Afscheidsrede

20 jaar cybersecurity

Lector dr. Marcel Spruit

22 mei 2025

DE HAAGSE HOGESCHOOL

20 jaar cybersecurity

Afscheidsrede lector dr. Marcel Spruit

22 mei 2025, De Haagse Hogeschool

Goedemiddag allemaal.

Meer dan twintig jaar geleden stond ik hier ook, toen voor mijn intreerede.[1] Ik was toen net begonnen als lector op het gebied van informatiebeveiliging en zoals jullie op de foto kunnen zien, had ik toen nog een snor en was wat minder grijs.

Foto 1: Marcel Spruit in 2003 (Fotograaf onbekend).

Zo lang ik lector ben, kreeg het vakgebied dat begon als *informatiebeveiliging*[2] geregeld een andere naam, zoals digitale veiligheid, cybersecurity, cyberweerbaarheid, cyberveerkracht en de Engelse varianten ervan. De meeste van deze termen worden nog steeds en door elkaar gebruikt. Steeds wordt ongeveer hetzelfde bedoeld en steeds zijn er mensen die proberen uit te leggen dat er echt sprake is van verschillende vakgebieden. Dat is niet zo.

Tegenwoordig is de term cyberweerbaarheid populair, maar die term suggereert meer een doel dan een actie. De term cyberveerkracht is in opkomst, maar die benadrukt vooral de reactieve component. In deze presentatie houd ik het dan ook op de term cybersecurity. Maar dit betekent in de praktijk dus hetzelfde als informatiebeveiliging, of cyberweerbaarheid, of een van die andere termen.

Figuur 1: Verschillende termen voor hetzelfde vakgebied.

[1] Spruit, M. (2003). *Waardevol maakt kwetsbaar: het belang van informatiebeveiliging*. De Haagse Hogeschool.

[2] NEN (20215). *NEN-EN-ISO/IEC 27000:2020 en, Information technology – Security techniques – Information security management systems – Overview and vocabulary*. NEN.

In mijn presentatie ga ik eerst in op een paar algemene aspecten van cybersecurity en mijn lectoraat. Daarna loop ik langs de drie thema's van mijn lectoraat. Dat zijn:

1. Het verbeteren van het cybersecuritybewustzijn van mensen.
2. Het verbeteren van cybersecurity in organisaties.
3. Het verbeteren van cybersecurityonderwijs.

1. Algemene aspecten

Aan het begin van mijn lectoraat was de digitalisering van de maatschappij nog niet zo ver gevorderd en bestond het internet nog maar een paar jaar. Sociale media stonden nog in de kinderschoenen en computers zagen er anders uit dan nu.[3,4]

Figuur 2: Computers anno 2003 en 2025 (Viachaslau Rutkouski en Manaemedia).

In de jaren daarna is er veel veranderd. De digitalisering is overal in de maatschappij doorgedrongen en we zijn er helemaal afhankelijk van geworden. Miljarden mensen zitten op sociale media en voor velen is dat hun belangrijkste nieuwsbron.[5,6,7,8,9,10,11]

---

3 Phillips, S. (2007). A brief history of Facebook. *The Guardian*, 25 juli 2007.

4 Vanian, J. (2022). Twitter is now owned by Elon Musk - here's a brief history from the app's founding is 2006 to the present. *CNBC*, 29-10-2022.

5 https://www.nu.nl/tech-achtergrond/6161315/dit-moet-je-weten-over-frances-haugen-de-klokkenluider-van-facebook.html

6 Wynn-Williams, S. (2025). *Careless People*. MacMillan Books.

7 Oldemburgo de Mello, V., Cheung, F. & Inzlicht, M. (2024). Twitter (X) use predicts substantial changes in well-being, polarization, sense of belonging, and outrage. *Communications Psychology*, 2 (15), 1-11.

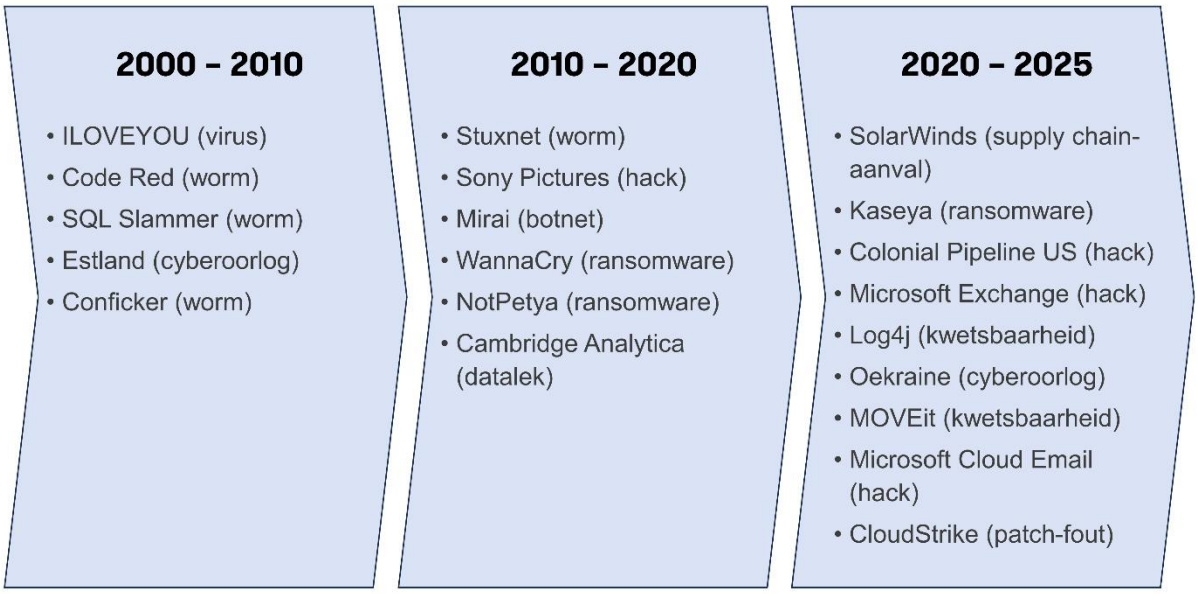
8 De Keulenaar, E., Magelhaes, J.C. & Ganesh, B. (2023). Modulating moderation: a history of objectionability in Twitter moderation practices. *Journal of Communication*, 73 (3), 273-287.

9 Kerr, D. (2023). Meta failed to address harm to teens, whistleblowers testifies as senators vow action. *NPR*, 7 november 2023.

10 Cinelli, M., et al. (2021). The echo chamber effect on social media. *Proc. Natl. Acad. Sci. U.S.A.*, 118 (9), 1-8.

11 Nyhan, B., et al. (2023). Like-minded sources on Facebook are prevalent but not polarizing. *Nature*, 620, 137-144.

Onze afhankelijkheid van de digitalisering is zo groot dat als er maar iets mee misgaat we meteen problemen hebben. En dan gaat er natuurlijk ook van alles mis; we hebben niet voor



Figuur 3: Enkele cyberincidenten met wereldwijde schade.

niets de *wet van Murphy*. Een groeiende stroom incidenten laat zien dat er veel mis kan gaan. Enkele beruchte incidenten, met wereldwijd veel schade, staan in figuur 3. Maar ook in Nederland zijn veel incidenten geweest, denk aan Diginotar, Hof van Twente, Universiteit van Maastricht, TU Eindhoven, enzovoort. En nog veel meer incidenten bleven onder de radar, maar hebben wel voor veel schade en overlast gezorgd.

Ruim twintig jaar geleden was een lectoraat op het gebied van cybersecurity niet vanzelfsprekend. En al helemaal niet met een focus op mens en organisatie. Als in die tijd ergens op de wereld cybersecurityonderzoek werd gedaan dan richtte zich dat meestal op techniek. Bijvoorbeeld op het ontwikkelen van nieuwe cryptografische technieken.

Het was dan ook een vooruitstrevend idee om in het hoger onderwijs een lectoraat op het gebied van cybersecurity op te zetten, met als focus de menselijke en organisatorische aspecten. Dat die er toen gekomen is, is vooral te danken aan Jan Dirk Schagen, toentertijd opleidingsmanager Technische Informatica, en Ineke van der Meule, directeur Onderzoek.

