Publieke Managementletter

Digitale weerbaarheid vraagt bestuurlijke daadkracht

NOREA, de beroepsorganisatie van IT-auditors
Mercuriusplein 3
2132 HA Hoofddorp
norea@norea.nl,
www.norea.nl
tel +31 (0) 88 496 0380

Publieke Managementletter: Digitale weerbaarheid vraagt bestuurlijke daadkracht

Kernboodschap

Digitale systemen en processen zijn bepalend voor het functioneren van organisaties. Die omgeving is sterk verweven geraakt met ketens daarbuiten, vaak buiten de invloedsfeer van individuele organisaties. Hierdoor nemen de afhankelijkheden toe en worden de risico's op incidenten serieuzer. Verweven ketens, verouderde systemen (legacy) en beperkte grip op cybersecurity vergroten de kans dat incidenten direct doorwerken in de eigen dienst-verlening, veiligheid en continuïteit. Ook geopolitieke ontwikkelingen, zoals hybride oorlogsvoering en het strategisch inzetten van technologische en economische machtsposities om invloed uit te oefenen, introduceren nieuwe risico's.

Dit alles vraagt van bestuurders doordachte strategische keuzes en aantoonbare sturing. Dat vergt integraal ketenoverzicht plus één samenhangende digitale governance-aanpak die is ingebed in de algehele governance. Daarbij hoort een structurele aanpak voor het plannen, uitvoeren, controleren en bijsturen van beveiligingsmaatregelen, evenals een bewuste risicoacceptatie.

De Cyberveiligheidswet (Cbw), die sinds 15 augustus 2026 geldt, maakt dit tot een wettelijke verplichting voor organisaties die cruciaal zijn voor essentiële en belangrijke diensten – met daarbij de mogelijkheid van risicoaansprakelijkheid voor bestuurders.

NOREA ziet digitale weerbaarheid als een bestuurlijke opdracht. Daarom richten we ons nadrukkelijk tot raden van bestuur, raden van commissarissen, raden van toezicht en het kabinet. Dit document is bedoeld voor besturen als collectief, en niet uitsluitend voor de Chief Information Officer (CIO), de Chief Information Security Officer (CISO) of andere functionarissen die verantwoordelijk zijn voor aspecten van digitale weerbaarheid.

Digitale weerbaarheid begint bij bestuurlijke keuzes, expliciete regie en blijvende aandacht. Deze publieke managementletter biedt bestuurders daarom informatie, advies en richting in hun digitale weerbaarheidsvraagstukken, tegen de achtergrond van een snel groeiend dreigingsbeeld en structurele digitale kwetsbaarheden die organisaties raken.

Generatieve AI en privacy zijn in deze publieke managementletter niet opgenomen. Deze onderwerpen zijn omvangrijk en raken meerdere bestuurlijke thema's, waardoor ze aparte aandacht verdienen. NOREA komt hier op een later moment afzonderlijk op terug.

Van auditobservaties naar handvatten voor actie

Observaties uit de IT-auditpraktijk laten zien dat bestuurders nog onvoldoende overzicht van en grip hebben op hun digitale omgeving en op digitale diensten van externe partijen. Vanuit de visie van NOREA vertalen we dit in deze publieke managementletter naar urgente opgaven voor het hoogste bestuursniveau en bieden we een bestuurlijk actieplan als houvast.

Bestuurlijke verantwoordelijkheid

Bestuurders dragen op grond van hun algemene zorgplicht een eigen, niet-delegeerbare verantwoordelijkheid voor continuïteit, veiligheid en beheersing van zowel de eigen digitale omgeving als het bredere digitale ecosysteem waarin hun organisatie opereert. Dat ecosysteem bestaat uit systemen, leveranciers, platforms en ketenpartners die samen bepalend zijn voor de kwaliteit, continuïteit en veiligheid van de processen en waarvan die processen afhankelijk zijn. Door hierop regie te voeren versterken bestuurders de digitale weerbaarheid van de eigen organisatie en dragen ze bovendien bij aan de digitale weerbaarheid van Nederland.

Met de invoering op 15 augustus 2026 van de Cyberbeveiligingswet (Cbw), de Nederlandse implementatie van NIS2, is digitale veiligheid een bestuurlijke verplichting voor bestuurders van organisaties die cruciaal zijn voor essentiële en belangrijke diensten, die daarvoor ook juridisch risicoaansprakelijkheid dragen. De Cbw maakt deze verantwoordelijkheid expliciet en toetsbaar. Voor bestuurders van deze organisaties betekent dit dat zij inzicht moeten hebben in digitale risico's, getroffen maatregelen, de werking van beheersmaatregelen en resterende kwetsbaarheden.

