“IK DENK DAT IK VEILIG WERK, MAAR WEET HET NIET ZEKER”

SECTORRAPPORTAGE 2022 OVER SECURITY- EN PRIVACY-AWARENESS IN ONDERWIJS EN ONDERZOEK

BDO

SURF

SAMENVATTING

In opdracht van SURF heeft BDO voor het tweede jaar op rij security- en privacy-awarenessmetingen uitgevoerd bij onderwijs- en onderzoeksinstellingen. De metingen bestonden uit online vragenlijsten voor de medewerkers. De vragenlijsten werden in het voorjaar van 2022 verspreid binnen de 26 deelnemende instellingen. In totaal hebben ruim 4.500 respondenten de vragenlijst ingevuld. Na afloop ontvingen de instellingen een rapportage met bevindingen en aanbevelingen. Voor deze sectorrapportage, een overkoepelende analyse van de metingen, zijn ook interviews gehouden.

De basis van de metingen is het COM-B gedragsmodel van Susan Michie. Volgens dit model is het om een gedragsverandering tot stand te brengen nodig dat mensen bekwaam en gemotiveerd zijn en gefaciliteerd worden.

Uit de metingen komt allereerst naar voren dat de respondenten overtuigd zijn van het belang van security en privacy, maar beperkt gemotiveerd zijn om hiermee aan de slag te gaan. Verder is een krappe minderheid van de respondenten tevreden met de ondersteuning die zij van instellingen op deze thema's krijgen. Veel respondenten zeggen dat het onduidelijk is wat hun instelling precies van medewerkers verwacht op het gebied van security en privacy en dat hun leidinggevenden hier geen actieve rol in spelen. Deelnemen aan awarenesstrainingen is meestal niet verplicht. Een deel van de respondenten zou beter ondersteund willen worden met instructies, software, tools en andere middelen.

Een andere bevinding is dat de acht toetsvragen van de meting gemiddeld door een krappe meerderheid goed beantwoord zijn. De kennis over security en privacy behoeft nog verbetering. Tot slot is ondersteunend personeel meer bewust dan docenten en onderzoekers.

Op basis van de bevindingen en conclusies adviseren wij instellingen om duidelijk te maken aan medewerkers wat de verwachtingen zijn wat betreft informatieveilig en privacybewust werken. Doe dit middels heldere en praktische richtlijnen. Verder adviseren we om barrières voor veilig werken verder te onderzoeken en – indien mogelijk – weg te nemen. Bij het ontwikkelen van awareness-instrumenten is het van belang om goed aan te sluiten bij de risico's en dagelijkse werkzaamheden van de betreffende doelgroep. Een training dient relevant te zijn voor de ontvanger. De volgende thema's verdienen hierbij aandacht: wachtwoorden, phishing, social engineering, datalekken, beveiligd thuisnetwerk, ict-tools, verwerken persoonsgegevens, privacy en security bij nieuwe diensten en projecten, meldpunten en security- en privacycontactpersonen voor overleg. Onderzoek de mogelijkheden om trainingen verplicht te maken, zodat awareness minder vrijblijvend wordt. En besteed in het awarenessprogramma extra aandacht aan docenten, onderzoekers en leidinggevenden. Het is aan te raden om geregeld het informatieveilige en privacybewuste gedrag van de medewerkers te meten.

INHOUD

1 INLEIDING

"Only amateurs attack machines; professionals target people. And any solution will have to target the people problem, not the math problem."
(Bruce Schneier, internationaal gerenommeerd security-expert)

De dagelijkse handelingen op het werk van docenten, onderzoekers, HR-adviseurs, secretaresses en andere medewerkers, zijn van cruciaal belang voor de digitale weerbaarheid van onderwijs- en onderzoeksinstellingen. Want: 85% van de beveiligingsinbreuken ontstaat door menselijk gedrag[1]. Medewerkers klikken op phishing e-mails, vullen hun inloggegevens in op malafide sites of worden misleid om een valse factuur te betalen. CISO's van onderwijs- en onderzoeksinstellingen zien dan ook 'weinig awareness' van medewerkers als een van de grootste kwetsbaarheden binnen hun organisatie[2]. En de Inspectie van het Onderwijs noemt het 'vergroten van bewustzijn' als eerste standaard voor bestuurders om de cyberweerbaarheid van de sector te verhogen[3]. Genoeg reden om blijvend aandacht te besteden aan de menselijke kant van digitale weerbaarheid.

Voor de tweede maal heeft BDO in opdracht van SURF security- en privacy-awarenessmetingen uitgevoerd bij onderwijs- en onderzoeksinstellingen. Met deze metingen willen we op drie niveaus inzicht bieden. In de eerste plaats voor de individuele respondent, die feedback krijgt op de door hem of haar ingevulde vragenlijst. Ten tweede ontvangt de deelnemende instelling een rapport met bevindingen en aanbevelingen en tot slot is er deze sectorrapportage, met bevindingen die voor de hele sector gelden.

Over de auteurs

Voor het verbeteren van awareness heeft SURF de afgelopen jaren samen met de aangesloten instellingen een toolkit met awareness-materiaal ontwikkeld onder de noemer Cybersave Yourself (CSY). Ook wordt al jaren kennis en materiaal gedeeld binnen de community SCIPR, de SURF Community voor Informatiebeveiliging en PRivacy. Afgelopen jaar (2021) is vanuit die community een werkgroep awareness opgericht waarin 30 onderwijs- en onderzoeksinstellingen maandelijks informatie en materiaal met elkaar delen om hun awarenesscampagnes te verbeteren. In de komende jaren zal SURF extra capaciteit en kennis inzetten om instellingen te helpen bij het verbeteren van hun awarenessmateriaal. Hier speelt ook het op te richten Security Expertise Centrum[4] een belangrijke rol in.
Charlie van Genuchten is product manager bij SURF, met als specialisaties cybercrisismanagement en awareness.

BDO ondersteunt organisaties bij het versterken van hun digitale weerbaarheid. Hiervoor heeft de organisatie een integrale aanpak ontwikkeld, die bestaat uit het uitvoeren van assessments rond kwetsbaarheden en risico's, het implementeren van cybersecurity- en privacy-standaarden, het testen en monitoren van de IT-infrastructuur en het ondersteunen bij cyberincidenten. Daarnaast heeft BDO zich gespecialiseerd in het realiseren van gedragsveranderingen bij medewerkers.
Marijke Stokkel is werkzaam binnen het team Cybersecurity en trekker van de propositie security & privacy awareness.

1 Verizon Data Breach Investigations Report 2021
2 SURF Cyberdreigingsbeeld onderwijs en onderzoek 2021-2022
3 Inspectie van het Onderwijs, rapport 'Binnen zonder kloppen'
4 Security Expertise Centrum

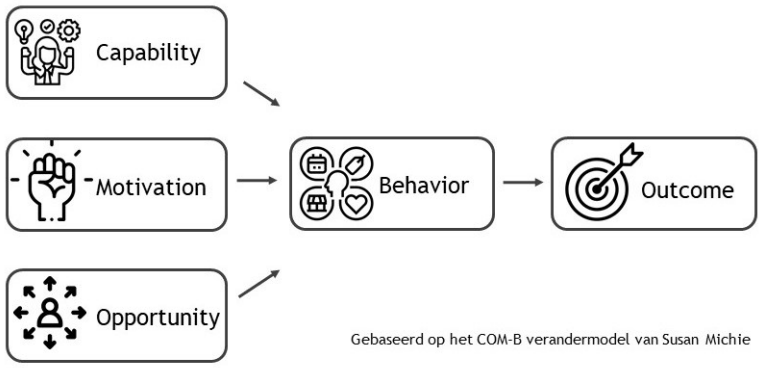
2 AANPAK METINGEN

In het voorjaar 2022 hebben we 26 security- en privacy-awarenessmetingen uitgevoerd bij onderwijs- en onderzoeksinstellingen. Na een oproep via de SCIPR-mailinglijst van SURF hebben zich 30 instellingen aangemeld, waarvan er vier tussentijds afhaakten. In dit hoofdstuk beschrijven we de aanpak van de metingen. We behandelen het gedragsmodel dat als basis van de metingen fungeerde, de centrale onderzoeksvragen, de werkwijze en tot slot vergelijken we de aanpak met die van vorig jaar.

Gedragsmodel

Om informatieveilig en privacybewust gedrag in kaart te brengen maakten we net als vorig jaar gebruik van het COM-B gedragsmodel van Susan Michie. Dit model stelt dat bekwaamheid (capability), gelegenheid (opportunity) en motivatie (motivation) aanwezig moeten zijn om gedrag (behavior) te laten plaatsvinden.

