Inspectie van het Onderwijs
Ministerie van Onderwijs, Cultuur
en Wetenschap

Digitale weerbaarheid in het onderwijs

Samen sterk in bestuurlijke verantwoordelijkheid

Juni 2026

Voorwoord

Als Inspectie van het Onderwijs zien we dat digitalisering het onderwijs in hoog tempo verandert. Lesmateriaal is er steeds vaker in digitale vorm, en ook communicatie, administratie en toetsing vinden meer en meer digitaal plaats. Dat biedt kansen, maar maakt het onderwijs ook kwetsbaar. De afgelopen jaren lieten cyberincidenten zien dat digitale verstoringen het onderwijsproces direct kunnen raken. Scholen en instellingen kregen al te maken met uitval van systemen en verlies van gegevens en daardoor ook: toenemende onzekerheid en zorgen onder studenten en medewerkers. Dat raakt niet alleen de techniek, maar óók de kern van het onderwijs.

Daarom hebben we met dit onderzoek gekeken in hoeverre besturen zicht hebben op de digitale weerbaarheid van hun instelling en hoe zij hieraan sturing geven. Ook onderzochten we in hoeverre zij kunnen waarborgen dat het onderwijs ook na een cyberincident kan doorgaan. En welke factoren hen helpen of juist belemmeren bij het versterken van deze digitale weerbaarheid. Want onderwijs moet altijd kunnen doorgaan, óók als digitale systemen uitvallen.

Wat is, in het kort, onze conclusie? We zien dat besturen zich bewust zijn van de toenemende digitale dreiging en dat zij maatregelen nemen om risico's te beperken. Veel instellingen hebben incidentprocedures, investeren in bewustwording en werken aan informatiebeveiliging en privacy. In het middelbaar beroepsonderwijs en het hoger onderwijs is digitale weerbaarheid vaak formeel georganiseerd, onder meer via (de aanstelling van) een Chief Information Security Officer (CISO). In het primair, voortgezet en speciaal onderwijs zien we eveneens groeiende aandacht en verdere professionalisering.

Tegelijkertijd zien we dat digitale weerbaarheid nog niet overal strategisch en integraal is ingebed in de bestuurscyclus. Maatregelen zijn op operationeel niveau vaak verder ontwikkeld dan op bestuurlijk en strategisch niveau. Structurele risicoanalyses, een meerjarenplanning, monitoring en bijsturing maken nog niet altijd systematisch deel uit van deze cyclus. Ook zijn de verschillen tussen besturen groot. Vooral kleinere besturen zijn relatief kwetsbaar, onder meer door beperkte capaciteit en expertise.

Digitale weerbaarheid is geen opgave die instellingen alléén kunnen oplossen. Het is een collectieve opgave. Onderwijsinstellingen zijn onderling verbonden en afhankelijk van veelal gedeelde systemen en een beperkt aantal leveranciers. Dat vraagt om samenwerking tussen besturen en sectoren, deelname aan netwerken voor kennisdeling en ondersteuning, en gezamenlijk optrekken richting ICT-leveranciers zodat de sector meer regie kan houden op digitale veiligheid.

Daarom roep ik besturen op om digitale weerbaarheid nadrukkelijker mee te nemen in hun strategische sturing. De verschillen tussen sectoren zijn namelijk groot: in het middelbaar beroepsonderwijs en het hoger onderwijs is digitale weerbaarheid al verder ontwikkeld en structureler georganiseerd, terwijl in andere sectoren nog veel stappen gezet moeten worden. Ook binnen sectoren lopen de verschillen tussen besturen sterk uiteen. Dit alles benadrukt het belang om van elkaar te leren en ervaringen te delen. Zorg voor betrouwbare risicoanalyses, concrete doelen, structurele planning, centrale regie en voortdurende monitoring. Toon als bestuur zichtbare betrokkenheid en stimuleer een cultuur waarin digitale veiligheid als een gedeelde verantwoordelijkheid wordt gezien. Digitale weerbaarheid vraagt immers blijvende aandacht, investeringen en het vermogen om vooruit te plannen.

Daarnaast vragen wij als inspectie besturen om actief samen te werken en meer gebruik te maken van de beschikbare ondersteuningsstructuren in de onderwijssector. Sluit u aan bij en maak gebruik van organisaties als SIVON, Kennisnet, SURF en MBO Digitaal, en zet u zich ook actief in. Alleen door gezamenlijk op te trekken kan de sector zijn digitale weerbaarheid versterken.

Dit rapport brengt in beeld wat er nodig is om de digitale weerbaarheid van het onderwijs te versterken. Aan besturen wil ik zeggen: pak die handschoen op en werk met elkaar aan het realiseren van een digitaal weerbare onderwijssector.

Alida Oppers
Inspecteur-generaal van het Onderwijs

Inhoud

Samenvatting

De Inspectie van het Onderwijs heeft een onderzoek uitgevoerd naar de digitale weerbaarheid in het onderwijs. Aanleiding zijn de toenemende digitalisering van het onderwijs en de groeiende digitale afhankelijkheid en bedreigingen. Digitale incidenten kunnen de continuïteit van onderwijs verstoren en de bescherming van persoonsgegevens onder druk zetten. De centrale vraag is daarom in hoeverre besturen bijdragen aan de digitale weerbaarheid die nodig is om het onderwijs ook bij digitale verstoringen te kunnen laten doorgaan.

Het onderzoek heeft een verkennend en agenderend karakter en richt zich op patronen op stelselniveau. Op basis van een vragenlijst en verdiepende interviews met bestuurders en functionarissen Informatiebeveiliging en Privacy (IBP) hebben we onderzocht welke maatregelen instellingen hebben genomen, hoeveel zicht en sturing besturen hebben en welke factoren hen belemmeren en/of helpen bij het waarborgen van digitale weerbaarheid.

De resultaten laten zien dat besturen vooral zicht hebben op concrete maatregelen om digitale risico's te beperken. In het primair, voortgezet en speciaal onderwijs weten veel besturen steeds beter welke maatregelen nodig zijn om digitale risico's te beheersen, zoals incidentmanagement, bewustwordingscampagnes en toegangsbeheer. Minder goed in beeld zijn de vereiste basisvoorwaarden om digitale weerbaarheid duurzaam te organiseren, zoals ook blijkt uit *IBP in beeld* (Digitaal Veilig Onderwijs, 2026). Denk aan het bepalen hoe kritisch en gevoelig systemen en gegevens zijn, het werken met een duidelijke meerjarenplanning en het structureel opnemen van digitale weerbaarheid in de planning- en controlcyclus. In het middelbaar beroepsonderwijs en het hoger onderwijs is digitale weerbaarheid vaker formeel georganiseerd, bijvoorbeeld rond een Chief Information Security Officer (CISO) en de inrichting van vaste crisis- en auditprocessen. Tegelijkertijd wordt risicogestuurd werken ook daar nog niet overal volledig benut. Informatie en rapportages over digitale dreigingen worden nog niet altijd en overal systematisch gebruikt om bestuurlijke keuzes te maken en beleid bij te stellen.

Verschillen tussen besturen zijn aanzienlijk. In het primair, voortgezet en speciaal onderwijs hangen die vooral samen met schaalgrootte, actieve deelname aan netwerken en interne expertise. Grotere besturen hebben doorgaans meer zicht en sturingsmogelijkheden op het gebied van digitale weerbaarheid, terwijl kleinere besturen relatief kwetsbaarder zijn. Ook in het middelbaar beroepsonderwijs en het hoger onderwijs speelt schaalgrootte een rol. Hier zijn verschillen in organisatiegraad echter beperkter en hangen verschillen sterker samen met de betrokkenheid, affiniteit en prioritering van digitale weerbaarheid door bestuurders.

Helpende factoren hierbij zijn een integrale visie op veiligheid, duidelijke regie, een sterke veiligheidscultuur en actieve bestuurlijke betrokkenheid. Wanneer digitale veiligheid expliciet wordt gezien als een organisatiebrede verantwoordelijkheid en niet alleen als een ICT-onderwerp, ontstaat meer samenhang in beleid en uitvoering. Ook samenwerking en kennisdeling binnen en tussen sectoren versterken de positie van besturen, onder meer richting ICT-leveranciers. Samenwerkingsverbanden in de sector kunnen daarbij helpen.

Belemmeringen liggen vooral in beperkte capaciteit, schaarste aan gespecialiseerde professionals en afhankelijkheid van leveranciers. De prioriteit van digitale weerbaarheid hangt soms ook af van de kennis en betrokkenheid van individuele bestuurders. Daarnaast ervaren met name kleinere besturen de complexiteit van normenkaders voor informatiebeveiliging en informatievoorziening als belastend. Ook kan spanning ontstaan tussen autonomie en veiligheid: scholen of faculteiten willen zelfstandig blijven werken, terwijl digitale veiligheid vaak vraagt om meer centrale afspraken en sturing.

Overkoepelend dragen besturen weliswaar bij aan digitale weerbaarheid, maar verschilt de mate waarin onderwijscontinuïteit duurzaam is geborgd. Ook al zijn operationele maatregelen vaak wel aanwezig, we zien ook dat digitale weerbaarheid lang niet overal een vast en samenhangend onderdeel vormt van beleid, planning en sturing. De grootste kans ligt dan ook in het beter verbinden van beleid, uitvoering en samenwerking tussen onderwijsinstellingen, sectororganisaties, ICT-leveranciers en de overheid. Het grootste risico daarentegen ligt in versnippering, zonder structurele bestuurlijke inbedding. Digitale weerbaarheid is daarmee een gezamenlijke bestuurlijke opgave. Onderwijsbesturen dragen de eerste verantwoordelijkheid, maar zijn voor hun digitale veiligheid ook afhankelijk van sectorale samenwerkingsverbanden, ICT-leveranciers en de overheid. Het versterken van digitale weerbaarheid vraagt dan ook om zowel duidelijke bestuurlijke sturing binnen instellingen als om samenwerking binnen het onderwijsveld.

1. Inleiding

1.1 Aanleiding en maatschappelijke context

De Inspectie van het Onderwijs verwacht dat besturen de continuïteit van het onderwijs en de (digitale) veiligheid van leerlingen, studenten en medewerkers waarborgen. Deze verantwoordelijkheid staat onder toenemende druk door de snelle digitalisering van onderwijs en samenleving. Digitale leermiddelen, administratiesystemen en communicatieplatforms zijn onmisbaar geworden, terwijl digitale dreigingen in aantal en complexiteit toenemen.

Recente cyberincidenten, waarbij onderwijsprocessen verstoord raakten en persoonsgegevens mogelijk zijn buitgemaakt, benadrukken de urgentie van digitale weerbaarheid. Digitale verstoringen raken direct aan de continuïteit van onderwijs, de bescherming van persoonsgegevens en het vertrouwen in onderwijsdata. Tegelijkertijd geven niet alle besturen aan zich voldoende toegerust te voelen om digitale weerbaarheid structureel vorm te geven.

Tegen deze achtergrond heeft de inspectie onderzoek gedaan naar de borging van digitale weerbaarheid in het onderwijs. Dit onderzoek sluit aan bij de Monitor digitale weerbaarheid en veiligheid (2025; 2026), die op basis van jaarverslagen een kwantitatief beeld geeft van de verantwoording door besturen. Waar de monitor zich richt op de verantwoording van besturen, richt dit stelselonderzoek zich op de praktijk: in hoeverre dragen besturen bij aan digitale weerbaarheid om zo de onderwijscontinuïteit te garanderen?

1.2 Beleids- en wetgevingscontext

De beleidscontext rond digitale weerbaarheid ontwikkelt zich momenteel snel. Voor het hoger onderwijs wordt de Europese NIS2-richtlijn[1] in Nederland geïmplementeerd via de Cyberbeveiligingswet (Cbw)[2] Deze wet introduceert onder meer een zorgplicht en een meldplicht en versterkt de bestuurlijke verantwoordelijkheid voor cybersecurity. Voor mbo-instellingen geldt de Cbw niet. Zij zullen via bestuurlijke afspraken moeten werken aan versterking van de cyberweerbaarheid en binnen het programma Cyberveiligheid mbo[3]. De mbo-sector is via bestuurlijk overleg wel betrokken bij de uitwerking van de Cbw in het hoger onderwijs, om op die manier de huidige samenwerking in het vervolgonderwijs zoveel mogelijk te kunnen continueren.

Voor het funderend onderwijs voert het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) samen met sectorpartners[4] het programma Digitaal Veilig Funderend Onderwijs[5] uit. In dit kader is het Normenkader Informatiebeveiliging en Privacy (IBP) ontwikkeld, als sectorbreed referentiekader voor digitale veiligheid. Met de sectorraden is afgesproken dat besturen in 2027 inzicht hebben in hun positie ten opzichte van dit normenkader en uiterlijk in 2030 aan de normen voldoen. Daarnaast moeten besturen sinds het verslagjaar 2024 in hun jaarverslag rapporteren over informatiebeveiliging en privacy.

Hoewel wetgeving en governance zich ontwikkelen, beschikt de inspectie nog niet over een volledig uitgewerkt wettelijk toezichtkader voor digitale weerbaarheid. Dit onderzoek draagt dan ook bij aan kennisopbouw en biedt inzicht in de huidige praktijk, mede ter voorbereiding op mogelijke toekomstige toezichttaken.

Definitie digitale weerbaarheid: In dit onderzoek verstaan we onder digitale weerbaarheid het vermogen van onderwijsinstellingen om risico's in de digitale omgeving te beheersen — door cyberdreigingen te voorkomen, tijdig te detecteren, schade te beperken en herstel te realiseren — en daarmee de continuïteit van onderwijs en bescherming van gegevens en gebruikers te waarborgen.

1 NIS 2 (Directive (EU) 2022/2555): https://eur-lex.europa.eu/eli/dir/2022/2555
2 Kamerstukken II, 2024/25, 31 288, 26 643, nr. 1189 en Kamerstukken II, 2024/25, 36 764, nr. 2
3 https://mbodigitaal.nl/programmas/programma-cyberveiligheid-mbo/
4 Kennisnet, SIVON, de PO-Raad en de VO-raad
5 https://www.digitaalveiligonderwijs.nl/programma/

1.3 Onderzoeksvragen

Tegen de achtergrond van toenemende digitale dreiging en veranderende regelgeving onderzoekt de inspectie hoe besturen invulling geven aan digitale weerbaarheid en in hoeverre zij bijdragen aan het waarborgen van onderwijscontinuïteit. De centrale onderzoeksvraag luidt:

> *In hoeverre dragen besturen bij aan digitale weerbaarheid om onderwijscontinuïteit te garanderen in het onderwijs?*

Onder de centrale onderzoeksvraag onderscheiden we verschillende verkennende en verdiepende deelvragen voor alle sectoren:

Verkennend:

1. In hoeverre hebben besturen zicht op digitale weerbaarheid?
2. Hoe geven besturen sturing aan digitale weerbaarheid om onderwijscontinuïteit te garanderen?
3. Hoe verschillen besturen in het waarborgen van digitale weerbaarheid met betrekking tot onderwijscontinuïteit?

Verdiepend

4. Welke factoren helpen besturen in het waarborgen van digitale weerbaarheid met betrekking tot onderwijscontinuïteit?
5. Welke factoren belemmeren besturen in het waarborgen van digitale weerbaarheid met betrekking tot onderwijscontinuïteit?

1.4 Doel en afbakening

Dit stelselonderzoek heeft een verkennend en agenderend karakter. Het biedt inzicht in de huidige stand van digitale weerbaarheid in het onderwijs en in de bestuurlijke, organisatorische en externe factoren die daarop van invloed zijn. Het onderzoek is niet gericht op individuele oordelen over instellingen, maar op het identificeren van patronen, kansen en knelpunten op stelselniveau.

Met deze inzichten wil de inspectie bijdragen aan verdere versterking van digitale weerbaarheid in het onderwijs, zodat besturen beter in staat zijn de digitale veiligheid te waarborgen en de continuïteit van het onderwijs ook bij digitale incidenten te beschermen.