Bij een lectoraat horen natuurlijk onderzoekers. In de jaren zijn er heel wat wisselingen van de wacht geweest. In figuur 4 zien jullie de eerste groep – links – en de huidige groep – rechts. Zoek de overeenkomst.

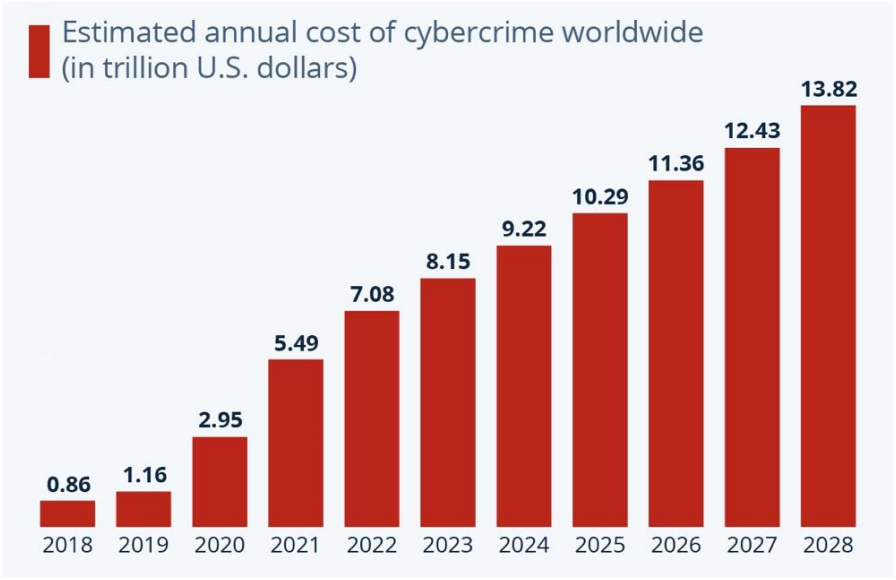
Figuur 4: De onderzoekers van het lectoraat in 2003 en 2025.

Het heeft nog jaren geduurd voordat andere universiteiten en hogescholen binnen cybersecurity significant aandacht gingen besteden aan de factoren mens en organisatie. Terwijl het twintig jaar geleden al duidelijk was dat binnen cybersecurity de uitdaging vooral op deze factoren lag. Sterker nog, al in de jaren negentig heb ik, toen ik nog hoofddocent was aan de TU Delft, een onderzoek gepubliceerd over aantallen incidenten en de oorzaken ervan.[12] Daaruit bleek al duidelijk dat de mens als oorzaak van incidenten met stip op de eerste plaats stond. Dat is ook de reden voor het opnemen van een heel hoofdstuk over de menselijke factor in het leerboek *Informatiebeveiliging onder controle*, al vanaf de eerste editie uit 2000.[13,14]

Figuur 5: Het boek 'Informatiebeveiliging onder controle' in 2000 en 2023.

12 Spruit, M.E.M. & Looijen, M. (1996). IT security in Dutch practice. *Computers & Security*, 15 (2), 157-170.
13 Houten, P. van, Spruit, M. & Wolters, K. (2023). *Informatiebeveiliging onder controle. Vijfde editie*. Pearson.
14 Zimmermann, V. & Renaud, K. (2019). Moving from 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187.

De vele incidenten veroorzaken bij elkaar zeer veel schade. Zoals je in het schema van Statista kan zien (figuur 6), is alleen al de schade door cybercrime immens en neemt deze in rap tempo toe.[15,16,17] Dat is ook niet zo gek, nu elke scholier die de pik heeft op zijn school voor een habbekrats op het Darkweb een cyberaanval kan kopen om zijn school digitaal plat te leggen.[18] Je hoeft er zelfs geen nerd meer voor te zijn, want je krijgt er een gebruiksaanwijzing bij. En als je er dan nog niet uitkomt dan raadpleeg je de helpdesk. Cybersecurity is dan ook hard nodig om de schade door cyberincidenten te beperken.



Figuur 6: Geschatte schade wereldwijd door cybercrime in biljoenen dollar (Statista, 2024).

Foto 2: Evenwichtsartiest boven vangnet (Gemaakt met AI)

Het onderzoek naar cybersecurity heeft een nogal tweeslachtige relatie met deze schade. Aan de ene kant hebben we onderzoek om wereldwijd cybersecurity te verbeteren en zo de schade te beperken. Aan de andere kant maken criminelen, statelijke actoren en anderen met dubieuze intenties even hard gebruik van nieuwe cybersecurityontwikkelingen om de schade juist te vergroten. Ze gebruiken de nieuwe kennis voor het maken van nog betere virussen, wormen, scan-tools, enzovoort.

Doordat we met cybersecurity de digitale wereld nog niet veilig hebben kunnen

15 Fleck, A. (2024). Cybercrime Expected to Skyrocket in Coming Years. *Statista*, 22 februari 2024. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

16 FBI-IC3 (2024). *Federal Bureau of Investigation Internet Crime Report 2024*. FBI Internet Crime Complaint Center.

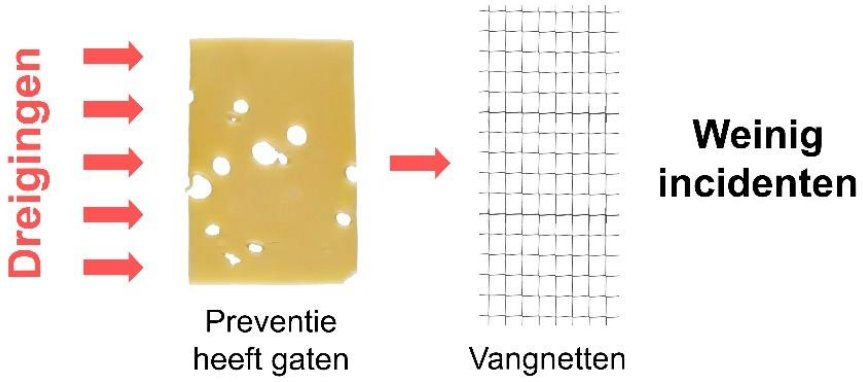
17 Anderson, R., et al. (2019). *Measuring the Changing Cost of Cybercrime*. University of Cambridge.

18 https://www.vo-raad.nl/artikelen/141

krijgen, komt de laatste jaren steeds meer nadruk te liggen op het reactief vermogen van mensen en organisaties, oftewel vangnetten. Vangnetten zijn de achtervang voor als de preventieve maatregelen niet voldoende zijn. Denk aan het vangnet onder een evenwichtsartiest in het circus. Normaal gesproken vallen evenwichtsartiesten nooit, maar ja, het zal toch maar een keer gebeuren. In cybersecurity is een bekend voorbeeld van een vangnet de back-up. Ik hoop dat jullie deze maatregel allemaal kennen èn toepassen. Normaal gesproken heb je de back-up nooit nodig, maar als er onverhoopt wat gebeurt met de informatie op je computer, dan zet je alles weer terug met de back-up. Die moet je natuurlijk wel van tevoren maken èn regelmatig bijhouden. In het circus werkt het ook niet als je het net pas ophangt nadat de artiest is neergestort.

Het uitgangspunt voor vangnetten is dat preventieve maatregelen nooit in staat zijn om cyberincidenten helemaal te voorkomen, dus moet iedereen voorbereid zijn om cyberincidenten zo goed mogelijk op te vangen. Denk aan het advies van de banken om voldoende contant geld in huis te hebben voor als er een grote storing in de financiële systemen komt.[19] Hebben jullie zelf al veel contanten in huis? En vonden jullie het ook jammer, dat er niet bij werd verteld hoe we met die contanten kunnen betalen bij al die winkels met elektronische kassa's die het dan niet meer doen?