Figuur 1 **COM-B gedragsmodel**



Gebaseerd op het COM-B verandermodel van Susan Michie

Vaak zijn deze componenten met elkaar verweven. Als mensen de juiste competenties hebben en goed gefaciliteerd worden, is de kans groot dat zij ook meer gemotiveerd raken om zorgvuldig met vertrouwelijke gegevens om te gaan. Door deze componenten alle drie te adresseren, en oog te hebben voor hun onderlinge afhankelijkheid, verhoog je de kans op een succesvolle gedragsinterventie.

Bekwaamheid heeft betrekking op de juiste kennis en vaardigheden om de verandering te kunnen uitvoeren. Dit gaat bijvoorbeeld over het herkennen van risicovolle situaties, weten wat te doen bij een datalek, een sterk wachtwoord kunnen opstellen en in staat zijn om phishing e-mails te herkennen.

- Bij **motivatie** draait het om de (intrinsieke) motivatie van de medewerkers om informatieveilig en privacybewust te werken. Willen zij zich daar uit eigen overtuiging voor inzetten, of doen ze dat vooral omdat ze bang zijn voor negatieve consequenties?
- **Gelegenheid** gaat over het faciliteren van medewerkers om veilig te werken. Medewerkers hebben de juiste middelen, zoals software/tooling, heldere richtlijnen en ondersteuning van de leidinggevende nodig. Veilig werken moet zo makkelijk mogelijk worden gemaakt, zonder veel extra handelingen en andere barrières.

Vraagstelling

De vragen van de meting sluiten aan bij het gedragsmodel dat we hanteren en luiden als volgt:

- In hoeverre kunnen medewerkers informatieveilig en privacybewust werken?
- In hoeverre willen medewerkers informatieveilig en privacybewust werken?
- In hoeverre worden medewerkers in staat gesteld om informatieveilig en privacybewust te werken?

We hebben er – net als vorig jaar – voor gekozen om zowel security als privacy te adresseren in de metingen. Dit omdat er een grote overlap tussen beide thema's is met betrekking tot het wenselijke gedrag van medewerkers.

Begrippen

- Met **privacybewust werken** bedoelen we dat medewerkers tijdens hun werk zorgvuldig omgaan met gegevens van studenten, respondenten, medewerkers of andere betrokkenen. Bijvoorbeeld: voor een onderzoeks- of onderwijsproject verzamelen medewerkers alleen persoonsgegevens als ze hier een grondslag en specifiek doel voor hebben. Ook verwerken ze niet méér gegevens dan strikt noodzakelijk. Ze delen uitsluitend persoonsgegevens met partijen die deze mogen ontvangen, doen dat via veilige kanalen en zorgen ervoor dat de gegevens niet bij de verkeerde ontvanger terecht komen. Mocht er toch een fout zijn gemaakt, dan weten ze waar ze dat kunnen melden en doen dat ook direct.
- **Informatieveilig werken** betekent dat medewerkers tijdens hun werk (vertrouwelijke) informatie beschermen tegen toegang of ontregeling door onbevoegden. Het houdt in dat medewerkers alert zijn op informatie-beveiligingsrisico's en volgens een minimale beveiligingsstandaard werken. Voorbeelden zijn: sterke wachtwoorden creëren en voor elk account een ander wachtwoord instellen, alert zijn op phishing bij het openen van mails en sms'jes, veilige kanalen gebruiken om informatie op te slaan en te delen met anderen, via een veilige (wifi-)verbinding het internet op gaan, extra alert zijn met zeer vertrouwelijke gegevens en beveiligingsincidenten en datalekken herkennen en direct melden.

Doelgroepen

Binnen de metingen hebben we gekeken naar de verschillende functiegroepen, waarbij we de volgende onderverdeling hebben gemaakt:

- onderwijs/onderzoek
- ondersteunend
- bibliotheek
- overig

Werkwijze

De metingen zijn uitgevoerd via een online vragenlijst en interviews.
De vragenlijst is geschikt om een globaal inzicht te krijgen in het (zelf-gerapporteerde) gedrag en de kennis, de mening en ervaringen van een grote groep mensen. De interviews zorgen voor extra duiding en diepgang.

De online vragenlijst, die is opgesteld in afstemming met het awarenessteam van de SCIPR-community van SURF, bevat meningvragen en quizvragen.
De meningvragen zijn om te achterhalen hoe gemotiveerd de medewerkers zijn om veilig te werken, en hoe goed ze daartoe worden gefaciliteerd.
De quizvragen toetsen privacy- en securitykennis van de respondenten.
De respondenten krijgen na het invullen van de meting direct terugkoppeling over hun quizresultaten, met advies voor (verdere) verbetering. Op deze wijze is de awarenessmeting een awarenessinterventie en meetinstrument in één.

Er zijn in totaal 8 interviews gehouden met 14 medewerkers, bij vijf instellingen.
De vragenlijsten zijn in maart en april uitgezet bij 26 instellingen. In totaal zijn er 4.524 vragenlijsten ingevuld. De interviews vonden plaats in april en mei.

Vergelijking aanpak 2021

In 2021 heeft BDO ook in opdracht van SURF, awarenessmetingen uitgevoerd, en is er tevens een sectorrapportage opgesteld. Op basis hiervan is er dit jaar een aantal wijzigingen doorgevoerd:
De metingen worden niet alleen via een online vragenlijst, maar ook via interviews gehouden;

- Een aantal vragen van de online vragenlijst is aangescherpt.
  - De vragen ten aanzien van het component 'motivatie' zijn uitgebreid en aangescherpt en gaan specifieker in op de redenen *waarom* mensen cyberveilig werken. Doen ze dat vooral omdat het verplicht of noodzakelijk is, of ook omdat ze interesse hebben in de thema's en hier uit zichzelf mee bezig willen gaan?
  - Het component 'bekwaamheid' bevat toetsvragen en deze zijn ook aangepast. Anders zou het voor respondenten die de vragenlijst vorig jaar ook ingevuld hebben, erg eenvoudig zijn om ze goed te beantwoorden.

Verder is de groep respondenten dit jaar niet geheel vergelijkbaar met die van vorig jaar. Een deel van de instellingen deed dit jaar voor het eerst mee en van de instellingen die vorig jaar ook deelnamen, is niet bekend of hiervan ook dezelfde respondenten de vragenlijst hebben ingevuld.

Deze punten samen maken het lastig om een precieze vergelijking met de sectorrapportage van vorig jaar te maken. In hoofdstuk 5 zullen we hier toch een poging toe doen, maar meer in globale en beschrijvende zin.

Maatstaf

In onze optiek dienen instellingen een minimale awareness-totaalscore van 7 of hoger te ambiëren. Je zou kunnen zeggen dat de medewerkers dan gemiddeld redelijk weerbaar zijn tegen mensgerichte cyberaanvallen en security-incidenten. Aangezien cyberaanvallers maar een enkele mogelijkheid nodig hebben – één medewerker die klikt op een phishing e-mail – om flinke schade aan te richten, raden wij aan om een awareness-score van 7,5 na te streven (wenselijke score).
Deze maatstaf komt overeen met de maatstaf van vorig jaar. Hierbij moet wel opgemerkt worden dat de scores slechts een globale indicatie geven. Ze zijn een vertaling van een aantal meetpunten en geven geen context of duiding over het gehele thema security- & privacy-awareness. Het is verstandig om de scores in samenhang met de (overige) bevindingen en conclusies te bekijken.

Leeswijzer

Deze rapportage over de security- en privacy-awareness in onderwijs en onderzoek bevat vier onderdelen. Het eerste onderdeel bestaat uit bevindingen. Dit zijn de resultaten per component, per doelgroep en in cijfers, en verbeterpunten die respondenten aandragen (hoofdstuk 3 en 4). Het tweede onderdeel is een vergelijking met de awarenessmetingen vorig jaar (hoofdstuk 5). Het derde onderdeel bestaat uit conclusies (hoofdstuk 6) en het vierde onderdeel, tot slot, bevat aanbevelingen (hoofdstuk 7).

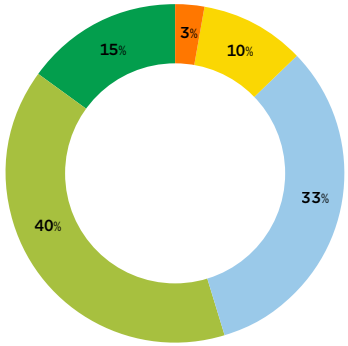
3 RESULTATEN

In dit hoofdstuk staan de resultaten per component, per doelgroep en in cijfers.

