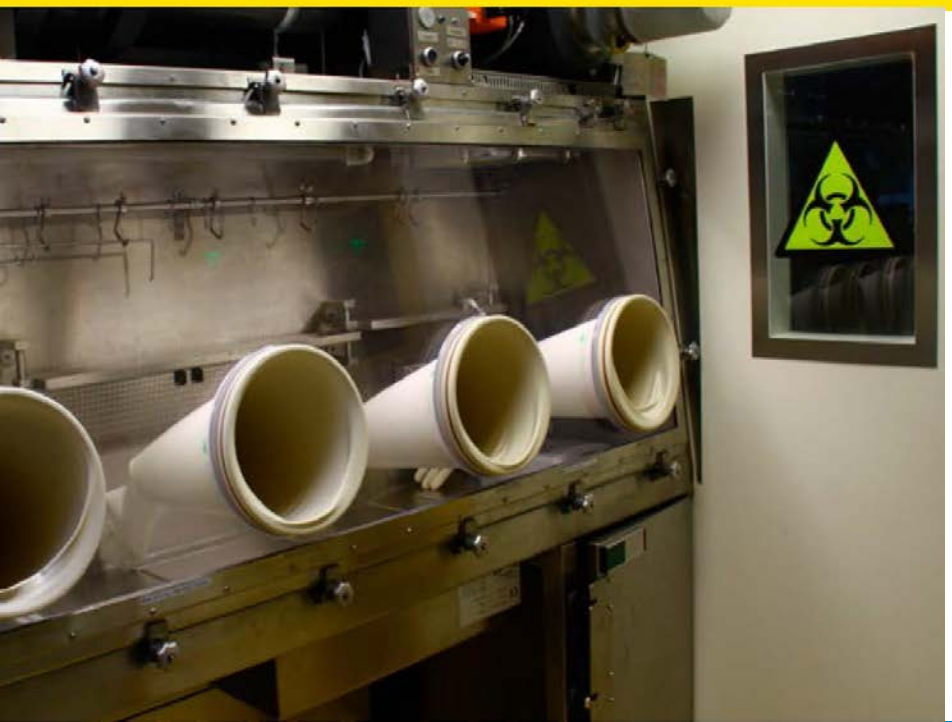
Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

Bureau Biosecurity

Landelijk kennis- en informatiepunt, opgericht door de overheid,
voor organisaties die met risicovolle biologische stoffen en ziekteverwekkers werken

Workshop 7

Inbraak veroorzaakt uitbraak



Uiteraard is de gsm niet verboden,
Trilstand wordt gewaardeerd!

006788

Inbraak veroorzaakt uitbraak

- Bij wie is er ingebroken in de afgelopen 5 jaar?
  - Huis
  - Auto

Kwetsbaarheid – inbraak

Huizen

Inbraak statistieken (sinds 13 november 2013)

In Nederland
67056

Zuid-Holland	Noord-Holland	Noord-Brabant	Gelderland	Utrecht	Limburg
14585	12342	10119	6658	6083	5326

Overijssel	Groningen	Flevoland	Friesland	Drenthe	Zeeland
3454	1995	1888	1849	1624	1126

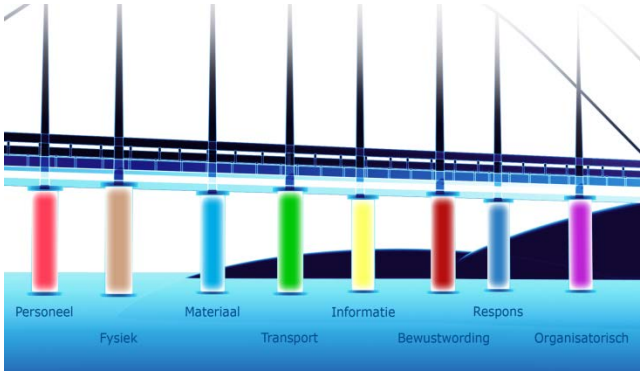
http://drimble.nl/inbraken/ (15 oktober 2014)