Bij het verplaatsen van de aandacht van preventie naar vangnetten zou je de denkfout kunnen maken dat je de preventieve maatregelen dan met een korreltje zout kan nemen, want er zijn toch vangnetten. Dit beeld zit ook achter de stijgende populariteit van de term cyberveerkracht. Helaas, dit klopt niet. Ten eerste zijn vangnetten gebaseerd op detectie en tegen de tijd dat een incident gedetecteerd is, kan het al te laat zijn. Denk bijvoorbeeld aan het op internet publiceren van gestolen digitale informatie. Je kan daarna hoog en laag springen, maar op het internet geldt "eens gepubliceerd, blijft gepubliceerd". Een tweede reden is dat preventieve maatregelen noodzakelijk zijn om vangnetten te ontlasten. Preventieve maatregelen kunnen namelijk al het merendeel van de bedreigingen tegenhouden. En dat is hard nodig, want vangnetten hebben maar een beperkte capaciteit. Af en toe een cyberincident opvangen die door de gaten van de preventieve maatregelen is geslipt, is prima te doen, maar de hele dag cyberincidenten oplossen is dat niet. Goede cybersecurity

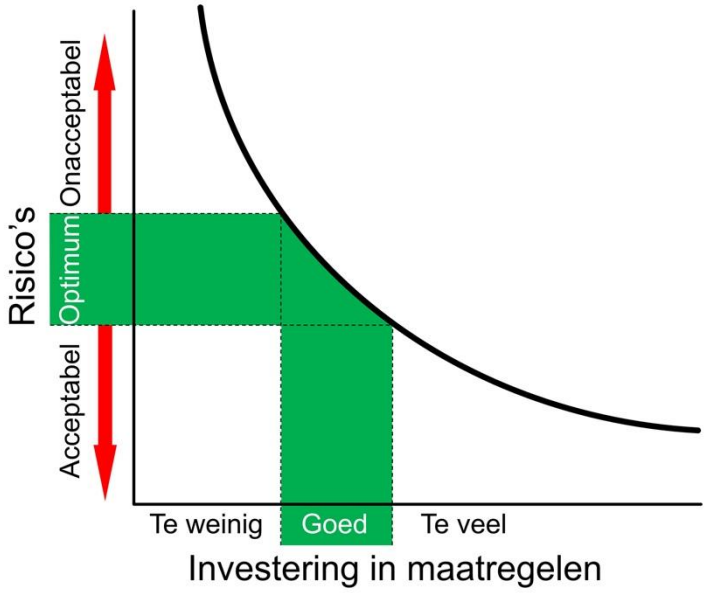


Figuur 7: Een combinatie van preventie en vangnetten is nodig.

[19] https://www.banken.nl/nieuws/25777/zorg-voor-een-voorraad-contant-geld-in-huis

bestaat daarom al jaar en dag uit een combinatie van preventie en vangnetten en dat is anno 2025 nog steeds zo. En dat blijft zo.

Naast het vinden van een goede combinatie van preventie en vangnetten, moet je ook voor zorgen dat je niet te weinig aan beveiliging doet, maar ook niet te veel. Dat eerste is zonder meer duidelijk, maar dat je ook niet te veel aan beveiliging mag doen, ligt lastiger. Je zou denken “baat het niet, schaadt het niet”, maar grosso modo hinderen beveiligingsmaatregelen het gewone werk. Dus onnodige, of onnodig zware, maatregelen geven onnodige hinder voor het werk. Daarom moet je in cybersecurity steeds de gulden middenweg zoeken. En daar hoort bij dat je er geregeld voor moet kiezen om bepaalde maatregelen niet te treffen, onder het motto “baat het niet, het schaadt wel”. Studenten presenteren we de grafiek in figuur 8, over risico’s versus maatregelen.[20] Hierin zie je dat hoe meer je investeert in cybersecuritymaatregelen, des te kleiner de overblijvende risico’s. Maar je mag dus niet te hard van stapel lopen, want dan begin je ook het werk steeds meer te hinderen. Dus je moet te allen tijde in het groene gebied zitten, het optimum. Dat klinkt makkelijk, maar dat is het niet.

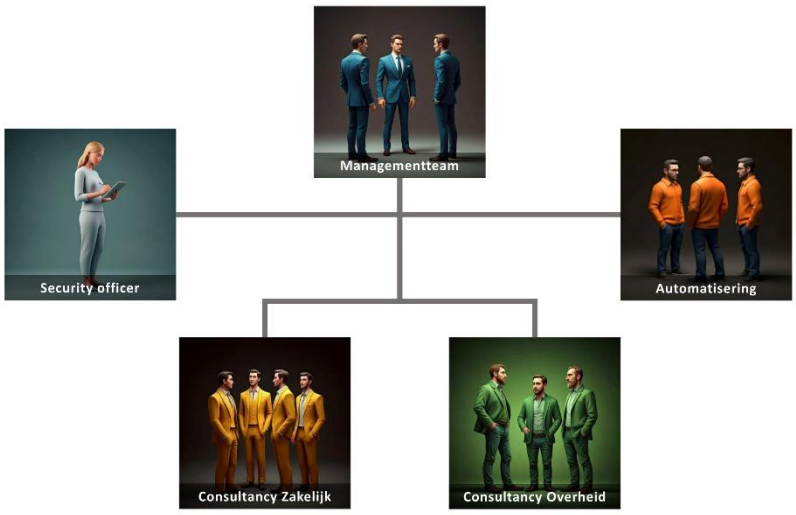


Figuur 8: Risico's versus maatregelen (Houten, Spruit & Wolters, 2023).

We hebben namelijk gemerkt dat mensen van nature slecht aanvoelen waar de gulden middenweg ligt tussen te weinig en te veel beveiligen. Daarom hebben we een cybersecuritygame ontwikkeld die zich juist hierop richt.[21] De game is een managementgame die zich afspeelt in een hypothetische organisatie, een adviesbureau met de naam Insecure. Meestal wordt die naam wel waargemaakt.

Studenten, of andere deelnemers, krijgen in deze organisatie verschillende rollen die meer of minder met cybersecurity te maken hebben, zie figuur 9. Maar in elke rol moet de deelnemer wel iets aan cybersecurity doen. En de security officer is er zelfs de hele tijd mee bezig. De deelnemers merken in deze game welke keuzes ze geneigd zijn te maken met betrekking

[20] Houten, P. van, Spruit, M. & Wolters, K. (2023). *Informatiebeveiliging onder controle. Vijfde editie*. Pearson.
[21] Spruit, M. (2009). Een serious game voor informatiebeveiliging. *Informatiebeveiliging*, 9 (8), 18-20.



Figuur 9: Rollen in de cybersecuritygame (Spruit, 2009).

tot cybersecurity en wat daarvan de consequenties zijn. Meestal gaat de organisatie Insecure failliet, dus blijkbaar is het niet zo makkelijk om steeds de goede keuzes te maken.

Op foto 3 zien we de game in actie bij de postdoctorale opleiding voor IT-audit in Amsterdam. De deelnemers met de oranje kaarten zijn in de game IT'ers en de deelnemers met de lichtblauwe kaarten zijn managers. De CISO staat voor de tafel en is net aan het overleggen met de managers. Hun uitdaging is niet te weinig tijd aan cybersecurity te besteden, maar ook niet te veel en daarbij niet te weinig maatregelen te treffen, maar ook niet te veel. En daarvoor moeten ze gaan denken in risico's in plaats van dreigingen. Zo leidt bijvoorbeeld spam per keer maar tot marginale schade, maar het komt zo vaak voor dat het risico (= kans x schade) toch groot genoeg wordt om er maatregelen tegen te gaan treffen.

Foto 3: Cybersecuritygame in actie (Spruit).

Als de deelnemers goed in risico's denken dan beveiligen ze de organisatie niet als Fort Knox, maar dan treffen ze juist de maatregelen die nodig zijn. In een huissituatie betekent dat bijvoorbeeld dat als je het risico op inbraak te groot vindt, dat je dat dan kleiner kan maken door jouw buitendeuren beter te beveiligen dan die bij de buren. Dus mensen, vanavond nog even checken of de sloten op jullie deuren meer sterren hebben dan die bij de buren; ook de achterdeur checken.

2. Cybersecuritybewustzijn

Cybersecurity gaat vooral over mensen en hun gedrag.

Rondom de eeuwwisseling was al duidelijk dat de grootste uitdaging voor cybersecurity zit in mensen en hun gedrag.[22] Dat geldt zowel voor individuen, als voor medewerkers in organisaties. Door Ponemon Institute is recent gemeten dat in organisaties het aantal incidenten door eigen medewerkers nog steeds verder stijgt.[23] Het grootste deel hiervan wordt overigens veroorzaakt door ònopzettelijke fouten.