3.1 Motivatie

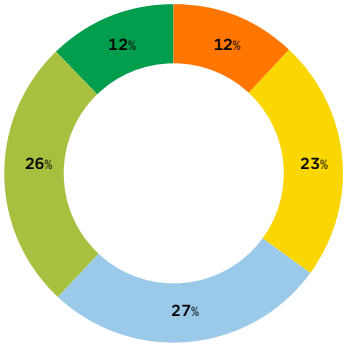
Respondenten zeggen dat goede security en privacy essentieel zijn voor hun instelling. Ze weten dat cyberaanvallen en datalekken veel schade kunnen aanbrengen en vinden het belangrijk dat er goede maatregelen worden genomen. Een meerderheid van de respondenten zegt actief bezig te zijn met security en privacy: 55% van de respondenten spendeert hier naar eigen zeggen veel of zeer veel tijd aan.

Hoeveel aandacht besteed jij over het algemeen tijdens je werk aan privacy en informatiebeveiliging?



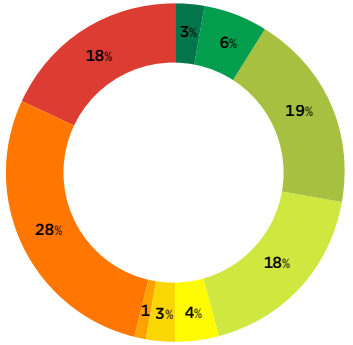
- Helemaal geen
- Weinig
- Neutraal
- Veel
- Zeer veel

Stelling: *Uit persoonlijke interesse volg ik nieuwe ontwikkelingen op het gebied van privacy en informatiebeveiliging.*



- Helemaal oneens
- Oneens
- Neutraal
- Eens
- Helemaal eens

Waarom besteed jij tijdens je werk aandacht aan privacy en informatiebeveiliging?



- Ik vind het leuk en interessant
- Ik wil me graag bekwamen in privacy en ib
- Het is nodig om mijn werk goed uit te voeren
- Het is nodig om de instelling digitaal weerbaarder te maken
- Het is eenvoudig en niet tijdrovend
- Ik word goed ondersteund door de organisatie
- De directie van de instelling vindt het belangrijk
- Ik zou me schamen als ik een incident zou veroorzaken
- Het is verplicht

De deelnemers aan het onderzoek lijken vooral veilig te werken omdat het moet, niet omdat ze interesse hebben in het thema cybersecurity. Met de stelling: ‘uit persoonlijke interesse volg ik nieuwe ontwikkelingen op het gebied van privacy en informatiebeveiliging’ is slechts 38% van de respondenten het eens of helemaal eens. Weinigen gaan dus uit zichzelf actief aan de slag met dit thema. En op de vraag ‘waarom besteed je tijdens je werk aandacht aan privacy en informatiebeveiliging?’ is het meest genoemde antwoord: “ik zou me schamen als er door mij een incident of datalek zou ontstaan”.

“De (online) wereld verandert heel snel naar een plek waar privacy en informatiebeveiliging enorm belangrijk is. Zowel voor mij als persoon als voor de instelling waarvoor ik werk.”

Deze ambivalente houding zien we terug in de toelichtingen in de open tekstvakken van de vragenlijst. Veel respondenten zeggen dat ze zich (nog) niet in de security en privacy richtlijnen van hun instelling hebben verdiept. Dat ze al zoveel op hun bord hebben, en er niet aan toe komen om er actief mee aan de slag te gaan. En dat ze bij het werken met gevoelige gegevens vooral varen op hun gezonde verstand. Anderen vertrouwen erop dat de instelling het goed geregeld heeft. Daarnaast geven sommigen eerlijk toe dat ze er gewoon geen zin in hebben om met security en privacy aan de slag te gaan.

"Het is belangrijk je te wapenen tegen cybercriminaliteit maar ik vind het niet leuk. Sterker nog, ik vind het vervelend."

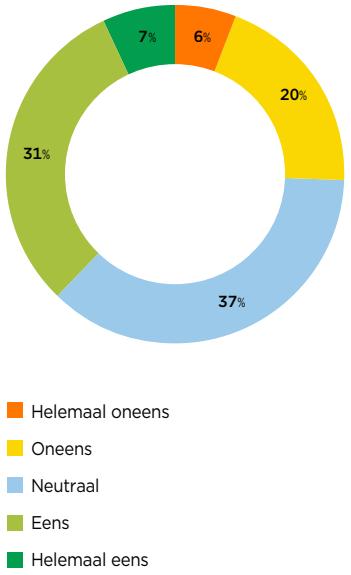
3.2 Gelegenheid

Onderwijs- en onderzoeksinstellingen zijn anders dan banken of multinationals. Het zijn open leeromgevingen, met als doel om kennis te delen. Er worden weinig zaken verboden of verplicht gemaakt en dat is ook nodig om academische vrijheid en kennisdeling te bewerkstellingen. Dit staat echter op gespannen voet met het realiseren van digitale weerbaarheid[5]. Instellingen leveren in de regel matige sturing en ondersteuning aan hun medewerkers om informatieveilig en privacybewust te werken. Het is bijvoorbeeld niet duidelijk wat instellingen precies van medewerkers verwachten. Slechts 38% van de respondenten is het (helemaal) eens met deze stelling 'de regels en richtlijnen voor privacybewust en informatieveilig werken zijn duidelijk voor mij'. Respondenten zeggen dat er – voor zover zij weten – geen richtlijnen zijn. Of, als ze er wel zijn, ze niet weten waar ze die kunnen vinden. En als de richtlijnen wel vindbaar zijn, ze niet praktisch toepasbaar zijn.

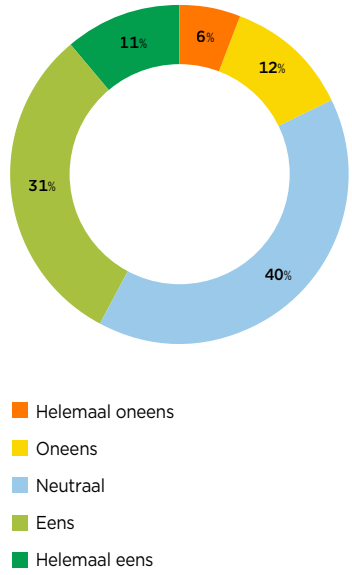
"Ik ken de regels eigenlijk niet, maar ik ga er ook niet actief naar op zoek."

5 Cyberveiligheid in het onderwijs [kamerbrief], Ministerie van Onderwijs, Cultuur en Wetenschap, 14-2-2020

Stelling: *De regels en richtlijnen voor privacybewust en informatieveilig werken zijn duidelijk voor mij.*



Stelling: *Mijn leidinggevende geeft mij het juiste voorbeeld als het gaat om privacybewust en informatieveilig werken.*



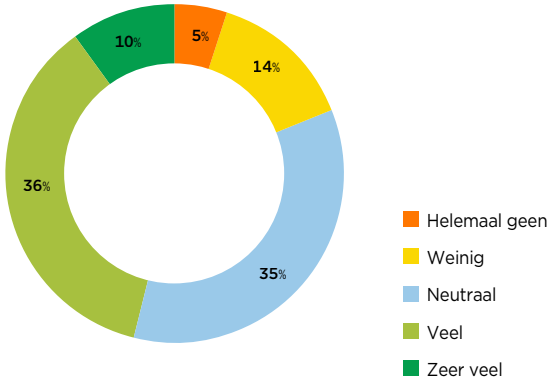
Leidinggevenden houden zich doorgaans niet actief bezig met security en privacy. Een minderheid van de respondenten is het (helemaal) eens met de stelling dat de leidinggevende het juiste voorbeeld geeft met betrekking tot informatieveilig en privacybewust werken. Bij navraag zeggen veel respondenten dat security en privacy geen onderwerpen van gesprek zijn op het werk en dat de leidinggevende hier geen actieve aandacht aan besteedt. Dat ze informatie over security en privacy nooit van hun leidinggevende, maar eerder van de ict-afdeling of security officer ontvangen. Sommigen zeggen dat zij per toeval achter relevante informatie moeten komen. *"Ik zet mijn spullen op OneDrive of Teams. Wat ik laatst toevallig hoorde: voor hooggevoelige informatie is dat niet veilig genoeg. Je moet andere programma's gebruiken. Ik heb daar geen idee van. Dat wordt niet aangeboden. Ik word hier niet op aangesproken. Als je niet zelf op zoek gaat, gebeurt er niets."*

"Voor wat betreft de vraag over mijn leidinggevende: ik weet echt niet of hij het juiste voorbeeld geeft. We hebben het nooit over dit onderwerp, dus geen idee."

Gebrekkige ondersteuning blijkt ook uit de constatering dat de meeste instellingen geen verplichte awarenesstraining hebben, en dat er vanuit de instelling of leidinggevende veelal geen opvolging aan de richtlijnen gegeven wordt. Er vindt geen handhaving plaats en consequenties als men niet volgens de richtlijnen werkt, blijven uit. Veel respondenten denken dat dit laatste ook weinig zin zal hebben. *"Volgens mij houdt iedereen een eigen archief(je) bij en kan daar nauwelijks enige controle op worden uitgevoerd."* Wanneer security-maatregelen wel worden afgedwongen, is er ook kritiek van respondenten. Dit geldt bijvoorbeeld bij een strikte toepassing van multifactorauthenticatie of maatregelen om mobiele apparaten te beveiligingen.