Auto's

- 1 op de 15 automobilisten per jaar
- meer dan 438 miljoen euro schade per jaar
  - Laptops
  - Telefoons

Inbraak veroorzaakt uitbraak

Kwetsbaarheden van organisaties op het gebied van fysieke en informatiebeveiliging



Ing. Ruud van den Berg
- Beveiligingscoördinator, RIVM

Ing. Henriette Westerling, MSSM
- Informatiebeveiliging, RIVM

Ing. Harold van den Berg
- Bureau Biosecurity

Opbouw van ‘inbraak veroorzaakt uitbraak’

- Kennis van kwetsbaarheden [15 min]
  - Fysieke beveiliging
  - Informatie beveiliging

- Scenario’s in groepjes [35 min]
  - Beschrijven van kwetsbaarheden en bijbehorende maatregelen

- Kwetsbaarheidsanalyse [15 min]
  - Praktische tool (in ontwikkeling)

- Interactief!
- Informerend, niet concluderend
- Chatham House Rules

Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

Informatiebeveiliging
Fysieke beveiliging

Henriette Westerling
Ruud van den Berg

RIVM

Introductie film

Beveiliging

- Beveiliging
  - Fysieke beveiliging
  - Informatie beveiliging

- Beveiliging is noodzakelijk om de belangen van de organisatie te beschermen tegen alle vormen van (be)dreiging
  - Te beschermen belangen
  - Vormen van (be)dreiging

Informatie beveiliging

- Informatiebeveiliging omvat drie gebieden:
  - beschikbaarheid
  - integriteit
  - exclusiviteit

- Voor biosecurity gaat het voornamelijk om de exclusiviteit. Het beveiligen van gevoelige informatie tegen onbevoegde toegang:
  - Informatie over opslag van biologisch materiaal (wat, waar)
  - Test procedures en uitslagen van diagnostiek
  - Personele informatie van medewerkers van hoog risico labs
  - **Informatie gerelateerd aan beveiligingssystemen en gebouw management systemen**

Informatie beveiliging

- Voorbeelden van maatregelen:
  - Classificatie van informatie
  - Authenticatie en Autorisaties
  - Compartimentering van data
  - Encryptie
  - Logging en monitoring
  - Awareness van medewerkers

Fysieke beveiliging

- Fysieke beveiliging omvat het beveiligen, autoriseren en controleren van de toegang tot vitale ruimten en de aanwezige hoog-risico materialen. Hierdoor wordt de mogelijkheid dat onbevoegden toegang krijgen tot deze ruimten geminimaliseerd.

- Voorbeelden van fysieke maatregelen:
  - Toegangsbeveiliging (terrein-gebouw-vitale ruimte = zonering)
  - Inbraakdetectie met opvolging door (eigen) beveiligingsdienst
  - Cameratoezicht

Film fysieke beveiliging

https://www.youtube.com/watch?v=WABv1gQfT44

Te beschermen belangen (1)

- Hoog-risico biologisch materiaal
  - Materiaal
  - Informatie
  - Proefdieren

Te beschermen belangen (2)

- Bedrijfsgeheimen

- Persoonsgegevens (bijvoorbeeld patiëntgegevens)

- Geclassificeerde / gerubriceerde informatie
  - Detailinformatie opslagruimte

- Bedrijfscontinuïteit

Vormen van (be)dreigingen (1)

- Onbewuste foute handelingen
  - het niet goed inschakelen van de inbraakbeveiliging

- Sabotage / beschadiging IT-systemen / social engineering

- Verlies / diefstal van gevoelige informatie
  - Laptop, harde schijf, USB-stick
  - Hacken van systemen
  - Phishing

Vormen van (be)dreigingen (2)

- Diefstal goederen door
  - (ingehuurde) externen
  - eigen labmedewerkers

- Bedreiging/omkoping medewerker
  - Fraude in combinatie met loonbeslag
  - Via social media is veel informatie over medewerkers te vinden