2. Zicht, sturing en verschillen tussen besturen

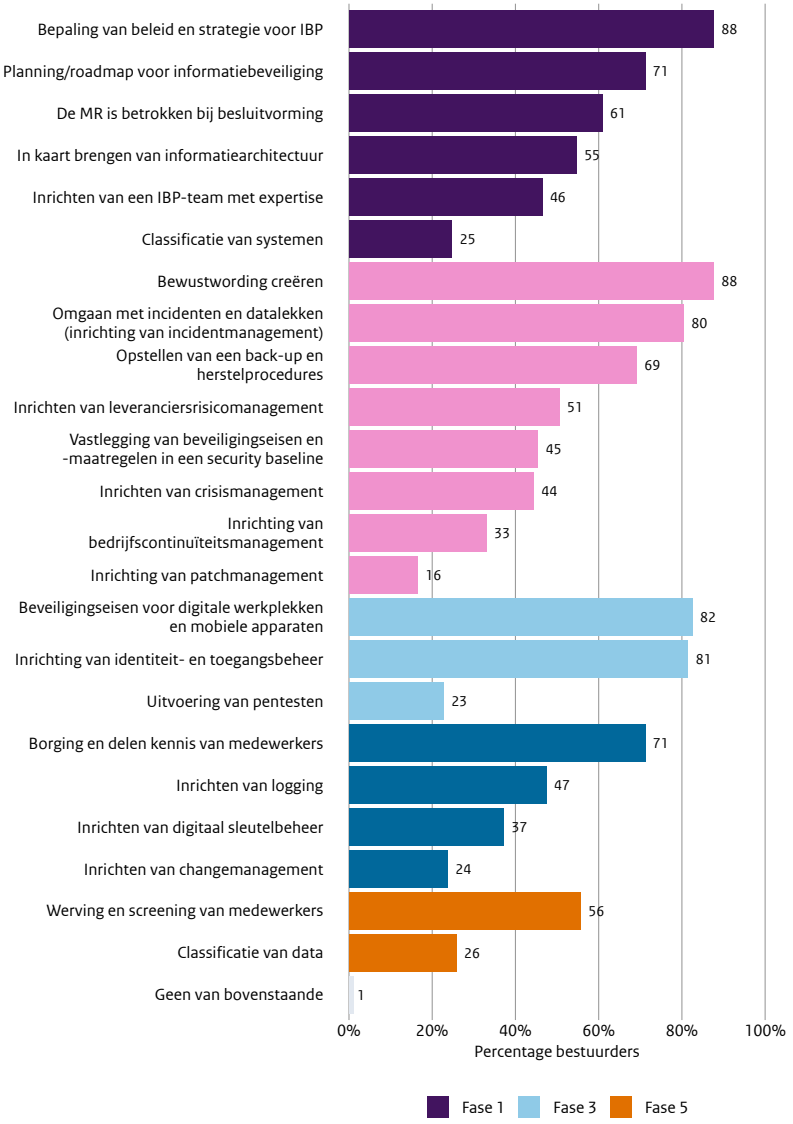
In dit hoofdstuk presenteren we de resultaten van deelvragen 1, 2 en 3. Deze resultaten zijn gebaseerd op een vragenlijst afgenomen onder een representatieve steekproef van 176 onderwijsbesturen in het bekostigd onderwijs: 97 in het funderend onderwijs (primair, voortgezet en speciaal onderwijs) en 79 in het vervolgonderwijs (mbo en hoger onderwijs). De vragenlijst is ingevuld door bestuurders met digitale weerbaarheid in hun portefeuille en betrokken IBP-functionarissen. Op basis van hun zelfrapportage is onderzocht in hoeverre maatregelen voor digitale weerbaarheid zijn geïmplementeerd, hoeveel zicht en sturing besturen hierop hebben en hoe dit samenhangt met bestuurskenmerken. Daarnaast zijn stellingen over bewustwording, capaciteit en expertise samengevoegd tot gemiddelde scores, om zo de verschillen tussen besturen en sectoren in het waarborgen van onderwijscontinuïteit inzichtelijk te kunnen maken. Hierbij verwijst bewustwording naar het onderkennen van digitale risico's, expertise naar de aanwezige kennis en vaardigheden en capaciteit naar beschikbare tijd, mensen en middelen.

2.1 Digitale weerbaarheid in het funderend onderwijs

2.1.1 Zicht op onderdelen van digitale weerbaarheid

We zien duidelijke verschillen in hoeverre bestuurders bekend zijn met de maatregelen voor digitale weerbaarheid (zie figuur 2.1.1). Deze analyse is geplaatst in het perspectief van het Groeipad informatiebeveiliging en privacy (IBP) van Kennisnet[6], dat maatregelen ordent van basis naar meer geavanceerd. Het groeipad kent opeenvolgende fasen: van het op orde brengen van de basis (fase 1), via het aanpakken van de grootste risico's (fase 2), het uitbreiden van maatregelen (fase 3) en het verder verbeteren van processen (fase 4) tot het optimaliseren van digitale weerbaarheid (fase 5). Een groot deel van de bestuurders is vooral bekend met maatregelen die direct helpen om risico's te verkleinen, zoals beveiliging en incidentaanpak. Maatregelen die gaan over organisatie, beleid en langetermijnplanning zijn minder bekend. Dit laat zien dat bestuurders vooral zicht hebben op wat er direct moet gebeuren bij risico's, maar minder op wat er nodig is om digitale weerbaarheid structureel te organiseren. Met name maatregelen op gebieden als governance, structuur en langetermijnplanning lijken minder bekend te zijn dan maatregelen gericht op directe beveiliging.

Figuur 2.1.1 Zicht op onderdelen van digitale weerbaarheid in het funderend onderwijs (n = 97)



6 Zie voor meer informatie over het groeipad: https://normenkaderibp.kennisnet.nl/groeipad/

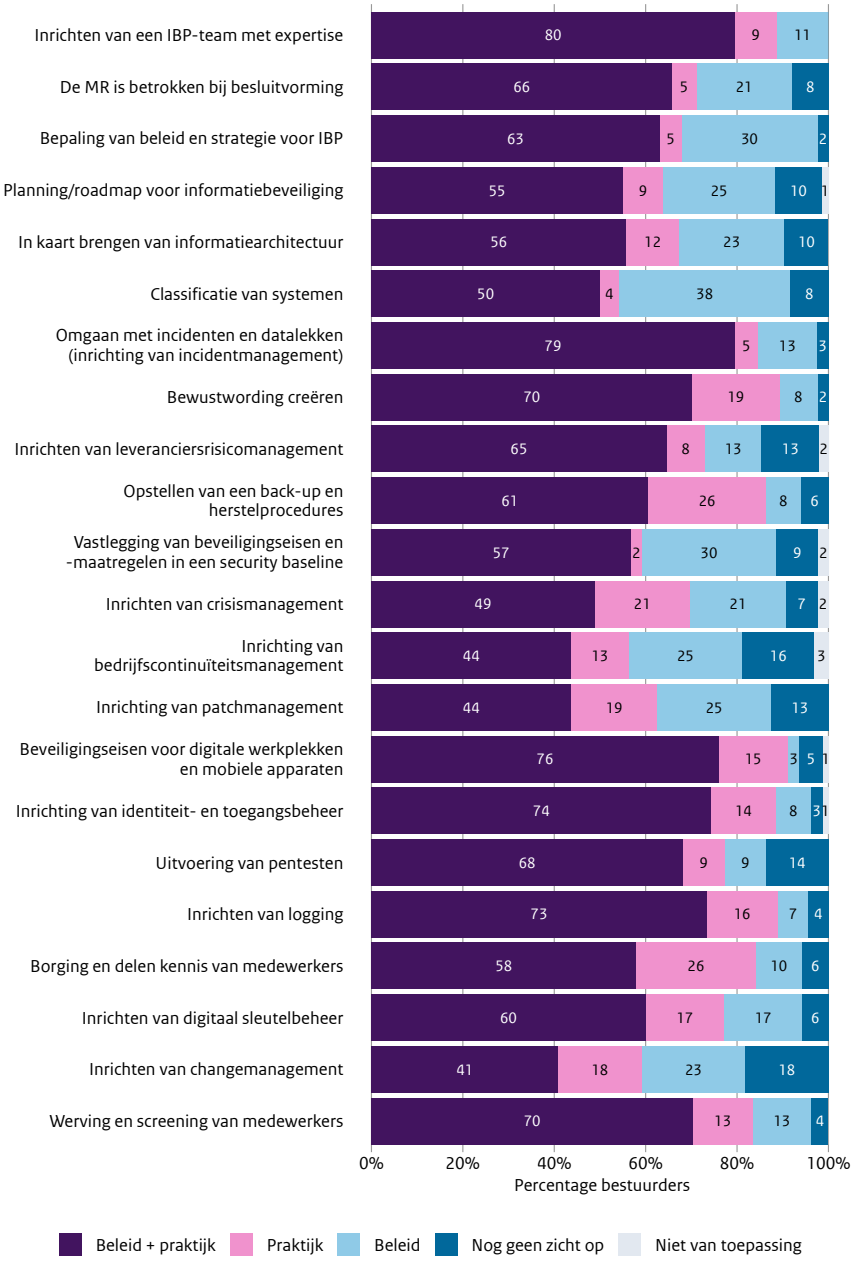
2.1.2 Implementatie van onderdelen van digitale weerbaarheid

Bestuurders geven aan dat niet alle bekende maatregelen ook daadwerkelijk zijn ingevoerd in beleid en praktijk. Er is een duidelijk verschil: maatregelen voor directe beveiliging en incidentaanpak worden vaak toegepast terwijl maatregelen voor organisatie, beleid en structurele borging achterblijven (zie figuur 2.1.2).

Fundamentele randvoorwaarden die nodig zijn om digitale weerbaarheid duurzaam te organiseren, zoals het vaststellen van beleid, het maken van een langetermijnplanning en het in kaart brengen en indelen van systemen, zijn vaak nog niet volledig ingevoerd. Hoewel veel besturen hiermee zijn begonnen, blijft de verdere uitwerking vaak achter. Ook maatregelen voor continuïteit en crisisaanpak zijn minder vaak ingevoerd. Besturen richten zich dus vooral op het voorkómen van incidenten, en minder op wat er moet gebeuren als het toch misgaat. Een klein deel van de besturen heeft zelfs geen goed beeld van de eigen voorbereiding op grote verstoringen. Dit betekent dat het waarborgen van onderwijscontinuïteit nog niet overal goed is geregeld.

In het geheel laat dit zien dat veel besturen in een overgangsfase zitten: ze nemen maatregelen voor dagelijkse risico's, maar hebben digitale weerbaarheid nog niet volledig vastgelegd in beleid en organisatie.

Figuur 2.1.2 Implementatie van onderdelen van digitale weerbaarheid in het funderend onderwijs (n = 97)



2.1.3 Organisatie van digitale weerbaarheid

In het funderend onderwijs verschilt het sterk hoe besturen digitale weerbaarheid organiseren. Bestuurders met digitale weerbaarheid in hun portefeuille besteden hier gemiddeld ongeveer 7 procent van hun tijd aan. De verschillen zijn echter groot: in het po en so loopt dit op tot ongeveer 20 procent, en in het vo tot 16 procent.

Het overgrote merendeel van de bestuurders heeft medewerkers in dienst die de inregeling van digitale weerbaarheid in hun takenpakket hebben én daarvoor zijn uitgerust. Voor een kleinere groep besturen is deze capaciteit echter nog niet structureel ingericht.

Digitale weerbaarheid wordt over het algemeen deels op bestuursniveau en deels op schoolniveau georganiseerd en in mindere mate op het niveau van het samenwerkingsverband. Daarnaast geeft een meerderheid van de bestuurders aan dat bepaalde onderdelen van digitale weerbaarheid worden uitbesteed aan commerciële partijen.

Tot slot zien we dat het overgrote deel van de besturen lid is van de PO-Raad of de VO-raad en een minderheid van SIVON. Een klein deel van de besturen heeft een lidmaatschap van het BIC-Netwerk. Daarbij zijn de meeste besturen betrokken bij één of meer van de verschillende activiteiten aangeboden door ondersteunende organisaties zoals Kennisnet, SIVON, het platform Digitaal Veilig Onderwijs of andere aanbieders in het veld. Toch zien we ook dat een klein deel van de bestuurders aangeeft nog geen gebruik te hebben gemaakt van dergelijke activiteiten om hun kennis over digitale weerbaarheid te vergroten.

2.1.4 Sturing op strategisch, tactisch en operationeel niveau

Om digitale weerbaarheid goed te organiseren, moet informatiebeveiliging en privacy (IBP) onderdeel zijn van beleid én uitvoering. Daarbij is het belangrijk dat bestuur, management en uitvoering goed op elkaar aansluiten om voor een goede overdracht tussen het strategische, tactische en operationele niveau te zorgen (PO-Raad & VO-raad, 2024). In deze analyse kijken we in hoeverre bestuurders en IBP-functionarissen het met elkaar eens zijn over uitspraken op deze 3 niveaus (zie figuur 2.1.4).

Op **strategisch niveau** is het bestuur eindverantwoordelijk. Het bestuur bepaalt de koers, stelt prioriteiten en zorgt dat digitale weerbaarheid terugkomt in beleid en verantwoording. In het funderend onderwijs gaat het daarbij vooral om het kunnen laten doorgaan van onderwijs en het beschermen van leerlinggegevens. Het bestuur belegt rollen en verantwoordelijkheden en legt verantwoording af, onder meer richting de inspectie.

Figuur 2.1.4 Sturing op digitale weerbaarheid in het funderend onderwijs (n = 43)

Een groot deel van de bestuurders erkent het belang van digitale weerbaarheid voor de organisatie. Tegelijkertijd geeft de meerderheid van de bestuurders aan dat het soms lastig is om de verantwoordelijkheid voor digitale weerbaarheid te vertalen naar concrete keuzes of merkbare impact binnen de organisatie. Over dit punt bestaat overeenstemming tussen ongeveer de helft van de bestuurders en IBP-functionarissen. Ook zien we verschillen in beeldvorming over de tijdsinvestering en bestuurlijke prioriteit. Een klein deel van de bestuurders vindt dat digitale weerbaarheid veel tijd kost; slechts enkele bestuurders en IBP-functionarissen denken daar hetzelfde over.

Op **tactisch niveau** gaat het om het uitwerken van beleid in afspraken, risicoanalyses, procedures en ondersteuning. Hier spelen management en de IBP-functionaris een belangrijke rol. Veel bestuurders geven aan zich bewust te zijn van de digitale risico's waar hun organisatie mee te maken kan krijgen. In de meeste gevallen bevestigen IBP-functionarissen dit beeld. Daarnaast geven veel bestuurders aan dat hun zicht op digitale weerbaarheid in de organisatie mede afhankelijk is van de IBP-functionaris. Ook hier is er in meer dan de helft van de gevallen overeenstemming. Verder geven veel bestuurders aan dat zij duidelijke verwachtingen hebben van de IBP-functionaris als het gaat om digitale weerbaarheid. Ook denken zij dat de IBP-functionaris tevreden is met zijn of haar verantwoordelijkheid. Bestuurders en IBP-functionarissen zijn het hier in meerderheid over eens.

Op **operationeel niveau** gaat het om de dagelijkse praktijk: veilig werken, procedures volgen en goed handelen bij incidenten. De meerderheid van de bestuurders geeft aan dat zij weten welke stappen er ondernomen moeten worden bij een cyberincident. Opvallend is dat IBP-functionarissen dit in mindere mate voor hun bestuurder inschatten. Dit wijst op een verschil in beeldvorming tussen bestuurders en IBP-functionarissen over de operationele paraatheid van de organisatie.

De resultaten laten zien dat bestuurders en IBP-functionarissen vooral op tactisch niveau redelijk hetzelfde beeld hebben. Op strategisch en operationeel niveau lopen hun antwoorden vaker uiteen. Dit suggereert dat digitale weerbaarheid wel in beleid is uitgewerkt, maar nog minder stevig is verankerd in bestuurlijke keuzes en in de dagelijkse praktijk.

2.2 Digitale weerbaarheid in het vervolgonderwijs

2.2.1 Inbedding informatiebeveiliging

In het vervolgonderwijs werkt men inmiddels richting een risicogestuurde aanpak van informatiebeveiliging en integrale veiligheid. In deze analyse kijken we naar 4 onderdelen: de plek van informatiebeveiliging in de bestuurscyclus, het gebruik van risico-informatie, de gekozen maatregelen en de veiligheidscultuur (IV-HO, 2021; IV-HO & KPMG, 2024).

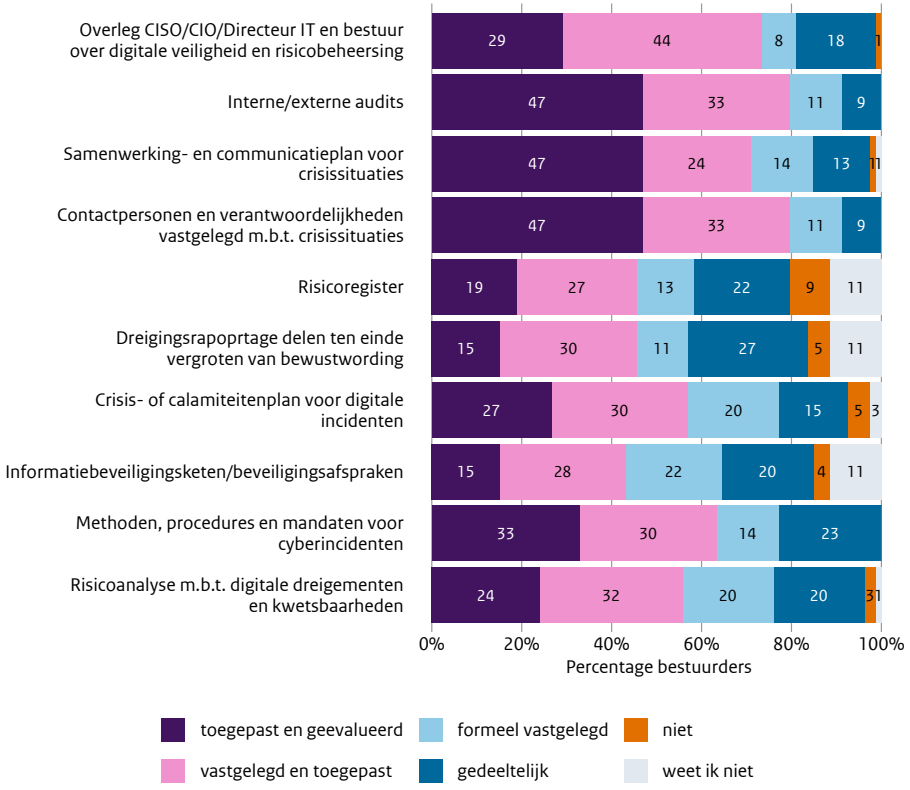
Bij veel instellingen is de **bestuurscyclus** wel ingericht, maar is er nog geen (volledig) doorlopende verbetercyclus. Uit de resultaten (zie figuur 2.2.1) blijkt dat verschillende onderdelen zijn vastgelegd en worden toegepast, maar nog niet altijd worden geëvalueerd. Zo worden audits van procedures en crisisplannen bij minder dan de helft van de instellingen uitgevoerd én geëvalueerd. Ook is de crisisorganisatie bij minder dan de helft volledig ingericht. Dat betekent dat rollen en afspraken er soms wel zijn, maar dat ze nog niet overal regelmatig worden getoetst en bijgesteld.