"Op papier zijn de regels duidelijk, in de praktijk lang niet altijd praktisch uitvoerbaar. Dan moet je keuzes maken en dat leidt soms tot onduidelijkheid."

Stelling: *Ik word goed gefaciliteerd om privacybewust en informatieveilig te kunnen werken (bijvoorbeeld door software, tools, instructies, en andere middelen).*



Tot slot vindt slechts een minderheid van de respondenten dat zij goed gefaciliteerd worden met software, tools, instructies en andere middelen. Een aantal medewerkers is positief over wat hun instelling doet. Zij roemen onder andere de maatregelen die hun instelling neemt met betrekking tot multifactorauthenticatie, VPN, trainingen en versleuteling van devices. Ook zijn ze blij met voorzieningen die SURF aanbiedt, zoals SURFfilesender. Eén van de respondenten verwoordt het als volgt: *"Teams, OneDrive en 2-factor: ik ben fan."* Veel anderen zeggen dat zij niet weten of ze goed ondersteund worden, wat een goede ondersteuning zou moeten inhouden en of zij die krijgen. Ze weten nu ook niet of ze veilig werken, zij hebben hiervoor onvoldoende kennis van het thema. Anderen zeggen dat ze graag kwalitatief beter ondersteund willen worden.

Respondenten vertellen over barrières die het werken minder veilig maken. Hier volgt een aantal voorbeelden, die niet voor elke instelling in dezelfde mate zullen gelden.

"Ik ben niet bewust hoe ik word gefaciliteerd. Wellicht word ik dat wel, maar ik heb geen idee hoe."

De aangeboden tooling sluit niet aan bij de werksituatie en wensen van medewerkers

- De functionaliteiten van de elektronische leeromgeving (ELO) of learning managementsysteem (LMS) sluiten niet geheel aan bij de behoeften van de docenten. Het is in sommige gevallen niet mogelijk om informatie per klas of groep bij te houden. Docenten maken daarom apart lijstjes in Word/Excel en verspreiden deze via mail.
- Tools, zoals datamanagement voor onderzoek, sluiten niet goed aan bij de werkzaamheden van een aantal onderzoekers en daarom worden er (onveilige) workarounds bedacht.
- OneDrive ondersteunt samenwerking met andere instellingen volgens respondenten onvoldoende. Samenwerken in een gedeelde omgeving gaat moeizaam. Ze wijken daarom uit naar Dropbox.

- Bronsystemen sluiten niet goed op elkaar aan, waardoor het nodig is om exports in Excel te maken om goed te kunnen werken. Dit brengt risico's met zich mee omdat de exports vaak per e-mail gedeeld en op meerdere locaties opgeslagen worden.

"De instelling biedt ontzettend veel software/tooling aan om privacybewust te werken, maar je moet het wel weten. Ik ken nog veel collega's die gerust met Dropbox werken, of eindeloos lang persoonsgegevens bewaren in excelletjes."

Het ontbreekt aan tooling om goed en veilig te kunnen werken

- De instelling biedt geen geschikte tools aan om onderwijs interactiever te maken. Docenten nemen daardoor zelf accounts op bijvoorbeeld Mentimeter, Padlet en Kahoot.
- Veilige opslag van onderzoeksdata en veilige onderzoekstools zijn niet geregeld voor studenten.
- Het ontbreekt aan tooling om veilig wachtwoorden op te slaan (passwordmanager).
- Er zijn te veel verschillende systemen waar (gevoelige) informatie wordt opgeslagen.

Werkprocessen zijn niet veilig ingericht

- Er is geen eenduidige werkwijze voor het ontwikkelen van toetsen, waardoor er geen inzicht is in het aantal locaties waar (concept-)toetsen zijn opgeslagen en het aantal mensen dat hier toegang tot heeft.
- De instelling zendt de (theoretische) regels, maar denkt niet mee over concrete situaties. Er is bijvoorbeeld alleen aandacht voor wetenschappelijk onderzoek en studentenprivacy, maar niet voor het veilig verwerken van beleidsgegevens.
- Het toekennen en intrekken van rechten is een omslachtig proces. In de praktijk wordt bij het wisselen van rol vaak vergeten om rechten weg te halen.
- Te veel medewerkers hebben toegang tot studentgegevens.

De gebruikte communicatiekanalen voldoen niet

- Instellingen communiceren nieuwe informatie via de centrale nieuwsbrief en verwachten dat medewerkers dan op de hoogte zijn. Veel medewerkers zien de nieuwsbrief echter niet als primaire informatievoorziening, ze lezen deze slechts af en toe en doen dat niet grondig.
- Informatie over privacy en security op intranet is vaak moeilijk vindbaar.

Securityregels bemoeilijken het dagelijkse werkproces

- Door de extra beveiligde werkomgeving voor telefoons kan de werkmail niet meer op een privé-telefoon worden geopend.
- Het automatisch forwarden van e-mail is niet toegestaan, waarvan sommigen zeggen dat het ongemakkelijk is en de veiligheid niet verbetert.

3.3 Bekwaamheid

De vragenlijst van de awarenessmeting bevat acht toetsvragen. Elke vraag is gemiddeld door 57,5% van de respondenten juist beantwoord. Het merendeel van de respondenten gaf op drie van de acht vragen een foutief antwoord. Het betreft de volgende vragen:

1 **Welk van de onderstaande situaties is geen datalek?**
   - **a** Het klikken op een link in een spam-mail.
   - **b** Een ict-storing waarbij het studenteninformatiesysteem (zoals OSIRIS of SIS) een dag niet beschikbaar is.
   - **c** Een e-mail over een open dag naar 100 aankomende studenten, met alle ontvangers in de cc ipv de bcc.

Deze vraag is door 91% van de respondenten onjuist beantwoord. Het juiste antwoord is *a Het klikken op een link in een spam-mai*l. Waarschijnlijk verwarden de meeste respondenten spam-mail (ongewenste reclame die

in bulk wordt verstuurd) met een phishing mail (valse mails waarbij een internet-crimineel je probeert op te lichten) en zijn ze zich niet bewust dat het niet-beschikbaar zijn van systemen met persoonsgegevens ook een datalek is. Het is een lastige vraag, maar het is wel belangrijk dat medewerkers weten welke situaties datalekken zijn, zodat ze die kunnen herkennen en daarop kunnen acteren.

2 Welk van deze wachtwoorden is het sterkst?

a P_&k@q
b QWERTY123
c FietsstallingGerbilBoeken

Voor 71% van de respondenten bleek deze vraag te moeilijk. Ze veronderstelden waarschijnlijk dat het belangrijkste kenmerk van een sterk wachtwoord de mate van complexiteit is. Dus: hoe meer verschillende leestekens, hoe beter. En dit terwijl het vooral om de lengte van het wachtwoord gaat. Het juiste antwoord was dus *c FietsstallingGerbilBoeken*. Volgens de wachtwoordkraaktest op de website Veilig Internetten is *'P_&k@q'* binnen een minuut gekraakt, en *'FietsstallingGerbilBoeken'* pas na '18 quintiljoen jaar'. Aangezien wachtwoorden, ondanks securitybezwaren, nog steeds een noodzakelijk authenticatiemiddel zijn voor de meeste digitale diensten, is kennis over het creëren van sterke wachtwoorden onontbeerlijk voor cyberbewuste medewerkers.

3 Waarom is de kwetsbaarheid in Log4j zo gevaarlijk?

a Er is nog geen patch voor beschikbaar.
b Organisaties weten vaak niet welke applicaties gebruik maken van Log4j.
c Het heeft effect op alle applicaties in een organisatie.

Een krappe meerderheid (51%) heeft deze vraag fout geantwoord. Misschien is Log4j geen onderdeel van de dagelijkse werkzaamheden van de meeste medewerkers, maar deze kwetsbaarheid "met in potentie de grootste gevolgen (...) voor de hele wereld" aldus SURF in het meest recente Cyberdreigingsbeeld[6], geeft medewerkers relevant inzicht in de wereld van de cybersecurity. Log4j laat zien hoe afhankelijk systemen en organisaties van elkaar zijn en hoe belangrijk het is om een actuele en complete inventarisatie van systemen en applicaties te hebben, om adequaat te kunnen reageren op een kwetsbaarheid. Het juiste antwoord was overigens: *b Organisaties weten vaak niet welke applicaties gebruik maken van Log4j*.