Essentiële en belangrijke entiteiten onder de Cbw

De Cbw besteedt bijzondere aandacht aan 'essentiële' entiteiten en 'belangrijke' entiteiten. Tot de essentiële entiteiten behoren onder meer elektriciteitsnetbeheerders, drinkwaterbedrijven en ziekenhuizen. Voorbeelden van belangrijke entiteiten zijn post- en pakketdiensten, voedselproducenten en chemische bedrijven. Bestuurders van beide typen entiteiten moeten zelf beschikken over actuele kennis van cyberrisico's, actief sturen op risicobeheersing, regelmatig overleg voeren met de CISO en expliciet besluiten

nemen over maatregelen onder de zorgplicht. Ook moeten zij ervoor zorgen dat digitale weerbaarheid altijd op de agenda van het bestuur staat. Verder zijn bestuurders persoonlijk aansprakelijk wanneer zij deze zorgplicht niet naleven.

De Cbw-bepalingen over zorgplicht, meldplicht, toezicht en handhaving zijn niet van toepassing op financiële entiteiten die onder de DORA-verordening vallen, zo staat in de Memorie van Toelichting.

Het is goed om te beseffen dat de Cbw slechts een ondergrens vastlegt; digitale weerbaarheid vraagt vaak om een hogere ambitie, gelet op de te beschermen belangen van de organisatie. Het Cbw/NIS2 Control Framework, ontwikkeld door de Auditdienst Rijk en NOREA, kan organisaties helpen om hun eigen ambitieniveau te bepalen en planmatig en aantoonbaar te realiseren. Het framework kan bovendien dienen als inspiratie voor organisaties die niet onder de wet vallen.

In deze publieke managementletter bieden we bestuurders vanuit de visie van NOREA een aantal handvatten voor actie. We baseren ons daarbij op onze observaties in de praktijk als IT-auditors.

Tot slot: digitale weerbaarheid vraagt niet alleen om goede beveiliging, maar ook om goede informatievoorziening hierover aan de boardroom van bedrijven of de bestuursraad van departementen.

Niet doorschuiven naar CIO of CISO

Wij vragen bestuurders met klem dit document niet door te schuiven naar de CIO of CISO, maar er zelf mee aan de slag te gaan. Dat betekent in de boardroom het gesprek voeren over digitalisering, knelpunten en risico's bepalen, inzicht krijgen in de belangrijkste keuzes, duidelijke prioriteiten stellen en afspraken maken over de uitvoering. Vervolgens komt het aan op actief sturen op voortgang, onderbouwd met regelmatige voortgangsrapportages. Zo blijft de verantwoordelijkheid voor de digitale beheersing waar die hoort, bij het bestuur.

De digitale opgave

Digitale processen lopen dwars door organisaties, ketens en infrastructuren. Daar komt bij dat organisaties sterk afhankelijk zijn van een klein aantal grote aanbieders van cruciale digitale diensten. Ook missen bestuurders vaak zicht op het geheel van onderaannemers, cloudketens en geografische spreiding. Het gevolg is dat risico's verkeerd worden ingeschat en de feitelijke beheersing van de dienstverlening en de onderliggende systemen bij leveranciers ligt.

Dit belemmert de digitale transformatie, doordat organisaties hierdoor ontoereikende informatie hebben om hun digitale omgeving gericht te vernieuwen. Andere belemmeringen zijn de beperkte onderhoudbaarheid en integreerbaarheid van legacy-systemen, versnipperde governance en complexe projecten die vertragen of vastlopen. Verder is operationele technologie – cruciaal voor de besturing van fysieke processen – vaak onvoldoende in de governance opgenomen, wat risico's voor digitale en fysieke veiligheid en continuïteit vergroot.

Daarbovenop komt een groeiend dreigingsbeeld. Denk aan cybercrime en hybride dreigingen – vijandelijke activiteiten van statelijke actoren die onder de drempel van open conflict blijven en gericht zijn op het ondermijnen van de Nederlandse veiligheid, stabiliteit en democratische rechtsorde.