In het begin van deze eeuw werd wereldwijd nog weinig onderzoek gedaan naar menselijk gedrag in relatie tot cybersecurity. Daarom was er ook weinig informatie over te vinden. Dus lag het voor ons voor de hand om binnen de gedragswetenschappen naar die informatie te zoeken. We zochten een eenvoudig en duidelijk model, met bollen en pijlen, waarmee we menselijk gedrag goed konden verklaren. We hebben er allerlei leerboeken op nageslagen, maar zo'n model konden we niet vinden. Misschien vindt men in de gedragswetenschappen dat studenten heel goed zelf zo'n model kunnen bedenken. Vanuit andere domeinen, zoals marketing, communicatie, ergonomie en veiligheidskunde, waren wel modellen geïntroduceerd, zoals Theory of Planned Behavior[24], Protection Motivation Theory[25] en Theory of Situational Awareness[26]. Probleem voor ons was dat deze modellen voor òns niet voldeden. Bij de ene ontbrak alles op het gebied van kennis, bij de andere juist alles op het gebied van attitude en bij sommige zaten er fouten in.[27]

---

22 Spruit, M.E.M. & Looijen, M. (1996). IT security in Dutch practice. *Computers & Security*, 15 (2), 157-170.

23 Ponemon Institute (2022). 2022 Cost of Insider Threats Global report. *Ponemon Institute*.

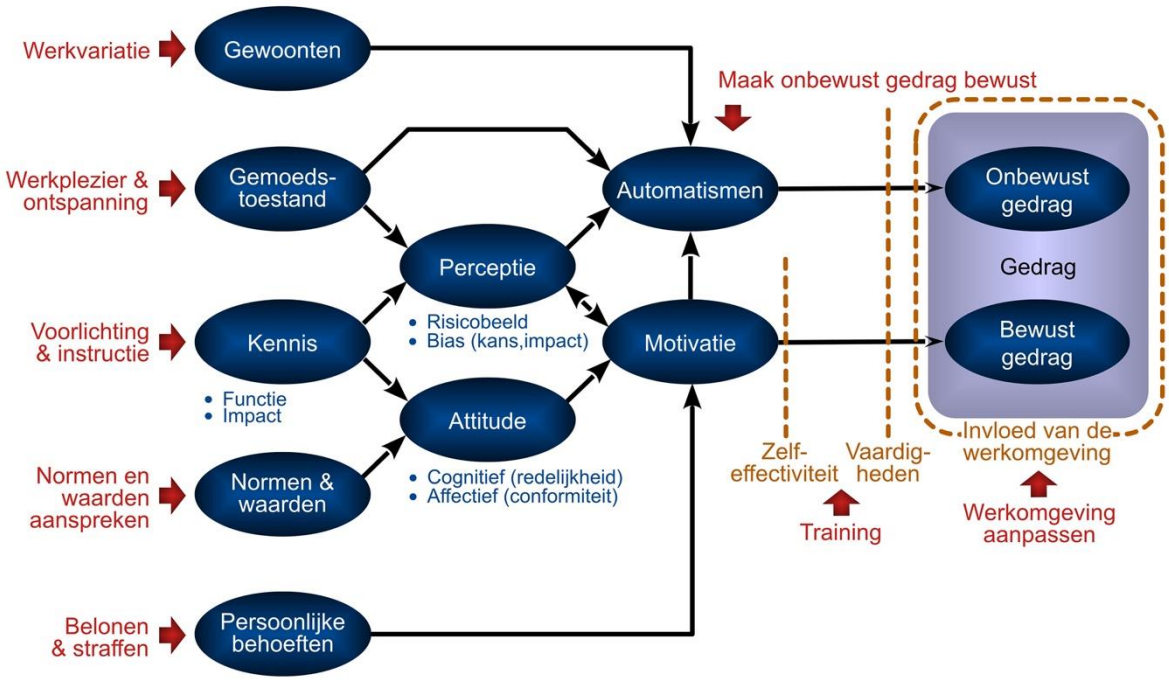
24 Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. In J. Kuhl, & J. Beckmann (Eds.), Action Control (pp. 11-39). Berlin: Springer.

25 Rogers, R.W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology*, 91, 93-114.

26 Endsley, M.R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, 37 (1), 32-64.

27 Sniehotta, F.F., Presseau, J. & Araújo-Soares, V. (2014). Time to retire the theory of planned behaviour. *Health Psychology Review*, 8 (1), 1-7.

We hebben toen maar zelf, op basis van alle literatuur een model samengesteld, zie figuur 10.[28,29] De gedragsbeïnvloedende factoren zijn in blauw, de verbeteraanpakken zijn in rood. Dit model is ook opgenomen in het leerboek *Informatiebeveiliging onder controle*, al vanaf de eerste editie uit 2000.[30] Daardoor hebben inmiddels heel wat studenten dit model bestudeerd en zo hopelijk meer gevoel gekregen voor de rol van menselijk gedrag in cybersecurity.



Figuur 10: Gedragsbeschrijvend model met mogelijke interventies (Spruit, 2000; Houten, Spruit & Wolters, 2023).

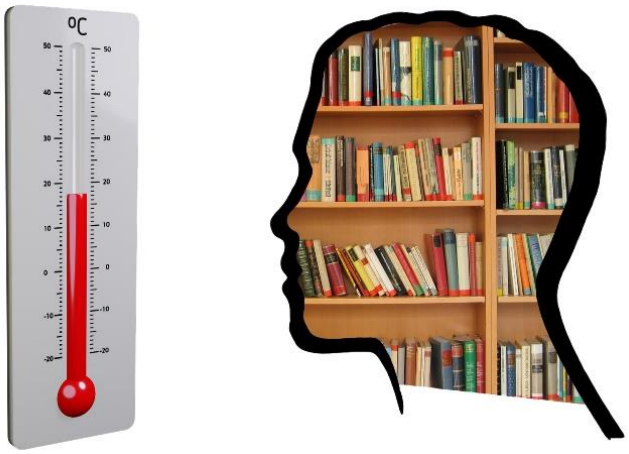
In de jaren nadat we ons model hadden geïntroduceerd, zijn hier en daar pogingen gedaan om nieuwe modellen te ontwikkelen, maar dat leverde weinig op. Mogelijk leunde het onderliggende onderzoek te veel op het meten van correlaties. Dat is heel erg gangbaar, maar het heeft helaas wel een paar problemen. Ten eerste kan je uit correlaties niet halen wat de oorzaak is en wat het gevolg. En dat is juist wat je wil weten. Ten tweede komen correlatiemetingen in het algemeen met grote onzekerheden en die laat de statistische software niet zien. Dit wordt verergerd doordat steeds meer onderzoekers steeds minder tijd besteden aan het reviewen en valideren van bijvoorbeeld vragenlijsten, want dat kost zo veel tijd en moeite. En dan zijn interpretatiefouten gauw gemaakt en dan kun je zomaar fouten in je model krijgen.

---

[28] Spruit, M.E.M. (1998). Competing against human failing. In: *Proceedings of the IFIP TC11 14th international conference on Information Security (SEC '98), Wenen/Boedapest, 1998,* 392-401.

[29] Spruit, M.E.M. (2000). *Human Error and Information Security*. Whitepaper. Technische Universiteit Delft.

