21 juli 2026

BDO

SURF

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Security en privacy awareness 2026

SECTORRAPPORT

MBO, HBO en Universiteiten

VAN INFORMEREN NAAR ACTIVEREN

Managementsamenvatting

Waar staat de sector in 2026?

Introductie

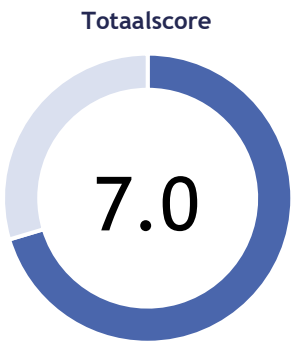
- In opdracht van SURF heeft BDO voor het vijfde jaar security- en privacy awarenessmetingen uitgevoerd bij onderwijs- en onderzoeksinstellingen;
- De metingen bestaan uit online vragenlijsten voor de medewerkers, daarnaast is er voor de sectorrapportage 1 interview gehouden;
- Na de meting zijn door de Haagse Hogeschool aanvullende onderzoeksvragen gesteld aan de respondenten over hun ervaringen met cyberincidenten.
- Deelnemende instellingen: 30, aantal respondenten: 7.049.

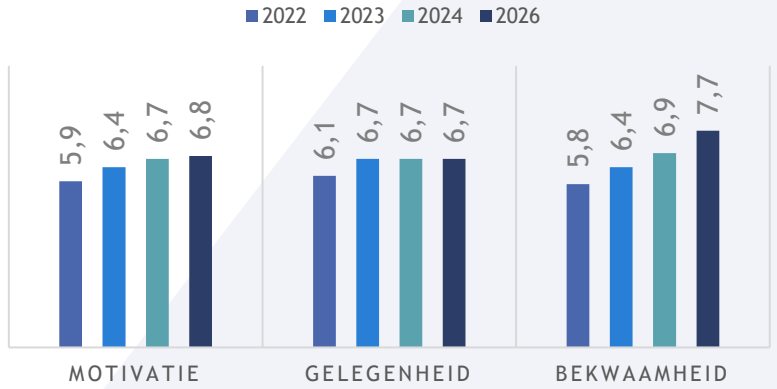
Conclusie

- De resultaten laten een stabiel beeld zien, maar verdere groei lijkt af te vlakken; de sector lijkt een plateau te hebben bereikt;
- De kennisbasis is relatief sterk, maar kennis vertaalt zich nog niet vanzelf naar consistent veilig gedrag in de praktijk;
- Medewerkers hebben vooral behoefte aan duidelijke, praktische richtlijnen voor concrete werksituaties, zoals het delen van gegevens, incidenten en het gebruik van tools;
- De motivatie blijft kwetsbaar: informatieveiligheid wordt belangrijk gevonden, maar de intrinsieke betrokkenheid en blijvende aandacht in het dagelijks werk blijven beperkt;
- AI en toolgebruik vormen een dominant spanningsveld. Medewerkers gebruiken nieuwe toepassingen in de praktijk, terwijl beleid en richtlijnen niet altijd voldoende houvast bieden;
- Verdere verbetering vraagt om het verlagen van drempels, het bieden van concreet handelingsperspectief en het beter ondersteunen van veilig gedrag in de dagelijkse praktijk.

Aanbevelingen

1. Maak informatieveilig werken concreet en herkenbaar in de praktijk door awareness en communicatie in te richten op specifieke werksituaties en handelingsperspectief;
2. Verlaag drempels voor veilig gedrag door maatregelen beter te laten aansluiten op het dagelijkse werk;
3. Bied duidelijke kaders en actieve sturing op toolgebruik, met specifieke aandacht voor AI en externe toepassingen;
4. Investeer in voorbeeldgedrag en cultuur, zodat informatieveiligheid zichtbaar een gezamenlijke norm wordt in teams en management;
5. Zet in op onboarding en periodieke herhaling, met aandacht voor rol-specifieke risico's en ontwikkelingen (zoals AI);
6. Vernieuw de awareness-aanpak: van informeren naar activeren, met nadruk op gedragsveranderingen in plaats van alleen kennisoverdracht.





Inhoudsopgave

Inleiding

Inleiding

Digitale weerbaarheid in onderwijs en onderzoek wordt in toenemende mate bepaald door het dagelijks handelen van medewerkers. Niet alleen grote incidenten of geavanceerde dreigingen vormen daarbij een risico, maar juist de optelsom van kleine keuzes in de praktijk: het delen van informatie, het gebruik van tools en de manier waarop met nieuwe technologieën wordt omgegaan.

In de afgelopen jaren is binnen de sector zichtbaar ingezet op het vergroten van kennis en bewustzijn rondom informatieveiligheid en privacy. Daarmee is een belangrijke basis gelegd. Tegelijkertijd laat de praktijk zien dat bewustzijn alleen niet voldoende is om gewenst gedrag duurzaam te borgen. De context waarin medewerkers werken speelt hierin een minstens zo bepalende rol.

Dit sectorrapport presenteert de resultaten van de awarenessmetingen die in het voorjaar van 2026 in opdracht van SURF zijn uitgevoerd. De metingen geven inzicht in hoe medewerkers omgaan met informatieveiligheid en privacy in hun dagelijkse werk en in hoeverre zij daartoe in staat worden gesteld. Daarbij wordt gekeken naar drie samenhangende factoren: bekwaamheid, motivatie en gelegenheid.

De resultaten laten zien dat de sector zich in een nieuwe fase bevindt. Waar in eerdere jaren vooral sprake was van groei en ontwikkeling, is nu een stabieler beeld zichtbaar. De grootste uitdaging ligt niet langer primair in het vergroten van kennis, maar in het vertalen daarvan naar consistent gedrag in de praktijk. Tegelijkertijd zorgen ontwikkelingen zoals de snelle opkomst van AI en het toenemende gebruik van externe tools voor nieuwe vraagstukken. Deze ontwikkelingen maken duidelijk dat kaders, ondersteuning en praktische richtlijnen blijvend moeten meebewegen met de dagelijkse realiteit van medewerkers.

Dit rapport biedt inzicht in de huidige stand van zaken binnen de sector en helpt bij het duiden van de belangrijkste knelpunten en kansen. Het vormt daarmee een basis voor gerichte verbeteringen, met als doel om informatieveilig en privacybewust werken beter te laten aansluiten op de praktijk van alle dag.

Aanpak awarenessmeting

Aanpak awarenessmeting

Om informatieveilig gedrag te begrijpen is het niet voldoende om alleen naar kennis te kijken. Gedrag ontstaat in de wisselwerking tussen wat medewerkers weten, wat zij belangrijk vinden en de context waarin zij werken. Het doel van deze metingen is inzicht te krijgen in informatieveilig gedrag in de praktijk en de factoren die dit gedrag beïnvloeden.

In het voorjaar van 2026 hebben medewerkers van onderwijs- en onderzoeksinstellingen een online vragenlijst ingevuld, gericht op hun kennis, houding en gedrag rondom informatieveiligheid en privacy. Daarnaast is een interview gehouden om de resultaten te verdiepen en beter te begrijpen hoe deze zich vertalen naar de dagelijkse praktijk.

Voor de analyse is gebruik gemaakt van het COM-B model van Susan Michie, waarin gedrag wordt verklaard vanuit drie componenten:

- Bekwaamheid: kennis en vaardigheden om veilig te handelen;
- Motivatie: de bereidheid en drijfveren om dit gedrag te vertonen;
- Gelegenheid: de mate waarin de omgeving dit gedrag faciliteert.

