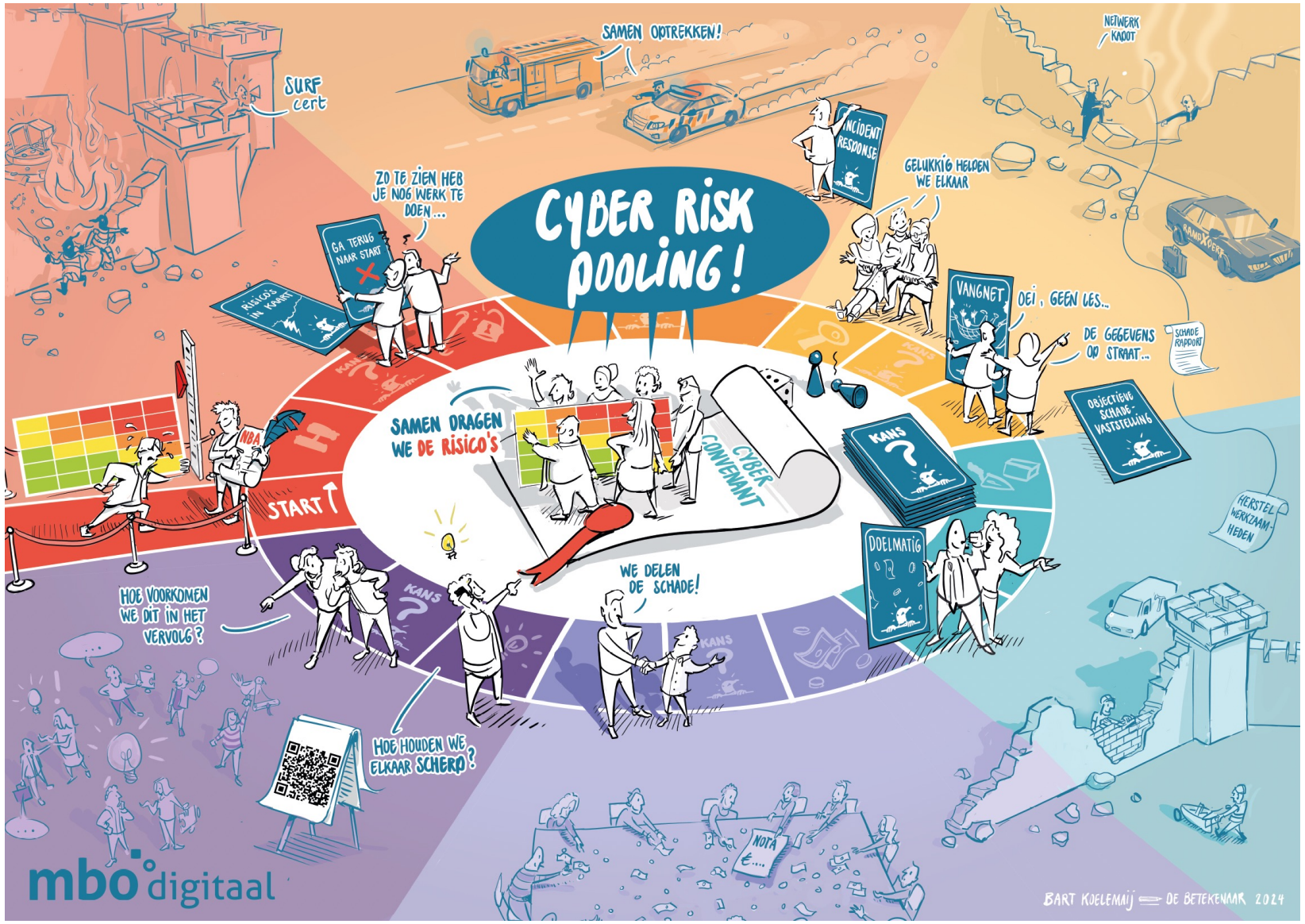
Cyberrisicopooling als alternatief voor cyberverzekeringen

- Aanleiding
- Ervaringen met cyberverzekeringen
- De voordelen van een risicopool
- Randvoorwaarden voor een risicopool
- Uitwerking van scenario’s
- Conclusies en vervolgstappen