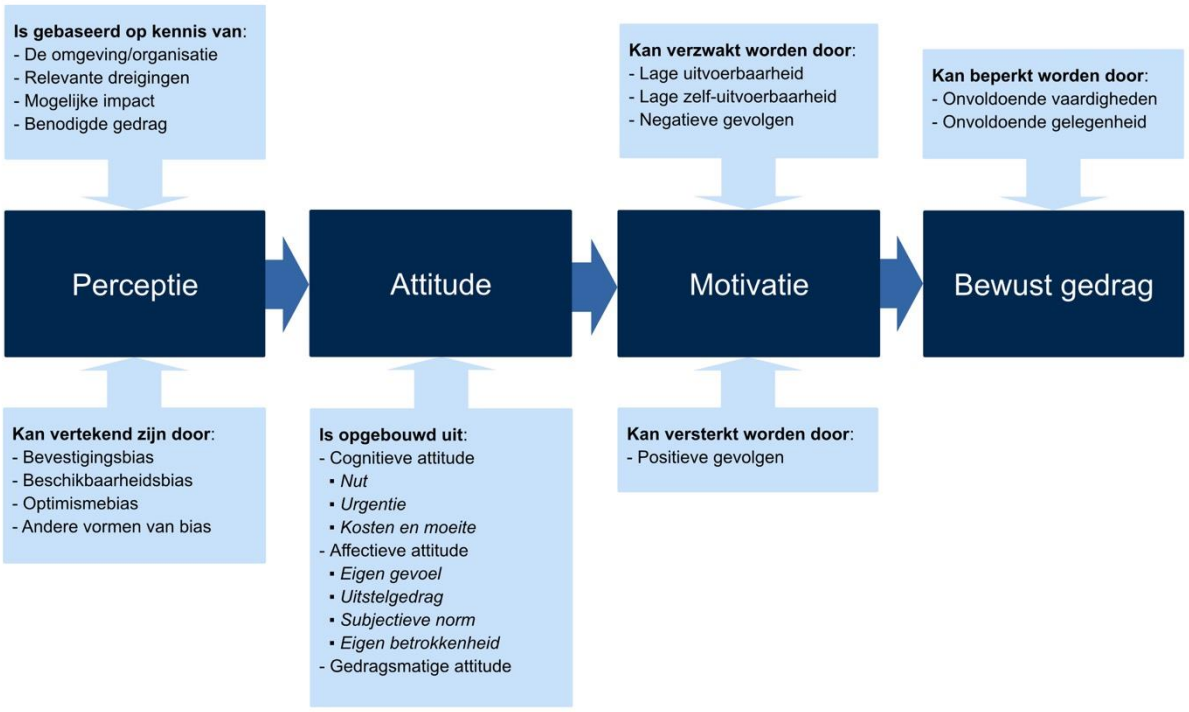
[30] Houten, P. van, Spruit, M. & Wolters, K. (2023). *Informatiebeveiliging onder controle. Vijfde editie*. Pearson.



Figuur 11: Temperatuur is een enkelvoudige factor, kennis niet (Thor_Deichmann en Geralt op Pixabay).

Een ander probleem waar cybersecuritytyonderzoek veel last van heeft, is de misvatting dat factoren zoals kennis en gedrag enkelvoudige factoren zouden zijn die je ieder in één waarde kan vangen. Net zoals je temperatuur kan vangen in één waarde, bijvoorbeeld 20°C. Maar factoren zoals kennis en gedrag zijn meervoudige factoren. Zo is kennis een verzameling van kenniselementen die onafhankelijk van elkaar en in verschillende volgorde aangeleerd worden. Iemand die veel van malware weet, is niet per se beter of slechter in cybersecurity dan iemand die veel van cookies weet. Kennis over malware kan een van de eerste dingen zijn die je hebt geleerd over cybersecurity, bijvoorbeeld omdat je een keer een malware-besmetting hebt opgelopen. Maar voor anderen zal het misschien het laatste zijn dat ze over cybersecurity leren. Als je factoren zoals kennis en gedrag platslaat tot enkelvoudige factoren en die gaat correleren, dan krijg je onzin.

Al met al zagen we na 2000 geen beter gedragsbeschrijvend model dan het model dat we al hadden gepubliceerd. Maar in de praktijk merkten we dat studenten en cybersecurityprofessionals dit model eigenlijk te moeilijk in het gebruik vonden. Ze hadden behoefte aan een model dat in de praktijk makkelijker te gebruiken is, maar wel alle relevante factoren bevat.



Figuur 12: Nieuw gedragsbeschrijvend model (Spruit, Oosting & Kreffer, 2024).

Dat is het model in figuur 12 geworden dat we vorig jaar hebben gepubliceerd.[31,32] Het model geeft aan welke factoren welke invloed hebben op veilig digitaal gedrag. Het nieuwe model lijkt misschien niet eenvoudiger dan het oude model, maar dat is het wel. Vooral het toepassen ervan is een stuk makkelijker.

Aangezien elke factor in het schema om een andere verbeteraanpak vraagt, hebben we bij het model in figuur 12 een tabel opgesteld (tabel 1) waarin je kan opzoeken welke verbeteraanpak je kan gebruiken voor het bijsturen van een gegeven factor.[33] Probeer maar niet om de hele tabel nu al te lezen; zie het maar als een naslagtabel.

Factor	Deelfactor	Verbeteraanpak
Kennis	Functionaliteit	• Geef de medewerkers relevante cursus(sen) en toets de opgedane kennis.
	Impact	• Voorzie medewerkers van relevante informatie. Voorzie managers bijvoorbeeld van test-, audit- en incidentrapportages. • Laat managers en andere interne/externe autoriteiten uitleggen wat de impact kan zijn.
Bias	Bevestigings-, beschikbaarheids- en optimismebias	• Geef de medewerkers inzicht in hun bias met simulaties of spellen zodat ze risico's en veilig gedrag beter in leren schatten.
Cognitieve attitude	Nut	• Zorg dat de maatregelen voor medewerkers effectief en logisch zijn.
	Urgentie	• Laat managers en ervaren collega's uitleggen welke maatregelen waarom en wanneer nodig zijn. En laat ze zelf het goede voorbeeld geven.
	Kosten en moeite	• Integreer het veilig gedrag in het 'gewone' werk. • Maak maatregelen niet onnodig lastig of tijdrovend.
Affectieve attitude	Eigen gevoel, Uitstelgedrag	• Verlaag drempels voor maatregelen en richt ze in als 'hapklare brokken'. • Werk in teams waarin een sfeer ontstaat van 'we doen dit samen'. • Pas (zachte) dwang toe voor de benodigde maatregelen.
	Subjectieve norm	• Schakel gewaardeerde collega's in voor het geven van het goede voorbeeld en het stimuleren van medewerkers.
	Eigen betrokkenheid	• Betrek medewerkers bij het selecteren, uitwerken en evalueren van maatregelen.
Lage uitvoerbaarheid		• Maak maatregelen zo dat het uitvoeren ervan goed te doen is.
Lage zelf-uitvoerbaarheid		• Deze factor veroorzaakt voor beveiliging meestal weinig problemen. Overweeg anders coaching.
Positieve en negatieve gevolgen		• Zorg dat maatregelen niet leiden tot negatieve consequenties en zorg dat onveilig gedrag niet wordt beloond. Overweeg veilig gedrag te belonen.
Onvoldoende vaardigheden		• Verbeter ontbrekende vaardigheden door training, in simulatie of op de werkvloer.
Onvoldoende gelegenheid		• Ruim hindernissen voor beveiligingsmaatregelen op.

Tabel 1: Opzoektabel voor verbeteraanpak per factor (Spruit & Kreffer, 2025).

[31] Spruit, M., Oosting, D. & Kreffer, C. (2024). Factors that influence secure behaviour while using mobile digital devices. *Information and Computer Security*, 32 (5), 729-747.
[32] Spruit, M. & Kreffer, C. (2024). Informatie(on)veilig gedrag van medewerkers. *IB Magazine*, 24 (5), 8-13.
[33] Spruit, M. & Kreffer, C. (2025). Veldonderzoek naar (on)veilig gedrag. *IB Magazine*, 25 (2), 28-34.

Als je bij iemand onveilig gedrag constateert, dan kun je met behulp van het nieuwe model bepalen welke factoren daar de oorzaak van zijn en in de tabel kan je dan vinden welke verbeteraanpakken je kunnen helpen. Dan moet je natuurlijk wel eerst het gedrag meten, zodat je vervolgens kan bepalen of dat gedrag onveilig is. Daarna kan je dan de oorzaak bepalen en daar een verbeteraanpak bij zoeken.