De combinatie van deze componenten maakt zichtbaar waar de belangrijkste verbeterkansen liggen: in het vergroten van kennis, het versterken van motivatie, of juist in het beter inrichten van de werkomgeving. Dit rapport brengt deze dynamiek sectorbreed in kaart en legt daarmee de basis voor gerichte interventies.

De sector in context

De sector in context

Van groei naar plateau

Huidige situatie: sterke basis, beperkte doorvertaling

De resultaten van 2026 laten een consistent beeld zien. Informatieveiligheid wordt breed als belangrijk ervaren en medewerkers geven aan hier in hun werk aandacht aan te besteden. Tegelijkertijd blijft de intrinsieke betrokkenheid achter en voelt slechts een deel van de medewerkers zich voldoende gefaciliteerd of duidelijk gestuurd in het gewenste gedrag.

Daarbij valt op dat medewerkers in grote mate weten wat er van hen verwacht wordt, terwijl de organisatorische randvoorwaarden – zoals duidelijke regels, ondersteuning en voorbeeldgedrag – duidelijk achterblijven. Deze combinatie wijst op een sector waarin de basis op orde is, maar waarin verdere verbetering niet vanzelf optreedt.

Vergelijking met eerdere jaren

In vergelijking met 2024 is het beeld verschoven van groei naar stabilisatie. Waar destijds nog sprake was van een duidelijke stijgende lijn, is in 2026 vooral sprake van bestendiging van bestaande patronen.

De belangrijkste knelpunten – zoals beperkte intrinsieke motivatie en onvoldoende facilitering – blijven terugkomen en laten weinig ontwikkeling zien. Dat bevestigt dat deze vraagstukken niet tijdelijk zijn, maar structureel van aard.

Interpretatie: overgang naar een nieuwe fase

De sector is daarmee in een volgende fase terechtgekomen. Awareness is geen nieuw onderwerp en meer en kennis is breed aanwezig, maar dit vertaalt zich nog onvoldoende naar consistent gedrag in de praktijk.

De verschillen tussen weten, willen en kunnen blijven bestaan en laten zien dat de uitdaging niet langer ligt in het vergroten van bewustzijn alleen, maar in het daadwerkelijk ondersteunen en borgen van gedrag in de dagelijkse praktijk.

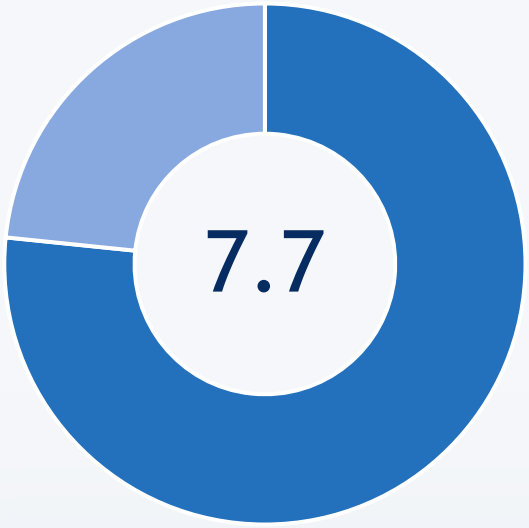
Conclusie: doorbreken van het plateau

De sector heeft een plateau bereikt. De belangrijkste patronen zijn stabiel en verdere vooruitgang vraagt om een andere benadering dan in voorgaande jaren.

Om dit te doorbreken, zullen awarenesscampagnes vernieuwend moeten zijn. De nadruk verschuift van informeren naar activeren: campagnes moeten sterker aansluiten op de dagelijkse praktijk, concreet gedrag adresseren en inspelen op de context waarin medewerkers werken. Alleen op die manier kan de stap worden gezet van begrijpen naar daadwerkelijk handelen.

Resultaten

Scores per onderdeel



Bekwaamheid

Motivatie

Gelegenheid

Bekwaamheid

Wanneer kennis niet langer de beperkende factor is

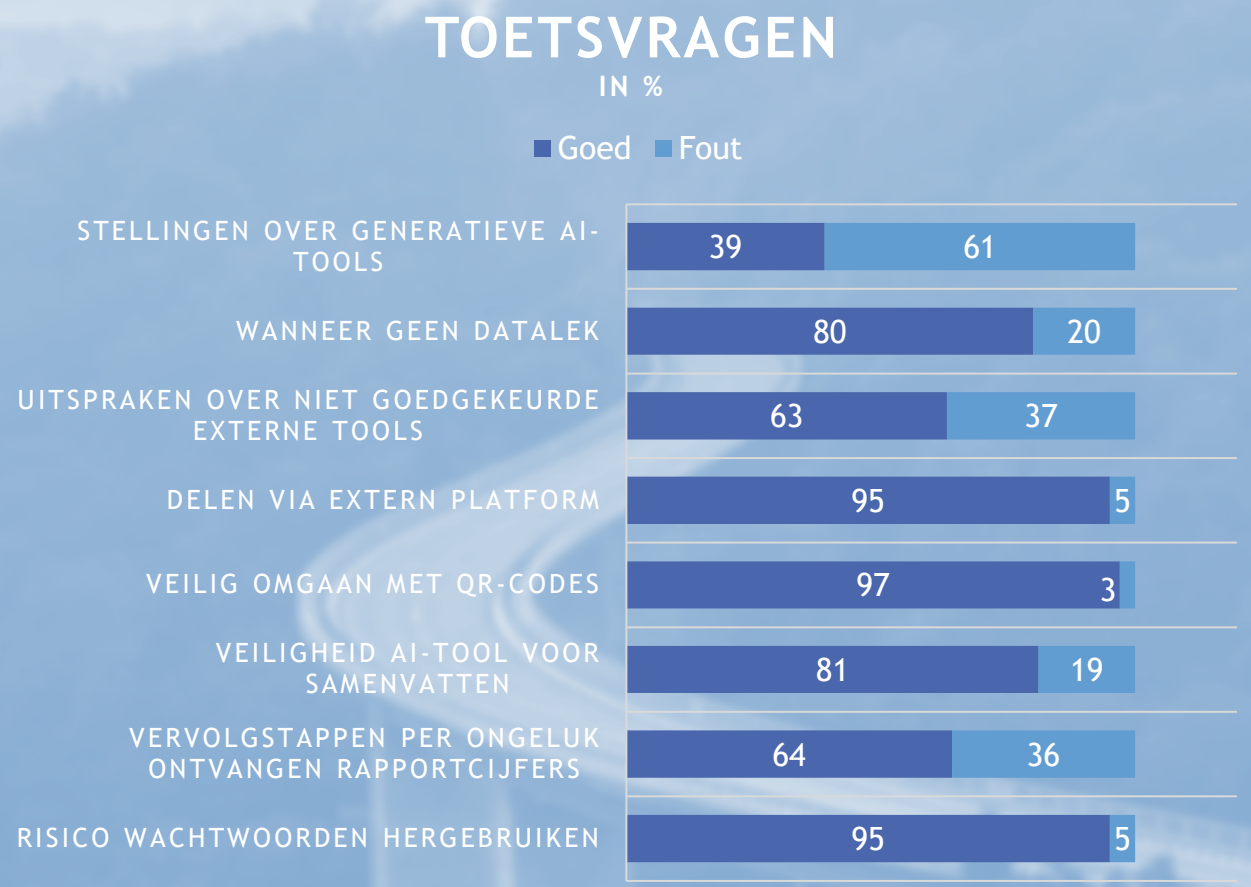
Relatief hoog kennisniveau onder medewerkers

De resultaten laten zien dat een groot deel van de medewerkers beschikt over de kennis die nodig is om informatieveilig te handelen. Ook bij meer recente thema's, zoals het gebruik van AI-tools, laat een meerderheid van de respondenten zien zich bewust te zijn van belangrijke risico's en voorwaarden. Dit duidt erop dat nieuwe onderwerpen in korte tijd onderdeel worden van het bredere kennisniveau binnen de sector.