Ook **risicogestuurd werken** is nog beperkt ontwikkeld. Instrumenten zoals risicoregisters, dreigingsrapportages en evaluaties van de beveiligingsketen worden maar in een klein deel van de instellingen structureel gebruikt. Risico's worden dus wel herkend, maar nog niet overal gebruikt om bestuurlijke keuzes te maken.

Verder zien we een duidelijk verschil tussen **operationele maatregelen** en een **meer strategische aanpak**. Operationele maatregelen, zoals crisisprocedures, audits en het vastleggen van rollen, zijn in ongeveer de helft van de instellingen aanwezig. Maatregelen die helpen om vooruit te kijken en bij te sturen, zoals strategische risicoanalyse, ketenrisico's beoordelen en dreigingsinformatie delen, blijven vaker achter (zie figuur 2.2.1).

Ook op het gebied van **veiligheidscultuur** is nog winst te behalen. Een open cultuur, waarin dreigingen en incidenten worden gedeeld en besproken, komt nog niet overal van de grond. Daardoor blijft digitale veiligheid in veel instellingen vooral een onderwerp voor specialisten in plaats van een organisatiebreed leerproces (zie figuur 2.2.1).

Figuur 2.2.1 Inbedding informatiebeveiliging in het vervolgonderwijs (n = 79)



2.2.2 Organisatie van digitale weerbaarheid

In het vervolgonderwijs is informatiebeveiliging over het algemeen ondergebracht bij een CISO-afdeling onder het bestuur. Gemiddeld genomen besteden bestuurders met digitale weerbaarheid in hun portefeuille in het vervolgonderwijs 7,2% van hun tijd aan digitale weerbaarheid. De spreiding laat echter zien dat er aanzienlijke variatie bestaat, met scores die oplopen tot 33% in het hoger onderwijs en 25% in het mbo.

De overgrote meerderheid is lid van één of meer van de ondersteunende organisaties. Bijna alle besturen in het mbo zijn lid van de MBO Raad en de meeste besturen in het ho zijn lid van koepels hoger onderwijs (VH, UNL). Omdat sommige besturen multisectoraal zijn, zien we ook dat enkele bestuurders lid zijn van organisaties uit het funderend onderwijs zoals SIVON en de VO-raad. Ook zien we dat veel besturen gebruikmaken van SURF-diensten om kennis over digitale weerbaarheid te vergaren. Een meerderheid van besturen geeft aan gebruik te maken van generieke trainingen over digitale weerbaarheid.

2.2.3 Sturing op strategisch, tactisch en operationeel niveau

Om digitale weerbaarheid goed te organiseren, moet informatiebeveiliging niet alleen in beleid staan, maar ook zichtbaar zijn in de uitvoering. Dit vraagt om samenhang tussen strategisch, tactisch en operationeel niveau: van richting bepalen naar organiseren en sturen tot uitvoering in de praktijk. In onderstaande analyse wordt daarom gekeken naar de mate waarin bestuurders en IBP-functionarissen overeenstemming laten zien op stellingen die betrekking hebben op deze verschillende niveaus (zie figuur 2.2.3).

Op **strategisch niveau** gaat het om de vraag of het bestuur digitale weerbaarheid echt ziet als een onderwerp van bestuurlijke keuzes, prioriteiten en verantwoording. Het gaat hier om het vaststellen van beleid: het 'waarom' van informatiebeveiliging (SURF, z.j.). Juist op dit niveau kunnen verschillen bestaan in urgentiebeleving en bestuurlijke betrokkenheid (MBO Digitaal, 2024). Strategische sturing omvat niet alleen het formuleren van beleid, maar ook het actief monitoren van risico's en het afleggen van verantwoording over de mate waarin informatiebeveiliging effectief is ingericht.

Hier ontstaat een gemengd beeld. De meeste bestuurders zien digitale weerbaarheid als onderdeel van de primaire processen van hun instelling. Toch zijn bestuurders en CISO's het daarover maar in ongeveer de helft van de gevallen volledig eens. Ook zegt ongeveer de helft van de bestuurders dat het moeilijk is om verantwoordelijkheid voor digitale weerbaarheid te vertalen naar concrete keuzes in de organisatie. Juist hierover is de overeenstemming tussen bestuurders en CISO's beperkt: ongeveer een derde denkt daar hetzelfde over.

Bestuurders en CISO's verschillen ook in hun beeld van de tijd die digitale weerbaarheid vraagt. Ongeveer de helft van de bestuurders vindt niet dat het onderwerp veel tijd kost, terwijl de overeenstemming hierover laag is. De meeste bestuurders ervaren weinig terughoudendheid bij het melden van een ICT-incident bij de inspectie, al vindt een kleine groep dat wel lastig. Bijna alle bestuurders zeggen bovendien dat zij zich niet alleen zorgen maken om digitale weerbaarheid na een incident. Daarover is in driekwart van de gevallen overeenstemming met CISO's.

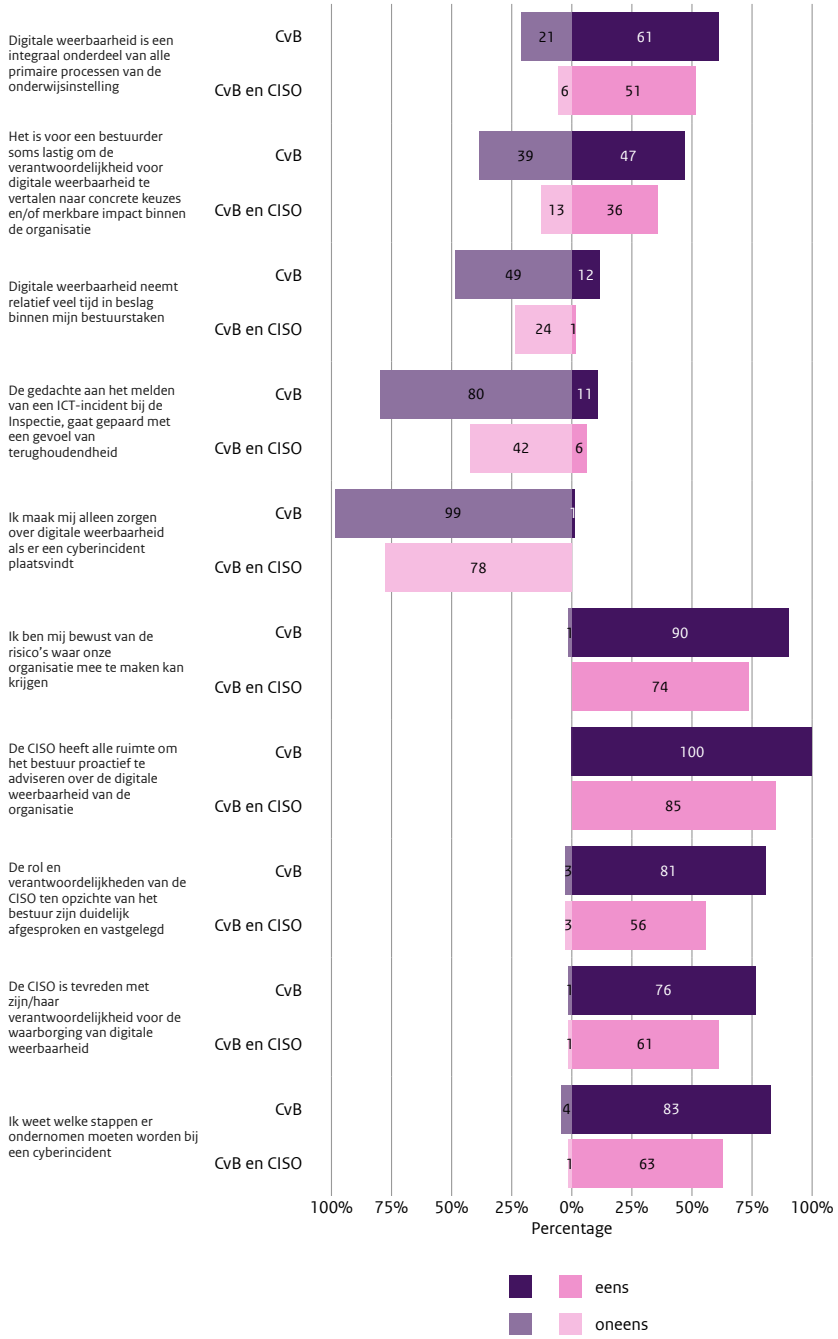
Op **tactisch niveau** gaat het om het vertalen van beleid naar afspraken, rollen, normen en ondersteuning. Dat wil zeggen: het omzetten van standaarden (wat moet geregeld zijn?) en richtlijnen (hoe wordt dit toegepast?) (SURF, z.j.) naar concrete beleidsdoelstellingen in normen, rollen en organisatorische afspraken. De IBP-functionaris opereert nadrukkelijk op dit niveau, onder meer via samenwerking met management, risicobeoordeling en bewustwording (MBO Digitaal, 2024).

Hier is het beeld duidelijk positiever. De meeste bestuurders zeggen dat zij zich bewust zijn van de digitale risico's van hun organisatie. Daarover zijn bestuurders en CISO's het in ongeveer driekwart van de gevallen eens. Alle bestuurders vinden dat de CISO genoeg ruimte heeft om het bestuur proactief te adviseren. Op dit punt is de overeenstemming het grootst. Tegelijk is er een kleinere groep CISO's die die ruimte minder duidelijk ervaart dan hun bestuurder denkt. Ook vinden veel bestuurders dat de rol en verantwoordelijkheden van de CISO duidelijk zijn afgesproken en vastgelegd. Daarover is redelijke, maar minder sterke overeenstemming. Verder denkt driekwart van de bestuurders dat de CISO tevreden is over zijn of haar verantwoordelijkheid. De meeste CISO's delen dat beeld.

Op **operationeel niveau** gaat het om de uitvoering: weten medewerkers wat ze moeten doen, en gebeurt dat ook in de praktijk. Veel bestuurders zeggen dat zij weten welke stappen nodig zijn bij een cyberincident. In de meeste gevallen wordt dit door CISO's bevestigd.

De bevindingen laten zien dat er in het vervolgonderwijs vooral op tactisch en operationeel niveau veel overeenstemming is tussen bestuurders en CISO's. Op strategisch niveau verschilt hun beeld vaker, vooral als het gaat om prioriteiten stellen en verantwoordelijkheid omzetten in concrete keuzes. Dat suggereert dat digitale weerbaarheid in veel instellingen wel is georganiseerd in beleid en uitvoering, maar nog niet overal even sterk bestuurlijk is verankerd.

Figuur 2.2.3 Sturing op digitale weerbaarheid in het vervolgonderwijs (n = 73)



2.3 Hoe verschillen besturen in het waarborgen van digitale weerbaarheid?

Uit verschillende onderzoeken naar digitale weerbaarheid in het funderend onderwijs (De Moor et al, 2022; 2025a) blijkt dat 3 factoren belangrijk zijn voor de digitale weerbaarheid van scholen: bewustwording, expertise en capaciteit.

Figuur 2.3 Samenhang tussen bewustwording, expertise, capaciteit en digitale weerbaarheid en de invloed van organisatiegraad en ketenafhankelijkheid

Bewustwording houdt in dat bestuurders en medewerkers het belang van digitale veiligheid en de bijbehorende risico's onderkennen. Uit de nulmeting en impactanalyse van Digitaal Veilig onderwijs (De Moor et al, 2022; 2025a) blijkt dat bestuurders digitale risico's regelmatig onderschatten en digitale veiligheid soms als belemmering zien. **Expertise** betreft de aanwezigheid van voldoende kennis en vaardigheden om digitale risico's te herkennen en passende maatregelen te nemen. Zowel de nulmeting, impactanalyse (De Moor et al, 2022; 2025a) en het sectorbeeld (Autoriteit Persoonsgegevens, 2024) laten zien dat taken rond digitale veiligheid vaak worden belegd bij medewerkers zonder specifieke expertise, wat effectieve risicobeheersing bemoeilijkt. **Capaciteit** verwijst naar de beschikbare tijd, mensen en middelen. Eerder onderzoek naar digitale weerbaarheid in het onderwijs (De Moor et al, 2022; 2025a; Autoriteit Persoonsgegevens, 2024; SURF, 2024) toont aan dat onderwijsinstellingen hierin vaak tekorten ervaren.

Deze 3 factoren versterken elkaar: meer bewustwording stimuleert investeringen in expertise en capaciteit, expertise vergroot het bewustzijn en voldoende capaciteit maakt het mogelijk om expertise op te bouwen.

Daarnaast speelt **organisatiegraad** – dat wil zeggen: geïnstitutionaliseerde samenwerking en kennisdeling tussen instellingen - een belangrijke rol bij digitale weerbaarheid (Auditdienst Rijk, 2024), met name vanwege **ketenafhankelijkheid** (SURF, 2024). Meer samenwerking leidt vaak tot gedeelde systemen en daarmee tot grotere onderlinge afhankelijkheid. Juist daardoor neemt het belang van gezamenlijke regie en heldere afspraken toe. Een hogere organisatiegraad kan ketenrisico's beter beheersen, maar vraagt om goede afstemming en voldoende capaciteit op sectorniveau. In het onderwijs ondersteunen organisaties zoals SURF (met name in mbo en hoger onderwijs), SIVON en Kennisnet (met name in het funderend onderwijs) instellingen met gezamenlijke diensten, zoals incidentondersteuning (CERT en SOC), gezamenlijke risicoanalyses en sectorbrede afspraken met leveranciers. Ook koepelorganisaties en sectorraden, zoals de PO-Raad, VO-raad en MBO Raad, dragen bij aan de organisatiegraad door belangenbehartiging, agendering, bestuurlijke afstemming en het stimuleren van gezamenlijke afspraken.

In dit onderzoek is getoetst welke verschillen tussen besturen samenhangen met (1) waarborgen van digitale weerbaarheid, (2) bewustzijn, (3) capaciteit en (4) expertie.

2.3.1 Verschillen tussen besturen in het funderend onderwijs

Ten eerste blijkt uit de analyse dat deelname aan kennisvergrotende activiteiten van onder andere Kennisnet en SIVON significant samenhangt met meer zicht op maatregelen die **digitale weerbaarheid waarborgen**. We hebben hierbij ook gecontroleerd op relevante achtergrondkenmerken van bestuurders en hun organisatie. Zo blijkt dat zowel bestuurders die eerder in hun loopbaan digitale weerbaarheid in hun portefeuille hadden als jongere bestuurders meer zicht hebben op relevante kaders en standaarden voor digitale weerbaarheid. Deze resultaten suggereren dat naast organisatiegraad ook bestuurlijk relevante ervaring bijdraagt aan inzicht in wat er van scholen verwacht wordt op het gebied van digitale weerbaarheid.

Ten tweede blijkt dat grotere besturen significant meer **bewustwording** laten zien dan kleinere besturen. Ook hangt deelname aan activiteiten met als doel kennis vergaren over digitale weerbaarheid positief samen met bewustwording. Ook persoonlijke affiniteit van de bestuurder met IBP hangt positief samen met bewustwording. Deze bevindingen suggereren dat schaalgrootte en organisatiegraad bijdragen aan bestuurlijk bewustzijn. Grotere besturen zijn door schaalgrootte mogelijk beter in staat het onderwerp organisatorisch te borgen en worden vaker geconfronteerd met digitale risico's, waardoor het hoger op de agenda staat. De sterke samenhang met deelname aan activiteiten wijst erop dat kennisdeling en sectorbrede afstemming bijdragen aan meer bewustwording, wat aansluit bij de rol van samenwerking zoals beschreven door de Autoriteit Persoonsgegevens (2024). Andersom zou het ook kunnen zijn dat besturen met meer bewustzijn ook meer deelnemen aan georganiseerde activiteiten voor digitale weerbaarheid.

Ten derde zien we dat grotere besturen significant meer **capaciteit** rapporteren dan kleinere besturen. Daarnaast blijkt dat bestuurders die zich comfortabel voelen met hun verantwoordelijkheid voor digitale weerbaarheid eveneens meer capaciteit rapporteren dan bestuurders die zich daar niet comfortabel mee voelen. Schaalgrootte lijkt dan ook een belangrijke structurele factor te zijn voor het organiseren van capaciteit. Dit sluit aan bij eerdere bevindingen uit de nulmetingen (De Moor et al, 2022; 2025a) dat kleinere instellingen relatief kwetsbaarder zijn. De samenhang tussen ervaren verantwoordelijkheid en capaciteit kan wijzen op wederzijdse versterking: wie zich bekwaam voelt in deze rol, organiseert eerder middelen, of ervaart de beschikbare middelen als adequaat.

Ten vierde blijkt dat actieve deelname aan netwerken met als doel kennis vergaren over digitale weerbaarheid significant samenhangt met meer **expertise**. Ook lidmaatschap van sectororganisaties zoals SIVON/BIC náást lidmaatschap van de PO- of VO-Raad hangt positief samen met expertise. Daarbij beschikken bestuurders met eerdere verantwoordelijkheid voor digitale weerbaarheid over meer expertise. Expertise blijkt sterk samen te hangen met organisatiegraad en bestuurlijk relevante ervaring op het gebied van digitale weerbaarheid. Sectororganisaties fungeren hier waarschijnlijk als kennisinfrastructuur. De bevinding dat interne medewerkers bijdragen aan expertise benadrukt het belang van structurele kennisdeling en samenwerking.