Phishing

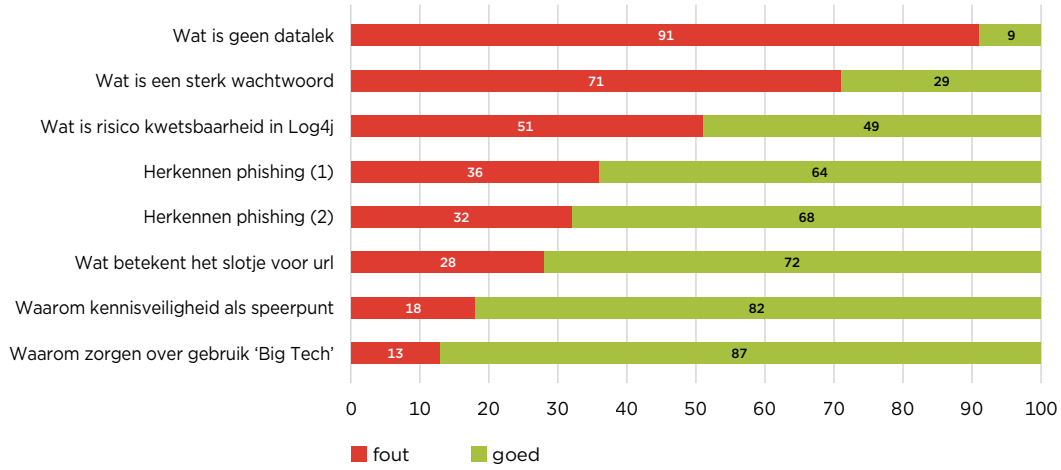
De toets bevatte twee vragen over phishing, waarbij we een sms-bericht en een mail toonden, beide met de vraag of dit phishing was. Deze vragen zijn door ongeveer twee derde van de respondenten goed beantwoord. Dit vinden we een matige score, omdat phishing zo'n groot risico is voor organisaties: phishing is de meest gebruikte eerste stap voor een cyberaanval[7] – en medewerkers kunnen dit risico verminderen door malafide berichten te herkennen.

De volgende vragen werden relatief vaak goed beantwoord:

- De betekenis van het slotje voor een url van een website ('https'); 72% antwoordde juist.
- De reden dat kennisveiligheid een speerpunt is voor onderwijsinstellingen; 82% antwoordde juist.
- De reden dat er zorgen zijn over het gebruik van 'Big Tech' (zoals Google en Microsoft) in het onderwijs; 87% antwoordde juist.

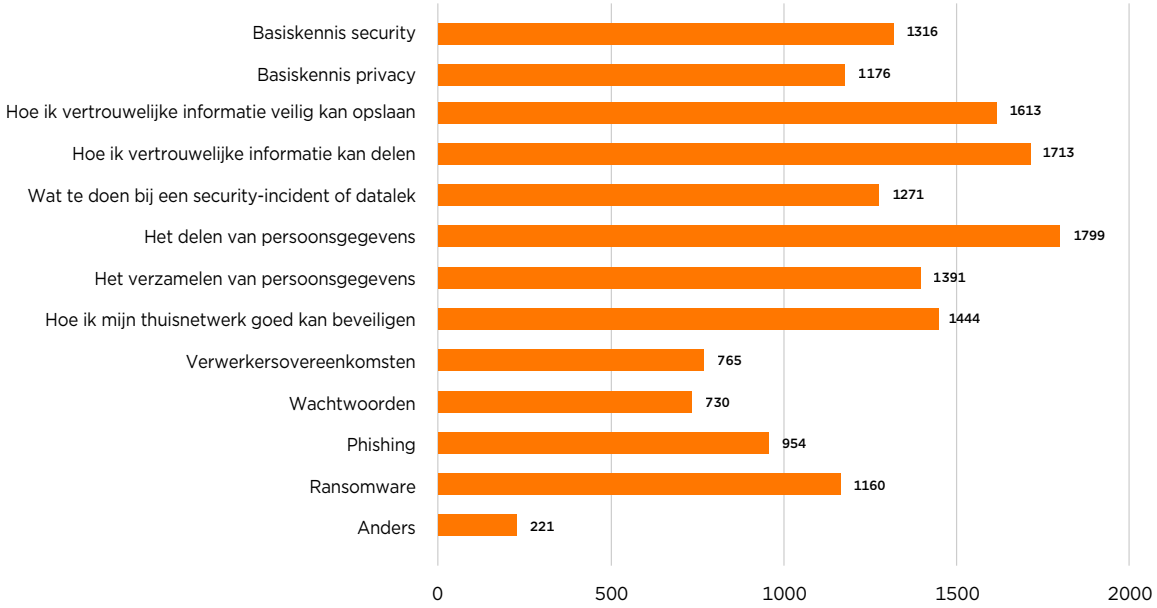
6 SURF Cyberdreigingsbeeld 2021-2022 SURF onderwijs en onderzoek 2021-2022, pdf p15
7 Cybersecuritybeeld-nederland-2020, pdf pagina 18

Resultaten toetsvragen



Tot slot hebben we gevraagd op welke thema's respondenten zichzelf nog niet (geheel) bekwaam achten. Daaruit komt naar voren dat men graag meer kennis opdoet over het opslaan en delen van persoonsgegevens en andere vertrouwelijke informatie, en over het beveiligen van het thuisnetwerk.

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



3.4 Resultaten per doelgroep

Uit de metingen blijkt dat de respondenten in de doelgroepen ‘ondersteuning’, ‘bibliotheek’ en ‘overig’ op alle componenten hoger scoren (6,2) dan docenten en onderzoekers (5,7). Ze zijn gemotiveerder om informatieveilig en privacybewust te werken, ze scoren beter op de toetsvragen en ze worden daar naar eigen zeggen beter in staat gesteld om veilig te werken.

Dat docenten en onderzoekers lager scoren heeft naar ons inzicht drie mogelijke oorzaken: werkdruk, perspectief en de aard van de werkzaamheden. Allereerst de werkdruk. Uit meerdere onderzoeken[8] [9] [10] blijkt dat de ervaren werkdruk bij docenten en onderzoekers van het mbo, hbo en wo hoog tot zeer hoog is. Bij het ondersteunend en beheerspersoneel (OBP) ervaart men gemiddeld minder hoge werkdruk.

Tabel 1 **Medewerkers die de werkdruk als hoog, zeer hoof of te hoog ervaren**

	WP/OP*	OBP**
MBO	55%	31%
HBO	72%	44%
WO	76%	50%

* WP/OP: wetenschappelijk personeel en onderwijspersoneel

** OBP: ondersteunend- en beheerspersoneel

Bron: FNV 2019[11] , FNV 2021[12] , Effectory 2019[13]

Een onderzoeker op een universiteit: *“Je moet het makkelijk maken voor wetenschappelijk personeel. We hebben geen tijd om dingen uit te zoeken. Het klikt verwend, maar we moeten al zoveel.”*

8 Onderzoek FNV 2019
9 Onderzoek FNV 2021
10 Onderzoek Effectory 2019
11 Onderzoek FNV 2019
12 Onderzoek FNV 2021
13 Onderzoek Effectory 2019

Perspectief

Een tweede mogelijke oorzaak sluit hierbij aan en heeft te maken met het perspectief van de medewerkers. We denken dat dat medewerkers in de doelgroep ‘ondersteuning’ eerder dan onderzoekers en docenten security en privacy als onderdeel van hun kerntaken zien. Dit omdat security en privacy ondersteunend zijn aan het primaire proces (onderwijs en onderzoek) en die ondersteunende taken juist voor deze groep de kerntaken zijn. Bij docenten en onderzoekers werkt het juist omgekeerd: zij richten zich op het primaire proces en zien overige onderwerpen mogelijk als iets dat een ander zou moeten oppakken, ook al hoort het formeel ook in hun takenpakket. Of dit echt zo werkt hebben we niet onderzocht, vervolgonderzoek zou dat moeten uitwijzen.