Zelfbeeld en daadwerkelijke toepassing

Tegelijkertijd blijft het belangrijk om te benadrukken dat dit niet direct iets zegt over de mate waarin deze kennis consequent en correct wordt toegepast in de praktijk.

In concrete werksituaties – waarin bijvoorbeeld tijdsdruk, gemak of onzekerheid een rol spelen – kan het maken van de juiste keuze complexer zijn dan op basis van theorie wordt verondersteld. Hierdoor ontstaat ruimte voor afwijking tussen wat medewerkers weten en hoe zij daadwerkelijk handelen.



Over welke onderwerpen heb jij meer kennis nodig om informatieveilig te kunnen werken?

Meerdere antwoorden waren mogelijk. De getoonde aantallen geven weer hoe vaak elk antwoord is geselecteerd

Bekwaamheid

1 2 3

Wanneer kennis niet langer de beperkende factor is

Kennis is niet hetzelfde als toepassing

Het kennisniveau van medewerkers over informatieveilig werken lijkt relatief hoog, maar opvallend is hoe vaak de roep om duidelijkere uitleg en beleid terugkomt. Dit gaat dan bijvoorbeeld over welke tools wel en niet toegestaan zijn en hoe zij in specifieke situaties – zoals bij incidenten – moeten handelen.

Deze combinatie wijst op een belangrijk onderscheid. Medewerkers beschikken over basiskennis, maar ervaren in de praktijk onvoldoende houvast in concrete situaties. Kennis op hoofdlijnen is aanwezig, maar blijkt niet altijd voldoende om onzekerheid weg te nemen op het moment dat keuzes gemaakt moeten worden. Daarbij speelt ook de organisatorische context een rol: wanneer kaders, beleid of ondersteuning niet eenduidig of toepasbaar zijn, wordt het lastiger om kennis consistent toe te passen.

Daardoor ontstaat een verschil tussen de kennis die wordt aangetoond in een toets en de kennis die wordt toegepast in het dagelijks werk. Dit onderstreept dat de uitdaging niet alleen ligt in kennis, maar vooral in de vertaling daarvan naar concrete situaties, ondersteund door duidelijke en toepasbare organisatiekaders.

Bekwaamheid

1 2 3

Wanneer kennis niet langer de beperkende factor is

Duiding: kennis is niet de beperkende factor

De resultaten wijzen erop dat de sector erin is geslaagd om een solide kennisbasis op te bouwen. Medewerkers hebben in toenemende mate inzicht in risico's en weten op hoofdlijnen hoe zij moeten handelen.

Tegelijkertijd wordt zichtbaar dat verdere verbetering niet primair ligt in het vergroten van kennis. De uitdaging verschuift naar de toepassing in de praktijk en de omstandigheden waarin keuzes worden gemaakt. Kennis alleen is daarvoor onvoldoende richtinggevend.

Conclusie

Bekwaamheid vormt in beperkte mate nog een belemmering voor informatieveilig gedrag. Medewerkers schatten hun kennisniveau relatief hoog in en laten zien dat zij bekend zijn met veel voorkomende risico's en handelingsopties.

Dit betekent dat verdere verbetering minder te realiseren is door het uitbreiden van kennis alleen. Effectiviteit ligt vooral in het beter ondersteunen van de toepassing daarvan in de praktijk, bijvoorbeeld door kennis te vertalen naar concrete situaties en keuzes waar medewerkers dagelijks mee te maken hebben.

Motivatie

Hoog belang, beperkt eigenaarschap

Voor het component motivatie zijn verschillende vragen gebruikt om te bepalen in hoeverre respondenten (uit zichzelf) gemotiveerd zijn om informatieveilig te werken.

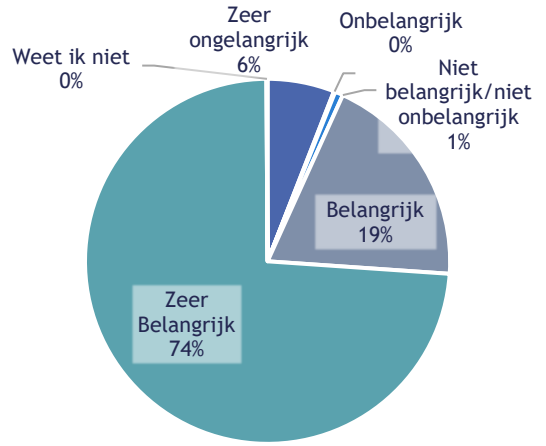
> *"Ik vind het prettig als er zorgvuldig wordt omgegaan met mijn gegevens, dus voor een ander doe je dat ook."*

Belang en aandacht voor informatieveiligheid

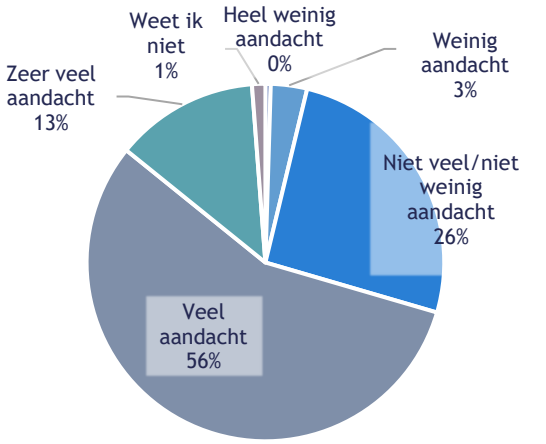
Informatieveiligheid wordt door respondenten duidelijk belangrijk gevonden: 93% bestempelt het als 'belangrijk' of 'zeer belangrijk' voor de instelling. Daarnaast geeft 69% aan hier in het dagelijkse werk 'veel' of 'zeer veel' aandacht aan te besteden. Deze uitkomsten onderstrepen dat informatieveiligheid serieus wordt genomen. Ten opzichte van 2024 is dit beeld stabiel gebleven en is geen verdere groei zichtbaar.

Hoewel informatieveiligheid duidelijk belangrijk wordt gevonden, betekent dit niet automatisch dat deze aandacht zich vertaalt naar consistent gedrag in de praktijk. Zoals ook blijkt uit de resultaten op bekwaamheid, beschikken medewerkers over de benodigde kennis, maar bepalen motivatie en context in sterke mate of deze kennis daadwerkelijk wordt toegepast.

In de praktijk betekent dit dat informatieveilig gedrag vooral achterblijft op momenten dat het extra tijd of moeite vraagt. Juist in die situaties is aanvullende ondersteuning nodig.



Hoe belangrijk vind jij informatieveiligheid voor jouw instelling?



Hoeveel aandacht besteed jij over het algemeen tijdens je werk aan informatieveiligheid?

Motivatie

Hoog belang, beperkt eigenaarschap

Drijfveren voor informatieveiligheid

Zoals eerder benoemd besteedt 69% van de respondenten ‘veel’ tot ‘zeer veel’ aandacht aan informatieveiligheid in het dagelijkse werk. Deze aandacht komt voort uit verschillende drijfveren. Enerzijds geven respondenten aan dat zij zich schamen als door het eigen handelen een incident of datalek zou ontstaan. Anderzijds benadrukken zij het belang van informatieveilig werken om de organisatie digitaal weerbaar te houden.

Naast de getoonde antwoordopties was er ook de mogelijkheid om een open antwoord te geven. Veel van de gegeven antwoorden gaan over vanzelfsprekendheid en wederkerigheid:

Vanzelfsprekendheid

- “Het is vanzelfsprekend, net zoals een arts zijn handen wast om infecties/problemen te voorkomen.”
- “Er is mij een werkwijze aangeleerd waar informatieveiligheid al in is opgenomen; het gaat dus vanzelf.”