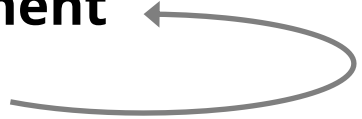
mbo digitaal



mbo digitaal

Convenant cyberveiligheid mbo

- Aangenomen in de AV in juni en ondertekend in september ‘23
- Afspraken over samenwerken aan cyberveiligheid
  - Governance IBP in het mbo
  - Normen/toetsingskaders IB en P
  - Volwassenheid en risicomanagement via GRC-applicatie
  - Deelname benchmarks IB&P en externe security-audits
  - Gezamenlijke optrekken met cloudleveranciers
  - **Gezamenlijke aanpak crisismanagement**
  - **Beperken impact cyberincidenten**



mbo digitaal

Wat is het (cyber)risico

- Onderwijssector is sterk afhankelijk geworden van ICT
- Kans op een hack is klein en statistisch moeilijk te bepalen
- Impact is groot
  - losgeld (reken met 2% jaaromzet)
  - kosten herstel IT-omgeving
  - kosten incidentrespons
  - inkomstenderving
  - schadeclaims
  - boetes
  - reputatieschade
- We rekenen met een schadebedrag van 2,5 miljoen

mbo digitaal

Omgaan met het risico

Drie opties

1. het risico zelf dragen > aanhouden reserve
2. het risico overdragen > cyberverzekering
3. gezamenlijk het risico dragen > risicopool

- Enquete cyberverzekeringen (35 mbo-scholen)
  - 9 hebben een cyberverzekering
  - 26 dragen het risico zelf (al dan niet vrijwillig)

mbo digitaal

Ervaringen met cyberverzekeringen

- Strikte toelatingseisen
  - Grote hoeveelheid vragen en bewijsstukken
  - Niet in lijn met ons eigen IB-assessment
  - (Nog) niet haalbaar voor veel (kleine) mbo-instellingen
- Veel uitsluitende bepalingen
  - Als schade (deels) toerekenbaar is aan de mbo-instelling
  - Bij wijdverspreide incidenten wordt de uitkering beperkt
- Hoog eigen risico
- Hoge premie
- Twijfel: komt het wel tot een uitkering bij een incident…

mbo digitaal

Gezamenlijk risico's dragen via een cyber risk pool

- Onderling delen van cyberrisico's zonder tussenkomst van een verzekeraar
- Op basis van een **contractuele afspraak** staan de instellingen garant voor elkaar
- De leden leveren alleen een financiële bijdrage als er **daadwerkelijk schade** is
- Schade wordt vastgesteld door een **onafhankelijke schade-afhandelaar**
- Het schadebedrag wordt gedeeld door de leden van de risicopool

➢ gekoppeld aan **strikte voorwaarden** voor deelname aan de pool

mbo digitaal

De voordelen van een risicopool

- Kent een ingebouwde prikkel voor **samenwerken** en elkaar helpen op het gebied van cyberveiligheid
- Stimuleert wederzijdse monitoring, **kennisdeling** en bewustwording
- Benchmarken en externe **security-audits** krijgen nog meer betekenis
- De **sterkste schouders** kunnen de zwaarste lasten dragen
- De **toelatingseisen** bepalen we als sector zelf (toetsingskader IB)
- **Incidentrespons** en schade-afhandeling kan mbo-breed georganiseerd
- De uitgespaarde verzekeringspremies kunnen door de scholen worden geïnvesteerd in **mitigerende maatregelen**

mbo digitaal

Randvoorwaarden voor een succesvolle risicopool

- De leden moeten elkaar **kennen en vertrouwen**
- De leden leggen naar elkaar **verantwoording** af over risico's en maatregelen (via self-assessments en externe audits)
- Leden zijn bereid **elkaar te helpen** om de weerbaarheid te verhogen
- De pool heeft **een zekere omvang** nodig om de schade te kunnen opvangen

➢ De mbo-sector voldoet aan alle randvoorwaarden voor een succesvolle risicopool!

mbo digitaal

Uitwerking: het aandeel in de pool

- Scenario's
  1. op basis van het **IB-volwassenheidsniveau** van de instelling
     - hogere volwassenheid leidt tot een lager risico en daarmee een lager aandeel in de pool
  2. op basis van de gekozen **dekking** en het **eigen risico**
     - instellingen die kiezen voor een beperktere dekking dragen in het collectief minder bij aan het risico wat zich vertaalt in een geringer aandeel
  3. op basis van het aantal **ingeschreven studenten**
     - een gebruikelijke manier voor mbo-instellingen om bij te dragen aan gemeenschappelijke voorzieningen
  4. de schade wordt **gelijk verdeeld**, ongeacht de grootte of het risico van de instelling
- Ook een combinatie is mogelijk, bijvoorbeeld scenario 1 en 3

mbo digitaal

Uitwerking: incidentrespons

- Gemeenschappelijk organiseren van processen
  - SOC, CERT, cyber-forensics, incidentrespons, schade-expertise, het bieden van uitwijkopties en herstel van de schade
- Niet gebonden aan een verzekeraar
- In plaats van individuele retainer-overeenkomsten
- Incidentrespons en schade-afhandeling gezamenlijk aanbesteden
  - betere informatie-uitwisseling
  - sneller reageren
  - doelmatig: kostenbesparing

mbo digitaal

Uitwerking: schade-afhandeling

- Onafhankelijke schade-afhandelaar
  - schade beperken: biedt tegenwicht aan partijen voor incidentrespons
  - doelmatige besteding van middelen
  - bewaakt dat getroffen instelling niet in een betere positie komt dan daarvoor