> *“Val medewerkers niet lastig met privacy en informatiebeveiliging. We zijn niet allemaal specialisten op dat gebied. We hebben wel iets anders te doen.”*

Aard werkzaamheden

Tot slot is het voor sommige medewerkers makkelijker om informatieveilig en privacybewust te werken dan voor anderen. Dit heeft te maken met de aard van de werkzaamheden. Enerzijds zijn er medewerkers met afgebakende taken, met heldere verwachtingen en waarbij een zekere mate van uniformiteit of voorspelbaarheid aanwezig is. Zij werken met ict die goed aansluit bij hun werkzaamheden. Voor hun werk zijn de verwachtingen duidelijk, er kunnen gemakkelijk specifieke richtlijnen opgesteld worden en zij kunnen goed uit de voeten met de software/tooling die ze aangeboden krijgen van de instelling. Denk aan medewerkers salarisadministratie, die veelal werken binnen duidelijke kaders en met een computersysteem dat hun handelingen stap voor stap ondersteunt. Aan de andere kant zijn er medewerkers met meer variëteit in de werkzaamheden. Zij hebben meestal geen gedetailleerde taakomschrijving, omdat er meer onvoorspelbaarheid is. Zij werken bijvoorbeeld samen met veel verschillende partners of met nieuwe soorten vertrouwelijke informatie. Bestaande richtlijnen van de instelling passen vaak niet goed bij de dagelijkse werkzaamheden van deze medewerkers. Ook de aangeboden tooling sluit

veelal niet goed aan bij de werkzaamheden, waardoor olifantenpaadjes worden gecreëerd. Dit geldt bijvoorbeeld voor onderzoekers die werken in internationale consortia en regelmatige nieuwe onderzoeksprojecten opstarten. Mogelijk worden in die consortia met andere samenwerkingstools gewerkt dan de instelling voorschrijft (denk aan Dropbox).

Dit onderscheid tussen medewerkers met 'vaste' werkzaamheden en medewerkers met 'variërende' werkzaamheden komt grotendeels, maar niet exact overeen met het verschil tussen docenten/onderzoekers enerzijds en ondersteunend personeel anderzijds. Beleidsmedewerkers hebben in de regel ook een meer variërend takenpakket, terwijl ze toch OBP zijn. Voor dit onderzoek spraken we een medisch onderzoeker die volgens strikte richtlijnen haar onderzoek uitvoert en daarbij nauwkeurig de privacy- en securityregels volgt, ook al behoort ze tot het wetenschappelijk personeel. Docenten bevinden zich ergens in het midden: ze werken redelijk volgens een eenduidig werkproces, maar bestaande IT ondersteunt velen niet optimaal. Hierdoor maken sommigen de keuze om zelf tools aan te schaffen of exports uit bronsystemen te maken.

3.5 Resultaten in cijfers

Er hebben 26 instellingen deelgenomen aan de metingen, met in totaal 4.524 ingevulde vragenlijsten. We gaan ervan uit dat één ingevulde vragenlijst gelijk staat aan één respondent.

Totaalscore

Op basis van de ingevulde vragenlijsten ontvangt elke deelnemende instelling een totaalscore (1-10). Het gemiddelde van alle 4.524 respondenten, de benchmark totaalscore, is een 5,9. Dit resultaat is flink lager dan de minimale score (7,0) en de wenselijke score (7,5), zoals geformuleerd als maatstaf in hoofdstuk 2. Slechts twee deelnemende instellingen voldoen aan de minimale score, geen enkele aan de wenselijke score.

14 SURF Cyberdreigingsbeeld onderwijs en onderzoek 2021-2022, p18

Tabel 2 **De awarenessmetingen in aantallen**

Categorie	Sub-categorie	Aantal
Aantal ingevulde vragenlijsten		4.524
Aantal deelnemende instellingen		26
Aantal respondenten voor de vragenlijst per functiegroep:		
	onderwijs/onderzoek	1.961
	ondersteuning	2.290
	bibliotheek	84
	overig	170
Aantal interviews		8
Aantal geïnterviewden		14
Aantal deelnemende instellingen per sector:		
	hbo	9
	wo	8
	mbo	6
	overig	3

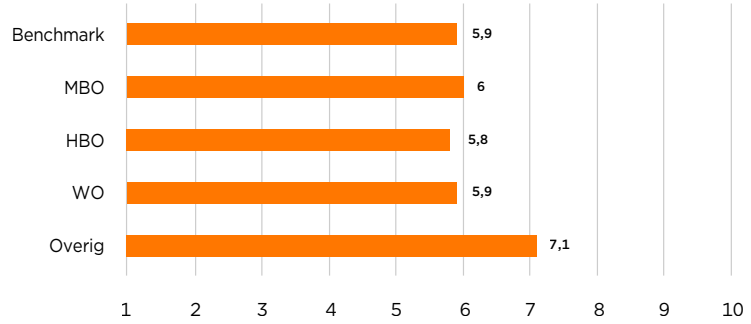
Ondanks de aangescherpte vragenlijst hebben we er toch voor gekozen om de awareness-maatstaf gelijk te houden. De security- en privacy-dreigingen nemen alleen maar toe en de aanvallers worden ook steeds professioneler en inventiever[14], dus het is niet onredelijk om eens steeds hoger niveau van digitale weerbaarheid te verwachten.

De totaalscores van de deelnemende instellingen liggen aardig dicht bij elkaar. De standaarddeviatie, de gemiddelde afwijking van het gemiddelde is 0,47, en dat is redelijk klein.

Scores per sector

Als we kijken naar de scores per sector, valt op dat de resultaten niet ver uit elkaar liggen, op de categorie ‘overig’ na. Deze categorie, die drie (bij SURF aangesloten) instellingen met in totaal 470 respondenten behelst, scoort een stuk hoger dan de overige sectoren.

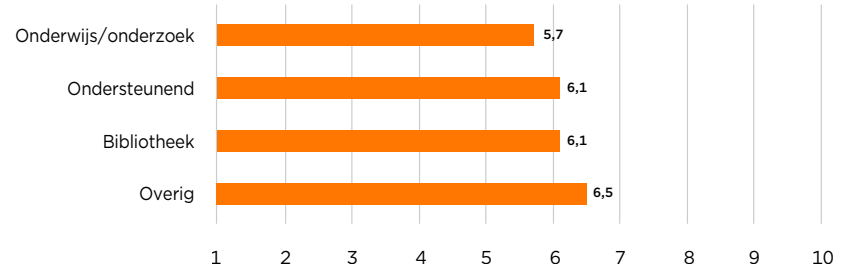
Figuur 2 **Benchmarkscore per sector**



Scores per functiegroep

Bij de functiegroepen zien we, zoals ook besproken in het vorige hoofdstuk, dat onderwijs en onderzoek lager scoren dan de overige functiegroepen.

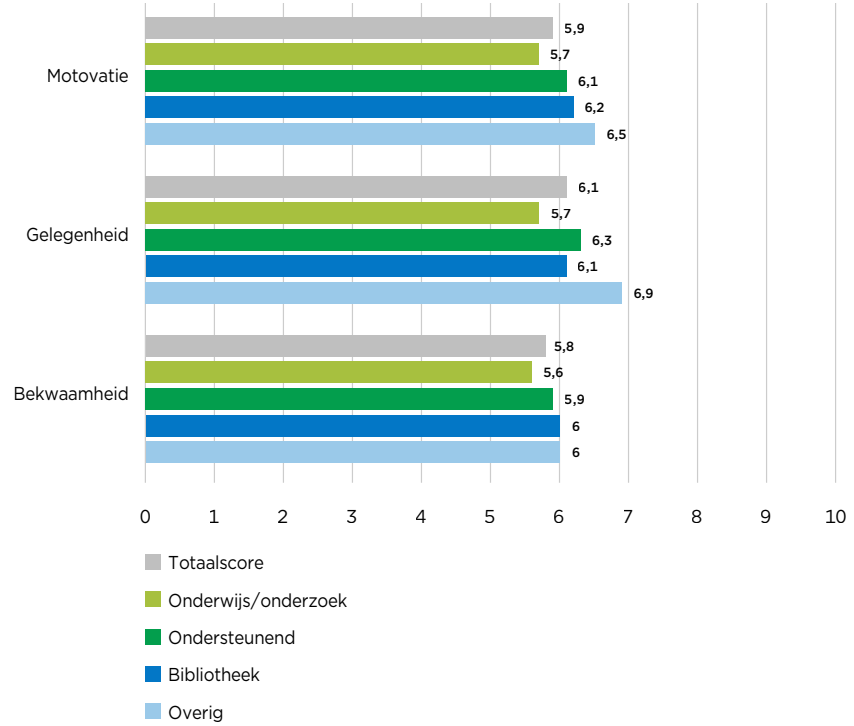
Figuur 3 **Benchmarkscore per functiegroep**



Componentscores

De totaalscores van de instellingen worden vastgesteld door het gemiddelde van de drie componentscores. Elk component (motivatie, gelegenheid, bekwaamheid) telt even zwaar mee. In deze paragraaf kijken we naar de scores per component (per functiegroep). Wat opvalt is dat de componentscores gemiddeld redelijk dicht bij elkaar liggen.

Figuur 4 **Benchmarkscore per component per functiegroep**



4 VERBETERPUNTEN RESPONDENTEN

In de meting hebben we respondenten gevraagd of zij opmerkingen of verbeterpunten hebben voor hun instelling zodat zij beter privacybewust en informatieveilig kunnen werken. Honderden respondenten gaven een reactie. Ondanks de individuele verschillen in wensen en behoeften, was er een duidelijke rode lijn zichtbaar.

