Digitalisering en data:

Nieuwe uitdagingen voor het risicomanagement van pensioenfondsen

De digitale transformatie verandert de bedrijfsvoering van pensioenfondsen: technologische vernieuwing is van steeds grotere waarde en bepalend voor het bedrijfsmodel. Naast kansen voor het versterken van de organisatie, zoals het maken van geautomatiseerde data-analyses, verbeterde communicatie met belanghebbenden en een lagere kostenstructuur, stelt digitalisering pensioenfondsen ook voor nieuwe risico's. Het voldoen aan stringentere wetgeving, opkomende dreigingen als cybercriminaliteit en uitbesteding van IT-zaken vergen dat het (operationeel) risicomanagement van fondsen hier beter op wordt toegerust. Een opvatting die ook steeds nadrukkelijker door externe toezichthouders wordt geventileerd: wat doen fondsen om IT-, informatie- en privacyrisico's adequaat te beheersen? Dit artikel biedt inzicht in de consequenties van digitalisering voor het risicomanagement van pensioenfondsen en schetst drie nieuwe rollen aan de hand waarvan nieuwe risico's beter worden beheerst: de rol van privacybeschermer, van ketenregisseur en van incidentmanager.

Bestaande organisatiemodellen en waardeketens wijzigen ingrijpend als gevolg van digitalisering en nieuwe toepassingen van data. Dit is uiteraard ook het geval voor pensioenfondsen, waar informatietechnologie een bepalende – zo niet onderscheidende – factor is geworden voor klanttevredenheid, efficiency, schaalvergroting en daarmee het voortbestaan op langere termijn. Kennis, vraagstukken en het inschatten van risico's met betrekking tot digitalisering en data komen hiermee nadrukkelijk op het terrein van de pensioenfondsbestuurders te liggen.

De nationale Cyber Security Raad constateerde in april 2017 dat organisaties in Nederland nog te weinig doen aan digitale veiligheid. Ook lezen we in het meest recente Cybersecuritybeeld Nederland van het Nationaal Cybersecurity Centrum (NCSC) dat gijzeling van systemen door cybercriminelen ('ransomware') een groeiend maatschappelijk probleem vormt. Hetzelfde geldt voor de kans op fraude door manipulatie van systemen. Goed beheer van IT- en informatierisico's is daarom cruciaal. Het gaat daarbij niet alleen om risico's als cybercrime, maar ook om technisch falen – zoals netwerkonderbreking – als ook om onzorgvuldige omgang met data. Dit is eveneens het standpunt van toezichthouders De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM), die zowel verkenning uitvoeren, als hun toezichtskaders op deze nieuwe risico's toerusten. Ook de aanstaande (verdere) aanscherping van de privacywetgeving en de toenemende uitbesteding van kernactiviteiten en IT-kernfuncties ('outsourcing') spelen daarbij een rol.

Het (operationeel) risicomanagement van pensioenfondsen moet nader op bovengenoemde risico's worden toegerust. Dat vergt dat het bestuur en management van pensioenfondsen het risicomanagement vanuit een drietal nieuwe rollen moet gaan versterken. We lichten de rollen van 1) privacybeschermer, 2) ketenregisseur en 3) incidentmanager hierna toe en maken duidelijk hoe fondsen nieuwe risico's beter kunnen beheersen.

Het perspectief van privacybeschermer

Pensioenfondsen en hun ketenpartners verwerken op steeds grotere schaal privacygevoelige informatie: data vormen daarmee een essentieel onderdeel van de taakuitvoering van pensioenfondsen. Het gaat daarbij uiteraard om de persoonsgegevens van belanghebbenden (voor het gemak hierna 'deelnemers') maar evengoed om personeelsgegevens. In veel gevallen gaat het om bijzondere persoonsgegevens, bijvoorbeeld om data die extra gevoelig zijn vanwege hun

Wij helpen u graag succesvol te ondernemen

Neem contact op met:

Dennis de Hoog
Managing Consultant
010 448 7847
06 558 527 68
dennis.de.hoog@aon.nl

Wessel Exterkate
Consultant
06 113 169 84
wessel.exterkate@aon.nl

aon.nl/agrc

medische karakter (verzuiminformatie), gegevens over arbeidsongeschiktheid of gegevens die van financiële aard zijn. Deze gegevens zijn binnen de fondsen zelf beschikbaar, maar worden doorgaans ook met uitbestedingspartners als pensioenuitvoerders, vermogensbeheerders en payroll providers gedeeld.