Verder zien we dat grote technologiebedrijven hun marktmacht niet uitsluitend commercieel inzetten, maar deze in bepaalde situaties ook strategisch kunnen aanwenden om druk uit te oefenen of gedrag te beïnvloeden. Dat blijkt onder meer uit het afsluiten van de e-mailtoegang van een ICC-rechter door Microsoft, de invloed van Starlink op militaire operaties en het gebruik van platformmacht door Meta en Google in conflicten rond nieuwsvoorziening in Australië en Canada. Ook de positie van Apple als poortwachter van zijn digitale ecosystemen illustreert hoe controle over essentiële infrastructuur kan worden ingezet om voorwaarden aan gebruikers en marktpartijen op te leggen. Ook regeringen zetten hun macht in voor geopolitieke invloed. Een voorbeeld zijn de Amerikaanse exportcontroles die de toegang tot geavanceerde AI-hardware voor bepaalde landen beperken. Gezamenlijk illustreren deze voorbeelden hoe controle over digitale infrastructuur, distributiekanalen en schaarse technologie kan uitgroeien tot een instrument van strategische macht.

Wat cyberincidenten laten zien

De cyberincidenten van de afgelopen jaren tonen hoe kwetsbaar Nederland is. Ze bevestigen nogmaals hoe sterk digitalisering inmiddels samenvalt met primaire processen. Daardoor kan één storing, één kwetsbare leverancier of één mislukte update cruciale processen stilleggen. Een cruciale industriële keten werd bijvoorbeeld getroffen door een ransomware-aanval op chipmaker Nexperia, een belangrijke schakel in die keten, en er waren cyberaanvallen op zorginstellingen met verstoring van de patiëntenzorg of privacyschendingen tot gevolg.

Grootschalige cloudstoringen hebben brede gevolgen voor de publieke en private dienstverlening. Zo legde CrowdStrike wereldwijd computers en servers plat, zorgden

cloudstoringen voor uitval bij overheid en bedrijfsleven en haalden DDoS-aanvallen publieke diensten onderuit.

Daarnaast laten cybersecurity-incidenten zoals Citrix Bleed zien hoe kwetsbaarheden in vitale toegangssystemen – waarmee medewerkers veilig op afstand inloggen – de maatschappij kunnen ontregelen. Ook de menselijke factor blijft een kwetsbare schakel. Dat bleek bij de grootschalige cyberaanval op telecomprovider Odido, waar hackers via voice phishing – telefonische misleiding van medewerkers – toegang kregen tot de persoonsgegevens van miljoenen klanten.

Het zijn slechts enkele voorbeelden van ernstige incidenten die laten zien dat digitale veiligheid en continuïteit van de bedrijfsvoering in het gedrang komen door trage digitale transformatie, sterke ketenafhankelijkheden en te weinig grip van organisaties op cybersecurity binnen hun volledige digitale ecosysteem.

Individuele organisaties kunnen hun digitale risico's niet meer alleen beheersen. Dat komt door ketencomplexiteit, technologische versnelling, geopolitieke ontwikkelingen, cloudgebruik en de concentratie van cruciale diensten bij weinig aanbieders met veel macht (vaak de facto monopolisten), die bovendien vaak buiten de Nederlandse jurisdictie vallen. Organisaties die hun digitale afhankelijkheden niet beheersen, verliezen de regie aan ketenpartners. Omgekeerd liggen er kansen voor organisaties die hun digitale infrastructuur en ketenregie op orde hebben: zij vergroten hun wendbaarheid, betrouwbaarheid en innovatievermogen.

Hoe te beginnen

Governance werkt alleen wanneer bestuurders zelf richting geven, fundamentele keuzes maken en verantwoording afleggen. Digitale governance moet daarom ingebed zijn in de strategische besluitvorming en mag niet bestaan uit losse acties of programma's. Anders ontstaat versnippering, waardoor ketenregie verloren gaat en risico's buiten beeld raken. Een pragmatische aanpak begint met inzicht in de huidige situatie, bijvoorbeeld door het Cbw/NIS2 Control Framework als nulmeting te gebruiken en een gap-analyse uit te voeren. Een eerste stap is het in kaart brengen van kernprocessen, kritieke systemen, cruciale of gevoelige data (de 'kroonjuwelen' van de organisatie) en afhankelijkheden die bepalend zijn voor de continuïteit van de dienstverlening.

Begin niet met alle verbeterpunten tegelijk, maar stel prioriteiten: pak eerst de grootste risico's aan en tref de maatregelen die het meeste effect hebben op de digitale weerbaarheid. Blijf die verder ontwikkelen door de maatregelen periodiek te toetsen en te verbeteren. Hierna schetsen we welke inhoudelijke gebieden blijvende aandacht verdienen.