2.3.2 Verschillen tussen besturen in het vervolgonderwijs

Ten eerste zien we dat grote besturen significant meer **waarborgen voor digitale weerbaarheid** hebben door het werken met een meer risicogestuurde aanpak van informatiebeveiliging en integrale veiligheid dan kleine besturen. Ook worden dergelijke werkwijzen vaker gerapporteerd door bestuurders met meer affiniteit met digitale weerbaarheid dan bestuurders met minder affiniteit.

Ten tweede zien we net als in het funderend onderwijs dat grote besturen meer **bewustwording** laten zien dan kleine besturen. Ook blijkt dat individuele kenmerken van bestuurders samenhangen met bewustwording. Bestuurders die een grotere affiniteit hebben met digitale weerbaarheid tonen significant meer bewustzijn. Daarnaast hangt ook het comfort dat bestuurders richting de verantwoordelijkheid voor digitale weerbaarheid hebben positief samen met bewustwording. Deze bevinding laat zien dat binnen het vervolgonderwijs bewustwording minder sterk wordt verklaard door organisatorische factoren, en meer door persoonlijke houding en betrokkenheid van bestuurders. Dit wijst erop dat individuele motivatie en zelfvertrouwen in dit domein mogelijk een belangrijkere rol spelen dan structurele kenmerken van het bestuur.

Ten derde zien we geen significante samenhang tussen bestuurlijke kenmerken en **capaciteit**. Wel blijken besturen in regio Noord (Friesland, Groningen en Drenthe) meer significant meer capaciteit te rapporteren dan besturen in regio Midden (Noord-Holland, Zuid-Holland en Utrecht). Ook blijkt opnieuw dat individuele factoren een rol spelen. Bestuurders die zich comfortabeler voelen met hun verantwoordelijkheid voor digitale weerbaarheid rapporteren significant meer capaciteit binnen hun

organisatie dan bestuurders die zich hier minder comfortabel bij voelen. Deze bevinding duidt erop dat ervaren capaciteit in het vervolgonderwijs samenhangt met hoe bestuurders hun eigen rol en verantwoordelijkheid ervaren. Het is daarbij niet vast te stellen of een groter gevoel van comfort leidt tot het organiseren van meer capaciteit, of dat beschikbare capaciteit bijdraagt aan een groter gevoel van comfort.

Tot slot zien we geen bestuurlijke kenmerken die samenhangen met **expertise**. Wel zien we opnieuw dat bestuurders met een grotere persoonlijke affiniteit met digitale weerbaarheid significant meer expertise rapporteren dan bestuurders met minder affiniteit. Dit suggereert dat expertise in het vervolgonderwijs vooral samenhangt met persoonlijke betrokkenheid, en minder met organisatorische kenmerken.

3. Factoren die digitale weerbaarheid versterken of belemmeren

In dit hoofdstuk presenteren we de resultaten van de verdiepende deelvragen 4 en 5. Hiertoe zijn interviews gehouden met bestuurders en IBP-functionarissen/CISO's uit de steekproef. In totaal zijn 25 besturen geïnterviewd: 13 in het funderend onderwijs en 12 in het vervolgonderwijs. De selectie varieerde in onder meer bestuursgrootte en organisatievorm. De geïnterviewde besturen zijn voorzien van een pseudoniem (bijvoorbeeld: PO1 en HO4). Aan de hand van een topiclijst is gesproken over helpende en belemmerende factoren bij het waarborgen van digitale weerbaarheid. De interviews zijn thematisch geanalyseerd om patronen te identificeren. Hiermee is inzicht verkregen in factoren die besturen helpen en belemmeren bij het waarborgen van digitale weerbaarheid.

3.1 Veelzijdigheid IBP

Tijdens het interview met een po-bestuurder vroegen wij naar diens mening over een IBP-functionaris die meerdere petten draagt. Dat wil zeggen: een IBP-functionaris die zich bekommert om meer dan alleen de technische kant van IBP. Denk hierbij aan beleidsvorming, communicatie en - zoals bij hen het geval was - ICT. De bestuurder antwoordde hierop het volgende:

> *"Ik ervaar het niet als verschillende petten. Ik denk wel dat het een pet is met verschillende, hoe zeg je dat, werkvelden daarin. En ik denk dat juist het feit dat we eigenlijk één iemand die veelkleurige pet op z'n hoofd hebben gezet, juist maakt dat er dus voortdurend focus ligt op het onderwerp, hoe breed ook, hè. Dus het hele IT-onderwerp, waarin dus privacy zit, maar ook bijvoorbeeld digitale geletterdheid en de link die daarnaartoe ligt. Ik denk dat dat juist, dus die veelzijdigheid van deze klus, maar het feit dat die bij één persoon belegd is, een kwaliteitsversterkend effect heeft op de samenhang tussen al die onderdelen." (bestuurslid, PO5)*

Het citaat raakt de kern van ons eerste thema: de veelzijdigheid van IBP. Ten grondslag aan de veelkleurige pet van de IBP-functionaris, ligt de multidimensionale aard van het domein. IBP reikt verder dan louter de techniek, en omvat ook organisatorische, juridische, beleidsmatige, psychologische en communicatieve aspecten (Ferdousi, 2024). Zo vatte de IBP-functionaris van HO6 het samen als 3 aspecten: een menselijke, procesmatige en technische kant. De interviewdata wierp licht op het belang om IBP in verbondenheid met alle aspecten te beschouwen, in plaats van los van elkaar. Oftewel, een veelkleurige pet in plaats van afzonderlijke petten. Het duurzaam borgen van digitale weerbaarheid vraagt daarom om een aanpak die recht doet aan deze veelomvattendheid. Op basis van de interviewdata stellen we dat dit een integrale aanpak betreft, gericht op het samenbrengen en borgen van al deze kanten. We identificeerden verschillende voorwaarden voor een integrale aanpak.

3.1.1 Integrale veiligheidsvisie

De visie van een schoolbestuur op digitale weerbaarheid en veiligheid stuurt hoe intern wordt omgegaan met IBP (PO-raad & VO-raad, 2024). Meerdere geïnterviewde besturen hadden digitale weerbaarheid opgenomen in hun integrale veiligheidsvisie. Binnen deze visie worden veiligheidsincidenten en -risico's in samenhang met elkaar benaderd via gemeenschappelijke processen en onderlinge samenwerking (IV-HO, 2021, p. 9). Een bestuurder van een mbo-instelling legde uit dat zij bewust niet vanuit afzonderlijke facetten denken, maar juist sociale, fysieke en digitale veiligheid aan elkaar koppelen:

> *"Die fysieke en digitale veiligheid raken elkaar ook. [...] Uiteindelijk, als je die digitale veiligheid niet op orde hebt, kan je je onderwijs gewoon niet meer verzorgen. En op het moment dat je dat in een onveilige situatie doet, breng je en medewerkers, en leerlingen of studenten in gevaar." (bestuurslid, MBO3)*

Digitale veiligheid is onlosmakelijk verbonden met de algehele veiligheid van een onderwijsinstelling. Cyberincidenten kunnen immers directe gevolgen hebben voor onder meer de continuïteit van het onderwijs (Inspectie van het Onderwijs, 2021). Het integreren van digitale veiligheid in de bredere veiligheidsvisie, is een belangrijke stap voor integraliteit en de verschuiving van IBP als 'ICT-feestje' naar een organisatiebrede prioriteit. Deze stap behelst namelijk de expliciete positionering van digitale veiligheid als een bestuurlijk vraagstuk.

3.1.2 Bestuurlijke betrokkenheid

Het belang van bestuurlijke betrokkenheid kwam duidelijk naar voren in de interviewdata. De organisatie van IBP is intern afhankelijk van een samenspel tussen capaciteit, expertise en bewustwording. Doordat school- en instellingsbesturen de strategische visie, de begroting en het personeelsbeleid vormgeven, beslissen zij welke prioriteiten en middelen beschikbaar komen voor IBP. Effectieve sturing vraagt om duidelijke strategie, heldere verantwoordelijkheden en voldoende middelen (Yusif & Hafeez-Baig, 2021). 2 IBP-functionarissen van een so-bestuur beschreven bestuurlijke betrokkenheid als voorwaarde van IBP:

> *IBP-functionaris 1: "Eigenlijk is het ook wel zo dat het wel belangrijk is dat je mensen hebt die tijd krijgen binnen een bestuur om dit te mogen doen. Dat denk ik wel dat dat ook wel een voorwaarde is om dit te kunnen realiseren."*

> *IBP-functionaris 2: "Ja, ja, want [onze] bestuurder die ondersteunt dat wel, dat we daar tijd aan besteden. [...] Ik denk dat het belangrijk is dat de bestuurder zelf enigszins op de hoogte is, inhoudelijk ook, en het faciliteert." (SO1)*

Een effectieve digitale veiligheidsstrategie berust op veerkracht (oftewel: het vermogen om snel te herstellen na cyberincidenten) en actieve verdediging, waarbij potentiële dreigingen worden gemonitord en bestreden (Yusif & Hafeez-Baig, 2021). De IBP-functionarissen vertelden dat hun bestuur over voldoende expertise beschikt om weloverwogen en geïnformeerde strategische keuzes te maken. Deze keuzes, waaronder de positie van 2 IBP-functionarissen, bewerkstelligden de kaders waarbinnen het IBP-team kon floreren.

Enkele besturen binnen het funderend onderwijs gaven daarentegen aan geen toegewezen IBP-functionaris in dienst te hebben. In plaats daarvan waren IBP-taken toegewezen of belegd bij medewerkers wier primaire taak niet IBP-gerelateerd is. Het ontbreken van een toegewijde IBP'er kan leiden tot onvoldoende borging van digitale weerbaarheid en een verhoogde werkdruk voor de medewerkers met dubbele rollen. De aanwezigheid van expertise werd veelvuldig aangehaald als helpende factor in de waarborging van digitale weerbaarheid. Daarom zien wij een informatiebeveiligingsspecialist (intern of via inhuur) als onmisbaar in het waarborgen van de digitale weerbaarheid.

Wij zien als risico dat de prioritering van IBP en de doelmatige inzet van middelen afhankelijk zijn van het bestuur, met name van hun expertise, gevoelde urgentie en betrokkenheid bij het onderwerp. Enkele geïnterviewden vertelden dat specifiek in het funderend onderwijs de individuele affiniteit en gevoelde urgentie van een bestuurder belangrijke aanleidingen vormen om digitale weerbaarheid hoog op de bestuurlijke agenda te plaatsen. Dit zou kunnen betekenen dat onderwijsbesturen met minder affiniteit en zonder urgentiegevoel het onderwerp onvoldoende prioriteren[7]. Het is noodzakelijk dat elk bestuur als collectief over voldoende kennis beschikt van onderwerpen als risicobereidheid en -beheersing, wet- en regelgeving en incidentrespons, om weloverwogen strategische keuzes te kunnen maken over de inrichting van IBP (Yusif & Hafeez-Baig, 2021). Hoewel niet van elk individueel bestuurslid diepgaande expertise kan worden verwacht, kan gerichte training wel bijdragen aan het versterken van het bestuurlijk inzicht en het vermogen om geïnformeerde beslissingen te nemen over cyberrisico's (Gale et al., 2022).

3.1.3 Multidisciplinaire inrichting van IBP

Een bekwaam bestuur en een passende visie vormen de bouwstenen voor een integrale aanpak van IBP. De IBP-doelstellingen, gebaseerd op de integrale veiligheidsvisie en -strategie van het bestuur, worden vervolgens door de centrale staforganisatie vertaald in tactische en operationele keuzes (IV-HO, 2021). Terugkerend naar de beeldspraak van IBP als veelkleurige pet, benadrukken we hier dat deze pet niet door één persoon of geïsoleerd team gedragen kan worden. Zo vertelde een IBP-functionaris het volgende in relatie tot bewustwording en het menselijke aspect van IBP:

> *"Dit is niet echt iets wat een CISO of een informatiebeveiliger alléén kan. Daar heb je een multidisciplinair team voor nodig." (IBP-functionaris, HO7)*

Deze participant omschreef digitale weerbaarheid als een multidisciplinair vraagstuk dat vraagt om nauwe samenwerking tussen verschillende interne domeinen. Binnen alle sectoren hoorden we voorbeelden van dergelijke samenwerkingen. Zo bundelt het IBP-team van HO7 de krachten met HR, de communicatieafdeling, psychologen en veiligheidsdeskundigen om bewustwording aan te pakken. Bij PO1 zijn de normen van het normenkader IBP toegewezen aan proceseigenaren binnen hun vakgebied, waaronder de afdelingshoofden van HR, IB en Financiën. Een projectteam ondersteunt de proceseigenaren en behoudt het overzicht.

7 Hoewel persoonlijke affiniteit van bestuurders ook in het vervolgonderwijs van invloed is, is digitale weerbaarheid daar doorgaans sterker organisatorisch verankerd. Hierdoor is het in het vervolgonderwijs in mindere mate een risico dan in het funderend onderwijs.

Een integrale aanpak vereist centrale coördinatie om het overzicht te bewaken en fragmentatie tussen teams en afdelingen te voorkomen. Bij HO4 gebeurt dit via een interdisciplinaire benadering, waarbij digitale weerbaarheidsborging op basis van een integrale veiligheidsvisie een samenspel is tussen afdelingen. Om deze samenwerking te structureren, heeft de IBP-functionaris een aparte regieafdeling opgericht. Daarbinnen komen hij en medewerkers met regierollen per domein samen. De veelkleurige IBP-pet manifesteert zich in een coördinerende rol voor de IBP-medewerker. Sprekend over de interne samenwerkingen benoemden geïnterviewden ook het belang van korte lijnen, frequente afstemming en een duidelijke afbakening van rollen en verantwoordelijkheden.

Een integrale IBP-aanpak implementeren en goed organiseren blijkt in de praktijk nog best uitdagend. Een IBP-functionaris van een mbo-bestuur vertelde:

> *"Dat is best wel een klus om dat, om daar ook een basis voor neer te zetten, om überhaupt voor elkaar te krijgen dat er verantwoordelijkheidsgevoel is op andere plekken, dat het een organisatie – ja, het klinkt zo cliché – organisatiefeestje is en niet een ICT-feestje. Om dat in beweging te krijgen, om daar een goede strategie voor te hebben staan. Dat kost ook allemaal tijd en dat kan niet allemaal... Je kunt ook niet vooruitrennen." (IBP-functionaris, MBO5)*

In de interviews werd digitale weerbaarheid dikwijls beschreven als een proces dat tijd en structurele inzet kost. Gebrek aan capaciteit kwam prominent naar voren als belemmering, met verschillende gevolgen. Financiële beperkingen brengen besturen in een positie waarbij men moeilijke keuzes moet maken: investeren in digitale weerbaarheid of het geld steken in andere processen binnen de organisatie. Zo deelde een bestuurder van HO4 dat zij vanwege bezuinigingen genoodzaakt waren hun strategische budget te verlagen, om zo onder andere het IBP-budget in stand te kunnen houden.

Schaalgrootte speelt een rol in de beschikbare capaciteit. De grote besturen die wij spraken, konden zich omvangrijkere IBP-teams veroorloven dan de kleinere instellingen, die het soms met 1 of 2 medewerkers moeten doen. Meerdere kleinere besturen gaven aan dat ze vanwege beperkte budgetten cyberrisico's in de breedte minder goed kunnen afdekken en genoodzaakt zijn hun risicobereidheid te vergroten. Een voorbeeld hiervan is de aanwezigheid van een Security Operations Center (SOC). Participanten bij PO1 benadrukten dat hun grote schaalomvang hen in staat stelde om een externe partij in te huren voor voortdurende monitoring. VO4 daarentegen (een klein bestuur) deelde het dilemma tussen enerzijds het belang van een SOC en anderzijds de financiële beperkingen. Hierover vertelde de bestuurder:

> *"Als ieder [bestuur] zijn eigen SOC moet gaan oprichten en betalen – ja, mensen lieve – dan ben je echt flink wat geld kwijt. En dat gaat van, dat slokt een flink stuk van het budget op. Dus dat is wel mijn zorg, hoewel ik absoluut het voordeel van zoiets wel zie; permanente radar van je systeem, dat is denk ik in de toekomst steeds meer nodig. Maar hoe houd je het als vo-school van onze omvang betaalbaar?" (bestuurslid, VO4)*

Ook hebben beperkte middelen met name bij kleine besturen tot gevolg dat deze scholen niet kunnen inspelen op *single points of failure,* doordat ze geen ruimte hebben om extra mensen aan te nemen of in te huren. Het Nationaal Cyber Security Centrum (NCSC) (z.d.-a) benadrukt dat maatregelen proportioneel moeten zijn ten opzichte van de risico's en omvang van de organisatie.

In het omgaan met beperkte capaciteit zien wij een kans in de vorm van *shared services* en sectorsamenwerkingen. Samenwerkingen bespreken we nader in hoofdstuk 4.4.

3.1.4 Monitoring en evaluatie

Overzicht van zaken diende voor vele besturen als startpunt om te bepalen waar ze staan en waar ze naartoe willen. Onafhankelijke en interne toetsing kwamen veelvuldig naar voren als hulpmiddel om de IBP-positie te bepalen en risico's in kaart te brengen. Deze toetsing biedt niet alleen inzicht in de huidige status, maar helpt ook om gerichte verbeterstappen te kunnen zetten. Vanwege financiële beperkingen is niet elk bestuur in staat om externe audits te in te zetten. Meerdere besturen gaven aan onzeker te zijn over het inschatten van hun eigen situatie. Self-assessments bieden weliswaar een eerste indicatie, maar missen de diepgang en objectiviteit van een externe blik. Ook vertelden besturen die zowel interne als externe toetsing hadden, dat er soms grote verschillen zaten tussen de beide uitkomsten, afhankelijk van hoe streng er gekeken werd.