Nu zijn we niet de eersten die gedrag willen meten, dus daar is veel ervaring mee, vooral buiten de cybersecurity. In principe kan je gedrag op meerdere manieren meten:

1. Gedrag observeren in de eigen omgeving.
2. Gedrag observeren in een simulatie.
3. Gedrag bevragen.

Gedrag in de eigen omgeving observeren, is de meest voor de hand liggende manier om te kijken wat iemand doet. Dan hobbel je aan achter degene van wie je het gedrag wil weten. Dat is heel representatief, want het is gewoon de situatie zoals die is. Je zou verwachten dat degene die wordt gevolgd daar een sik van krijgt, maar in de praktijk blijkt dat zo iemand daar na een korte gewenningstijd niet meer op let en gewoon z'n gang gaat. In de organisatiekunde heeft Henry Mintzberg zo in de vorige eeuw zijn befaamde onderzoek gedaan naar het gedrag van topmanagers van grote organisaties.[34] Daar kwam uit dat die managers helemaal niet zo rationeel en effectief stuurden als het gangbare idee was. Dat is overigens nog steeds zo; niet alle managers hebben de boeken van Mintzberg gelezen. Recent is zo'n zelfde aanpak gebruikt in het promotieonderzoek van Eline de Kok naar gedrag van verplegend personeel in ziekenhuizen.[35] Daar kwam uit dat verplegend personeel geregeld de procedures niet volgden, maar ze hadden daar dan steeds goede redenen voor en dus verdienden ze eigenlijk allemaal schouderklopjes voor het niet volgen van de procedures. In gedragsonderzoek in de context van cybersecurity werkt dit soort metingen wat minder, omdat een observator makkelijk gedragingen mist. Zo kan een observator bijvoorbeeld niet goed zien of iemand die even op z'n smartphone kijkt, typt en swipet dat wel veilig doet. En bovendien kost het heel veel tijd om zo bij veel mensen gedrag te meten. Daarom is zo'n aanpak voor gedragsmeting binnen de cybersecurity niet zo geschikt.

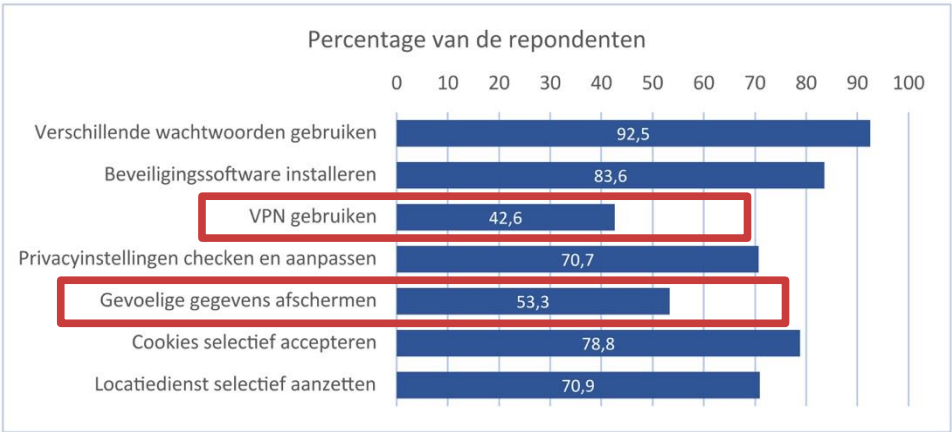
Een snellere manier om gedrag te meten, is het meten ervan in een simulatie. Dat klinkt handig, maar tot nu toe is het nog nergens gelukt om een goede representatieve simulatie op te zetten. In principe is een gedragsmeting in een simulatie wel haalbaar, maar het vergt veel inspanning, met name in het review- en validatieproces. Bovendien kan je zo'n meting nog steeds niet snel bij veel mensen doen. En al helemaal niet in een enquêteomgeving, want die is niet representatief. Een recent onderzoek laat dan ook zien dat een simulatie in een niet-gevalideerde enquêteomgeving tot verkeerde resultaten komt: in de enquêteomgeving

[34] Mintzberg, H. (1973). *The nature of managerial work*. Harper & Row.
[35] Kok, E. de (2025). *Deviating in white, Rebel nurse leadership in the nursing practice*. Proefschrift, Universiteit Utrecht.

vertonen de deelnemers heel ander gedrag dan in hun gewone context.[36] Dat helpt voor het meten natuurlijk niet. Een simulatie is dus in principe wel bruikbaar, maar na grondig voorbereiden en uittesten en alleen voor kleine aantallen mensen. Dus voor ons is zo'n aanpak ook niet zo handig.

Dan blijft de makkelijkste manier om gedrag te meten over, namelijk er gewoon naar vragen. Dat kan ook anoniem. Je kan de mensen dan meteen vragen waarom ze zich zo gedroegen. Bijvoorbeeld: "Gebruik je een VPN op je smartphone? Zo ja, waarom? Zo nee, waarom niet?". Sommigen van jullie denken nu wellicht: "Een VPN? Wat is dat nou? En waarom heb ik die nodig? Mijn smartphone doet het prima zonder!" Als dit voor jou geldt, dan ben je in goed gezelschap, want meer dan de helft van de mensen gebruikt geen VPN, terwijl het wel een van de basismaatregelen is.[37] In een notendop: Een VPN stuurt al je communicatie over het internet via een computer die heel ergens anders staat. Iedereen die jou probeert te traceren volgt daardoor een verkeerd spoor. En dat is weer goed voor je privacy. Als je dit fenomeen niet kent maar wel op je privacy bent gesteld, dan zou ik daar ná deze seminar werk van maken. Gedrag meten door er rechtstreeks naar te vragen, werkt goed, is representatief, betrouwbaar en goed te analyseren.[38] En door ook de 'waarom'-vraag te stellen, weet je meteen wat de oorzaak van het gedrag is. En ook dat blijkt behoorlijk betrouwbaar te zijn. De kritische noten hierover in de literatuur zijn grotendeels te herleiden naar onderzoeksaanpakken die onvoldoende gereviewd en gevalideerd zijn.

Wij hebben de gewoon-vragen-aanpak zelf gebruikt om bij een grote representatieve groep Nederlanders (1000) een gedragsmeting te doen. In onze meting ging het over de omgang met smartphones en laptops.



Figuur 13: Hoeveel respondenten gedrag uitvoeren (Spruit & Kreffer, 2025).

Uit de meting bleek dat veel mensen zich niet veilig gedragen. Voor het onderzoek hebben we zeven basale veilige gedragingen geselecteerd. In figuur 13 is te zien hoeveel mensen deze gebruiken. Naast

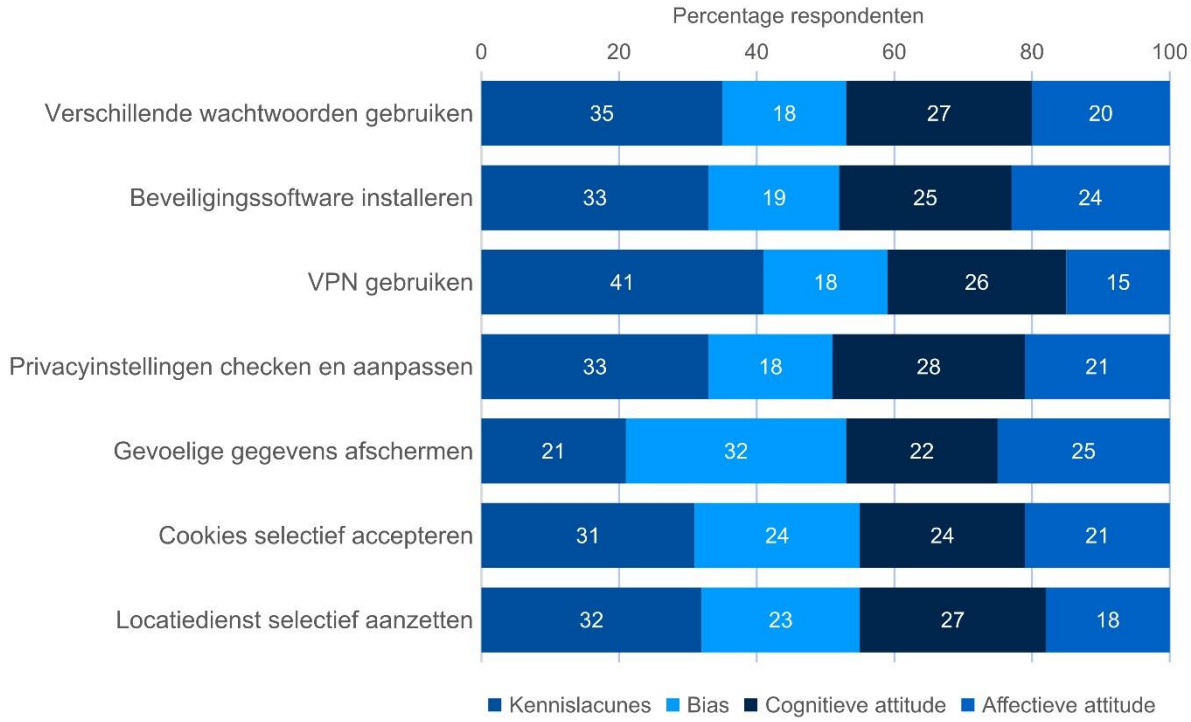
[36] Van 't Hoff-de Goede, M.S., Leukfeldt, E.R., Van de Weijer, S.G.A. & Van der Kleij, R. (2025). Does protection motivation predict self-protective online behaviour? Comparing self-reported and actual online behaviour using a population-based survey experiment. *Computers in Human Behavior Reports*, 18.

