Leeswijzer:

- In onderstaande tekst wordt met 'bestuur' het bestuur van de desbetreffende essentiële entiteiten of belangrijke entiteiten bedoeld.
- Risicomanagement kan je op vele vlakken doen. In onderstaande tekst wordt met risicomanagement het beheersen van risico's rondom informatie (zowel digitaal als analoog) bedoeld. Een ander woord hiervoor is informatiebeveiliging.
- Naast informatie zijn OT-systemen ook belangrijk om mee te nemen in cybersecurity. Op belangrijke plekken zijn OT-systemen daarom benoemd, maar om de tekst leesbaar te houden dus niet overal. De grote lijn wat betreft governance is namelijk ook hetzelfde.

Inhoudelijke reactie:

Mijn reactie gaat over artikel 26. Het op een juiste manier verdelen en beleggen van verantwoordelijkheden is een cruciaal onderdeel van governance. Dit gaat in deze concepttekst naar mijn idee niet goed. Lid 2 van artikel 26 stelt namelijk dat ieder lid van het bestuur in staat moet zijn om cybersecurityrisico's te kunnen identificeren en maatregelen om die risico's te verkleinen te kunnen beoordelen. Dat vraagt om gedegen inhoudelijke cybersecuritykennis van al deze bestuursleden. Dit is niet realistisch. Daarnaast benoemt het enkel de bestuursleden en niet de overige mensen die een belangrijke rol hebben in de governance. Dat maakt deze aanpak onvolledig.

Ja, het bestuur is eindverantwoordelijk voor alles, ook voor risicomanagement. Maar het bestuur kan niet alles doen. Lijnmanagers zijn niet voor niets aangesteld om de werklast van het bestuur te verdelen. Wetgeving dient daar rekening mee te houden. Deze concepttekst doet dat niet door alles weer terug te leggen op het bordje van het bestuur. Ja, er zijn ook kleine organisaties waarbij er niet echt sprake is van lijnmanagement. Deze reactie richt zich vooral op die vele organisaties waarbij er wel sprake is van lijnmanagement.

Risicomanagement hoort voornamelijk in de lijn te liggen. Dat is de plek waar de verantwoordelijkheid ligt voor het daadwerkelijk uitvoeren van de processen en werkzaamheden die horen bij het behalen van de organisatiedoelen. Dat is de plek waar informatie, die ondersteunend is aan die processen en werkzaamheden, daadwerkelijk gebruikt wordt. Dat is dus ook de plek waar de bijbehorende risico's het beste inzichtelijk gemaakt kunnen worden en waar mitigerende maatregelen kunnen worden bepaald. De rol van het lijnmanagement ontbreekt in artikel 26 en dat is een groot gemis!

De rol van het bestuur is om het hele proces van risicobeheersing in te richten, in gang te zetten en daarop toe te zien. Zij moeten dus organiseren dat informatie en/of OT-systemen inzichtelijk zijn, dat ze zijn toegewezen aan een eigenaar en dat de bijbehorende zorgtaken, waaronder die voor risico's, duidelijk zijn. Zij moeten via een risicobereidheidsverklaring sturing geven aan de lijnmanagers, zodat risico's op een eenduidige manier beoordeeld worden. Voor dit alles geldt veelal dat het bestuur niet per se zelf de benodigde expertise moet hebben, maar dat zij ervoor moet zorgen dat die expertise beschikbaar is, in de vorm van een CIO, CTO, CISO, informatiemanager, functioneel beheerder, etc. Periodieke overleggen met deze inhoudelijke experts, door henzelf en door lijnmanagement, zijn vele malen waardevoller dan over deze onderwerpen op cursus gaan. Dat soort cursussen worden ongetwijfeld dure algemene managementpraatjes, maar waarbij geen specifieke kennis wordt opgedaan over de eigen organisatie, de eigen situatie en de daarbij horende specifieke risico's.

Stellen dat het bestuur naarst hun huidige werkzaamheden risico's voor de beveiliging van netwerk- en informatiesystemen gaan identificeren en risicobeheersmaatregelen op het gebied van

cyberbeveiliging gaan beoordelen, is niet realistisch. Het doet ook geen eer aan die vakgebieden. Om dat te kunnen doen is vele jaren aan opleiding en/of ervaring nodig. Een training voor een bestuurder of manager gaat zeker niet iets gelijkwaardigs opleveren. De daarbij horende aanwezigheids-certificaten gaan al helemaal nietszeggend zijn. Dit zal een papieren werkelijkheid worden.