Een mogelijke kans voor het realiseren van externe audits binnen financiële beperkingen is het benutten van sectorspecifieke samenwerkingsverbanden. Uit de interviews kwamen verscheidene praktijkvoorbeelden naar voren. Zo voerden enkele mbo-instellingen gefaciliteerd door MBO Digitaal gezamenlijk mbo-brede security-audits uit via een externe partij.

3.2 Veiligheidscultuur

Tijdens de interviews vertelden de geïnterviewden over hun ervaringen met cyberincidenten op de scholen en instellingen. Zo werd er gesproken over een DDOS-aanval geïnitieerd door een technisch zeer vaardige leerling in het funderend onderwijs, en over honderden computers die tijdelijk onvindbaar waren in een instelling binnen het vervolgonderwijs. De meest gedeelde verhalen betroffen datalekken door (niet-opzettelijk) toedoen van een medewerker. Denk aan het per abuis klikken op een phishing link, of het verzenden van een e-mail naar de verkeerde afzender. Binnen elke sector hadden besturen hiermee te maken: de *human factor*. In deze paragraaf richten wij ons nader op dit menselijke aspect van IBP.

Menselijk handelen wordt dikwijls aangemerkt als een grote kwetsbaarheid voor de digitale weerbaarheid en veiligheid van organisaties (Sutton & Tompson, 2025; Wiley et al., 2020; Flores & Ekstedt, 2016; Hu et al., 2012). Cybercriminelen maken misbruik van deze kwetsbaarheid met *social engineering* en het voortdurend aanpassen van hun tactieken (Flores & Ekstedt, 2016). Technische en beleidsmatige maatregelen bieden tot op zekere hoogte bescherming. Echter, er valt nooit uit te sluiten dat een medewerker op een malafide link klikt van een e-mail die het spamfilter wist te omzeilen. Een veelvoorkomende valkuil van IBP-strategieën is dan ook de eenzijdige focus op technologie en beleid, zonder rekening te houden met menselijk gedrag (Cheng & Wang, 2022). Hoewel menselijk gedrag vaak wordt gezien als het resultaat van louter individuele besluitvorming, speelt de sociale context waarin het gedrag gesitueerd is eveneens een belangrijke rol in de keuzes die een persoon uiteindelijk maakt (Wiley et al., 2020).

Een integrale aanpak vereist daarom - naast formeel-organisatorische en technische maatregelen - ook wat wij het informele aspect van IBP noemen: de culturele verankering van digitale weerbaarheid en veiligheid binnen de organisatie. Een organisatiecultuur van digitale veiligheid omvat daarom ook de gedeelde overtuigingen, waarden en attitudes binnen een organisatie die medewerkers helpen veilig te handelen en risico's te beheren (Huang & Pearlson, 2019, p. 6399). Deze cultuur heeft een belangrijke invloed op de houding van individuele medewerkers ten opzichte van cyberveiligheidshandelingen en speelt een belangrijke rol in het gedrag dat ze vertonen (Flores & Ekstedt, 2016; Hu et al., 2012). Op basis van de interviews identificeerden we 4 aspecten die tezamen bijdragen aan een organisatiecultuur van digitale weerbaarheid en veiligheid.

3.2.1 Digitale weerbaarheid als gedeelde verantwoordelijkheid

Uit de interviews kwam het creëren van een gedeeld verantwoordelijkheidsgevoel naar voren als helpende factor. Zo benadrukt de bestuurder van VO4 het belang van steun vanuit de organisatie en het actief betrekken van collega's: *"Iedereen is van cybersecurity, zal ik maar zeggen. Iedereen heeft daar een rol in."* Dit principe beoogt digitale veiligheid te integreren in dagelijkse werkprocessen, juist ook voor medewerkers zonder primaire IBP-taken. Om deze overtuiging direct mee te geven, hebben meerdere besturen digitale weerbaarheid opgenomen in hun onboardingsprogramma.

In de praktijk blijkt het creëren van een gedeeld verantwoordelijkheidsgevoel een lastige opgave te zijn. Vrijwel elk bestuur gaf aan dat er sprake was van weerstand vanuit de organisatie. Participanten wezen erop dat digitale weerbaarheid één van de vele prangende thema's is in het onderwijs. Met uitdagingen zoals het lerarentekort en bezuinigingen hebben onderwijsmedewerkers al veel op hun bord. Als digitale veiligheid ten koste gaat van de gebruiksvriendelijkheid van systemen, leidt dit vaak tot kritiek vanuit het personeel of zelfs het omzeilen van de maatregelen. Uit de interviews kwam naar voren dat bij besturen in het funderend onderwijs met een decentrale aansturing en bij besturen in het vervolgonderwijs (in het bijzonder universiteiten) er eveneens sprake was van een spanning tussen autonomie en veiligheid. Enerzijds willen scholen en faculteitsinstellingen hun autonomie behouden, anderzijds vereist digitale veiligheid een bepaalde mate van centralisatie.

Medewerkers die IBP als bijzaak beschouwen vertonen aanzienlijk minder veilig gedrag (Flores & Ekstedt, 2014). Draagvlak is daarom noodzakelijk voor de effectiviteit van IBP-protocollen en -beleid. Participanten benadrukten het belang van dialoog met de medewerkers die weerstand tonen. Actief naar hen luisteren en hen betrekken in het proces verhoogt het begrip, is de ervaring van de participanten. Uitleggen van het "waarom" achter de IBP-maatregelen en het illustreren van urgentie met actuele cyberincidenten als herkenbare voorbeelden werd veelvuldig genoemd als effectieve communicatiestrategieën. Tegelijkertijd benadrukten participanten dat grenzen nodig blijven: digitale weerbaarheid is geen vrijblijvend thema. Het creëren van draagvlak uit zich ook in het beleggen van rollen als i-coach en ambassadeurs bij medewerkers zonder primaire IBP-functie.

3.2.2 Open, lerende cultuur

Een open, lerende cultuur werd dikwijls aangehaald door participanten als een helpende factor in de digitale weerbaarheid. Hierin staat het sentiment centraal dat fouten maken mag; medewerkers worden aangemoedigd om cyberincidenten en mogelijke risico's te melden. Een pro-actieve meldcultuur wijst op een bewuste werkvloer (Huang & Pearlson, 2019; NCSC, z.d.-b).

Een ander aspect dat participanten noemden over een open, lerende cultuur, is laagdrempeligheid. Een concreet voorbeeld hiervan is de "biechtstoelvraag" toegepast door een bestuurder van een ho-bestuur tijdens structurele gesprekken met het IBP-team:

> *"De biechtstoelvraag betekent eigenlijk dat ik aan het eind van zo'n gesprek, ook op het gebied van IT en cyber[veiligheid], vraag: zijn er dingen die ik vanuit mijn verantwoordelijkheid zou moeten weten en die je nog niet verteld hebt? En het zal je verbazen. Dat zet mensen vaak aan het denken. Dan komen er toch altijd nog wel wat dingetjes naar boven, onder andere op het gebied van digitale weerbaarheid." (bestuurslid, HO2)*

Deze aanpak illustreert hoe openheid actief gefaciliteerd kan worden met gerichte interventies. Bovenop de formele meldstructuren binnen HO2 biedt de biechtstoelvraag IBP-functionarissen een laagdrempelige manier om informatie te delen, zonder schaamte of angst voor repercussies. Het benadrukt dat medewerkers soms een expliciete uitnodiging nodig hebben, mogelijk juist van iemand in een hogere hiërarchische positie. Daarnaast benadrukt dit het belang om erop te blijven wijzen dat je nooit 'te laat' kunt zijn met melden. Ook humor werd door sommige participanten aangehaald als instrument om laagdrempeligheid te creëren.

Een vo-bestuurder gaf aan dat een open cultuur ook openheid vanuit het bestuur vereist naar zowel de medewerkers als de buitenwereld:

> *"Je hoeft niet al je vuile was buiten [te hangen], maar gewoon transparant zijn: dit is ons overkomen. [...] Maak het open, maak het transparant en dan gaan mensen het begrijpen." (bestuurslid, VO3)*

3.2.3 Zichtbaar leiderschap

Het topmanagement heeft direct invloed op het vormen en bevorderen van een digitale veiligheidscultuur binnen een organisatie (Triplett, 2022; Flores & Ekstedt, 2016; Hu et al., 2012). Topmanagement verwijst hier zowel naar het bestuur als naar medewerkers in leiderschapsposities zoals afdelingshoofden, schooldirecteuren en decanen. De nalatigheid van het topmanagement op dit gebied is de achilleshiel van de organisatorische digitale weerbaarheid: zonder zichtbaar en transformatief leiderschap ontbreekt de basis voor een sterke veiligheidscultuur (Triplett, 2022).

Uit de interviews kwam het legitimeren van IBP-maatregelen naar voren als een belangrijke manier waarop het topmanagement kan bijdragen aan en sturen op een sterke veiligheidscultuur. Legitimering komt tot uiting met het openlijk steunen van maatregelen en het onderstrepen van de meerwaarde ervan. Ook noemden participanten de actieve en zichtbare deelname van topmanagement aan bijvoorbeeld bewustwordingstrainingen. Dergelijke betrokkenheid toont personeel het belang van IBP-beleid en -protocollen, én het belang om deze serieus te nemen. Ook draagt de ondersteuning van bovenaf bij aan het moreel van IBP-functionarissen. Meerdere IBP-functionarissen ervoeren dat hun inzet soms weinig waardering van collega's opleverde. Zo komt het voor dat de weerstand vanuit medewerkers leidde tot kritiek op de IBP-functionarissen. Een IBP-functionaris vertelde hierover:

> *"Toen wij bijvoorbeeld 2FA invoerden... Dan moet je wel stevig in je schoenen staan, want we hebben een hoop gedoe over ons heen gekregen. Als je iets wil veranderen en de mensen, het wordt een beetje lastiger voor mensen, dat vinden ze niet leuk." (IBP-functionaris, SO1)*

Het is belangrijk dat IBP-functionarissen gesteund en gefaciliteerd worden door topmanagement en dat ze ervaren er niet alleen voor te staan. Tot slot wezen interviewparticipanten op het belang van voorbeeldgedrag. Wanneer individuen in leiderschapsposities zelf de veiligheidsnormen naleven, stimuleren zij medewerkers om hetzelfde gedrag te vertonen.

3.2.4 Trainingen en scholing

Uit de interviews bleek een scala aan initiatieven te worden ingezet om bewustwording en digitale geletterdheid bij medewerkers, leerlingen en studenten te verhogen. Naast het overdragen en verhogen van kennis, zijn trainingen en scholing een belangrijke manier om het belang van digitale weerbaarheid te benadrukken en een gedeelde norm te creëren (Hu et al., 2012; Flores & Ekstedt, 2016). Echter, zonder de aanwezigheid van de 3 eerder besproken aspecten, zijn louter bewustwordingsinitiatieven onvoldoende (Huang & Pearlson, 2019). We constateren wel een risico bij een eenzijdige focus op trainingen. Bij gebrek aan een sterke veiligheidscultuur kunnen bewustwordingsinitiatieven worden ervaren als een verplichting om af te vinken in plaats van een gedeelde waarde (Triplett, 2022). Daardoor dreigen trainingen en scholing hun effectiviteit te verliezen. Anderzijds benadrukten enkele participanten het risico van een blinde vlek. Met name onderzoekspersoneel en technisch-geschoolde medewerkers in het vervolgonderwijs toonden weerstand tegen bewustwordingsinitiatieven omdat zij deze als irrelevant beschouwden. Toch behoren ook zij, net als het andere personeel, tot de doelgroep voor bewustwordingsinitiatieven.

HO4 gaf aan hoe zij omgingen met de weerstand vanuit het personeel; namelijk door hen te betrekken in de ontwikkeling van bewustwordingsinitiatieven en -producten. Meerdere participanten hanteren een soortgelijke aanpak. Door medewerkers te betrekken, ontstaat meer draagvlak en zijn trainingen beter op de praktijk afgestemd. Naast medewerkersbetrokkenheid noemden participanten als helpende factoren: introduceren van spelelementen, korte en gerichte trainingen en continu op bewustwording inzetten. Tegelijkertijd vormt de continuïteit van bewustwording juist een knelpunt voor sommige besturen, doordat dit vraagt om blijvende capaciteit die niet altijd beschikbaar is.

3.3 Ecosysteem en verantwoordelijkheid

Tijdens dit onderzoek kwam naar voren dat diverse partijen een rol spelen bij digitale weerbaarheid in het onderwijs: onderwijsbesturen, hun partners (zoals ICT-leveranciers en adviesbureaus), publieke (ondersteunings)organisaties en de overheid. Tussen deze partijen bestaan wisselwerkingen en afhankelijkheden, onder andere door uitbesteding en samenwerking. De partijen kunnen daardoor beschouwd worden als een soort ecosysteem (Jacobides et al., 2018; Kapoor, 2018). Binnen dit ecosysteem komen autonomie, keuzevrijheid en publieke waarden onder druk te staan, worden verantwoordelijkheden en governance complex en kunnen verstoringen en cyberincidenten zich verspreiden door de keten. Hieronder gaan we in op de verschillende afhankelijkheden en wisselwerkingen die tijdens de interviews ter sprake kwamen.

3.3.1 ICT-middelen

Onderwijsinstellingen zijn in alle sectoren afhankelijk van (inter)nationale ICT-leveranciers voor officepakketten, leermiddelen en andere ICT-middelen, wat als risicovol wordt beschouwd door het Rathenau Instituut (Hamer & Kool, 2021), de Autoriteit Persoonsgegevens (2024), SURF (Hoger Onderwijs Persbureau, 2025) en Kennisnet (2026). Eén po-bestuur geeft aan de haalbaarheid van een overstap naar opensource-alternatieven te onderzoeken:

> *"[W]ij willen eigenlijk naar het Duits model, volledig open source. En kunnen wij weg bewegen van [leverancier A] en [leverancier B]? [...] Dat is echt iets waarvan ik ook een vraag stel aan onze ICT-club, van: zoek dat nou eens uit [...]." (IBP-functionaris, PO4)*

Echter, overstappen naar andere leveranciers is zo makkelijk nog niet. Dit komt onder andere door de verminderde keuze dankzij marktverschraling (Van Elk, 2024) en 'vendor lock-ins', waarbij een organisatie dermate afhankelijk is van een leverancier, dat overstappen grote financiële en/of operationele gevolgen heeft (Hartholt, 2025). Daarnaast wijzen De Moor et al. (2025b) op de sterke marktmacht van grote technologiebedrijven, waardoor individuele onderwijsinstellingen vaak een zeer beperkte onderhandelingspositie hebben ten aanzien van contractvoorwaarden, prijsstelling en datagebruik. Dit beperkt niet alleen de keuzevrijheid, maar ook de handelingsruimte van onderwijsbesturen in de praktijk. Het is voor veel – zo niet alle – onderwijsbesturen ondoenlijk om volledig zelf te zorgen voor bepaalde software, servers of systemen en de dienstverlening die daarbij hoort. Zoals een mbo-bestuurslid het verwoordde:

> *"[J]e kan niet alles zelf, hè. Wij zijn een onderwijsinstelling en we zijn geen ICT-instelling, hè". (Bestuurslid, MBO2)*

Die afhankelijkheid kan de IBP-organisatie van onderwijsinstellingen zowel positief als negatief beïnvloeden, zo blijkt uit de interviews. Die invloed kan positief zijn in het geval van goede beveiliging en de specialistische kennis en kunde van ICT-leveranciers, die de implementatie en borging van IBP bij onderwijsbesturen kunnen ondersteunen. De ervaring van een mbo-bestuurder was als volgt:

> *"Deze [professionals] komen van [...] een commerciële IT-partner [...]. Die zijn hier zo gepokt en gemazeld in. Die hebben al zoveel NIS2-implementaties gehad. Die zijn zo goed doorgevoerd." (Bestuurslid, MBO1)*

De invloed kan ook negatief zijn: een aantal geïnterviewde besturen sprak over de problemen die zij door die afhankelijkheid ervaren bij het op orde brengen en houden van hun digitale weerbaarheid. Een ho-bestuurder vertelt hierover:

> *"Je kroonjuwelen zoals Osiris. Dat is weliswaar bij een extern bedrijf. Dat zou je elk jaar bij zo'n bedrijf moeten toetsen. Voldoen ze eraan, zijn die back-ups echt gemaakt? We vragen dat wel, dan krijg je een 'ja'. Dan vraag je om een DPIA en dat krijg je dan niet, of ze willen er niet aan meewerken, of dat kost ze te veel tijd, wie gaat dat betalen?" (IBP-functionaris, HO3)*

Een so-bestuur (SO1) gaf aan zich te kunnen voorstellen dat bepaalde vraagstellingen invloed hebben op het verdienmodel van ICT-leveranciers. Hier lijkt het commerciële belang van ICT-leveranciers te schuren met het maatschappelijke belang van de onderwijsbesturen, dit wordt ook door SURF opgemerkt (Van Elk, 2024).