Vijf bestuurlijke focusgebieden

Hieronder schetsen we vijf focusgebieden die het inhoudelijke kader vormen voor de keuzes, afwegingen en acties van het bestuur. Ze laten zien welke onderdelen structurele aandacht vragen, zodat de stappen uit het actieplan daadwerkelijk elect hebben en bijdragen aan aantoonbare digitale weerbaarheid.

1. **Integraal ketenoverzicht**
   Inzicht in het digitale ecosysteem en de onderlinge afhankelijkheden tussen systemen, data, leveranciers, onderaannemers en andere ketenpartners. Doel is dat risico's en afhankelijkheden binnen de keten tijdig kunnen worden geïdentificeerd en beheerst. Zie ook Cbw art. 21 lid 1, 21 lid 3d, 21 lid 4a–c.
2. **Samenhangende digitale governance**
   Samenhangende sturing op risico's, compliance, systeemvernieuwing en ketenafhankelijkheden. Digitale governance moet daarbij onderdeel zijn van de bredere governance. Doel is dat digitale risico's en afhankelijkheden in samenhang worden aangepakt en dat transformatieprojecten beheersbaar blijven. Zie ook Cbw art. 21 lid 1, 21 lid 3a, 21 lid 3f.
3. **Cyclische cybersecurity en toegangsbeheer**
   Een structurele aanpak van cybersecurity, waarbij plannen, uitvoeren, controleren en bijsturen elkaar steeds opvolgen in een cyclisch proces. Daarbij hoort ook het beheersen en monitoren van toegang tot systemen en data, met functiescheiding, roltoekenning en technisch afgedwongen beveiliging. Doel is dat cybersecurity structureel wordt beheerst en kwetsbaarheden tijdig worden geïdentificeerd en aangepakt. Zie ook Cbw art. 21 lid 1, 21 lid 3b, 21 lid 3i, 21 lid 3j, 21 lid 3f.
4. **Transparante risicoacceptatie**
   Bewuste besluitvorming over risico's en het beheersbaar houden van afhankelijkheden van kritieke ketenpartners. Doel is dat risicoacceptatie expliciet, onderbouwd en transparant is, zodat duidelijk is welke risico's de organisatie bewust accepteert en welke gevolgen daarvan worden aanvaard. Zie ook Cbw art. 21 lid 1–2, 21 lid 3a, 21 lid 3c, 21 lid 3d.
5. **Informatievoorziening en verantwoording**
   Tijdige en uniforme informatie over ontwikkelingen, risico's en voortgang op het gebied van digitale weerbaarheid, met aanvullende informatie bij incidenten. Doel is dat bestuur en toezicht tijdig beschikken over een betrouwbaar beeld van de digitale weerbaarheid en de belangrijkste risico's en ontwikkelingen. Zie ook Cbw art. 21 lid 1, 21 lid 3b–c, 24 lid 1, lid 2a–b, 35 lid 1–2, lid 2; 36 lid 1.

We willen benadrukken dat digitale kwetsbaarheden niet vanzelf verdwijnen. Daarvoor zijn expliciete keuzes, duidelijke regie en structurele sturing op bestuursniveau nodig. Daarom volgt hieronder een actieplan voor het bestuurlijke topniveau, als houvast bij het systematisch organiseren, monitoren en inzichtelijk maken van digitale weerbaarheid.

Bestuurlijk actieplan

- Voer een nulmeting uit op basis van het Cbw/NIS2 Control Framework
- Breng kritieke ketens in kaart
- Stel de *risk appetite* vast
- Stel jaarlijkse cybersecurity-prioriteiten vast
- Regel bestuurlijke opvolging: wijs eigenaarschap toe, monitor voortgang en stuur bij waar nodig
- Richt periodieke boardrapportages in
- Leg jaarlijks verantwoording af, en tussentijds bij ernstige incidenten

Onze werkwijze

Voor deze publieke managementletter hebben acht auditorganisaties – Deloitte, PwC, EY, KPMG, BDO, Forvis Mazars, de Auditdienst Rijk en de Algemene Rekenkamer – hun ervaringen en inzichten uit de IT-auditpraktijk gebundeld in een project dat is gecoördineerd door NOREA. Om een breed gedragen beeld te vormen van de belangrijkste digitale kwetsbaarheden hebben we een vertegenwoordiger van elke organisatie geïnterviewd, met als hoofdvraag hun top vijf digitale issues te benoemen en toe te lichten. Op basis hiervan heeft het projectteam de bijbehorende bestuurlijke opgaven geformuleerd. In deze publieke managementletter is die bestuurlijke duiding uitgewerkt vanuit de visie van NOREA.