[37] Spruit, M., & Kreffer, C. (2025). Veldonderzoek naar (on)veilig gedrag. *IB Magazine*, 25 (2), 28-34.

[38] Spruit, M., Oosting, D. & Kreffer, C. (2024). Factors that influence secure behaviour while using mobile digital devices. *Information and Computer Security*, 32 (5), 729-747.

het gebruik van VPN, komt ook het beschermen van gevoelige gegevens op sociale media er bekaaid vanaf. Hebben jullie het lijstje snel al gescand en gekeken welke gedragingen jullie zelf uitvoeren? Voor echt veilig gedrag moet je overigens meer doen dan alleen deze set. Maar dit is een aardig startpunt voor als je veilig met je digitale media wil werken.

Uit de resultaten van het onderzoek konden we ook afleiden dat het nalaten van veilig gedrag soms door gebrek aan kennis komt, maar dat het even goed kan komen door bias, of door attitudeproblemen, zie figuur 14.[39] En verschillende oorzaken vragen om verschillende verbeteraanpakken.



Figuur 14: De relatieve invloed van verschillende factoren op het nalaten van veilig gedrag (Spruit & Kreffer, 2025).

[39] Spruit, M., & Kreffer, C. (2025). Veldonderzoek naar (on)veilig gedrag. *IB Magazine*, 25 (2), 28-34.

3. Cybersecurity in organisaties

Organisatiefouten spelen een prominente rol in cybersecurity.

Ook in organisaties speelt onveilig gedrag met digitale media. Al die jaren dat ons onderzoek naar gedrag loopt, was het duidelijk dat binnen organisaties nog een wereld te winnen was.

Foto 4: Gemaal Lely, Wieringermeer (7794631 op Pixabay).

Zo'n tien jaar geleden zagen we dat bij de waterschappen. De verantwoordelijken voor cybersecurity hadden geconstateerd dat de cybersecurity nog niet in de pas liep met de voortvarende digitalisering. Dat gold met name voor de digitalisering in het veld, dus van bijvoorbeeld sluizen, gemalen en zuiveringsinstallaties. De waterschappen waren net een verbeterproject aan het opstarten en wij mochten daarbij ondersteunen. We begonnen met een nulmeting en daaruit bleek dat de zorgen terecht waren: de cybersecurity in het veld kwam niet in de buurt van hun eigen streefniveau. Wat vooral lastig bleek, was uit oude denkpatronen stappen. Zo gold al jaar en dag dat elke installatie – bijvoorbeeld een gemaal – in de fout kan gaan, of aangevallen kan worden. Als je heel veel pech hebt, dan kan dat zelfs met twee installaties tegelijkertijd gebeuren – kwestie van statistiek. En erg snel stijgt het water niet als een gemaal ermee stopt, dus je hebt genoeg tijd om het probleem handmatig op te lossen. Gewoon een monteur ernaartoe sturen en die fikst het wel. De kans dat meer dan twee installaties er tegelijkertijd mee stoppen is nagenoeg nul. Behalve, als je alle installaties vanuit dezelfde centrale digitaal aanstuurt. Dat is snel en handig, maar dan kan je met een paar simpele opdrachten alle installaties van het waterschap tegelijkertijd uitzetten. En een hacker die in het systeem is gekomen, kan dat dan ook. En daar helpt geen handmatig fiksen meer tegen. Dus dan moet de cybersecurity worden opgeschroefd. Om de bestuurders daarvan te overtuigen, hadden we nog wat extra overredingskracht nodig.

Foto 5: Simulator in opbouw (Fotograaf onbekend).

Daarom hebben we een simulator gebouwd om de problematiek zichtbaar te maken. Op foto 5 zie je de nagebootste polder met ringvaart in aanbouw. De simulator werd aangevuld met hardware en software die de waterschappen zelf in het veld gebruikten. Op foto 6 zie je de complete simulator.

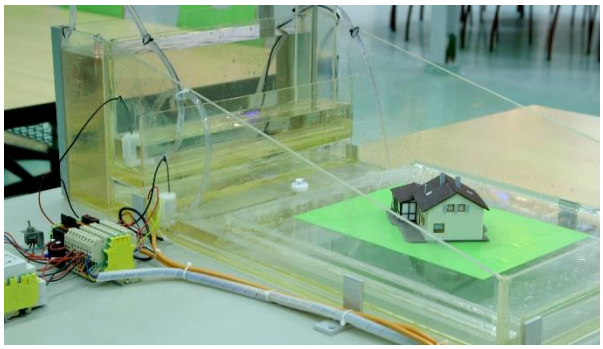


Foto 6: Simulator voor de hack (Fotograaf onbekend).

Toen we de simulator demonstreerden aan bestuurders van de waterschappen, duurde het niet lang voordat de opgetrommelde hacker het poldertje liet overstromen. Toen is foto 7 genomen. De ringvaart is leeggelopen en het boerderijtje staat onder water. En wij hadden alleen techniek gebruikt die de waterschappen zelf in het veld ook gebruikten.

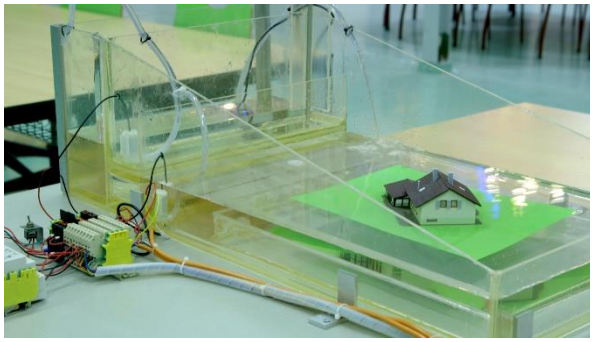


Foto 7: Simulator na de hack (Fotograaf onbekend).

Die boodschap is goed overgekomen. Een paar jaar later hebben we bij een paar waterschappen een vervolgmeting gedaan en de score voor hun cybersecurity was aanzienlijk gestegen.

Uit de onderzoeken die we bij andere organisaties hebben gedaan, blijkt dat medewerkers best vaak de fout in gaan met betrekking tot digitale media. Dat varieert van gebruikers die een usb-stick met belangrijke informatie verliezen, of een journalist van Atlantic magazine uitnodigen voor een top secret Signal-bespreking, tot beheerders die vergissingen maken bij het inregelen van beveiligingssystemen, zoals bijvoorbeeld een firewall.[40] Wat ons in het bijzonder opviel was dat de fouten af en toe worden veroorzaakt door onvoldoende kennis, bijvoorbeeld “Oh gut, is daar een regel voor?”. En af en toe door een verkeerde attitude, bijvoorbeeld “Ja die beveiliging, daar heb ik nu even geen zin in.”

[40] https://www.bbc.com/news/articles/cr52yrgq48no

Maar meestal werden de fouten veroorzaakt door organisatiefouten. De belangrijkste zijn:

1. De “tone at the top” klopt niet, oftewel het management stuurt niet effectief en zichtbaar op veilig gedrag. Vaak geven managers dan ook niet het goede voorbeeld van veilig gedrag, bijvoorbeeld “Ja, ik weet dat de standaard smartphone bij ons een Android-toestel is, maar ìk wil een iPhone”. Dan willen de anderen dat ook wel.
2. Cybersecurity is niet geïntegreerd in het dagelijkse werk, waardoor veilig werken een keuze is, die ook nog eens om extra inspanning vraagt. Dat roept ontwijkgedrag op, vooral als de cybersecuritymaatregelen ook nog eens niet goed zijn doordacht of niet goed zijn ingevoerd.