- Gefrustreerde / ontslagen medewerker

Medewerkers bevinden zich binnen de organisatie en zijn van veel processen op de hoogte – minder barrières in de fysieke en informatiebeveiliging

Vormen van (be)dreigingen (3)

- Een “gestoorde” persoon
  - een vreemde man die een pakketje (poederbrief) op de balie receptie deponeert

- Actievoerders
  - tegen proefdieren
  - tegen vaccinatiebeleid

Beveiliging

- Beveiliging is noodzakelijk om de belangen (hoog-risico materiaal) van de organisatie te beschermen tegen alle vormen van (be)dreiging

- Ondanks goede beveiliging kan een organisatie toch kwetsbaar zijn

Casus - werkwijze

- Opgesplitst in vier groepen
- Per groep wordt één casus uitgewerkt [15 minuten]
  - Ebola vaccin
  - Ontslagen ICT-medewerker
  - Mystery man
  - Storingsmonteur

- Per casus voor fysieke en informatiebeveiliging:
  - Wat zijn de kwetsbaarheden?
  - Welke maatregelen kunnen worden genomen?

- Feedback op flip-over kort toelichten [5 minuten per groep]

Casus 1: Ebola vaccin

Jolanda maakt voor het bedrijf een vertrouwelijk rapport over een nieuw vaccin tegen ebola. De deadline van oplevering aan het Ministerie is morgen om 11:00. Zij besluit het rapport en de labjournaals mee naar huis te nemen, waar ze het rapport afrondt.

Extra informatie:

- Jolanda woont 15 km van het bedrijf in een studentenflat;
- Ze gaat eerst met de bus en vervolgens met de trein;
- Ze werkt thuis op een eigen laptop met een verbinding van het bedrijf.

Casus 2: Ontslag van ICT-specialist

Jan werkt al 16 jaar bij een overheidsinstelling als ICT-specialist. Hij heeft de laatste jaren veel problemen gehad met zijn manager en dat heeft uiteindelijk geresulteerd in ontslag. Jan zal per 1 januari a.s. de instelling moeten verlaten en is hier erg gefrusteerd over.

Extra informatie:

- Binnen de instelling wordt met *Bacillus anthracis* gewerkt
- Jan heeft vanwege zijn functie als netwerkbeheerder toegang tot alle systemen en documenten.
- Jan heeft ook toegang tot E-mail van alle medewerkers

Casus 3: Mystery man

Een mystery man is op het terrein gekomen, in het gebouw waar een hoog-risico laboratorium is gevestigd, waar gewerkt wordt met *Yersinia pestis*. De mystery man is foto's aan het maken van het lab.

Extra informatie:

- De organisatie is zeer groot (1500 medewerkers), met name is het 's morgens erg druk bij de ingang;
- De toegang tot het gebouw is voorzien van een paslezer;
- Op de gang waar het hoog-risico laboratorium zit, zijn ook zitkamers aanwezig.

Casus 4: Storingsmonteur

Op vrijdagmiddag rond 15.00 uur raakt het luchtbehandelingssysteem van het laboratorium defect.

Op zaterdag moet de reparatie zijn afgerond, omdat een groot aantal monsters getest moet worden voor een langlopend experiment met *Coxiella burnetii*.

Via het facilitair bedrijf (FB) wordt een monteur van een extern bedrijf opgeroepen die zelfstandig zijn werkzaamheden gaat uitvoeren

Extra informatie:

- Het bedrijf heeft een raamcontract met uw organisatie;
- Ivm vakanties komt er een andere monteur dan normaal;
- De monteur gebruikt de pas van zijn afwezige collega;
- Door onvoldoende personeel laat bij het FB men de monteur alleen.

Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

Kwetsbaarheidsanalyse

Harold van den Berg
Bureau Biosecurity

Kwetsbaarheid

- Fysieke beveiliging
  - Voorbeelden gepresenteerd door Ruud van den Berg

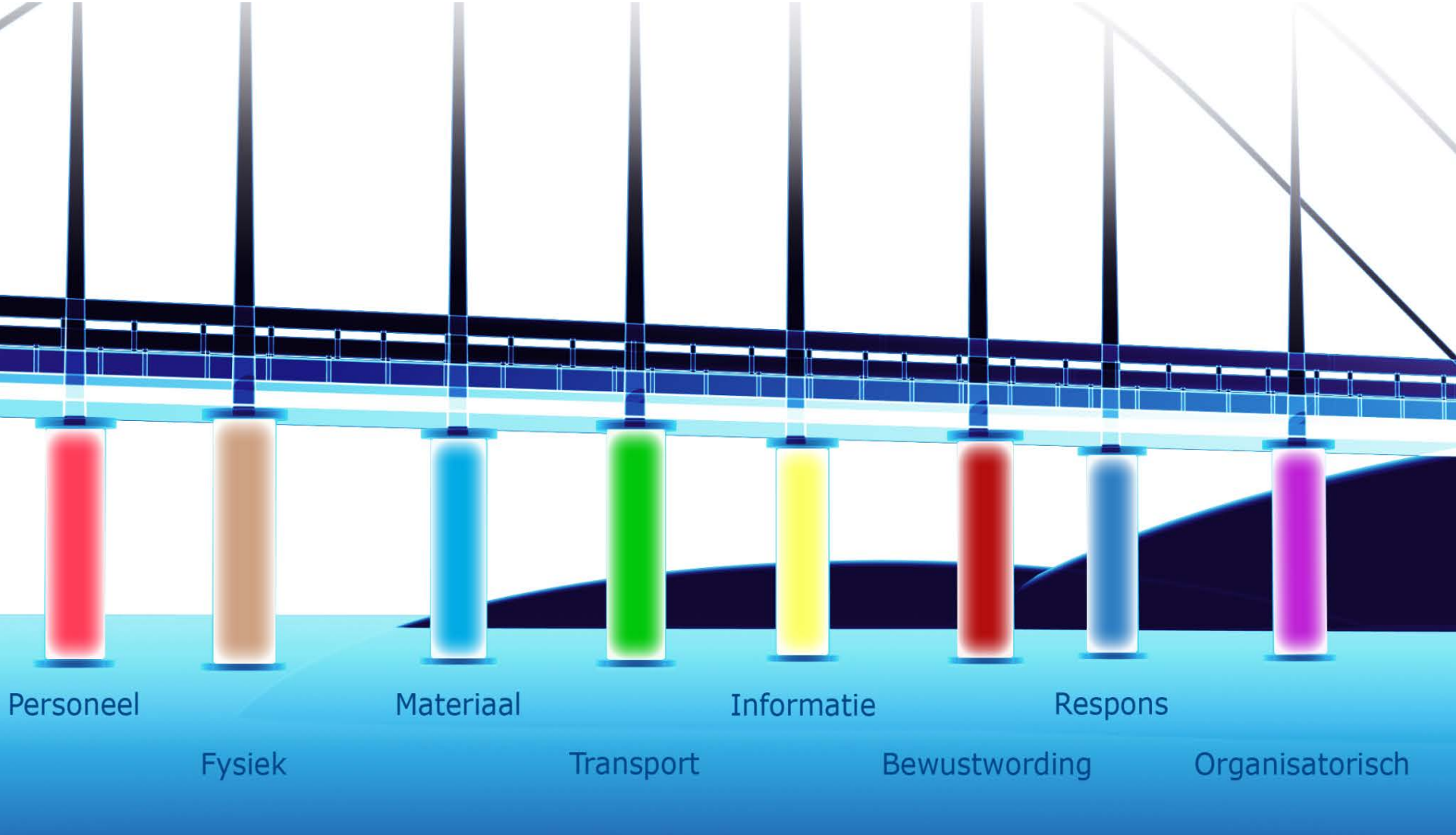
Foto: Bureau Biosecurity

Foto: Thinkstock

- Informatie beveiliging
  - Voorbeelden gepresenteerd door Henriette Westerling

Foto: Thinkstock

Alle 8 pijlers van biosecurity – mogelijke kwetsbaarheid



Voorbeelden van risico – kwetsbaarheidsanalyse

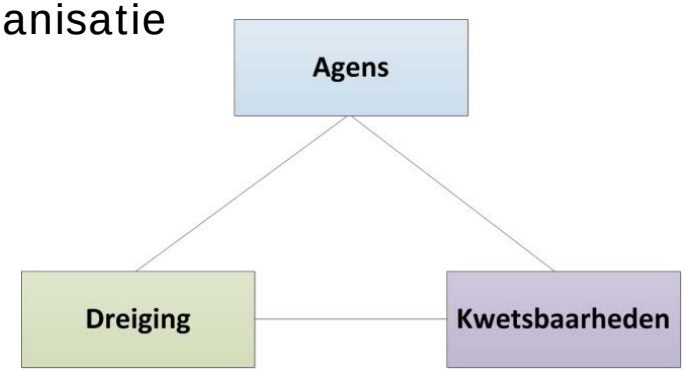