Pensioenfondsen moeten daarom in kunnen staan voor de adequate bescherming van aan hen toevertrouwde deelnemers- en personeelsgegevens. Naast dat de deelnemer dit van het pensioenfonds verwacht vanwege het belang van de bescherming van persoonsgegevens, wordt dit ook vereist vanwege de nieuwe wetgeving en het verscherpte toezicht. Een duidelijk zichtbare trend is dat de wetgever organisaties in toenemende mate expliciet verantwoordelijk maakt voor de bescherming van persoonsgegevens. Deze trend is reeds in 2016 ingezet met de aanscherping van de Wet bescherming persoonsgegevens (Wbp), in de vorm van de ingestelde meldplicht voor organisaties om datalekken te melden en de hieraan gekoppelde boetebevoegdheid. Deze ontwikkeling zet zich voort in de aanloop naar het van kracht worden van de Europese Privacyverordening (General Data Protection Regulation, kortweg 'GDPR') per 25 mei 2018. Deze nieuwe wetgeving legt aanvullende eisen op voor gegevensbescherming door pensioenfondsen. Dit heeft als gevolg dat het voor pensioenfondsen niet langer voldoende is om aan te nemen dat er aan de nieuwe eisen wordt voldaan: dit zal ook aantoonbaar moeten worden gemaakt. Het recent door de Pensioenfederatie uitgebrachte Servicedocument (april 2017) onderschrijft dit.

Het beschikken over bewijslast dat een pensioenfonds per 25 mei 2018 daadwerkelijk voldoet – leert onze ervaring – vergt aanvullende inspanningen en investeringen. Alle risicovolle verwerkingen van persoonsgegevens dienen bijvoorbeeld te worden onderworpen aan een risicoanalyse (een zogeheten Data Privacy Impact Assessment, afgekort DPIA). Ook dienen fondsen een 'verwerkingsregister' op te stellen welk inzicht geeft in alle persoonsgegevens die door de organisatie en haar partners worden beheerd. In dit register moet onder andere inzicht worden gecreëerd welke persoonsgegevens uw organisatie verwerkt, wat de verwerkingsdoeleinden zijn, hoe lang de gegevens worden bewaard en welke maatregelen zijn getroffen om privacyrisico's te beperken. Verder dienen pensioenfondsen hun activiteiten en processen conform de GDPR te hebben ingericht, als ook te documenteren, te evalueren, te wijzigen en te verbeteren. De boetes voor het niet voldoen aan de wettelijke vereisten kunnen oplopen tot EUR 20 miljoen. Met de inwerkingtreding van de nieuwe regelgeving wordt privacybescherming een vast aandachtspunt binnen het risicobeheer van fondsen. De wijze waarop het operationeel risicobeheer invulling krijgt dient daar dan ook op te worden toegerust.

1. Veranker privacy- en gegevensbescherming op het hoogste niveau binnen uw organisatie
2. Voer een analyse uit om uw privacyrisico's te identificeren en middels passende technische en organisatorische maatregelen te beheersen (DPIA)
3. Maak een verwerkingsregister met daarin de vastlegging hoe privacygevoelige gegevens worden verwerkt.
4. Classificeer uw persoonsgegevens zodanig dat u voldoet aan wettelijke bewaartermijnen én zodat u gegevens tijdig kunt verwijderen
5. Evalueer bestaande contracten met partijen waarmee u gegevens deelt. U bent verplicht verwerkersovereenkomsten te sluiten
6. Stel een procedure op voor het adequaat anticiperen en afhandelen van een datalek
7. Verhoog het privacybewustzijn van uw medewerkers door gerichte activiteiten
8. Stel op de Verordening gebaseerd privacybeleid op of pas het bestaande beleid hierop aan.
9. Informeer de betrokkenen over wat er met hun persoonsgegevens gebeurt
10. Stel vast of uw organisatie over een functionaris gegevensbescherming moet beschikken