"Bewustwording bij medewerkers kweken is meer dan soms een opmerking maken in een nieuwsbrief die niemand leest, je moet actief naar de medewerkers toe!"

1 Informatie overload

De respondenten maken duidelijk dat zij een hoge werkdruk hebben en dagelijks veel informatie ontvangen van de instelling, zoals nieuwsbrieven, uitnodigingen en teaminformatie. Informatie over security en privacy kan al snel op de grote hoop belanden. De instelling moet volgens hen niet verwachten dat een bericht dat geplaatst is in de nieuwsbrief, gelijk staat aan een bericht dat gelezen is door de medewerkers.

2 Kennisclips en persoonlijke begeleiding

Als oplossing ziet een deel van de respondenten dat informatie gedoseerd en in overzichtelijke vorm wordt aangeboden: via beknopte puntsgewijze teksten, korte online trainingen, infographics en kennisclips. Anderen zeggen juist dat er, gezien het belang van het onderwerp, tijd vrijgemaakt moet worden voor een langere training of voor een persoonlijke vorm van ondersteuning. Zij willen in gesprek over het onderwerp, kijken hoe de regels hun werk beïnvloeden en hoe die toegepast kunnen worden in het dagelijkse werk. Zij willen niet alleen schriftelijk geïnformeerd worden. Bij voorkeur hebben ze een contactpersoon waar ze altijd naartoe kunnen met vragen, iemand die kennis heeft van hun werk, die meedenkt en niet enkel doorverwijst naar standaard teksten. Opvallend genoeg zijn er weinig respondenten die de voorkeur uitspreken voor kennisontwikkeling via gamification. *"Ik hoef geen game, geen escape room, daar heb ik geen tijd voor. Tell me what to do, weet waar je het over hebt. Iemand met kennis van ons soort werk."*

"Faciliteren is één, maar ondersteuning is iets anders. Ik verwacht als docent ondersteund te worden, bewust gemaakt van risico's, ondersteund bij de maatregelen. Niet weer allemaal: lees de instructie of doe het lekker zelf."

3 Thema's

Wat betreft de inhoud van een training, geven de respondenten de volgende suggesties:

- behandel voorbeeldcases uit de praktijk,
- vertel hoe aanvallers te werk gaan, zoals via social engineering,
- leer hoe men phishing kan herkennen,
- bespreek welke tools men kan gebruiken om het werk veilig te doen.

"Ik zou inzetten op awareness waarbij er per doelgroep goed gekeken wordt wat van belang is. Mijn ervaring bij een vorige werkgever is dat er zeer actief voorlichting werd gegeven met voorbeeld cases uit de praktijk, interactieve gesprekken, verplichte deelname, verplicht online cursus over beveiliging et cetera."

4 Geen barrières

Respondenten benadrukken dat het belangrijk is dat de regels duidelijk en goed vindbaar zijn. Meerdere respondenten doen hun beklag over het intranet van de instelling, waar informatie lastig te vinden is. Ook geven zij aan

dat om veilig te kunnen werken barrières moeten worden weggenomen en dat er alternatieven worden geboden voor zaken die niet mogen. Blijf de balans zoeken tussen security en privacy aan de ene kant en gebruikersvriendelijkheid aan de andere kant, is het advies. *"Ik ben bang dat als je geblokkeerd wordt in je workflow, je op zoek gaat naar olifantenpaadjes. Maar overall vind ik dat mijn instelling het best goed doet."*

"Het zou mij helpen om aandacht te besteden aan waarom de eerdere datalekken zijn ontstaan en wat wij als docenten kunnen doen om dat te voorkomen."

5 Confrontatie

Een flink aantal respondenten zegt dat security en privacy nu te vrijblijvende thema's zijn. Zij opteren voor een verplichte training, in ieder geval voor nieuwe medewerkers, zodat iedereen weet dat de instelling het belangrijk vindt. Hun boodschap: schud de mensen wakker, bijvoorbeeld met regelmatig terugkerende phishing-testen. Vraag een *mystery guest* om te kijken of het lukt om beveiligde zones binnen te komen, om toegang te krijgen tot vertrouwelijke gegevens. Of laat diegene bellen met medewerkers, om te zien of deze vertrouwelijke informatie geven. Confronteer medewerkers vervolgens, op organisatie- of afdelingsniveau, met hun eigen gedrag.

5 VERGELIJKING SECTORRAPPORTAGE 2021

Zoals gesteld in hoofdstuk 2 is het maken van een precieze vergelijking met de resultaten van de metingen vorig jaar niet eenvoudig. Dit heeft te maken met de wijzigingen in de vragenlijst en de samenstelling van de groep respondenten.

Tabel 3 **Benchmarkscores 2021 en 2022**

	2021	2022
Totaalscore	6,8	5,9
Motivatie	7,6	5,9
Gelegenheid	6,3	6,1
Bekwaamheid	6,4	5,8

We hebben dit jaar de vragen over het component motivatie aangescherpt. De nieuwe vragen geven een accurater beeld van de mate van motivatie voor informatieveilig en privacybewust werken. Zoals verwacht is de score voor motivatie dit jaar gedaald (7,6 naar 5,9).

Verder zijn de toetsvragen (component bekwaamheid) aangepast, omdat anders de respondenten die vorig jaar ook meededen, de antwoorden al zouden weten. Deze vragen werden blijkbaar als moeilijker beschouwd dan vorig jaar, aangezien ook hier de score is gedaald (6,4 naar 5,8). Wat interessant is, is dat zelfs de score op 'gelegenheid', waarbij geen wijzigingen in de vragenlijst zijn doorgevoerd, iets is gedaald (van 6,3 naar 6,1).

Mate van awareness lijkt toch niet significant verminderd

Toch denken wij dat, op basis van de vragenlijsten maar vooral ook de interviews en de toelichtingen van de respondenten, de mate van awareness niet significant is verminderd. De problemen die ze noemen zijn vergelijkbaar. Net als vorig jaar maken instellingen onvoldoende helder wat ze verwachten van medewerkers en is de rol van leidinggevenden op het gebied van security en privacy beperkt. Vorig jaar werden twee (van de acht) toetsvragen door een meerderheid van de respondenten fout beantwoord. Dit jaar waren dat er drie. Het grootste verschil zien we bij het component motivatie. We hebben dit jaar gevraagd waarom mensen informatieveilig en privacybewust werken, en de redenen waren overwegend vanwege angst voor negatieve consequenties. We gaan ervan uit dat dit vorig jaar ook al het geval was, maar dat dit niet naar voren kwam omdat we er toen niet naar vroegen. Dus enerzijds kunnen we stellen dat de awareness min of meer gelijk is gebleven, omdat de lagere score hoogst waarschijnlijk veroorzaakt wordt door de scherpere vraagstelling. Anderzijds kunnen we ook redeneren dat de awareness is verminderd, omdat de medewerkers de verscherpte eisen voor informatieveilig en privacybewust werken blijkbaar niet kunnen bijbenen.

> ***"Het moet. Het thema is ook belangrijk, maar het is een enorme administratieve last bovenop het bestaande werk, vaak slecht gefaciliteerd en omgeven door veel onduidelijkheden."***

Dankzij de interviews hebben we dit jaar meer inzicht gekregen in de beweegredenen van de respondenten en de barrières voor informatieveilig en privacybewust werken. Dit geeft instellingen concrete handvatten om hun medewerkers beter te faciliteren en ondersteunen.

Veel overlap met verbeterpunten meting 2021

Wat betreft de verbeterpunten die de respondenten aandragen is veel overlap met verbeterpunten meting 2021. In beide jaren is er behoefte aan meer persoonlijke ondersteuning, aan het houden van een gesprek in plaats van het zenden van informatie. Ook wil men graag duidelijkheid over de

regels en richtlijnen. Uit de opmerkingen lijkt dit jaar meer urgentie te spreken. Vorig jaar benadrukten velen nog om een awarenesstraining simpel te houden, met informatie in hapklare brokken. Dit jaar waren er meer stemmen voor intensievere training met persoonlijke ondersteuning. Daarnaast waren er dit jaar opvallend veel voorstanders van het uitvoeren van phishingtesten en meer mensen die pleitten voor het verplicht maken van de awarenesstraining.

6 CONCLUSIE

In deze rapportage hebben we een analyse gemaakt van de 26 security- en privacy-awarenessmetingen die BDO in opdracht van SURF heeft uitgevoerd in het voorjaar van 2022. Op basis van de bevindingen in de voorgaande hoofdstukken, concluderen we het volgende.