➢ Cruciaal voor het vertrouwen van de leden in de risicopool

mbo digitaal

Uitwerking: financieel rekenvoorbeeld

- Financiele ruimte van de risicopool
  - Uitgaande van de gemiddelde jaarlijkse (!) verzekeringspremie:
    55 instellingen x € 60.000 = 3,3 miljoen euro in een (virtueel) fonds
  - afhankelijk van eventuele schade en andere kosten wordt dit aangevuld
  - het bestuur van de risicopool besluit hierover
- Vaste kosten
  - retainer voor schade-afhandeling en incidentrespons (=verschuiving van kosten)
  - bureaukosten (bijv. als dienst SURF)
  - ➢ via jaarlijkse bijdrage van de leden

mbo digitaal

Maar we benoemen hier ook de olifant…

- De leden moeten comfortabel zijn met een verdeelsleutel (aandeel in de pool) die niet 100% overeenkomt met het werkelijke individuele risico. Je loopt risico voor je collega-instelling die het welicht iets minder goed voor elkaar heeft dan jij.
- Er is een (hypothetisch) risico dat een groot deel, of zelfs alle instellingen tegelijkertijd getroffen worden en de risicopool zijn werking verliest.

➢ Is dit in een verzekeringsscenario beter geregeld?

mbo digitaal

Opstarten van een risicopool (1)

1. Bepaal wat wel/niet wordt gedekt
   - bijvoorbeeld incidentrespons, herstel, maar niet de betaling aan criminelen
2. Bepaal de maximale uitkering en eigen risico
   - bijvoorbeeld 2,5 miljoen in combinatie met een hoog eigen risico (€100.000)
3. Bepaal de toelatingseisen
   - bijvoorbeeld de aansluiting op een SOC en een minimale score op (delen) van het toetsingskader IB (eventueel aangevuld met specifieke CIS controls)
4. Bepaal de verdeling van het aandeel in de pool
   - iedere deelnemer voor een gelijk deel, of op basis van studentenaantal, volwassenheidsscore (of een combinatie van deze factoren)

mbo digitaal

Opstarten van een risicopool (2)

5. Selecteer een schadeafhandelaar
   - het contract met de gespecialiseerde onafhankelijke schadeafhandelaar wordt door de pool aanbesteed
6. Organiseer de incidentrespons-keten
   - de pool maakt bij voorkeur gebruik van een gemeenschappelijke SOC en CERT-functie, op basis waarvan een incident respons partij wordt gecontracteerd (voor zover deze functie niet door de schadeafhandelaar wordt verzorgd)
7. Organiseer een bureau voor de administratieve taken
   - mogelijk kan SURF dit als dienst aanbieden
8. Werk de statuten en het contract uit
9. Formeer het bestuur van de risicopool

mbo digitaal

Conclusies en vervolgstappen

- We hebben een goede voedingsbodem binnen het mbo
- Risicopooling is veel meer is dan enkel het afdekken van risico's: het is een extra drijfveer in de samenwerking en kennisdeling tussen de mbo-scholen op het gebied van cyberweerbaarheid
- Vertrouwen in elkaar cruciaal. Dat moet worden onderbouwd door middel van externe security-audits, in combinatie met het toepassen van de met elkaar afgesproken minimale set aan maatregelen op het gebied van cyberweerbaarheid.
- Informatierondes voor de netwerken van MBO Digitaal

mbo digitaal

Conclusies en vervolgstappen

mbo digitaal

Conclusies en vervolgstappen

MBO Digitaal conferentie

- workshop met de bestuurders op 7 maart
  - akkoord en opdracht om de aanpak verder uit te werken
  - plan van aanpak gereed op volgende conferentie (okt ‘24)
- workshop met de netwerken op 8 maart
  - ophalen aandachtpunten voor verdere uitwerking

➢Lees het rapport (op aanvraag beschikbaar)

➢Neem contact met ons op voor meer info en feedback

- Martijn Bijleveld (m.bijleveld@mbodigitaal.nl)
- Peter Vermeijs (p.vermeijs@mboraad.nl)