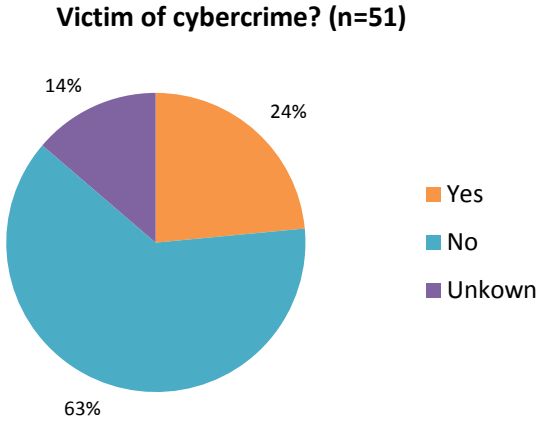


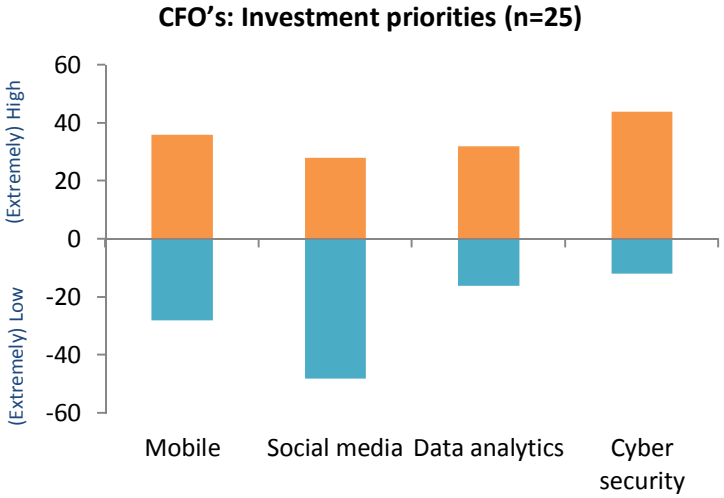
Another Dilemma

How much do I need to invest?



Board Members estimate the risks of digitalization to be high and claim to be adequately protected against cyber attacks. However, they want to invest in Cyber security.





Martijn van Maanen

Partner BarentsKrans