- Toolkit Bureau Biosecurity (www.biosecuritytoolkit.com)
  - Hoe is biosecurity in uw organisatie geregeld?
  - Aanreiken van handvatten voor opzetten en/of verbeteren van biosecurity.

- NCTV (https://cbrnsecurity.nctv.nl)
  - De staat van beveiliging van CBRN materialen bij uw organisatie.
  - Tips hoe het weerstandniveau verhoogd kan worden.

- BioRAM (http://www.sandia.gov/ram/BIORAM.htm)

Kwetsbaarheidsanalyse biosecurity

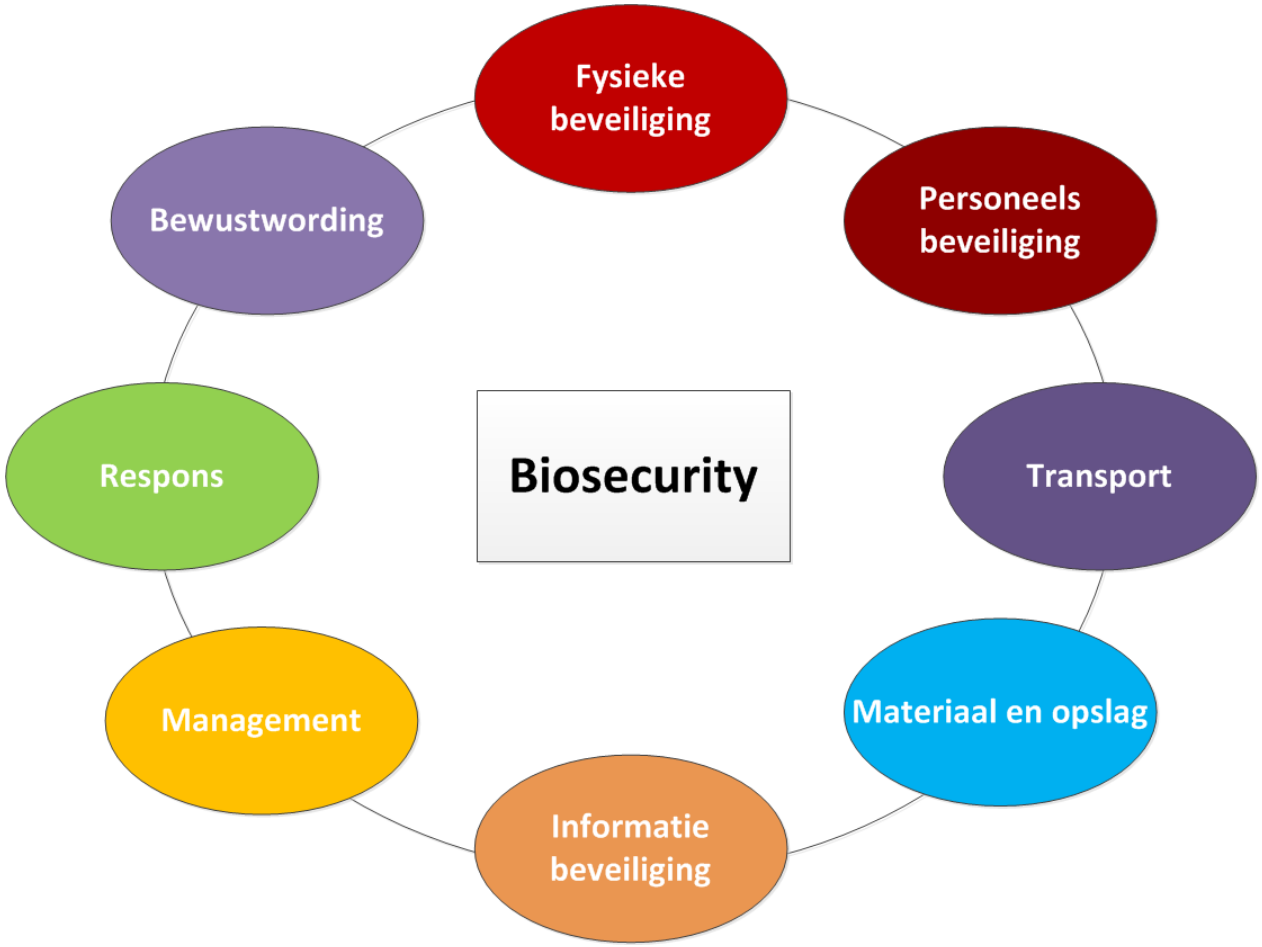
- Aanvulling op de biosecurity toolkit en de NCTV zelfanalyse
  - Kwetsbaarheden in de organisatie