1 **Overtuigd van het belang, maar beperkt gemotiveerd om aandacht te besteden aan security en privacy**
De respondenten zijn eensgezind over het belang van security en privacy. Om een weerbare organisatie te zijn, is structurele aandacht voor deze thema's onontbeerlijk en medewerkers spelen hier een belangrijke rol in. Hierover zijn ze het eens. Maar daarnaast lijken security en privacy voor velen geen échte prioriteit, vanwege werkdruk, onduidelijke regels en gebrek aan interesse. Respondenten besteden voornamelijk aandacht aan security en privacy omdat ze negatieve consequenties willen vermijden.

2 **Vrijblijvendheid en beperkte ondersteuning bij security en privacy**
Instellingen leveren in het algemeen matige sturing en ondersteuning aan hun medewerkers om informatieveilig en privacybewust te werken. Een krappe meerderheid van de respondenten is niet tevreden met de ondersteuning die zij krijgen. Enerzijds omdat ze niet weten wat goede ondersteuning inhoudt en of zij die krijgen. Zij komen via de instelling te weinig in aanraking met het thema en zij verdiepen zich er zelf ook onvoldoende in. Anderzijds omdat ze vinden dat ze onvoldoende ondersteund worden. Het is volgens hen niet duidelijk wat hun instelling precies van medewerkers verwacht. Leidinggevenden spelen geen actieve rol op het gebied van security en privacy en het is bij de meeste afdelingen geen onderwerp van gesprek op de werkvloer. De meeste instellingen hebben geen verplichte awarenesstraining en er wordt vanuit de instelling of leidinggevende veelal geen opvolging aan de richtlijnen gegeven.
Tot slot behoeft de ondersteuning verbetering met middelen als software, tools en instructies.

3 **Basiskennis over security en privacy behoeft verbetering**
We hebben in de meting acht toetsvragen over security en privacy gesteld en hiervan werden drie door de meerderheid van de respondenten onjuist beantwoord. Dit betreft vragen over datalekken, wachtwoorden en de kwetsbaarheid Log4j. Over alle acht vragen gaf gemiddeld 57,5% van de respondenten een juist antwoord. We vinden deze score ondermaats.
Een aanvaller heeft soms maar één klik op een phishingmail, of één andere fout van een medewerker nodig om een organisatie succesvol te hacken. Het is dus nodig om het kennisniveau van de medewerkers te verbeteren.

4 **Ondersteunend personeel is meer bewust dan docenten en onderzoekers**
Het ondersteunend personeel, bibliotheek en de doelgroep 'overig' scoren op alle componenten hoger dan de docenten en onderzoekers.
We denken dat dit te maken heeft met de ervaren werkdruk, die onder docenten en onderzoekers hoger is dan het ondersteunende personeel.
Een andere mogelijke reden is het perspectief op security en privacy. Voor het ondersteunende personeel is het wellicht meer vanzelfsprekend om deze thema's als onderdeel van hun kerntaken te zien, omdat hun andere taken ook ondersteunend zijn aan het primaire proces. Voor docenten en onderzoekers geldt mogelijk het omgekeerde. Tot slot kan een gevarieerd en onvoorspelbaar werkpakket leiden tot onduidelijkheid over informatieveilig en privacybewust gedrag. Dit obstakel kan ertoe leiden tot verminderd veilig gedrag.

7 AANBEVELINGEN

Op basis van de bevindingen en conclusies komen we tot de volgende aanbevelingen voor instellingen om de security- en privacy-awareness van hun medewerkers te verhogen.

1 **Wees duidelijk richting medewerkers wat je van hen verwacht**
Zorg dat de security- en privacy-richtlijnen aansluiten bij de werksituatie van de medewerkers. Differentieer eventueel per doelgroep. Betrek, indien mogelijk, de medewerkers bij het opstellen van de richtlijnen, zodat je zeker weet dat ze praktisch uitvoerbaar zijn. Stel indien nodig verschillende (sub)richtlijnen op voor verschillende doelgroepen. Doe dat in beknopte en heldere taal, eventueel met links naar meer informatie, zodat men de informatie in delen tot zich kan nemen. Publiceer de richtlijnen op een toegankelijke locatie.

2 **Neem barrières voor veilig werken weg**
Onderzoek voor je eigen instelling welke belemmeringen medewerkers ervaren bij informatieveilig en privacybewust werken. Is het bijvoorbeeld onmogelijk om te werken zonder Excel-exports uit bronsystemen te maken en per e-mail te delen? Kan er met Teams en OneDrive moeilijk informatie gedeeld worden met partners buiten de instelling? Biedt de instelling geen tooling aan om het onderwijs interactiever te kunnen maken? Door oplossingen te bieden voor dit soort zaken, wordt het makkelijker voor medewerkers om veilig te werken.

3 **Kies bij de instrumenten voor inhoud en aansluiting**
Richt je bij de keuze voor awareness-instrumenten vooral op inhoud en aansluiting bij de doelgroep. Medewerkers hebben meer behoefte aan een basale sessie of training die inhoudelijk goed aansluit bij de werkzaamheden, dan aan een gelikte game die dat minder doet. Houd er rekening mee dat de werkdruk hoog is, dus zorg dat de instrumenten niet langer tijd vergen dan noodzakelijk, en geen content bevatten die niet relevant is voor de doelgroep.

4 **Focus extra op docenten, onderzoekers en leidinggevenden**
Besteed in het awarenessprogramma extra aandacht aan leidinggevenden, docenten en onderzoekers. Ondersteun leidinggevenden bij het nemen van hun (lijn-)verantwoordelijkheid om privacybewust en informatieveilig te werken. Neem de moeite om docenten en onderzoekers te bereiken, bijvoorbeeld via afdelingsoverleggen en onderzoeksgroepen. Overweeg om aparte interventies voor docenten en onderzoekers te ontwikkelen.

5 **Maak awareness minder vrijblijvend**
Om een digitaal weerbare instelling te zijn, is het noodzakelijk dat alle medewerkers aantoonbaar bereikt worden met de awareness-activiteiten. Onderzoek daarom de mogelijkheden om security en privacy awareness een meer verplichtend karakter te geven. Dat kan door bij te houden of alle medewerkers aantoonbaar een sessie of training hebben gevolgd, door hen er vervolgens op te attenderen als ze dat niet hebben gedaan, en ook door hun leidinggevenden hier een actievere rol in te geven. Spreek met het college van bestuur af op welke wijze de instelling naleving wil garanderen.

6 **Meet gedrag via phishingtesten**
Zorg ervoor dat je regelmatig het informatieveilige en privacybewuste gedrag van medewerkers meet. Een goede methode is het houden van phishingtesten, omdat je daarmee het daadwerkelijke gedrag meet, in plaats van het zelf gerapporteerde gedrag. Je stuurt een nep-phishing mail of tekstbericht om te kijken of men meegaat in het verhaal van de oplichter en klikt op de link of inloggegevens invoert.
Zorg dat je de phishing-test op een ethische manier uitrolt. Denk na

over de template die je gebruikt[15]. Wees positief en constructief in de feedback aan medewerkers die hebben geklikt. Rapporteer over de resultaten op afdelings- of organisatieniveau (en niet op individueel niveau). Een andere manier om informatieveilig gedag te meten is het inzetten van *mystery guests*.

7 Behandel de volgende thema's

De richtlijnen, en ook de overige awareness-interventies, bevatten idealiter minimaal de volgende informatie:

- Het beschermen van accounts, inclusief (sterke) wachtwoorden
- Het herkennen van phishing
- Het beschermen van de fysieke werkomgeving
- Informatie over mensgerichte aanvalsmethoden van cybercriminelen (onder andere social engineering)
- Hoe een datalek te herkennen en welke acties ze vervolgens kunnen nemen
- Hoe het thuisnetwerk te beveiligen

Mogelijk is het nodig deze thema's per doelgroep uit te werken:

- Welke ict-tools mogen ze gebruiken, voor welke doeleinden en soorten gegevens?
- Welke persoonsgegevens mogen ze verzamelen en vastleggen, en voor welke activiteiten en onder welke voorwaarden?
- Welke (persoons)gegevens mogen ze delen, en met welke partijen, onder welke voorwaarden?
- Welke acties en beveiligingsmaatregelen moeten ze uitvoeren bij nieuwe (onderzoeks)projecten?
- Hoe en waar kunnen ze veilig (zeer) vertrouwelijke informatie opslaan en delen?
- Wat kunnen ze doen en met wie men kunnen ze overleggen, als ze problemen hebben om te voldoen aan de richtlijnen?

15 Een e-mail met de belofte van een bonus kan mogelijk veel weerstand oproepen, als die later nep blijkt te zijn

COLOFON

Auteurs
Marijke Stokkel, BDO
Charlie van Genuchten, SURF

Ontwerp
Studio Koelewijn Brüggenwirth BNO, Den Haag

Fotografie
Foto omslag: Sicco van Grieken

September 2022

Samen aanjagen van vernieuwing