Het perspectief van ketenregisseur

Was uitbesteding van IT-kernfuncties vijf jaar geleden nog omstreden, inmiddels zijn 'cloud' diensten voor derden gemeengoed geworden. Outsourcing (het uitbesteden van IT-processen, beheer en onderhoud) biedt pensioenfondsen de kans om de eigen IT-investeringslast te beperken. Verder biedt het uitbesteden van IT-beheer aan gespecialiseerde derden – in tegenstelling tot wat vaak wordt aangenomen – een impuls voor de kwaliteit, continuïteit en security van IT-diensten. Uitbesteding lijkt daarmee dé oplossing voor veel inherente IT-problemen en risico's. Naast uitbesteding van kernfuncties als de pensioenverwerking, het vermogensbeheer en de netwerkinfrastructuur maken organisaties meer en meer gebruik van door derden ontwikkelde en beheerde applicaties. Denk bijvoorbeeld aan applicaties voor beleggingsdoeleinden, boekhoudpakketten of HR-systemen. Deze applicaties zijn vaak cloud based en verminderen ook de kosten die gemoeid gaan met de ontwikkeling en beheer van eigen applicaties.

Deze ontwikkelingen maken dat pensioenfondsen steeds sneller verworden tot digitale netwerkorganisaties, actief in een landschap van verschillende uitbestedingspartners en IT-leveranciers. Naast evidente voordelen, noodzaakt samenwerking in de digitale supply chain ook tot gezamenlijke aandacht voor risico's. Deze verdwijnen immers niet na het ondertekenen van een contract. Sterker nog, deze blijven in de meeste gevallen de directe verantwoordelijkheid van de opdrachtgever. Daarnaast is het de vraag hoe uitbestedingspartners op hun beurt de kwaliteit, continuïteit, veiligheid en privacy van klanten in de dagelijkse praktijk waarborgen. Pensioenuitvoerders, leveranciers van IT-diensten en databewerkers kunnen immers net zo goed doelwit zijn van cybercriminaliteit of zelfs de oorzaak van een gevoelig datalek zijn. Dit kan een potentieel grote impact hebben op een pensioenfonds.

Ondanks dat de meeste fondsen al ervaring hebben met het uitbesteden van kernprocessen en functies, blijkt toch vaak dat het in de praktijk bewerkelijk en ingewikkeld is om toe te zien op het adequaat beheer van de risico's van fondsen door uitbestedingspartners. Onze observatie is dat deze samenwerking nieuwe eisen stelt aan het operationeel risicomanagement van fondsen:

1. Zicht op de risico's gemoeid met uitbesteding in de digitale keten voor de pensioenadministratie en verwerking is noodzakelijk;
2. Digital supply chain risk management moet worden ingebed in het operationeel risicomanagement van fondsen - waaronder ook in het risicoprofiel;
3. Beheersing van digitale en datarisico's moet vast onderdeel zijn van het inkoop- en aanbestedingstraject;
4. Het moet duidelijk zijn welke eisen er op het gebied van kwaliteit, continuïteit, security én privacy aan dienstverleners wordt gesteld, deze moeten congruent zijn aan de wetgeving en eisen die door DNB en de AFM worden gesteld;
5. IT-dienstverleners en databewerkers moeten aantoonbaar kunnen maken dat risicobeheer ook bij hen in goede handen is (bijvoorbeeld op basis van relevante certificering voor informatiebeveiliging zoals de ISO 27001);
6. Uitbestedingspartners dienen aantoonbaar te voldoen aan de nieuwe privacyrichtlijnen (GDPR);
7. Eisen ten aanzien van risicobeheer dienen te worden vervat in de af te sluiten contracten en service level agreements;
8. Opdrachtgevers moeten de mogelijkheid hebben om te allen tijde inzage te hebben in de voor hun relevante risico's bij uitbestedingspartners en – desgewenst – site visits, audits en testen te kunnen uitvoeren;
9. Het moet volstrekt duidelijk zijn hoe er in het geval van incidenten die impact kunnen hebben op de opdrachtgever, snel en adequaat wordt gehandeld om de gevolgen te beperken;
10. Uitbestedingspartners dienen te beschikken over toereikende financiële waarborgen voor de financiële schade door digitale en data-incidenten, bijvoorbeeld in de vorm van een (cyber)verzekering.