- Een praktische tool
  - Duidelijke en herkenbare voorbeelden
  - Handvatten om de kwetsbaarheid van uw organisatie te verlage

- Geschikt voor meerdere management niveaus

Kwetsbaarheidsanalyse - biosecurity



Kwetsbaarheidsanalyse biosecurity

Per pijler opgesplitst in 3 onderdelen

- Eén hoofdvraag
  - Quick scan, ongeveer 15-30 min voor alle 8 pijlers
- Verdiepende vragen
  - Verder ingaan op de pijler door verdiepende vragen
- Scenario's
  - Een lijst met realistische scenario's

Discussie / conclusie

- Momenteel bezig met de ontwikkeling van de kwetsbaarheidsanalyse: hoofdvragen, verdiepende vragen en scenario's

- Graag jullie reactie op:
  - Quick scan
  - Verdiepende vragen
  - Scenario's

- Wanneer je wilt meedenken over de invulling en testen van de kwetsbaarheidsanalyse
  - biosecurity@rivm.nl

Vragen?

www.bureaubiosecurity.nl
www.biosecuritytoolkit.com

biosecurity@rivm.nl

@B_Biosecurity

Presentaties beschikbaar op www.bureaubiosecurity.nl

Evaluatieformulier (digitaal)

Literatuurbronnen Informatiebeveiliging

		Site
PVIB	Platform voor Informatiebeveiliging	www.pvib.nl
NCSC	Nationaal Cyber Security Centrum[1]	www.ncsc.nl
CIP	Centrum Informatiebeveiliging en Privacybescherming	www.cip.nl
ENISA	European Union Agency for Network and Information Security	www.enisa.europa.eu
NIST	National Institute of standards and technology	www.nist.gov
Surf	ICT-samenwerkingsorganisatie van het hoger onderwijs en onderzoek	www.surf.nl
OWASP	Open Web Application Security Project	www.owasp.org
SANS	SANS Institute	www.sans.org
ISC2	ISC2 (CISSP)	www.isc2.org
NEN	NEN ISO 27001/ISO 27002/ISO 7510	www.nen.nl

[1] Zie voor het cybersecuritybeeld van Nederland het trendrapport 'Cybersecuritybeeld Nederland CSBN-4'.