Wederkerigheid

- “Ik wil ook dat anderen bewust omgaan met mijn persoonsgegevens en daarom maak ik er een punt van om dat ook te doen met andermans persoonsgegevens.
- “Ik vind het belangrijk dat we goed omgaan met de privacy van anderen, vooral als ze ons vertrouwen met privacy gevoelige gegevens”

Gelegenheid

1 2 3 4

Waar context en systemen gedrag beïnvloeden

Ervaren handelingsvermogen, maar geen garantie voor gedrag

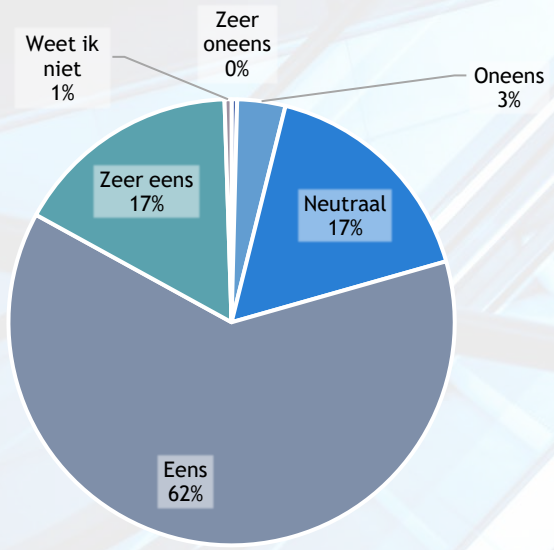
Een grote meerderheid van de medewerkers geeft aan dat zij weten hoe zij in hun dagelijkse werk invulling kunnen geven aan informatieveilig werken. Dit wijst erop dat veel medewerkers het gevoel hebben over voldoende handelingsperspectief te beschikken.

Tegelijkertijd moet deze uitkomst worden geduid als zelfgerapporteerd gedrag. Het zegt iets over hoe medewerkers hun eigen handelen inschatten, maar niet per definitie over de mate waarin dit gedrag consequent en correct in de praktijk wordt uitgevoerd.

Verschil tussen wat medewerkers aangeven en wat zij ervaren vanuit de instelling

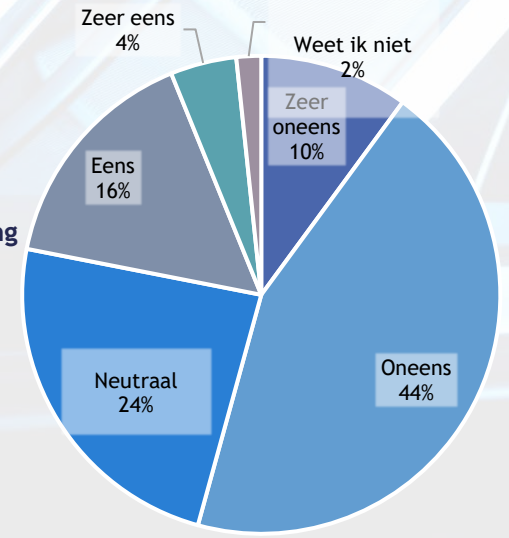
Wanneer wordt gekeken naar de ervaren ondersteuning vanuit de organisatie, ontstaat een ander beeld. Een duidelijk kleiner deel van de medewerkers geeft aan zich goed gefaciliteerd te voelen om informatieveilig te kunnen werken.

Dit laat een spanning zien tussen individueel ervaren handelingsvermogen en de organisatorische context. Medewerkers hebben het gevoel dat zij weten wat er van hen verwacht wordt, maar ervaren niet altijd dat de randvoorwaarden aanwezig zijn om dit eenvoudig en consistent toe te passen.



Ik weet hoe ik in mijn dagelijkse werk invulling moet geven aan informatieveilig werken.

Ik word goed gefaciliteerd door mijn instelling om informatieveilig te kunnen werken (bijvoorbeeld door software, tools, instructies, en andere middelen).

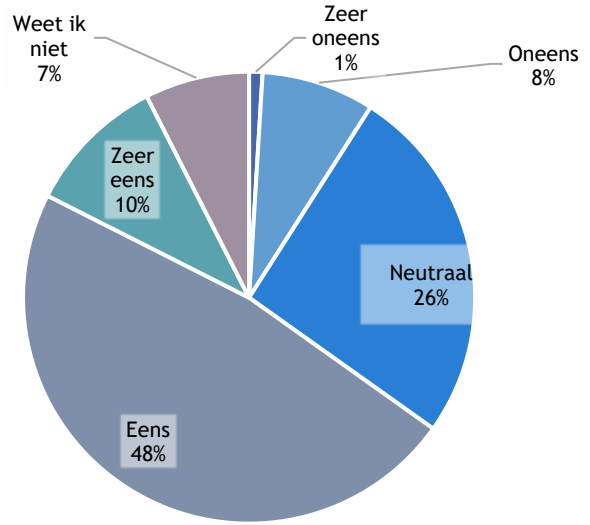


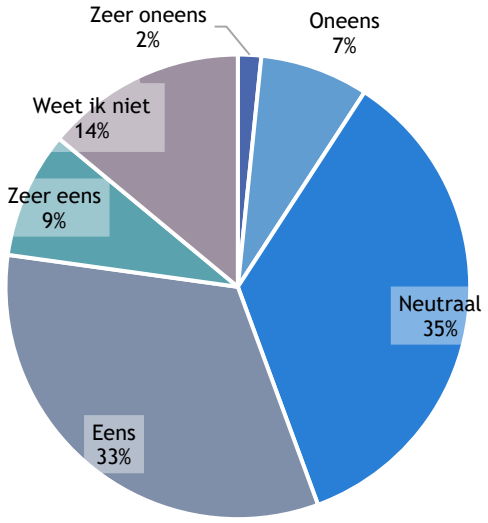
Gelegenheid

1 2 3 4

Waar context en systemen gedrag beïnvloeden

Mijn organisatie heeft duidelijke gedragsregels aan informatieveilig werken.





Mijn leidinggevende geeft mij het juiste voorbeeld als het gaat om informatieveilig werken.

Onduidelijke kaders vergroten afhankelijkheid van interpretatie

Ook op het gebied van richtlijnen en gedragsregels geeft een substantieel deel van de medewerkers aan dat deze niet altijd duidelijk zijn.

Wanneer kaders niet eenduidig of herkenbaar zijn, ontstaat ruimte voor eigen interpretatie. Dit vergroot de kans dat medewerkers informatieveilig gedrag verschillend invullen, afhankelijk van hun eigen ervaring of de context waarin zij werken. Hierdoor kan gedrag binnen en tussen instellingen minder consistent worden.

Voorbeeldgedrag blijft achter als normsteller

Het laagste resultaat binnen dit component heeft betrekking op het voorbeeldgedrag van leidinggevenden. Minder dan de helft van de medewerkers ervaart dat hun leidinggevende het juiste voorbeeld geeft.

Dit is relevant omdat voorbeeldgedrag een belangrijke rol speelt in het zichtbaar maken van normen. Wanneer dit beperkt aanwezig is, blijft informatieveiligheid sneller een individueel onderwerp, in plaats van een gedeelde standaard binnen teams.

Gelegenheid

1 2 3 4

Waar context en systemen gedrag beïnvloeden

Geen aanwijzing dat regels zelf het probleem zijn

Een meerderheid van de medewerkers geeft aan dat security- en privacyregels niet als directe belemmering worden ervaren in het dagelijks werk.