Het perspectief van incidentmanager

Digitale of 'cyber' risico's zijn een relatief nieuw en actueel fenomeen. Hierdoor ontbreekt het nog aan historische data, welke onderbouwd inzicht geven in de omvang van schade door cyberincidenten, zoals bij traditionele schadestatistieken. Daarbij komt dat de aard van deze risico's voortdurend en snel aan verandering onderhevig is en deze risico's daarmee fundamenteel onvoorspelbaar zijn: onzekere voorvallen die zich tot op heden niet goed lenen voor kansberekening.

Beheersing van digitale risico's dient zich niet alleen te richten op het reduceren van de kans maar tevens op hoe om te gaan met de gevolgen als incidenten zich daadwerkelijk voordoen: 'wat je niet kan voorkomen, daar moet je alsnog van kunnen genezen'. Uiteraard kan de kans op optreden van digitale risico's wel beperkt worden, maar (eventueel onacceptabele) restrisico's zullen blijven bestaan: incidents will happen. Dat is over het algemeen geen geruststellende gedachte, maar we een reële aanname voor bestuurders.

Pensioenfondsen zijn geen techbedrijven en investeren uiteindelijk proportioneel in het beperken van digitale risico's. Naast investeren in een robuuste en veilige IT, is het van belang om goed voorbereid te zijn op de impact van digitale incidenten. Wat kan er gebeuren als het mis gaat en wat is er dan nodig om de oplostijd zo kort en om de schade zo beperkt mogelijk te houden? Het systematisch herstellen van de continuïteit, het beschikken over crisismanagementcapaciteiten en het beperken van financiële schade maken daarmee onderdeel uit van het instrumentarium dat pensioenfondsen (moeten) hebben om de impact van digitale risico's te beperken.

Om de gevolgen van een groot datalek, stagnatie van de pensioenverwerking of gijzeling danwel corruptie (van data) te beperken, dienen fondsen over een 'Plan B' te beschikken. Het beperken van schade door digitale incidenten is gebaat bij een adequaat Business Continuity Management (BCM). Door planmatig te zijn voorbereid op de belangrijkste bedreigingen voor de digitale continuïteit – in samenwerking met uitbestedingspartners – kan de schade door incidenten voor het fonds en zijn deelnemers aanmerkelijk worden beperkt en de dienstverlening sneller worden hersteld. In dat verlengde beschikken pensioenfondsen lang niet altijd over crisismanagementcapaciteit: een vooraf ingerichte responsorganisatie voor incidenten met grote (bestuurlijke) impact. Het snel en adequaat reageren op onalledaagse incidenten met (potentieel) negatieve gevolgen voor fondsen, hun operationele activiteiten en hun stakeholders, vergt specifieke organisatie, voorbereiding en oefening. Daarnaast bestaan er ook steeds meer mogelijkheden om de (vervolg) schade van digitale risico's te verzekeren. Het betreft dan met name de eigen schade, maar ook schade aan derden als gevolg van bijvoorbeeld systeemuitval of cybercriminaliteit. Deze verzekeringen fungeren als een soort digitale EHBO-kit en garanderen onder andere het snel inroepen van expertisepartijen – op IT-, juridisch en communicatiegebied – om de schade van digitale incidenten te beperken.

Conclusie

Bestuurders van pensioenfondsen staan voor de uitdaging om hun operationeel risicomanagement toe te rusten op een steeds digitale(r) toekomst. Specifieke aandacht en expertise is nodig om nieuwe digitale dreigingen beter te kunnen beheersen. Verantwoordelijken en specialisten bij pensioenfondsen dienen risicomanagement daartoe vanuit drie aanvullende perspectieven te benaderen: als privacybeschermer, als regisseur in de digitale keten en als incidentmanager. Op die manier stellen zij de eigen organisatie en hun partners in staat om te handelen conform nieuwe privacyvereisten, om digitale uitbestedingsrisico's te beperken en een om betere voorbereiding op incidenten te realiseren.

1023-01-ArtikelAonPBM-A3-online