Een ander zorgpunt van de geïnterviewde besturen is dat die afhankelijkheid maakt dat een kwetsbaarheid van een ICT-leverancier nadelige gevolgen kan hebben voor onderwijsinstellingen die daarmee samenwerken. Een so-bestuurslid:

> *"[A]ls er een grootschalige hack plaatsvindt bij de leverancier van dat leerlingvolgsysteem. En waardoor alle gegevens van al onze leerlingen en ook die van 200 andere koepels op straat komen te liggen. Of zij weigeren losgeld te betalen, waardoor die gegevens ergens op het dark web verkocht kunnen worden. Ja, dan hebben we toch wel een probleem." (Externe IBP-functionaris, SO4)*

Een dergelijk risico wordt ook aangekaart door het NCSC (z.d.-c). Dat zoiets geen onwaarschijnlijk scenario is, blijkt wel uit de 2 DDoS-aanvallen die SURF in januari 2025 te verduren kreeg, waardoor diverse onderwijsinstellingen, met name in het hoger onderwijs, geen of een trage verbinding hadden (Meijer, 2025).

3.3.2 Inhuurkrachten

Meerdere besturen gaven bij de interviews aan dat zij gebruik maken van inhuurkrachten op het gebied van IBP, vanwege een tekort aan capaciteit en/of expertise. Die inhuur wordt geleverd door partners, zoals adviesbureaus en ICT-leveranciers. Daarnaast bieden publieke ondersteuningsorganisaties als SURF en SIVON expertondersteuning vanuit gezamenlijke initiatieven. (CISO-as-a-Service; Auditdienst Rijk, 2024). Wat inhuur betreft werden verschillende perspectieven zichtbaar gedurende de interviews: sommige besturen willen zoveel mogelijk IBP-professionals in dienst hebben terwijl andere besturen deze professionals inhuren omdat zij de expertise niet (voldoende) in huis hebben, bijvoorbeeld vanwege hun kleine omvang. Enkele besturen gaven aan dat zij IBP- (en ICT-) professionals liever zoveel mogelijk inhuren omdat deze hun expertise makkelijker kunnen bijhouden. Zij beschikken dus over meer up-to-date kennis dan soortgelijke professionals bij onderwijsinstellingen. Een mbo-bestuur stelde:

> *"Want uiteindelijk, als je het omslaat en je rekent het terug, is dat goedkoper dan om eigen mensen in dienst te nemen. [J]e krijgt die specialiteiten nooit zo opgeleid. Als ik zie bij collegascholen die een paar slagen groter zijn, hoe lang implementatieprocedure? Hoe moeizaam het allemaal loopt. [...] [D]an ben ik blij hoe wij hebben geregeld." (Bestuurslid, MBO1)*

Terwijl VO1 een medewerker een IBP-rol gaf omdat inhuur financieel niet haalbaar was. Het inhuren of in dienst nemen van IBP-professionals kan een lastige opgave zijn, aldus een aantal geïnterviewde besturen. Voor kleine(re) besturen of andere besturen met minder financiële middelen – denk aan verminderende leerlingaantallen in het speciaal onderwijs – was dit onhaalbaar of betekende het een constante (financiële) afweging tussen "het primaire proces" en IBP en/of ICT. Volgens sommige van de geïnterviewde besturen hielp het om kritischer te zijn op hun ICT-uitgaven, zoals de hoeveelheid licenties. Andere besturen gaven aan dat ze daarvoor moesten kijken naar bezuinigingen op andere plekken, zoals ondersteunend personeel.

Een ander probleem dat besturen noemden is de krappe arbeidsmarkt van IBP- (en ICT-) professionals, waardoor zij duur zijn. Deze professionals kunnen meer verdienen dan het salaris dat zij in dienst bij een onderwijsinstelling zullen krijgen, vertelden enkele besturen. De geïnterviewde besturen die wel succesvol waren in het aantrekken van dit soort professionals – in dit geval uitsluitend ho-instellingen – verklaarden dat dit vooral lag aan de keuze die professionals zelf maakten. Dat wil zeggen: door secundaire arbeidsvoorwaarden (onder andere meer vakantiedagen) of het maatschappelijke belang of profiel van hun werkgever boven het salaris te stellen. HO6 refereerde aan een collega die de bewuste keuze maakte om bij hun bestuur te werken omdat dit "duurzaam" en "groen" was.

3.3.3 Kennisdeling

Een paar van de geïnterviewde besturen bevestigden dat zij expertise van of via publieke organisaties verkrijgen, zoals van ondersteuningsorganisaties als Kennisnet, SIVON en SURF, en via de koepels PO-, VO- en MBO Raad. Die expertise bevat onder meer informatie over informatiebeveiliging en privacy in een onderwijscontext en de daarvoor opgestelde normenkaders. Het delen van die informatie gebeurt via mailings, publicaties, webinars, netwerken, bijeenkomsten, sessies, platforms (bijv. MBO Digitaal) en programma's (bijv. Digitaal Veilig Onderwijs). De normenkaders worden gewaardeerd: PO4 beschreef het als "een hele prettige maar enorm lange to-do-list, die voorheen ontbrak". Al zijn die normenkaders niet voor alle besturen even duidelijk of makkelijk toepasbaar binnen hun context. Uit de interviews blijkt dat het normenkader voor funderend onderwijs complex kan zijn voor met name de kleine(re) besturen, waardoor daar behoefte is aan een laagdrempeliger normenkader. Zo stelt een so-bestuur: "Ik denk dat het soms simpeler opgeschreven kan worden. Je bent al veel tijd kwijt aan het lezen: wat bedoelen ze nu?" (Docent met IBP-rol, SO4)

Daarnaast deden de kleinere besturen de suggestie voor versies die beter aansluiten bij de context van kleine besturen en éénpitters, waarbij zaken die alleen van toepassing zijn op grote(re) besturen worden weggelaten. Zoals een so-bestuur aangaf:

> *"Dat betekent dat heel veel van die dingen niet verklaart, niet van toepassing. Het is zonde om daar tijd in te steken, om daar een stuk papier voor te maken, überhaupt al. Laat staan om dat in een cyclus op te nemen die, waar je elk jaar op verantwoordt. [...] In die zin is het niet toegespitst op dit formaat organisatie, in ieder geval. [...] En al je data staat bij leveranciers. En dat zijn maar een paar leveranciers. Die zou je goed willen controleren. Daar zijn wij te klein voor, als [so4], om dat goed te kunnen doen, qua budget, expertise en logica." (IBP-functionaris, SO4)*

Een soortgelijke behoefte werd genoemd door 2 besturen van speciaal onderwijs; zij wilden graag een versie hebben die meer is toegespitst op het speciaal onderwijs. Eén van hen gaf aan dat de sjablonen van Kennisnet niet altijd toereikend zijn en dat er behoefte is aan meer maatwerk. Een ander verbeterpunt dat tijdens de interviews ter sprake kwam is de overdaad aan informatie(bronnen) die sommige besturen ondervinden, met name in het funderend onderwijs en bij een bestuur uit het vervolgonderwijs. Dit kan overweldigend zijn voor de medewerkers van de besturen en bijdragen aan de (werk)druk die wordt ervaren rondom IBP. Waar dit aan ligt verschilt per bestuur, maar uit de interviews lijkt het te maken te hebben met een tekort aan capaciteit, bijvoorbeeld door een klein(er) IBP-team of slechts één persoon die zich bezighoudt met IBP. Zo vertelde een klein so-bestuur (SO4) dat de vernieuwde versie van het normenkader ertoe leidde dat ze eerst moesten controleren wat er precies veranderd was en in hoeverre hun school aan de nieuwe versie voldeed.

Een andere door besturen veelgenoemde kennisbron vormen de netwerken die gefaciliteerd worden via de publieke ondersteuningsorganisaties, waarin besturen onderling kennis, ervaringen en formats kunnen uitwisselen. Hoewel via allerlei initiatieven wordt geprobeerd om de besturen in hun sector van kennis en ervaringen te voorzien, kwam uit de interviews naar voren dat niet alle besturen even goed worden bereikt. In alle sectoren ervaren sommige besturen minder aansluiting bij de netwerken of maken zij minder gebruik van de beschikbare informatie, omdat hun specifieke bestuurscontext daarin onvoldoende wordt gerepresenteerd. Een klein ho-bestuur lichtte bijvoorbeeld toe:

> *"Je zit op een hele andere schaal te werken ook, en... [...] waardoor je niet altijd helemaal aansluit bij de overige situatie. [...] Dus daar zijn we ook vaak afgehaakt, want daar misten we gewoon heel veel dingen of aan feeling met de rest. [A]ls ik dan praat met collega's van andere hoger onderwijsinstellingen, dan praat je op een heel ander niveau [...] dan zou het voor ons fijn zijn als dat, als daar meer, inderdaad, in voorzien zou worden. Maar ik begrijp het, besef tegelijkertijd ook dat dat misschien heel lastig uitvoerbaar is, omdat we misschien een beetje in een unieke positie zitten wat dat betreft. Omdat je een hele kleine organisatie bent [..] met een kleine groep studenten. [...] Die oplossingen die aangedragen worden om dingen te doen of om... Dan zit je bij zo'n SURF-conferentie en dan hoor je dat de, een CISO heeft een dreigingsbeeld gemaakt voor z'n bestuur. Ja, heel waardevol, maar daar heb ik geen tijd voor." (IBP-functionaris, HO1)*

Een andere reden waarom besturen niet of beperkt deelnemen aan netwerken is dat zij hiervoor onvoldoende capaciteit hebben. Zowel beperkte aansluiting als beperkte capaciteit om deel te nemen spelen voornamelijk bij kleine besturen in zowel het funderend als het vervolgonderwijs.

3.3.4 Verantwoordelijkheid en governance

Binnen dit ecosysteem ligt de verantwoordelijkheid voor digitale weerbaarheid bij de onderwijsbesturen (Inspectie van het Onderwijs, 2021), al vervult de overheid een regisserende rol via het zorgen voor normen, het maken van afspraken, het bepalen van wettelijke kaders en beleid, het verstrekken van subsidie e.d. (Becking, 2025; Bruins, 2025; Rijksoverheid, z.d.). Echter, in de interviews komt naar voren dat de regulering op een bepaald aspect tekortschiet: diverse besturen worstelen met de complexiteit rondom de verantwoordelijkheid en governance vanwege de afhankelijkheid van ICT-leveranciers. Hillman (2022) constateerde al dat in het onderwijs de verantwoordelijkheid voor digitale weerbaarheid wordt verschoven van de leveranciers naar de eindgebruikers: scholen, leerkrachten, docenten, leerlingen en studenten. In hoeverre zijn besturen verantwoordelijk voor het doen en laten van leveranciers? Meerdere geïnterviewde besturen maken zich zorgen hierover, omdat ze de regie kunnen verliezen over de informatiebeveiliging. SURF (2023) herkent dit probleem en stelt dat het lastig is om de kwaliteit van de informatiebeveiliging van leveranciers te bepalen. Het controleren van ICT-leveranciers en het opstellen van goede overeenkomsten of contracten met hen vereist tijd, capaciteit en expertise, wat onderwijsbesturen niet altijd hebben. Deze ervaring werd door besturen van alle sectoren besproken. Zo stelde een IBP-functionaris van HO3 dat zij als individuele instelling niet de technologische kennis hebben om zo diep te gaan, en: "als je 275 pagina's probeert vol te kladden, dan ben je weken c.q. maanden bezig." Waarop een bestuurslid aanvulde: "En dat is maar één applicatie." Een po-bestuur zei hierover:

> *"Maar hoe mooi zou het zijn als daar dan ook controles op komen? En dat ik ervan uit kan gaan, dat als een bedrijf A zegt, ook A doet. En niet dat ik elke keer maar weer, 4 keer per jaar moet vragen: doe je dat inderdaad nog zo? Mag ik die logs nog eens zien? [...] [ICT-leverancier] is ook zo'n organisatie waar je, als je vragen gaat stellen, je krijgt gewoon geen antwoord. Elke vraag die ik stel levert mij weer 5 vragen extra op die ik moet beantwoorden, in plaats van dat ik antwoord krijg op de vragen die ik stel." (IBP-functionaris, PO5)*

Het is tijdrovend en niet altijd even effectief om dit per bestuur of sector op te pakken. Om die reden hopen besturen dat de overheid en/of publieke ondersteuningsorganisaties dit geheel of grotendeels uit handen kunnen nemen. Mogelijkerwijs door de ICT-leveranciers te controleren en een keurmerk of certificering toe te kennen, zodat besturen weten welke leveranciers aan de eisen voldoen. Een vo-bestuur verklaarde:

> *"[...] het normenkader en een verwerkersovereenkomst legt in feite bij ons als scholen eigenlijk verantwoordelijkheden neer van controle op leveranciers die wij als schoolbestuur niet kunnen en misschien ook wel niet willen uitoefenen. En dan denk ik: daar zou je als sector gezamenlijk moeten optrekken. En ik zie dat waar we dat proberen als sector, dat dan een markt tegenwerking geeft. Uitgevers, distributeurs, die zetten de hakken in het zand." (IBP-functionaris, VO3)*

Een mbo-bestuur ziet in het gezamenlijk optrekken de potentie om makkelijker druk uit te oefenen wanneer dat nodig is: "*je kan wel [als ICT-leverancier] willen leveren, maar dit is voor ons cruciaal, dus zorg dat je dat op orde hebt.*" (Leidinggevende IBP, MBO3). Wat hieraan kan bijdragen is de Cyber Resilience Act[8], oftewel de CRA. Deze Europese verordening is sinds december 2024 van kracht en omvat vereisten waaraan bepaalde ICT-middelen moeten voldoen (Penman et al., 2026). Overtredingen kunnen potentieel leiden tot een terugroeping, verbod of boete (Teichmann & Sergi, 2025). Teichmann en Sergi (2025) zien de CRA en NIS2 als complementair: de NIS2 vereist het treffen van beheersmaatregelen om risico's te verminderen. Omdat die organisaties helpen om kwetsbaarheden te verminderen, zal een vraag ontstaan naar CRA-conforme producten. De bijbehorende kanttekening van de CRA is dat niet alle ICT-middelen eronder vallen, waaronder pure SaaS (Penman et al., 2026) en dat het geen veiligheidsgarantie is (Teichmann & Sergi, 2025). Desondanks zal het gebruik van veiligere ICT-middelen (en ICT-leveranciers) het voor besturen makkelijker maken om digitaal weerbaar te worden.

8 Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cybersecurity-eisen voor producten met digitale elementen (Cyber Resilience Act), PbEU 2024, L 2847.

3.4 Samenwerkingen

Omdat partijen in het ecosysteem van elkaar afhankelijk zijn, is een goede samenwerking noodzakelijk. Niet alleen met intern, maar ook met andere partijen. Vanuit de literatuur over digitale weerbaarheid als publiek goed (Taddeo, 2019) is deze onderlinge afhankelijkheid te duiden als een klassiek collectieve-actieprobleem: individuele besturen dragen kosten, terwijl de baten van verhoogde weerbaarheid grotendeels sectorbreed neerslaan. De noodzaak van meer samenwerking – zowel tussen besturen als tussen de publieke ondersteuningsorganisaties Kennisnet, SIVON en SURF – kwam bij meerdere besturen ter sprake. Dit sluit aan bij Olson (1965), die stelt dat zonder institutionele structuren en organisatiegraad grote, gefragmenteerde groepen moeite hebben om tot voldoende collectieve investeringen te komen. Een po-bestuurder illustreerde hoe een bestaande samenwerking tussen besturen ingezet kan worden voor IBP:

> *"[O]p een gegeven moment door met doorontwikkelen, en die coöperatie bestaat al best heel lang, ga je ook nadenken over: hoe kun je nog meer dienstverlening bundelen waardoor het goed is voor deze [...] schoolbesturen om daar gebruik van te maken? [...] [W]ij zijn [...] de grotere club in deze coöperatie [...]. Dus daarom faciliteren we toch intern onze eigen privacycoördinator. Omdat wij gewoon simpelweg wel geloven in dat je dan nog sneller kan handelen [...] op vraagstukken die d'r zijn. Zo simpel is het natuurlijk ook. Alleen, die andere schoolbesturen kunnen dat niet, omdat ze daar de middelen niet voor kunnen vrijmaken." (Bestuurslid, PO4)*

Deze passage illustreert het free-rider mechanisme (Olson, 1965): kleinere besturen profiteren van collectieve voorzieningen, maar hebben zelf minder capaciteit om individueel te investeren, wat zonder coördinatie kan leiden tot onderinvestering op sectorniveau. Naast het benutten van een samenwerking die al voorhanden is, biedt dit tegelijkertijd de mogelijkheid om medebesturen met te weinig capaciteit of middelen te ondersteunen.

Hoewel beide soorten samenwerkingen al plaatsvinden, blijkt de behoefte nog steeds te bestaan volgens de interviews. Mogelijk voldoen de huidige samenwerkingen niet aan de behoeftes van bepaalde besturen. Dit kan worden geïnterpreteerd als een tekortschietende organisatiegraad: bestaande structuren zijn nog niet voldoende om het collectieve-actieprobleem rond digitale weerbaarheid structureel te doorbreken. Het bevorderen van bovensectorale samenwerking tussen besturen kan specifieke behoeftes van kleine besturen uit alle sectoren vervullen, zoals een soortgelijke sparringpartner, of van besturen in het funderend onderwijs die op het gebied van IBP toe zijn aan een vervolgstap. Een kleine ho-instelling gaf bijvoorbeeld aan:

> *"Je mist soms misschien een sparringpartner in iemand die denkt van: hoe los je dit op zonder dat je... [...] Die de context begrijpt. [...] Ik ben één keer geweest bij een privacysessie van SURF en dat was voor kleine instellingen. [...] als je dan praat over kleine instellingen, zat er ook een Mbo met 50.000 studenten bij. [...] Voor hun klein, voor ons niet. [...] Dat was één van de weinige keren dat ik ook echt specifiek die aandacht heb gezien voor die kleine instellingen." (IBP-functionaris, HO1)*

Deze situatie laat zien dat kleine partijen in diverse groepen vaak in het gedrang komen, waardoor besluiten minder effectief zijn (Olson, 1965). Publieke ondersteuningsorganisaties kunnen samenwerking bevorderen door sectorale signalen en besturen te verbinden.