Dit nuanceert het beeld dat regels op zichzelf het grootste probleem vormen. De resultaten wijzen er eerder op dat de uitdaging ligt in de toepassing en ondersteuning van deze regels, en niet in de aanwezigheid ervan.

Duiding: spanning tussen zelfbeeld en context

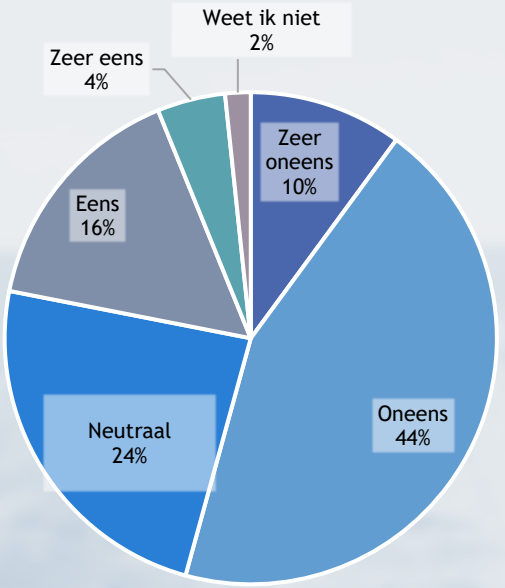
De resultaten binnen het component gelegenheid laten daarmee een terugkerend patroon zien. Medewerkers geven enerzijds aan dat zij weten hoe zij informatieveilig kunnen handelen, maar ervaren anderzijds beperkingen in de context waarin zij dat gedrag moeten toepassen.

Deze spanning kan op verschillende manieren worden geïnterpreteerd:

- het handelingsvermogen wordt mogelijk overschat;
- de organisatorische ondersteuning sluit onvoldoende aan op de praktijk;
- of een combinatie van beide.

Wat in ieder geval zichtbaar is, is dat de omgeving waarin medewerkers werken een bepalende rol speelt in de mate waarin gewenst gedrag tot stand komt.

Ik ervaar de security en privacy gedragsregels als een remmende factor tijdens mijn dagelijkse werkzaamheden.



Gelegenheid

1 2 3 4

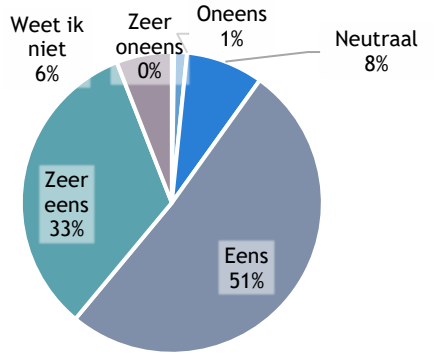
Waar context en systemen gedrag beïnvloeden

Incidenten melden als voorbeeld van de rol van context

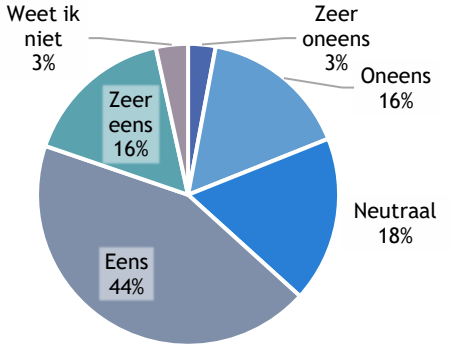
Het verschil tussen individuele intentie en organisatorische ondersteuning wordt ook zichtbaar bij het melden van incidenten. Een grote meerderheid van de medewerkers (84%) geeft aan dat zij een security- of privacy-incident zouden durven melden, terwijl een duidelijk kleiner deel aangeeft precies te weten wanneer en hoe dit moet gebeuren (60%).

Dit wijst erop dat de bereidheid om het juiste te doen aanwezig is, maar dat de praktische invulling daarvan minder duidelijk is. Het ontbreken van heldere en herkenbare procedures maakt dat medewerkers in de praktijk kunnen twijfelen over hoe zij moeten handelen.

Deze uitkomst onderstreept dat context een bepalende rol speelt. Niet de intentie ontbreekt, maar de mate waarin de instelling het handelen concreet ondersteunt en richting geeft.



Ik durf een security- of privacy incident altijd te melden, ook als ik die zelf heb veroorzaakt.



Ik weet wanneer en hoe ik een security- of privacy incident moet melden.

AI als sectorbreed thema

AI als sectorbreed thema

AI is onderdeel van de dagelijkse praktijk

In 2026 is AI geen experimenteel onderwerp meer, maar onderdeel van het dagelijks werk. Medewerkers komen ermee in aanraking en passen het toe in hun werkzaamheden. Tegelijkertijd is het gebruik nog niet volledig verankerd in beleid en werkwijzen, waardoor een spanningsveld ontstaat tussen gebruik en sturing.

Basisinzicht aanwezig, toepassing vraagt richting

De resultaten laten zien dat medewerkers zich in de basis bewust zijn van risico's en weten dat het gebruik van AI gebonden is aan kaders.

Tegelijkertijd zegt dit vooral iets over kennis op hoofdlijnen. In concrete werksituaties – bijvoorbeeld bij het verwerken van informatie of het kiezen van tools – blijft het maken van de juiste afweging afhankelijk van de context. Juist daar ontbreekt vaak duidelijke en toepasbare richting.

AI raakt alle onderdelen van gedrag

AI onderscheidt zich doordat het direct invloed heeft op alle componenten van gedrag. Het vraagt om kennis van risico's, beïnvloedt motivatie door de focus op efficiëntie en stelt eisen aan de organisatorische context in de vorm van duidelijke kaders en goedgekeurde middelen. Hierdoor ontstaat sneller ruimte voor individuele interpretatie, met name wanneer beleid en praktijk niet op elkaar aansluiten.

Conclusie

De resultaten laten zien dat medewerkers in toenemende mate te maken krijgen met AI-toepassingen in hun werk, terwijl de kaders en richtlijnen hiervoor niet altijd eenduidig zijn.

Dit maakt dat het voor medewerkers niet altijd duidelijk is welke toepassingen wel en niet passend zijn binnen de instelling. Meer expliciete en toegankelijke communicatie over toegestane tools en gebruiksvoorwaarden kan bijdragen aan meer consistente en veilige toepassing in de praktijk.

Awareness-initiatieven kunnen hierin een belangrijkere rol spelen door medewerkers concreet te ondersteunen bij het maken van keuzes over het gebruik van AI-tools in hun dagelijkse werk.

Verbeterpunten respondenten

Verbeterpunten respondenten

In de vragenlijst en tijdens de interviews is aan respondenten gevraagd welke opmerkingen of verbeterpunten zij hebben om informatieveilig en privacybewust werken binnen hun organisatie te versterken. De open antwoorden geven meer context aan de resultaten uit de vorige hoofdstukken en laten zien waar medewerkers in de praktijk tegenaan lopen. De belangrijkste verbeterpunten zijn hieronder beschreven.

Duidelijkheid rondom informatieveilig werken in de praktijk

Veel respondenten geven aan dat zij het belang van informatieveiligheid onderschrijven en weten dat zij hier aandacht aan moeten besteden. Tegelijkertijd blijkt uit de open antwoorden dat medewerkers in concrete situaties regelmatig twijfelen over wat wel en niet is toegestaan. Dit gaat onder andere over het delen en opslaan van informatie, het gebruik van samenwerkingsplatforms en het omgaan met persoonsgegevens in dagelijkse werkzaamheden. Hoewel een groot deel van de respondenten aangeeft te weten hoe zij in hun werk invulling moeten geven aan informatieveilig werken, blijkt uit de toelichtingen dat deze kennis vaak gebaseerd is op ervaring of ‘gezond verstand’.

