Cyberrisico's bij PUO's: inzicht voor bestuurders

Pensioenfondsbesturen zijn eindverantwoordelijk voor cyberrisico's, maar beschikken niet over de informatie die nodig is om die verantwoordelijkheid goed te dragen. Hoe verklein je dit structurele informatienadeel?

Door *Adam Barszczowski*

Pensioenfondsen leunen sterk op hun pensioenuitvoeringsorganisatie (PUO) voor administratie, IT-processen en gegevensuitwisseling. Daarmee ligt de digitale weerbaarheid van een fonds grotendeels buiten de eigen muren. Toch verlangt de toezichthouder dat het bestuur aantoonbaar 'in control' is met betrekking tot cyberrisico's. Hier ontstaat een complexe paradox: de verantwoordelijkheid ligt bij het fonds, maar de relevante informatie ligt bij de PUO. Dit is geen operationeel detail, maar een structureel governance- en informatieprobleem.

Waarom dit probleem ontstaat

De kern van dit probleem is informatieasymmetrie. De PUO heeft gedetailleerde kennis over systemen, kwetsbaarheden, incidenten en herstelcapaciteit. Het fonds ontvangt vooral dashboards, ISAE-rapporten en abstracte RAG-scores. Daardoor ziet het bestuur wel 'dat er controles bestaan', maar niet of die effectief zijn wanneer het echt misgaat.

Dit mechanisme sluit direct aan bij de economische theorie van verborgen kwaliteit van de Amerikaanse econoom George Akerlof: wanneer de afnemer kwaliteit niet kan beoordelen, ontstaat een prikkel voor de leverancier om te investeren in zichtbare compliance in plaats van echte weerbaarheid.

'Een gezamenlijke benchmark voor PUO-kwaliteit, zelfs geanonimiseerd, maakt verschillen tussen pensioenfondsen zichtbaar en stimuleert verbetering.'

Tegelijk is er sprake van moral hazard. De PUO draagt de kosten van extra beveiliging, terwijl de reputatieschade, maatschappelijke impact en toezichtdruk vooral bij het fonds terechtkomen. De prikkels zijn dus misaligned. Een incident bij een grote PUO heeft bovendien externe effecten: meerdere fondsen worden geraakt, met mogelijk systeemrisico voor de sector.

Hoe dit zich uit in de praktijk

Besturen ontvangen een overvloed aan documenten, maar de informatie is gefilterd, juridisch geoptimaliseerd en vaak te hoog-over. Formele assurance richt zich vooral op het 'design en bestaan' van controls. Het zegt weinig over:

- werkelijke kwetsbaarheden
- technische testresultaten
- detectievermogen en responssnelheid
- forensische paraatheid
- afhankelijkheden van ketenpartners

Hierdoor ontstaat schijnzekerheid. Bestuurders krijgen comfort, maar geen blauwdruk van de daadwerkelijke digitale weerbaarheid. De governance-afstand zorgt ervoor dat nuances verdwijnen. Een groene KPI-score verbergt vaak meer dan ze onthult.

De rol van DORA

DORA versterkt het toezicht, maar legt tevens het fundamentele probleem bloot. De wettelijke verantwoordelijkheid ligt bij het fonds, terwijl de implementatie grotendeels bij de PUO ligt. De PUO hoeft veel informatie nog niet wettelijk te delen, terwijl het fonds die informatie wél moet kunnen overleggen aan de toezichthouder. Hierdoor wordt de asymmetrie niet kleiner, maar zichtbaarder.

Impact voor bestuurders

De asymmetrie raakt drie elementen van goed bestuur:

1) **Risicobeoordeling wordt onbetrouwbaar**
   Besturen beoordelen abstracte rapportages die weinig zeggen over reële aanvalsscenario's.
2) **Toezicht wordt reactief in plaats van proactief**
   Incidentinformatie komt pas achteraf. Besturen missen zicht op near misses, trends en risicogedrag.
3) **Verantwoordelijkheid en invloed lopen uiteen**
   Het bestuur is juridisch verantwoordelijk, maar heeft beperkte toegang tot de kennis die nodig is om deze rol goed te vervullen.

In de praktijk betekent dit dat bestuurders vaak meer vertrouwen op 'vertrouwensrelaties' dan op toetsbare informatie. Dit maakt cybergovernance kwetsbaar, zeker in een sector met concentratierisico bij enkele grote PUO's.