Daarnaast kan de samenwerking van publieke ondersteuningsorganisaties helpen tijdens onderhandelingen met en controle van ICT-leveranciers. Een ho-bestuur redeneerde al in die richting:

> *"Stel dat SURF [...] services en diensten kan aanbieden, troubleshooting kan doen namens een groep kleinere hogescholen? Dan heeft dat een neutraler karakter [...]. SURF heeft een soort equalizingvermogen, [...] en dan doen zij iets voor die hele groep. Het maakt toewerken naar inkoopcombinaties of shared services misschien makkelijker dan dat iedereen op zoek moet naar zijn eigen samenwerkingsverband." (Bestuurslid, HO3)*

Dit betekent dat sectorbrede sturing en gezamenlijke onderhandeling nodig zijn om het tekort aan regelgeving op te vangen. Dit tekort ontstaat wanneer afzonderlijke organisaties niet groot of machtig genoeg zijn om leveranciers tot voldoende beveiliging te dwingen. Wellicht kan dit breder worden getrokken, waarbij alle publieke ondersteuningsorganisaties (SURF, SIVON en Kennisnet) de krachten bundelen. Zij kunnen dan namens alle sectoren als één collectief het reguleringshiaat opvullen door onderhandelingen en controles op zich te nemen, en zo de maatschappelijke belangen van de onderwijssector te behartigen tegenover de ICT-leveranciers waarvan scholen afhankelijk zijn. Een dergelijke constructie vergroot de organisatiegraad van de sector en kan het coördinatieprobleem helpen verkleinen door centrale regie te combineren met decentrale uitvoering.

Hoewel meer samenwerking volop kansen biedt, werd uit de interviews duidelijk dat ook dit risico's en belemmeringen met zich meebrengt. SURF (2024) ziet het risico dat meer samenwerking, bijvoorbeeld tussen onderwijsinstellingen, voor meer afhankelijkheid zorgt, ook wat betreft de digitale weerbaarheid. Dit raakt aan de spanning tussen collectieve efficiëntie en systeemrisico: gezamenlijke infrastructuren reduceren individuele kosten maar vergroten bij falen de potentiële impact op het gehele collectief; een kenmerkend dilemma bij publieke goederen. Daarnaast zijn er nog andere belemmeringen, waaronder de weerstand tegen een gedeelde verantwoordelijkheid. Zoals enkele mbo-besturen het duidden:

> *"Ik ga niet met jou solidair zijn als je denkt: nou ja, weet je, pff I don't care". (Bestuurslid, MBO3). En: "ik ga niet verantwoordelijk zijn voor een kleine instelling, die misschien te klein is om helemaal op orde te houden. [...] dan wordt je buitengrens [..] alleen maar groter met ook kwetsbare partners." (Bestuurslid, MBO2).*

Deze uitspraken illustreren het free-riderprobleem en het gebrek aan wederzijds vertrouwen dat collectieve-actieprocessen kan ondermijnen wanneer niet alle partijen bereid zijn proportioneel bij te dragen. Andere risico's waarmee rekening gehouden moet worden, gebaseerd op de interviews met besturen, zijn dat bepaalde partijen andere gaan overstemmen, en/of dat de groep niet openstaat voor andere input en daardoor een tunnelvisie krijgt. Voor de effectiviteit van samenwerkingen zijn besturen zelf ook aan zet: voor een zinvolle samenwerking is actieve deelname essentieel. Alleen met actieve deelname en een breed draagvlak kan de sector zich organiseren om digitale weerbaarheid als publiek belang gezamenlijk en structureel te versterken.

4. Conclusies

De uitkomsten van dit onderzoek maken duidelijk dat digitale weerbaarheid meer dan techniek is, namelijk een bestuurlijke verantwoordelijkheid. Zicht, sturing en verschillen tussen besturen hangen samen met de keuzes die besturen maken en de manier waarop digitale veiligheid is georganiseerd. Hieronder beantwoorden we de deelvragen één voor één.

4.1 In hoeverre hebben besturen zicht op digitale weerbaarheid?

In het funderend onderwijs weten veel besturen welke maatregelen er zijn om digitale risico's te beperken. Denk aan incidentmanagement, bewustwordingscampagnes en toegangsbeheer. Wat zij minder goed in beeld hebben, zijn de basisvoorwaarden om digitale weerbaarheid echt stevig neer te zetten, wat aansluit bij het beeld uit het rapport 'IBP in beeld' van het programma Digitaal Veilig Onderwijs (2026), waarin wordt vastgesteld dat besturen gemiddeld nog op een laag volwassenheidsniveau opereren. Voorbeelden van basisvoorwaarden zijn het classificeren van systemen, het werken met een duidelijke meerjarenplanning (roadmap) en het structureel opnemen van digitale veiligheid in de planning- en controlcyclus. Een deel van de besturen is zelfs niet bekend met belangrijke onderdelen van digitale weerbaarheid. Het beeld ontstaat dat veel besturen weliswaar weten wat ze moeten doen bij incidenten, maar minder overzicht hebben over de langere termijn en de samenhang tussen maatregelen.

In het vervolgonderwijs is digitale weerbaarheid vaker formeel georganiseerd, bijvoorbeeld rond een CISO met vaste crisis- en auditprocessen. Toch wordt ook hier risicogestuurd werken nog niet overal volledig benut. Dreigingsinformatie wordt niet altijd systematisch vertaald naar bestuurlijke keuzes.

Kortom, in alle sectoren werken besturen aan hun zicht op digitale weerbaarheid, maar dat zicht is vaak praktisch en procedureel. Het is nog niet overal stevig verankerd in de bestuurlijke cyclus van doelen stellen, monitoren en bijsturen. Dat vraagt om meer actieve betrokkenheid van besturen zelf. Digitale weerbaarheid kan niet uitsluitend worden overgelaten aan specialisten; het vraagt om bestuurlijke regie.

4.2 Hoe geven besturen sturing aan digitale weerbaarheid om onderwijscontinuïteit te garanderen?

In het funderend onderwijs verschilt de organisatie van digitale weerbaarheid sterk per bestuur: soms is dit intern belegd, soms uitbesteed, vaak verdeeld over bestuurs- en schoolniveau. Bestuurders en IBP-functionarissen zitten redelijk op één lijn als het gaat om beleid en rolverdeling. Maar op strategisch niveau (prioriteiten stellen, risico's wegen) en op operationeel niveau (weten wat te doen bij een crisis) lopen de beelden vaker uiteen. Met name continuïteitsmanagement en crisisvoorbereiding zijn nog niet overal structureel geregeld. Veel besturen hebben maatregelen tegen incidenten, maar zijn minder goed voorbereid op langdurige uitval van systemen of grootschalige verstoringen. Juist daar ligt het risico voor onderwijscontinuïteit.

In het vervolgonderwijs is de aansturing formeler georganiseerd, met een duidelijke rol voor de CISO en meer vaste overleg- en verantwoordingsstructuren. Dat geeft een stevige basis. Tegelijkertijd blijft het ook daar een uitdaging om digitale risico's expliciet te verbinden aan strategische keuzes en prioriteiten.

We kunnen concluderen dat in alle sectoren wordt gewerkt aan digitale weerbaarheid, maar vooral in het funderend onderwijs moet continuïteitsdenken steviger worden ingebed. Dat vereist dat besturen niet alleen beleid vaststellen, maar ook actief sturen, doorvragen en scenario's bespreken. Onderwijscontinuïteit is uiteindelijk een bestuurlijke verantwoordelijkheid.

4.3 Hoe verschillen besturen in het waarborgen van digitale weerbaarheid met betrekking tot onderwijscontinuïteit?

In het funderend onderwijs hangen verschillen tussen besturen vooral samen met structurele factoren. Grotere besturen en besturen die actief deelnemen aan netwerken (zoals via Kennisnet en SIVON) hebben meer inzicht, meer expertise en meer capaciteit. Organisatiegraad en interne professionalisering maken hier aantoonbaar verschil. Ook bestuurders met eerdere bestuurlijke ervaring op het gebied van digitale weerbaarheid tonen meer inzicht en expertise. Kleinere besturen zonder deze randvoorwaarden zijn relatief kwetsbaar in het borgen van onderwijscontinuïteit. Voor deze groep lijkt versterking van de organisatiegraad een logische oplossingsrichting, al wordt dit bemoeilijkt door beperkte schaalgrootte en een minder goede aansluiting op relevante (kennis)netwerken.

Ook in het vervolgonderwijs speelt bestuursgrootte een rol, met name bij de waarborgen voor digitale weerbaarheid en de mate van bewustwording. In tegenstelling tot het funderend onderwijs is de invloed van organisatiegraad hier beperkter. Verschillen hangen in deze sector sterker samen met individuele factoren, zoals de persoonlijke affiniteit van bestuurders met digitale weerbaarheid en het comfort dat zij ervaren in hun verantwoordelijkheid.

Het verschil tussen funderend en vervolgonderwijs lijkt samen te hangen met de mate waarin digitale weerbaarheid organisatorisch is verankerd. In het funderend onderwijs zijn schaalgrootte en netwerkdeelname sterk bepalend voor het niveau van inzicht, expertise en capaciteit. Dat wijst erop dat digitale weerbaarheid daar in belangrijke mate afhankelijk is van beschikbare structuren en externe ondersteuning. In het vervolgonderwijs daarentegen is digitale weerbaarheid, met name bij grotere besturen, vaker formeel georganiseerd, bijvoorbeeld via CISO-structuren en vaste governanceprocessen. Kortom, hoewel schaalgrootte in beide sectoren een belangrijke randvoorwaarde vormt, is digitale weerbaarheid in het funderend onderwijs vooral afhankelijk van organisatiegraad en collectieve structuren. In het vervolgonderwijs speelt dit een minder grote rol.

4.4 Welke factoren helpen besturen in het waarborgen van digitale weerbaarheid?

Digitale weerbaarheid is een veelzijdige opgave waarin voldoende capaciteit, expertise en bewustwording de randvoorwaarden vormen. Het onderwijsbestuur vervult een sleutelrol hierin. Tegelijkertijd opereren besturen niet in isolatie: ze maken deel uit van het bredere ecosysteem en zijn voor hun digitale veiligheid medeafhankelijk van externe partijen, waaronder commerciële IT-partners, publieke organisaties en het ministerie van OCW

Ten eerste vereist de veelzijdigheid van informatiebeveiliging en privacy (IBP) een integrale aanpak die recht doet aan de multidimensionale aard ervan. Bij deze aanpak worden besturen in de eerste plaats geholpen door een integrale visie op veiligheid. Daarin is de digitale weerbaarheid expliciet verbonden met de bredere veiligheidsaanpak en met de continuïteit van het primaire proces. Wanneer digitale veiligheid niet wordt gezien als een technisch dossier, maar als een bestuurlijk vraagstuk, maakt dit de strategische inbedding van IBP binnen de gehele onderwijsorganisatie mogelijk. Ook helpt een duidelijke organisatorische inrichting met centrale regie. Een IBP-functionaris die of een IBP-team dat coördinerend optreedt en multidisciplinair samenwerkt met bijvoorbeeld HR, ICT en juridische zaken, voorkomt versnippering. Belangrijk hierbij is dat het werk van IBP niet op de schouders van één persoon of team rust, maar als gezamenlijke verantwoordelijkheid door de organisatie wordt gedragen.

Ten tweede is een sterke veiligheidscultuur van grote waarde. Wanneer IBP wordt ervaren als gedeelde verantwoordelijkheid, wanneer fouten bespreekbaar zijn en incidenten laagdrempelig worden gemeld, neemt het lerend vermogen toe. Trainingen en bewustwordingsinitiatieven werken vooral effectief wanneer zij zijn ingebed in zo'n cultuur en geen losse verplichting zijn.

Een derde cruciale factor is actieve en zichtbare bestuurlijke betrokkenheid. Besturen bepalen prioriteiten, middelen en personele inzet. Waar bestuurders voldoende kennis hebben van risico's, wetgeving en incidentrespons, of op zijn minst bereid zijn zich daarin te verdiepen, worden gerichtere keuzes gemaakt. Daarbovenop speelt zichtbaar leiderschap een noodzakelijke rol in het vormen en uitdragen van een veiligheidscultuur. Dit draagt bij aan draagvlak in de organisatie en versterkt de positie van IBP-functionarissen.

Tot slot bieden sectorale samenwerking en kennisdeling belangrijke steun. Netwerken en ondersteuningsorganisaties helpen besturen bij het delen van expertise, het gezamenlijk aanpakken van ketenrisico's en het versterken van hun positie ten opzichte van leveranciers. ICT-leveranciers beschikken over specialistische kennis en kunnen bijdragen aan een hoger beveiligingsniveau dan individuele instellingen ooit zelfstandig zouden kunnen realiseren. Uiteindelijk is het belangrijk dat de gehele keten verantwoordelijkheid neemt voor digitale veiligheid.

4.5 Welke factoren belemmeren besturen in het waarborgen van digitale weerbaarheid?

Tegelijkertijd signaleren we meerdere belemmerende factoren waaraan een tekort aan capaciteit, expertise en/of bewustwording ten grondslag ligt.

Ten eerste zien wij dat prioritering van digitale weerbaarheid soms sterk afhankelijk is van de persoonlijke affiniteit of expertise van individuele bestuurders. Wanneer bestuurlijke kennis of betrokkenheid ontbreekt, kan het onderwerp onvoldoende aandacht krijgen en blijft de borging kwetsbaar.

Daarnaast vormen beperkte capaciteit en een krappe arbeidsmarkt een structurele belemmering, met name voor kleinere besturen. Besturen staan voor de financiële uitdaging om digitale weerbaarheid te waarborgen, zonder dat de bijbehorende afwegingen ten koste gaan van de kwaliteit van het onderwijs. Ook het aantrekken of behouden van gespecialiseerde IBP-professionals is kostbaar en complex. Dit kan leiden tot tijdelijke of ad-hoc invulling van taken, wat de effectiviteit ondermijnt. Uit de verkennende analyse blijkt dat kleine besturen vaak over minder bewustwording, expertise, capaciteit en toegang tot netwerken beschikken, waardoor zij kwetsbaarder zijn in het waarborgen van onderwijscontinuïteit. Tegelijkertijd vraagt digitale weerbaarheid juist in deze context om actieve bestuurlijke regie. Hoewel beperkte capaciteit het invullen van die regierol complexer maakt, is deze wel noodzakelijk om prioriteiten te stellen en continuïteit te borgen.

De complexiteit van het digitale ecosysteem vormt eveneens een uitdaging. Binnen dit ecosysteem zijn meerdere partijen betrokken met verschillende belangen die kunnen schuren. Vanuit de literatuur over collectieve actie kan digitale weerbaarheid hierbij worden opgevat als een publiek goed: de baten van investeringen werken ketenbreed door, terwijl de kosten primair individueel worden gedragen.

Goede samenwerking is essentieel om het collectieve-actieprobleem te doorbreken, maar kent ook obstakels. Niet alle besturen staan positief tegenover gedeelde verantwoordelijkheid; wanneer verwacht wordt dat anderen investeren of het voortouw nemen, kan de prikkel om zelf actief bij te dragen afnemen. Bovendien zien we dat er spanning bestaat tussen autonomie en veiligheid: scholen en faculteitsinstellingen willen hun zelfstandigheid behouden, terwijl digitale veiligheid vraagt om een zekere mate van centrale coördinatie. Tegelijkertijd brengt nauwere samenwerking het risico met zich mee dat cyberincidenten zich sneller door de keten verspreiden. De voordelen van gezamenlijke efficiëntie gaan daarmee gepaard met een groter systeemrisico.

Daarnaast vraagt samenwerking om aandacht voor inclusiviteit en evenwichtige besluitvorming. Het is van belang tunnelvisie en machtsconcentratie te voorkomen en te waarborgen dat ook kleine besturen kunnen deelnemen, ondanks hun beperkingen in tijd, middelen of capaciteit. Wanneer zij minder profiteren van gezamenlijke initiatieven, blijft het beschermingsniveau binnen de sector immers ongelijk, wat uiteindelijk de digitale weerbaarheid van het gehele ecosysteem kan ondermijnen.

Voor ICT-middelen, zoals officepakketten en leermiddelen, zijn onderwijsinstellingen in alle sectoren afhankelijk van (inter)nationale ICT-leveranciers. Deze afhankelijkheid wordt in meerdere interviews als risico aangeduid. Hoewel leveranciers kunnen bijdragen aan professionalisering en beveiliging, ervaren besturen dat die afhankelijkheid hun regie beperkt. Leveranciersafhankelijkheid, ketenrisico's en beperkt zicht op beveiligingskwaliteit maken het lastig om grip te houden op digitale weerbaarheid. Dit raakt direct aan de eerder gesignaleerde noodzaak om bestuurlijke regie op digitale continuïteit te versterken. Juist op een domein waar de afhankelijkheid groot is, wordt zichtbaar hoe complex het is om die regierol in de praktijk waar te maken. Hier ontstaat een spanningsveld tussen de ervaren beperkte handelingsruimte en de opgave om als bestuur nadrukkelijker te sturen op digitale weerbaarheid. Er is daarom een duidelijke behoefte om de krachten te bundelen binnen het hele onderwijsveld, inclusief overheid en publieke ondersteuningsorganisaties,. Door gezamenlijk op te trekken in de onderhandeling met en controle op ICT-leveranciers kunnen de maatschappelijke belangen van de sector beter worden geborgd en wordt het voor besturen eenvoudiger om digitaal weerbaar te worden. Dit sluit aan bij De Moor et al. (2025b), die pleiten voor een meer gecoördineerde en sectorbrede strategie om de afhankelijkheid van grote ICT-leveranciers te verkleinen en publieke waarden beter te borgen.