Medewerkers kunnen zorgvuldig handelen naar algemene richtlijnen, tegelijkertijd laat de praktijk zien dat deze houvast afneemt wanneer nieuwe toepassingen, tools of werkwijzen worden geïntroduceerd. Hierdoor ontstaat onzekerheid over wat wel en niet is toegestaan. Er is behoefte aan meer concrete, praktijkgerichte uitleg.

> *“Het zou fijn zijn om als team een uitleg, in welke vormen dan ook, te krijgen over informatieveilig werken dat vooral toegespitst is op onze werkzaamheden. Uitleg op maat dus, zodat we vooral datgene weten wat nodig is om ons werk zo goed mogelijk informatieveilig te doen. Anders zie ik door de bomen (van te veel informatie/regels/input) het bos niet meer.”*

Informatieveiligheid en dagelijkse werkprocessen

In de open antwoorden komt een herkenbaar spanningsveld naar voren tussen informatieveilig werken en de dagelijkse praktijk. In de gesloten vragen geeft slechts een beperkte groep aan dat security- en privacyregels het werk echt belemmeren. In de toelichtingen wordt dit beeld genuanceerder. Respondenten geven aan dat informatieveiligheid vooral lastig wordt wanneer maatregelen extra stappen vragen, het werk vertragen of niet goed aansluiten bij onderwijs- of onderzoeksactiviteiten. Daarbij gaat het niet om weerstand tegen informatieveiligheid, maar om praktische knelpunten.

Tegelijkertijd laten zowel de open antwoorden als het interview zien dat instellingen steeds vaker investeren in ondersteuning zoals trainingen, metingen en awareness-activiteiten. De uitdaging verschuift daarmee van het beschikbaar maken van middelen naar het daadwerkelijk inbedden van veilig gedrag in de dagelijkse werkprocessen. Medewerkers willen graag veilig werken, maar ervaren dat dit makkelijker wordt wanneer processen en systemen beter aansluiten op hun werkzaamheden.

> *“Informatieveiligheid staat vaak op gespannen voet met fijn je werk kunnen doen. Als er een keuze is tussen het laatste en het eerste kies ik vrijwel altijd voor het laatste, mijn werk kunnen doen. Zo lang dat spanningsveld niet is opgelost, blijft voor mij informatieveiligheid tweede plan”*

Verbeterpunten respondenten

1 2 3

Omgaan met nieuwe digitale ontwikkelingen

Medewerkers benoemen in de open antwoorden de onzekerheid over het gebruik van nieuwe technologieën, zoals generatieve AI en cloudapplicaties. Zij vragen zich af wat binnen hun functie kan en mag, en welke risico's daarbij een rol spelen. Deze onzekerheid hangt samen met het ontbreken van duidelijke richtlijnen en ondersteuning. In de praktijk speelt ook het tempo mee waarin nieuwe tools worden gebruikt, bijvoorbeeld bij het ontwikkelen van lesmateriaal of het gebruik van externe tools. AI wordt daarbij vooral genoemd als voorbeeld van een ontwikkeling waarvoor de bestaande afspraken weinig houvast bieden. Respondenten geven aan dat zij behoefte hebben aan duidelijke en toepasbare kaders, zodat zij weten hoe zij hier in hun dagelijkse werk mee om kunnen gaan.

Tegelijkertijd wordt zichtbaar dat instellingen hier actief op inspelen door ondersteuning dichter bij de medewerker te organiseren, bijvoorbeeld via 'digitale coaches' of 'I-coaches', die collega's begeleiden bij digitale vraagstukken en het gebruik van AI. Dit helpt medewerkers om nieuwe technologieën verantwoord toe te passen in hun dagelijkse werk.

Ondersteuning door systemen en tools

In de open antwoorden wordt regelmatig gewezen op het belang van goede ondersteuning en hulpmiddelen. Medewerkers geven aan dat zij passende tools nodig hebben om informatieveilig te kunnen werken, bijvoorbeeld voor het veilig delen van bestanden of door duidelijke keuzes in toegestane software. Als die ondersteuning ontbreekt of niet goed functioneert, ontstaat de neiging om zelf oplossingen te zoeken om het werk toch uit te kunnen voeren.

"Indien het gebruik van een applicatie niet meer is toegestaan zou het fijn zijn als er een alternatief wordt gecommuniceerd en daarbij een handleiding of training wordt aangeboden. "

Verbeterpunten respondenten

Voorbeeldgedrag en gezamenlijke norm

Tot slot laten de open antwoorden zien dat informatieveilig werken vaak als individuele verantwoordelijkheid wordt ervaren. Respondenten geven aan dat zij zelf hun afwegingen maken, maar tegelijkertijd behoefte hebben aan meer eenduidigheid en zichtbare normstelling binnen de organisatie. Voorbeeldgedrag van leidinggevenden en collega's wordt hierbij als belangrijk genoemd.

> *"Ik denk dat managers en andere leidinggevende meer aandacht moeten besteden aan dit thema, het belang beter uitdragen."*

Tijdens het interview is benadrukt dat het gesprek over informatieveiligheid hierbij een belangrijke rol speelt, bijvoorbeeld door medewerkers regelmatig bij te praten over ontwikkelingen en door het delen van concrete praktijkvoorbeelden, zoals incidenten of hacks binnen de sector. Dit helpt om informatieveiligheid tastbaarder te maken en draagt bij aan een gezamenlijk normbesef.

Het aanspreken van elkaar op onveilig gedrag blijkt in de praktijk lastig, vooral wanneer onduidelijkheid bestaat over regels of verwachtingen. Respondenten benoemen dat informatieveiligheid helpt wanneer het onderwerp regelmatig terugkomt in gesprekken en niet alleen via beleid of incidentele communicatie.

Conclusie

Conclusie

Wat kunnen instellingen hiervan leren?

Dit rapport bevat een analyse van de 30 security- en privacy- awarenessmetingen die BDO in opdracht van SURF heeft uitgevoerd in het voorjaar van 2026. De conclusies hieronder zijn gebaseerd op de resultaten uit de meting.

Aan de start van de meting is, net als in voorgaande jaren, uitgegaan van drie onderzoeksvragen:

1. In hoeverre kunnen medewerkers informatieveilig en privacybewust werken (bekwaamheid)?
2. In hoeverre willen zij dat (motivatie)?
3. In hoeverre worden zij daartoe in staat gesteld (gelegenheid)?

De volgende conclusies geven antwoorden op deze vragen.

De sector laat een stabiel beeld zien

In de instellingsrapportages is zichtbaar dat veel instellingen rond het minimale streefbeeld scoren of daar net boven zitten, met een relatief beperkte spreiding tussen instellingen. Daarmee ontstaat een sectorbeeld waarin het niveau overwegend “voldoende” is. Dit sluit aan op het beeld uit 2024 waarin verbetering zichtbaar was.

Bekwaamheid is relatief sterk, kennisvragen verschuiven naar nieuwe praktijksituaties

Hoewel bekwaamheid in de instellingsrapporten relatief hoog scoort, verschuiven de kennisvragen steeds meer naar nieuwe praktijksituaties. In de kennisquiz blijven met name onderwerpen als generatieve AI, het gebruik van alternatieve tools en het omgaan met onbedoeld ontvangen (student)gegevens terugkomen als aandachtspunt. De open antwoorden maken duidelijk waar dit vandaan komt. Medewerkers zoeken vooral naar duidelijke en toepasbare richtlijnen: welke keuzes zijn toegestaan en hoe maak je veilige afwegingen in situaties die zij in hun dagelijkse werk tegenkomen.