Vergelijk kennis op dit vlak met onderwerpen zoals financiën en personeel. Je hoeft als manager geen boekhoud- of belastingexpert te zijn om zorg te kunnen dragen voor een afdelings- of projectbudget. Je hoeft geen medisch of psychologisch expert te zijn om zorg te kunnen dragen voor de medewerkers binnen je afdeling. Zo hoef je dus ook geen beheer- en risico-expert te zijn om zorg te kunnen dragen voor de informatie(systemen) die aan jou zijn toegewezen. Je moet als manager de boel slechts organiseren. Ga met experts in gesprek, geef jouw behoeftes, uitdagingen en doelen aan en maak op basis van de verschillende adviezen en eigen inzichten een beslissing. Als bestuurder moet je slechts zorgen dat het lijnmanagement haar verantwoordelijkheid kent en oppakt. En bij verantwoordelijkheid hoort verantwoording. Als bestuurder moet je het lijnmanagement dus afrekenen op de invulling van hun verantwoordelijkheid. Ja, dat vraagt wellicht om een cultuurverandering binnen de overheid. Wellicht is het goed om te realiseren dat bij risicomanagement cultuur een grotere uitdaging is dan de inhoud. Dat erkennen is een belangrijke stap bij het verbeteren van risicomanagement binnen de overheid.

Informatiebeveiliging moet iets zijn dat je als manager bij de CISO komt halen, omdat jij als manager de zorgplicht hebt, omdat het jouw proces is dat verstoord raakt bij een incident met informatie of een OT-systeem. Het moet dus niet iets zijn dat een CISO moet gaan brengen omdat het van de wet moet. Aan de bestuurder om die cultuur binnen een organisatie af te dwingen.

En net als bij financiën en personeel, als er zaken zijn die groter zijn dan waar een lijnmanager een beslissing over kan/mag/wil nemen, dan pak je als bestuurder je rol. Ga met de betreffende lijnmanager en de CIO, de CTO en/of CISO in gesprek en neem op basis van de adviezen en eigen inzichten een beslissing.

De rol van het bestuur moet dus anders zijn dan wat artikel 26 nu aangeeft. Samengevat zijn dat de volgende punten:

- Zorg dat hetgeen waar risico's over beheerst moet worden, inzichtelijk is gemaakt. Dat betekent dus informatiemanagement en goed beheer van OT-systemen.
- Zorg dat iedere informatieverzameling en OT-systeem een eigenaar kent. Hoe ver je gaat in het onderverdelen van informatieverzamelingen kan per organisatie verschillen.
- Zorg dat de verantwoordelijkheid behorende bij eigenaarschap duidelijk is. Dat is dus inclusief de verantwoordelijkheid om risico's te beheersen.
- Zorg voor een risicobereidheid. Dit is een lastige, waar goede gesprekken met deskundigen op dit vlak nodig voor zijn. Dit is waarschijnlijk iets waar je als organisatie in moet groeien en wat je gaat ontdekken door ermee aan de slag te gaan. En dat is prima.
- Zorg dat voor eigenaars de juiste ondersteuning beschikbaar is om invulling te kunnen geven aan hun verantwoordelijkheid. Een CIO/CTO voor beheer, een CISO voor risico's, etc.
- Reken eigenaars periodiek af op de invulling van hun verantwoordelijkheid. Dit maakt het verschil tussen een papieren werkelijkheid en de praktijk.

Uiteraard komt er bij risicomanagement meer detail kijken dan wat hier beschreven staat, met name over wat precies de verantwoordelijkheden voor het lijnmanagement zijn. Die details zouden denk ik voorbij gaan aan het doel van de wettekst. Mijn doel is vooral om aan te geven welke richting het wel op moet gaan en dat de huidige tekst van artikel 26 naar mijn idee zeker niet de juiste weg is.

Ja, ik weet dat artikel 20 van de NIS zegt dat het bestuur een opleiding moet volgen zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerspraktijken kunnen beoordelen. Naar mijn idee is dat dus verkeerd. De vraag is of wij in Nederland de NIS2-tekst letterlijk gaan nemen of dat we een invulling gaan geven in nationale wetgeving die beter aansluit bij de realiteit en die gewoon juist is. We krijgen niet zo vaak de kans om dit soort cruciale cybersecurity-wetgeving op te stellen. Laten we het dus goed doen!