Verder ervaren sommige besturen overbelasting door complexe of versnipperde informatievoorziening. Met name in het funderend onderwijs zijn meerdere organisaties betrokken bij normstelling en ondersteuning (zoals Kennisnet, SIVON, PO-Raad en VO-raad). Dit kan leiden tot een overvloed aan informatie en uiteenlopende communicatie, wat voor kleinere besturen overweldigend kan zijn. Uit de interviews blijkt bovendien dat het normenkader in het funderend onderwijs soms als complex wordt ervaren, vooral door kleine besturen en éénpitters. Zij geven aan behoefte te hebben aan laagdrempeligere versies die beter zijn toegespitst op hun schaal en context, bijvoorbeeld voor kleine besturen of het speciaal onderwijs. Meer maatwerk in normering en communicatie kan helpen om de toepasbaarheid te vergroten.

4.6 Structurele aanpak en samenwerking nodig voor digitale weerbaarheid

De bevindingen laten zien dat besturen bezig zijn met het verbeteren van de digitale weerbaarheid en daar erg verschillend mee omgaan. Veel besturen hebben operationele maatregelen getroffen en sturen op onderdelen van informatiebeveiliging maar hebben digitale weerbaarheid nog niet echt structureel ingebed in hun beleid en besluitvorming. Hierdoor ontstaat een wisselend niveau van weerbaarheid binnen het bredere onderwijsveld.

Een terugkerend thema is ook dat de verantwoordelijkheid voor digitale weerbaarheid in de praktijk diffuus is. Binnen organisaties is deze niet altijd helder belegd of breed gedragen, terwijl instellingen tegelijkertijd opereren in een ecosysteem waarin zij afhankelijk zijn van andere partijen. Dit maakt het voor besturen complex om regie te voeren en verantwoordelijkheid daadwerkelijk waar te maken.

Besturen die digitale weerbaarheid echt integraal aanpakken, die daar zichtbaar leiderschap in tonen en die investeren in expertise, capaciteit en samenwerking, zijn beter in staat om onderwijscontinuïteit te waarborgen. Zij dragen ook actief bij aan kennisdeling en gezamenlijke versterking binnen de sector. Waar deze voorwaarden ontbreken, blijft hun bijdrage beperkt en blijft de continuïteit kwetsbaar bij digitale verstoringen. Verschillen in prioriteit, capaciteit en organisatie leiden zo tot uiteenlopende beschermingsniveaus binnen de sector.

Daarmee luidt het antwoord op de hoofdvraag dat besturen wel degelijk werken aan digitale weerbaarheid, maar dat duurzame garantie van onderwijscontinuïteit vraagt om digitale weerbaarheid structureel onderdeel te maken van beleid en sturing, om samenhang tussen maatregelen te creëren én om de coördinatie en samenwerking binnen de sector te versterken.

5. Kansen en risico's voor versterking van digitale weerbaarheid

De bevindingen laten zien dat digitale weerbaarheid in het onderwijs versterkt kan worden wanneer bestuurlijke regie, expertise, cultuur en samenwerking samenkomen. Tegelijkertijd ontstaan risico's wanneer capaciteit, samenhang en betrokkenheid ontbreken. Om deze risico's en kansen te structureren, zijn de bevindingen geclusterd in 4 overkoepelende versterkingsrichtingen: bestuurlijke verankering, bestuurlijke kennis en regie, (boven-) sectorale samenwerking en keten- en leveranciersrisico's. Hieronder worden per doelgroep de belangrijkste kansen en risico's beschreven.

5.1 Bestuurlijke verankering

Digitale weerbaarheid is in veel organisaties nog sterker ontwikkeld op operationeel niveau dan op strategisch niveau. Versterking vraagt daarom om expliciete bestuurlijke borging en structurele inbedding in de bestuurscyclus.

Belangrijk voor: besturen, met ondersteuning van sectororganisaties.

Voorbeelden:
- Veranker digitale weerbaarheid in strategie, begroting en planning- en controlcyclus.
- Verbind digitale veiligheid expliciet aan onderwijscontinuïteit en risicomanagement.
- Zorg voor structurele monitoring en bespreking in bestuur en toezicht.

5.2 Bestuurlijke kennis en regie

De prioritering van digitale weerbaarheid blijkt in sommige gevallen afhankelijk van de persoonlijke affiniteit of expertise van bestuurders. Het versterken van bestuurlijke kennis en duidelijke regie kan bijdragen aan beter onderbouwde strategische keuzes. De invulling van bestuurlijke regie verschilt daarbij naar gelang de schaal en capaciteit van besturen, maar blijft in alle gevallen een noodzakelijke voorwaarde.

Belangrijk voor: besturen, ondersteund door sectororganisaties.

Voorbeelden:
- Investeer in bestuurlijke kennis over risicobereidheid, risicobeheersing, wetgeving en incidentrespons.
- Organiseer gerichte scholing of training voor bestuurders waar deze kennis ontbreekt.
- Richt digitale weerbaarheid integraal in (mens, proces, techniek) met een duidelijke centrale regie.
- Een sterke veiligheidscultuur vormt daarbij een belangrijke randvoorwaarde en vraagt zichtbaar leiderschap van bestuurders.

5.3 (Boven-)sectorale samenwerking

Onderwijsinstellingen opereren in een onderling verbonden (digitaal) ecosysteem. Samenwerking en kennisdeling kunnen helpen om expertise te bundelen en verschillen tussen besturen te verkleinen.

Belangrijk voor: sectororganisaties en ondersteuningsorganisaties, met deelname van besturen.

Voorbeelden:
- Stimuleer actieve deelname aan sectorale netwerken en kennisdeling tussen instellingen.
- Zorg dat ondersteuning en normenkaders beter aansluiten bij de schaal en context van verschillende besturen.
- Faciliteer gerichte samenwerking tussen vergelijkbare besturen.

5.4 Keten- en leveranciersrisico's

Onderwijsinstellingen zijn voor hun digitale voorzieningen sterk afhankelijk van externe ICT-leveranciers en gedeelde digitale systemen. Dit vraagt om gezamenlijke aandacht voor ketenrisico's en om sterkere regie richting leveranciers.

Belangrijk voor: OCW en sectororganisaties, samen met instellingen.

Voorbeelden:
- Bundel krachten binnen het onderwijsveld om gezamenlijk eisen te kunnen stellen aan leveranciers.
- Verken sectorbrede afspraken of toetsing van leveranciers, gekoppeld aan normenkaders.
- Stimuleer collectieve oplossingen om ketenrisico's beter te beheersen.

5.5 Een gezamenlijke bestuurlijke opgave

De belangrijkste kans ligt in het versterken van de samenhang: tussen strategie en uitvoering, tussen kleine en grote besturen en tussen individuele instellingen en het bredere digitale ecosysteem. Het grootste risico is dat digitale weerbaarheid versnipperd blijft en uiteenvalt in losse technische maatregelen, individuele inzet en afzonderlijke initiatieven, zonder dat deze structureel bestuurlijk zijn verankerd.

Digitale weerbaarheid is daarmee geen optelsom van maatregelen maar een gezamenlijke bestuurlijke verantwoordelijkheid. Alleen wanneer verantwoordelijkheden duidelijk zijn belegd, wanneer bestuurlijke regie wordt genomen en instellingen binnen het onderwijsveld samenwerken, kan de continuïteit van het onderwijs bij digitale verstoringen duurzaam worden geborgd.

Literatuurlijst

Auditdienst Rijk. (2024). *Governance normenkader informatiebeveiliging en privacy voor het funderend onderwijs*. https://open.overheid.nl/documenten/58478050-15a4-4e5c-adde-3aa403f7885f/file

Autoriteit Persoonsgegevens. (2024). *Sectorbeeld onderwijs 2021–2023*. https://www.autoriteitpersoonsgegevens.nl/uploads/2024-01/Sectorbeeld%20Onderwijs%202021-2023.pdf

Becking, K. (2025, 5 november). *Digitale veiligheid in het funderend onderwijs* [Kamerbrief]. Geraadpleegd op 25 februari 2026, van https://www.rijksoverheid.nl/documenten/kamerstukken/2025/11/05/digitale-veiligheid-in-het-funderend-onderwijs

Bruins, E. (2025, 24 april). *Kamerbrief over voortgang cyberweerbaarheid in het vervolgonderwijs* [Kamerbrief]. Geraadpleegd op 23 februari 2026, van https://www.rijksoverheid.nl/documenten/kamerstukken/2025/04/24/voortgang-cyberweerbaarheid-in-het-vervolgonderwijs

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information, 13*(4), 192.

De Moor, G., Kemman, M., Hanswijk, M., & Nederlof, N. (2022). *Nulmeting normenkader IBP FO*. Dialogic Innovatie & Interactie. https://dialogic.nl/wp-content/uploads/2024/03/Dialogic-Nulmeting-Normenkader-IBP-FO.pdf

De Moor, G., Kemman, M., Tossaint, E., Paardekooper-Lim, K., Roos, J., & ten Brummelhuis, A. (2025a). *Impactanalyse normenkader IBP FO*. https://www.digitaalveiligonderwijs.nl/app/uploads/2025/06/07_DialogicO21Serendip_ImpactanalyseNormenkaderIBPFO-.pdf

De Moor, G., Stone, S., Paardekooper-Lim, K., Urselmann, E., & Van der Vorst, T. (2025b). *Afhankelijkheid en autonomie: Big tech-dienstverlening in het funderend onderwijs. Dialogic Innovatie & Interactie*. https://dialogic.nl/wp-content/uploads/2026/02/Afhankelijkheid-en-Autonomie-Bigtech-dienstverlening-in-het-funderend-onderwijs-1.pdf

Digitaal Veilig Onderwijs. (2026). *IBP in beeld: Een verkenning van het volwassenheidsniveau van het normenkader informatiebeveiliging en privacy voor het onderwijs.* https://open.overheid.nl/documenten/7b6c157a-b597-42d0-9b0b-d4de44732b7b/file

Ferdousi, B. (2024). The importance of defining cybersecurity from a transdisciplinary approach. *Journal of Systemics, Cybernetics and Informatics, 22*(1), 150–164.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26–44.

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security, 121*, 102840.

Hamer, J., & Kool, L. (2021). *De stand van digitaal Nederland: Naar zeggenschap en vertrouwen in de digitale samenleving*. Rathenau Instituut. https://www.rathenau.nl/nl/digitale-samenleving/de-stand-van-digitaal-nederland

Hartholt, S. (2025, 13 februari). 'Er mag niets met Microsoft gebeuren, want dan hebben we een probleem'. *Binnenlands Bestuur*. Geraadpleegd op 18 februari 2026, van https://www.binnenlandsbestuur.nl/digitaal/it-personeel/er-mag-niets-met-microsoft-gebeuren-want-dan-hebben-we

Hillman, V. (2022). *The state of cybersecurity in education: Voices from the EdTech sector* (Working paper). Department of Media and Communications. https://www.lse.ac.uk/media-and-communications/assets/documents/research/working-paper-series/WP72.pdf

Hoger Onderwijs Persbureau. (2025, 17 november). Strafhof dumpt Microsoft. Kan een hogeschool of universiteit dat ook? *Erasmus Magazine*. Geraadpleegd op 18 februari 2026, van https://www.erasmusmagazine.nl/2025/11/17/strafhof-dumpt-microsoft-kan-een-hogeschool-of-universiteit-dat-ook/

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615–660.

Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 6398–6407).

Inspectie van het Onderwijs. (2021). *Binnen zonder kloppen: Digitale weerbaarheid in het hoger onderwijs*. Ministerie van Onderwijs, Cultuur en Wetenschap.

Inspectie van het Onderwijs. (2025). Digitale weerbaarheid en veiligheid in jaarverslagen: Monitor digitale weerbaarheid en veiligheid. Ministerie van Onderwijs, Cultuur en Wetenschap.

Inspectie van het Onderwijs. (2026). Digitale weerbaarheid en veiligheid in jaarverslagen. Monitor digitale weerbaarheid en veiligheid 2025. Ministerie van Onderwijs, Cultuur en Wetenschap.

Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal, 39*(8), 2255–2276. https://doi.org/10.1002/smj.2904

Kapoor, R. (2018). Ecosystems: Broadening the locus of value creation. *Journal of Organization Design, 7*, Article 12. https://doi.org/10.1186/s41469-018-0035-4

MBO Digitaal. (2024). *Eindrapportage governance van de informatieveiligheid in het mbo*. https://mbodigitaal.nl/wp-content/uploads/2024/03/Eindrapportage-governance-van-de-informatieveiligheid-in-het-mbo.pdf

Meijer, E. (2025, 16 januari). SURF en onderwijsinstellingen opnieuw getroffen door ddos-aanval. *Tweakers*. Geraadpleegd op 20 februari 2026, van https://tweakers.net/nieuws/230886/surf-en-onderwijsinstellingen-opnieuw-getroffen-door-ddos-aanval.html

Olson, M. (1965). The logic of collective action: Public goods and the theory of groups. Harvard University Press.

Nationaal Cyber Security Centrum. (z.d.-a). *Hoe stuur je op effectieve informatiebeveiliging?* Geraadpleegd op 11 maart 2026, van https://www.ncsc.nl/risicomanagement/hoe-stuur-je-op-effectieve-informatiebeveiliging

Nationaal Cyber Security Centrum. (z.d.-b). *Ontwikkel een positieve cybersecuritycultuur*. Geraadpleegd op 2 maart 2026, van https://www.ncsc.nl/mensgerichte-beveiliging/ontwikkel-een-positieve-cybersecuritycultuur

Nationaal Cyber Security Centrum. (z.d.-c). *Maak je eigen keteninventarisatie*. Geraadpleegd op 25 februari 2026, van https://www.ncsc.nl/toeleveringsketen/maak-je-eigen-keteninventarisatie

Penman, L., Wheatley, R., Nahid, S., & Burke, L. M. (2026, 16 februari). Cyber resilience act: The fine line between SaaS and digital products. *DLA Piper*. Geraadpleegd op 27 februari 2026, van https://www.dlapiper.com/en/insights/publications/2026/02/cyber-resilience-act-the-fine-line-between-saas-and-digital-products

Platform Integrale Veiligheid Hoger Onderwijs. (2021). *Toolkit implementatie IV-framework*. https://integraalveilig-ho.nl/instrument/toolkit-implementatie-iv-framework/

Platform Integrale Veiligheid Hoger Onderwijs, & KPMG. (2024). *Handreiking: De inrichting en governance van integrale veiligheid*. https://integraalveilig-ho.nl/nieuws/handreiking-governance-van-integrale-veiligheid/

PO-Raad, & VO-raad. (2024). *Handreiking sturen op digitale veiligheid* (versie december 2024). https://www.poraad.nl/system/files/inline/Handreiking_Sturen-Op-Digitale-Veiligheid%20-%20v%20dec%202024.pdf

Rijksoverheid. (z.d.). *Veilige en goede ICT in het onderwijs*. Geraadpleegd op 27 februari 2026, van https://www.rijksoverheid.nl/onderwerpen/digitalisering-onderwijs/veilige-en-goede-ict-in-het-onderwijs

Stichting Kennisnet. (2026, 5 februari). *Dreigingsbeeld cybersecurity 2025: Kwetsbaarheden herkennen en veiligheid verhogen*. Geraadpleegd op 18 februari 2026, van https://www.kennisnet.nl/informatiebeveiliging-en-privacy/dreigingsbeeld-primair-en-voortgezet-onderwijs-2025-kwetsbaarheden-herkennen-veiligheid-verhogen/

SURF. (2023). *Cyberdreigingsbeeld 2023: Onderwijs en onderzoek*. https://www.surf.nl/files/2023-06/cyberdreigingsbeeld-onderwijs-en-onderzoek-2023_0.pdf

SURF. (2024). *Cyberdreigingsbeeld 2014–2024: Onderwijs en onderzoek* (Speciale editie). https://www.surf.nl/files/2024-10/surf-cyberdreigingsbeeld-2014-2024-def.pdf

SURF. (z.d.). *Beleidspiramide informatiebeveiliging: Van strategisch beleid tot uitvoering in de praktijk*. https://sec.surf.nl/beleidspiramide-informatiebeveiliging/

Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security, 148*, 104110.

Taddeo, M. (2019). Is cybersecurity a public good? Mind & Machines, 29(3), 349–357. https://doi.org/10.1007/s11023-019-09507-5

Teichmann, F., & Sergi, B. S. (2025). The EU cyber resilience act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem. *Computer Law & Security Review, 59*, 106209. https://doi.org/10.1016/j.clsr.2025.106209

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy, 2*(3), 573–586.

Van Elk, W.-J. (2024, 7 november). Zorgen om marktkracht van big tech en edtech in het onderwijs. *Kennisnet*. Geraadpleegd op 18 februari 2026, van https://www.kennisnet.nl/trends/zorgen-om-marktkracht-van-big-tech-en-edtech-in-het-onderwijs/

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security, 88*, 101640.

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research, 16*(4), 490–513.

Colofon
Inspectie van het Onderwijs
Postbus 2730 | 3500 GS Utrecht
www.onderwijsinspectie.nl

Foto omslag: Marieke Duijsters

Deze publicatie is te downloaden via de website van de Inspectie van het Onderwijs: www.onderwijsinspectie.nl