Motivatie blijft kwetsbaar: het belang wordt erkend, maar aandacht concurreert met werkdruk en prioriteiten

Net als in 2024 erkennen medewerkers het belang van informatieveiligheid, maar de open antwoorden laten zien dat aandacht en naleving onder druk komen te staan wanneer het werk “doorgaat” en informatieveilig werken extra stappen vraagt. De resultaten laten zien dat motivatie het component is waarop instellingen winst kunnen boeken. Dit wijst erop dat het onderwerp wel wordt erkend als belangrijk, maar moet concurreren met andere prioriteiten in het dagelijks werk.

Conclusie

Wat kunnen instellingen hiervan leren?

Gelegenheid blijft een structureel aandachtspunt: medewerkers missen ondersteuning en houvast

De uitkomsten bevestigen het beeld uit 2024: de randvoorwaarden om informatieveilig te kunnen werken staan onder druk.

Medewerkers geven aan behoefte te hebben aan meer duidelijkheid en minder vrijblijvendheid in faciliteiten en richtlijnen. In de resultaten wordt herhaaldelijk gewezen op versnipperde informatie, onduidelijke meldroutes, het ontbreken van praktische hulpmiddelen en duidelijke instructies bij het gebruik van (nieuwe) tools. Hiermee wordt zichtbaar dat informatieveilig werken niet zozeer struikelt op bereidheid, maar op de aanwezigheid van duidelijke en toepasbare ondersteuning.

AI en toolgebruik vormen een dominant spanningsveld

Generatieve AI en toolgebruik nemen een prominente plaats in binnen de resultaten. Medewerkers worden in hun dagelijkse werk geconfronteerd met nieuwe toepassingen en werkwijzen, terwijl het onderscheid tussen toegestaan en niet-toegestaan gebruik niet altijd scherp of werkbaar is. Dit levert spanning op rond dataveiligheid en verantwoordelijkheid, bijvoorbeeld bij het gebruik van externe tools. AI wordt daarbij vooral genoemd als een concreet voorbeeld van een bredere ontwikkeling waarin bestaande kaders onvoldoende richting geven.

Aanbevelingen

Aanbevelingen

Op basis van de bevindingen en conclusies komen we tot de volgende aanbevelingen. Deze aanbevelingen zijn sectorbreed geformuleerd en sluiten aan op de terugkerende patronen uit de awarenessmeting.

Maak informatieveilig werken concreet per werksituatie (van regels naar handelingsperspectief)

Medewerkers vragen niet vooral om meer beleid, maar om praktische duidelijkheid: wat is de veilige werkwijze in herkenbare situaties (delen van bestanden, samenwerken met externen, omgaan met onbedoeld ontvangen gegevens). Richt communicatie en trainingen daarom op concrete scenario's die aansluiten bij het dagelijkse werk, zodat medewerkers sneller weten wat te doen.

Maak onboarding en periodieke herhaling standaard en rolgericht

In 2024 werd onboarding al genoemd als belangrijke bouwsteen. De open antwoorden van dit jaar bevestigen dat medewerkers behoefte hebben aan herhaling, vooral wanneer ontwikkelingen snel gaan (zoals bij AI). Zorg dat nieuwe medewerkers standaard de basis krijgen en dat er periodiek herhaling is, met aandacht voor rol-specifieke situaties (onderwijs, onderzoek, ondersteuning).

Faciliteer veilige alternatieven voor veelgebruikte 'schaduwtools', met extra aandacht voor AI

De meting laat zien dat AI en niet-goedgekeurde tools structureel terugkeren als verbeterpunt. Dat vraagt om heldere kaders en werkbare alternatieven. Wanneer veilige alternatieven ontbreken of minder bruikbaar zijn, neemt het risico toe dat medewerkers zoeken naar andere (minder veilige) mogelijkheden. Faciliteer daarom (sectorbreed waar mogelijk) veilige varianten en maak duidelijk wat de spelregels zijn voor gebruik.

Verlaag drempels voor veilig gedrag

Open antwoorden laten zien dat frictie vooral ontstaat wanneer informatieveilig werken extra stappen vraagt of processen vertraagt. Breng de belangrijkste fricties in kaart (bijvoorbeeld veilig gegevens delen, toegang en autorisaties, praktische instructies) en neem waar mogelijk belemmeringen weg. Dit versterkt met name de component gelegenheid en voorkomt onbedoelde olifantenpaadjes.

Aanbevelingen

1 2

Investeer in cultuur en voorbeeldgedrag: maak informatieveiligheid bespreekbaar

De resultaten en op antwoorden laten zien dat de behoefte ligt bij een aanspreekcultuur waarbij leren centraal staat en fouten bespreekbaar zijn. Dit vraagt om zichtbaar voorbeeldgedrag van leidinggevenden en ruimte om het onderwerp terug te laten komen in werkoverleggen.

Zorg voor een centrale en goed vindbare plek voor richtlijnen, meldroutes en hulpmiddelen

Respondenten geven aan dat informatie vaak versnipperd of lastig vindbaar is, met als gevolg dat men moet zoeken of op aannames vaart. Richt een centrale plek in waar medewerkers snel kunnen vinden: wat mag wel en niet, hoe melden zij incidenten, en welke tools zijn toegestaan. Zorg dat deze plek actueel is en regelmatig onder de aandacht wordt gebracht.

Onderzoek HHS

Onderdeel 3 van de meting had betrekking op de ervaringen van medewerkers van de deelnemende instellingen met cyberincidenten en de gevolgen die zij hebben ervaren door deze incidenten.

Dit onderzoek is uitgevoerd door Sifra Matthijsse en Susanne van ‘t Hoff-de Goede van De Haagse Hogeschool.

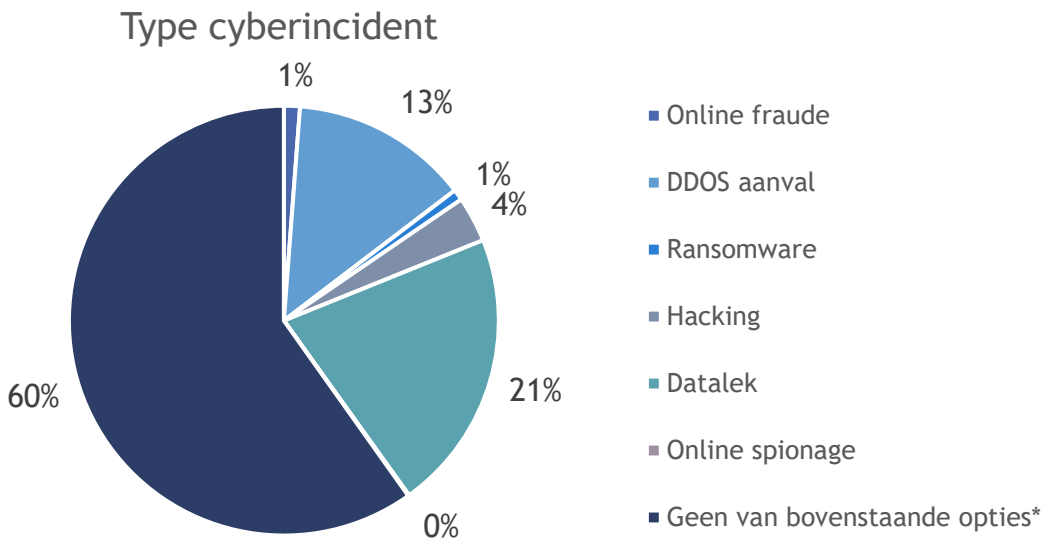
Ervaring met cyberincidenten

Onderzoek uitgevoerd door Sifra Matthijsse en Susanne van ‘t Hoff-de Goede

ONDERZOEK VAN DE HAAGSE HOGESCHOOL

Cyberincidenten vormen een steeds grotere uitdaging voor organisaties en kunnen niet alleen leiden tot technische en organisatorische problemen, maar ook tot gevolgen voor medewerkers. Om een beter inzicht te krijgen in deze menselijke impact is binnen deze meting door de Haagse Hogeschool onderzocht welke ervaringen medewerkers hebben met cyberincidenten binnen hun instelling en welke gevolgen zij daarvan hebben ondervonden.