Mogelijke oplossingsrichtingen

1) Van compliance naar effectiviteit
Besturen hebben minder behoefte aan nóg een assurance-rapport en meer aan bewijs dat beveiliging werkt. Denk aan:
- inzage in red-teamresultaten (geanonimiseerd, onder NDA)
- outcome-gerichte indicatoren: detectietijd, hersteltijd, lessons learned
- periodieke evaluaties van responskwaliteit
- trendanalyses van kwetsbaarheden en near misses

Dit verplaatst de discussie van 'bestaan controles?' naar 'werken controles ook als het er echt toe doet?'

2) Continu toezicht in plaats van jaarlijkse momenten
Cyberdreigingen veranderen dagelijks. Jaarlijkse ISAE-toetsing is onvoldoende. Een werkbaar model bevat:
- kwartaalgesprekken tussen CISO's
- halfjaarlijkse thematische deep dives
- tussentijdse updates bij significante wijzigingen

Hiermee ontstaat een dynamische informatiepositie en een vroegsignalerend toezichtmodel.

3) Sectorbrede benchmarking
Omdat individuele fondsen weinig zicht hebben op elkaars PUO-kwaliteit, ontbreekt een reputatiemechanisme dat kwaliteitsdruk creëert. Een gezamenlijke benchmark, zelfs geanonimiseerd, maakt verschillen zichtbaar en stimuleert verbetering.

Het vermindert asymmetrie niet door meer informatie, maar door vergelijkbare informatie.

4) Structurele toegang tot near misses
Near misses geven vaak meer inzicht dan echte incidenten, omdat ze laten zien waar het bijna misging. Een categorie-rapportage (zonder operationele details) helpt bestuurders te beoordelen:
- waar zwakke plekken zitten
- of de organisatie lerend vermogen toont
- of verbetermaatregelen effect hebben

Dit is precies het type 'praktisch verifieerbare' informatie dat ISAE-rapporten niet bieden.

5) Versterken van de governancecapaciteit van het fonds
Meer transparantie heeft alleen waarde als het bestuur de kennis heeft om deze te duiden. Daarom is het volgende noodzakelijk:
- structurele versterking van audit- en risicocommissies
- periodieke scholing voor bestuurders
- directe, niet-gefilterde gesprekken op MT-niveau (CISO, CTO)

Goede cybergovernance kan alleen bestaan wanneer de informatie-ontvanger in staat is de inhoud te doorgronden.

6) Prikkelstructuren herzien
Zolang de PUO investeert en het fonds de schade draagt, blijft asymmetrisch gedrag rationeel. Mogelijkheden om dit te corrigeren zijn:
- het koppelen van performance-indicatoren aan cybersecurityresultaten
- het delen van contractueel risico bij onvoldoende weerbaarheid
- verzekeraars laten toetsen op daadwerkelijke effectiviteit (niet op papieren compliance)

Dit maakt waarheidsgetrouwe informatie voor beide partijen economisch aantrekkelijker.

Nuance: waarom dit in de praktijk lastig is

Het verkleinen van asymmetrie vergt niet alleen technische maatregelen, maar vooral een andere informatierelatie tussen fonds en PUO. Bestuurders willen diepere inzichten op basis van hun fiduciaire verantwoordelijkheid, maar zijn voor die informatie afhankelijk van dezelfde PUO. Transparantie wordt zo deels een onderhandelingsvraag.

Ook prikkelherziening vraagt zorgvuldigheid. Wat in de literatuur logisch klinkt, kan in de relatie worden ervaren als wantrouwen. Governance is daarom altijd een balans tussen controle en samenwerking.

DORA helpt om extra informatie te kunnen vragen, maar lost de kern niet op: de kennis blijft bij de PUO, de verantwoordelijkheid bij het fonds. Bestuurders moeten daarom actief sturen op 'verifieerbare informatie', en niet alleen op rapportages. ■

Adam Barszczowski
bestuurslid pensioenfondsen, geschreven op persoonlijke titel

IN HET KORT

Pensioenfondsbesturen dragen de verantwoordelijkheid voor cyberrisico's, maar missen toegang tot essentiële informatie.

Informatie-asymmetrie, misaligned incentives en sectorafhankelijkheid versterken dit probleem.

Oplossingen liggen in effectiviteitstoetsing, continu toezicht, deling van near-misses, benchmarking en governance-versterking.

DORA biedt steun, maar verandert het fundamentele informatienadeel niet.

Alleen door andere informatierelaties kan een bestuur echt 'in control' komen.

FOTO: ARCHIEF SPF