40,1% van de medewerkers heeft een cyberincident meegemaakt bij hun instelling in de afgelopen twee jaar. Datalekken zijn daarvan de meest voorkomende cyberincidenten.



Gevolgen voor werk

36% van de medewerkers die een incident heeft meegemaakt geeft aan dat zij daar gevolgen van ervaren voor hun werk. Als mensen gevolgen ervaren voor hun werk, gaat het vaak om de tijd die zij besteden aan het oplossen van het incident of inlichten van betrokkenen (47%) en/of om hinder bij dagelijkse werkzaamheden (40%).

* De categorie *‘geen van de bovenstaande opties’* kan betrekking hebben op respondenten die in de afgelopen twee jaar geen cyberincident hebben meegemaakt of een ander type incident hebben ervaren dan in de vragenlijst is opgenomen.

Colofon

Sectorrapportage 2026

Over security en privacy awareness in onderwijs en onderzoek.

Juni 2026

Het rapport is opgesteld door

- **BDO Risk Advisory**

  Donna Moens, MSc donna.moens@bdo.nl

  mr. Linda van Liempt linda.van.liempt@bdo.nl

- **SURF**

  Rosanne Pouw, MSc, MPIM, MBA, CISM, CISSP, CIPM, rosanne.pouw@surf.nl

- **De Haagse Hogeschool**

  Dr. Susanne van ’t Hoff - de Goede M.S.vantHoff-deGoede@hhs.nl

  Sifra R. Matthijsse, MSc s.r.matthijsse@hhs.nl

Bijlagen

Bijlage 1 – Vragenlijst

‘Meningvragen’

1. Hoe belangrijk vind jij informatieveiligheid voor jouw instelling?
2. Hoeveel aandacht besteed jij over het algemeen tijdens je werk aan informatieveiligheid?
3. Waarom besteed jij tijdens je werk aandacht aan informatieveiligheid? Je kunt meerdere opties kiezen en een eventuele toelichting of opmerking geven.
4. Binnen mijn instelling hechten medewerkers veel belang aan informatieveiligheid.
5. Uit persoonlijke interesse volg ik nieuwe ontwikkelingen op het gebied van informatieveiligheid.
6. Ik weet hoe ik in mijn dagelijkse werk invulling moet geven aan informatieveilig werken.
7. Mijn instelling heeft duidelijke gedragsregels voor informatieveilig werken.
8. Ik word goed gefaciliteerd door mijn instelling om informatieveilig te kunnen werken (bijvoorbeeld door software, tools, instructies, en andere middelen).
9. Mijn leidinggevende geeft mij het juiste voorbeeld als het gaat om informatieveilig werken.
10. Ik durf een security- of privacy incident altijd te melden, ook als ik die zelf heb veroorzaakt.
11. Ik ervaar de security en privacy gedragsregels als een remmende factor tijdens mijn dagelijkse werkzaamheden.
12. Ik weet wanneer en hoe ik een security- of privacy incident moet melden.

Inventarisatie

1. Over welke onderwerpen heb jij meer kennis nodig om informatieveilig te kunnen werken? Je kunt meerdere opties kiezen.
2. Heb jij nog opmerkingen of verbeterpunten voor jouw instelling over informatieveilig werken?

Toetsvragen

1. Je gebruikt voor meerdere systemen hetzelfde wachtwoord , en past steeds één teken aan.

Wat is het grootste risico van deze aanpak? *(onderwerp: wachtwoorden)*

A. Je weet niet meer welk wachtwoord bij welk systeem hoort

B. Deze aanpak is eenvoudig te kraken door cybercriminelen

C. Het aanpassen van één teken kan ervoor zorgen dat je wachtwoord niet meer voldoet aan de speciale teken-eisen.

2. Je krijgt per ongeluk een bestand met namen en rapportcijfers die niet voor jou bedoeld zijn. Je opent het bestand, maar deelt het niet verder. Wat moet je doen? *(onderwerp: datalek melden/privacy)*

A. Een melding maken bij de Autoriteit Persoonsgegevens

B. De afzender vertellen dat hij/zij een datalek heeft veroorzaakt

C. Het bestand verwijderen en er verder niets mee doen

D. Het melden als datalek volgens de procedure van mijn instelling

Bijlage 1 – Vragenlijst

Toetsvragen (vervolg)

3. Je wilt een AI-tool gebruiken om een document te laten samenvatten met interne gegevens van jouw instelling. Is dat veilig? *(onderwerp: toegestaan AI gebruik)*

A. Altijd veilig, want AI-tools bewaren geen informatie

B. Alleen doen als de tool door de instelling is goedgekeurd

C. Dit is alleen veilig als je vooraf toestemming hebt van je leidinggevende of de IT-afdeling.

4. Je komt een QR-code tegen in een openbare ruimte. Wat is de veiligste manier om hiermee om te gaan? *(onderwerp: QR-code)*

A. Scan de code, open de URL en kijk of de website betrouwbaar oogt

B. Vertrouw op de afzender en scan direct

C. Gebruik een QR-scannerfunctie die de URL controleert voordat je deze opent

5. Een collega wil gegevens delen via een extern platform, omdat het sneller gaat dan het interne platform van de instelling. Wat doe je? *(onderwerp: data delen via tooling)*

A. Dit is alleen mogelijk als het externe platform een door jouw instelling goedgekeurde applicatie is

B. Dit kan alleen als het bestand met een wachtwoord is beveiligd

C. Dit is geen probleem, want het externe platform verwijdert bestanden na drie dagen

6. Een collega wil een online webinar organiseren en kiest hiervoor een externe tool die speciaal geschikt is voor grote groepen en het webinar soepel laat verlopen. Deze tool is (nog) niet goedgekeurd door jouw instelling. Welke van de onderstaande uitspraken is/zijn juist?

A. Het gebruik van een externe tool is alleen verantwoord als de privacy-instellingen volledig zijn geoptimaliseerd om persoonsgegevens te beschermen.

B. Het gebruik van een niet-goedgekeurde tool kan leiden tot onbedoelde verwerking van persoonsgegevens buiten de beveiligde omgeving van de instelling.

A. Stelling I en II zijn beide juist

B. Stelling I en II zijn beide onjuist

C. Stelling I is juist, stelling II is onjuist

D. Stelling I is onjuist, stelling II is juist

7. Bij welk van de onderstaande situaties is er géén sprake van een datalek? *(onderwerp: datalek herkennen/privacy)*

A. Je stuurt een e-mail naar studenten die interesse hebben in de workshop ‘slim studeren, minder stress’ en zet alle ontvangers in de bcc.

B. Een medewerker ontvangt per ongeluk het pensioenoverzicht van een collega.

C. Een ICT-beheerder downloadt studentengegevens om de nieuwe versie van de elektronische leeromgeving te testen in de testomgeving.

8. Welke stelling(en) over het gebruik van generatieve AI-tools, zoals ChatGPT/Copilot/Gemini, is/zijn waar? *(onderwerp: kennis over AI-gevaren)*

I. Je kunt de kwaliteit van een door de instelling goedgekeurde AI-tool volledig vertrouwen.

II. Je mag gebruik maken van openbare AI-tools, zolang je vertrouwelijke informatie anonimiseert.

A. Stelling I en II zijn beide waar

B. Stelling I en II zijn beide niet waar

C. Stelling I is waar, stelling II is niet waar

D. Stelling I is niet waar, stelling II is waar