We zagen nog meer oorzaken, zoals niet-passende procedures, onwerkbaar dichtgetimmerde systemen, te hoge werkdruk, enzovoort. We zagen eigenlijk soortgelijke organisatiefouten als De Kok zag in ziekenhuizen en daarvan hadden we al geconstateerd dat de overtreders schouderklopjes verdienden.[41]

Nu zijn organisatiefouten natuurlijk zelf weer menselijke fouten, maar dan van managers en stafmedewerkers. Kort door de bocht kunnen we stellen dat de meeste incidenten ontstaan doordat managers en stafmedewerkers fouten maken, waardoor activiteiten van ‘gewone’ medewerkers tot problemen leiden.

Organisatietype	Urgentiegevoel	Organisatie van cybersecurity	Cybersecurity voor IT				Cybersecurity voor OT			
			Elementaire maatregelen	Baseline, ISMS	Risicoanalyses	Monitoren, testen, auditen	Elementaire maatregelen	Baseline, ISMS	Risicoanalyses	Monitoren, testen, auditen
Productieorganisaties										
Zaadveredelingsorganisaties										
Technisch toeleveranciers										
Handelsorganisaties										

Tabel 2: Resultaten uit cybersecurityvolwassenheidsmeting Westland (Kerpershoek & Spruit, 2022).

Als we bij organisaties de volwassenheid van de cybersecurity meten, dan komen de organisatiefouten naar boven. In tabel 2 staan de groepsgewijze resultaten van een meting bij organisaties in het Westland.[42] Elke rij is een groep vergelijkbare organisaties. De eerste groep zijn productorganisaties, oftewel kwekers. Elke kolom is een aspect waar de organisaties voldoende aandacht aan moeten besteden. Als dat allemaal goed gaat dan kleurt de hele rij groen en dan is de cybersecurity van behoorlijk niveau. Maar elke oranje of rode cel wijst op

[41] Kok, E. de (2025). *Deviating in white, Rebel nurse leadership in the nursing practice*. Proefschrift, Universiteit Utrecht.

[42] Kerpershoek, E. & Spruit, M. (2022). *Digitale veiligheid van Greenport West-Holland*. De Haagse Hogeschool.

onacceptabele zwakheden. Ik neem aan dat de teneur in het schema jullie zo op het eerste gezicht wel duidelijk is.

Al met al is er voldoende reden om in organisaties meer aandacht te schenken aan de menselijke factor. En aan organisatiefouten, maar die vallen dus ook onder de menselijke factor.

4. Cybersecurityonderwijs

We hebben meer en beter onderwijs op het gebied van cybersecurity nodig.

Mensen zitten steeds vaker en langer op digitale media, zoals een computer of een smartphone, en verwerken daar steeds meer digitale informatie.[43,44,45] Maar hoe veilig gaan mensen hiermee om?[46,47,48] Veilig kunnen omgaan met digitale informatie is een belangrijke 21e-eeuwse vaardigheid.[49] Maar in het onderwijs komt die er nogal bekaaid vanaf. Zo leren scholieren in het primair onderwijs eerst dat “gratis in de cyberwereld niet bestaat” en vervolgens worden ze achter gratis educatieve software gezet.[50] Dat mag natuurlijk niet: “pratice what you preach”. Je zou verwachten dat dan in ieder geval het middelbaar en hoger onderwijs meer aandacht besteden aan het veilig omgaan met digitale informatie, maar dat gebeurt eigenlijk alleen in opleidingen die specifiek opleiden voor het werken met digitale informatie, zoals cybersecurity. Bij andere opleidingen valt het erg tegen.

Hoog tijd voor verbetering in het onderwijs, te beginnen bij het primair onderwijs, maar ook in het middelbaar en hoger onderwijs. Iedereen moet veilig kunnen werken met digitale informatie. Uit de metingen die ik eerder liet zien, is het duidelijk dat we nog lang niet zover zijn. Het zou mooi zijn als op redelijke termijn iedereen de basis van cybersecurity beheerst.

---

43 Highberg (2025). *Verdiepend onderzoek Iene Miene Media*. Netwerk Mediawijsheid.

44 Nawaz, S. (2024). Distinguishing between effectual, ineffectual, and problematic smartphone use. *Computers in Human Behavior Reports*, 14, 100424.

45 Siebers, T., Beyens, I., Pouwels, J.L. & Valkenburg, P.M. (2022). Social Media and Distraction: An Experience Sampling Study among Adolescents. *Media Psychology*, 25 (3), 343-366.

46 Watson, A. (2024). *False news worldwide - Statistics & facts*. Statista.

47 Powell, J. & Pring, T. (2024). The impact of social media influencers on health outcomes: Systematic review. *Social Science & Medicine*, 340, 116472.

48 Echeverria, M., Santamaria, S.C. & Hallin, D.C. (2025). *State-sponsored disinformation around the globe*. Routledge.

49 Thijs, A., Fisser, E. & Hoeven, M. van der (2014). *21e eeuwse vaardigheden in het curriculum van het funderend onderwijs*. SLO.

50 https://www.privacycompany.eu/nl/blog/onderzoek-google-workspace-g-suite-enterprise-rijk-vraagt-advies-autoriteit-persoonsgegevens-over-hoge-privacyrisicos

Daarnaast hebben we dan cybersecurityprofessionals nodig om mensen en organisaties op cybersecuritygebied te ondersteunen.[51] Daarvan hebben we er nog te weinig, hoewel dat nog niet goed terug te zien is in het aantal vacatures voor cybersecurityprofessionals.[52,53] Dat laatste komt doordat veel besturen en directies nog niet goed beseffen welke risico's ze door digitalisering lopen en dat ze daarvoor cybersecurityprofessionals nodig hebben.[54,55] Dus de noodzaak is er wel, maar de vraag nog niet. En degene die ze dat uit kan leggen, de cybersecurityprofessional, die hebben ze nog niet aangenomen. Om uit deze vicieuze cirkel te komen, moeten we eerst de besturen en directies van organisaties bewuster maken van de cyberrisico's voor hun organisaties en van het feit dat goede cybersecurity zo complex is dat ze daar ondersteuning voor nodig hebben. En dàn zou de vraag naar cybersecurityprofessionals moeten gaan stijgen. En dàn moeten opleidingsinstellingen voldoende aanbod klaar hebben staan.

Met dat laatste is mijn lectoraat al vroeg begonnen. We hebben als lectoraat een bachelor- en een masteropleiding ontwikkeld, en meerdere minoren en cursussen. Allemaal op het gebied van cybersecurity. En allemaal met aandacht voor de menselijke factor en organisatieproblematiek. Ook in de technisch georiënteerde opleidingen. Tenslotte moeten ook nerds uit kunnen leggen wat ze hebben gedaan, wat daaruit is gekomen en hoe dat hun collega's gaat helpen.

CAP	Certified Authorization Professional	ISMES	Information Security Management Expert
CBCP	Certified Business Continuity Professional	ISSAP	Information Systems Security Architecture Prof.
CEH	Certified Ethical Hacker	ISSEP	Information Systems Security Engineering Prof.
CGEIT	Certified in the Governance of Enterprise IT	ISSMP	Information Systems Security Management Prof.
CIA	Certified Internal Auditor	MBCP	Master Business Continuity Professional
CIPP	Certified Information Privacy Professional	MISM	Master of Information Security Management
CISA	Certified Information Systems Auditor	MSIT	Master of Science in Information Technology
CISM	Certified Information Security Manager	OPSA	OSSTMM Professional Security Analyst
CISSP	Certified Information Systems Security Prof.	OPST	OSSTMM Professional Security Tester
CITP	Certified Information Technology Professional	QiCA	Qualification in Computer Auditing
CRISC	Certified Risk and Information Systems Control	RE	Register EDP auditor
CSSLP	Certified Secure Software Lifecycle Professional	RIB	Register Informatie Beveiliger
FBCI	Fellow of the Business Continuity Institute	RO	Register Operational auditor

Tabel 3: Een greep uit mogelijke cybersecuritytitels.

[51] Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, 100, 102080.

[52] PTvT & Dialogic (2024). *Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity*. Platform Talent voor Technologie (PTvT) en Dialogic.

[53] Ruijsendaal, M., Benthem, M. van, Kager, P., Kroes, M. & Kokkeler, B. (2023). *Human Capital Agenda Security 2023-2026*. Security Delta en Centrum voor Veiligheid en Digitalisering.

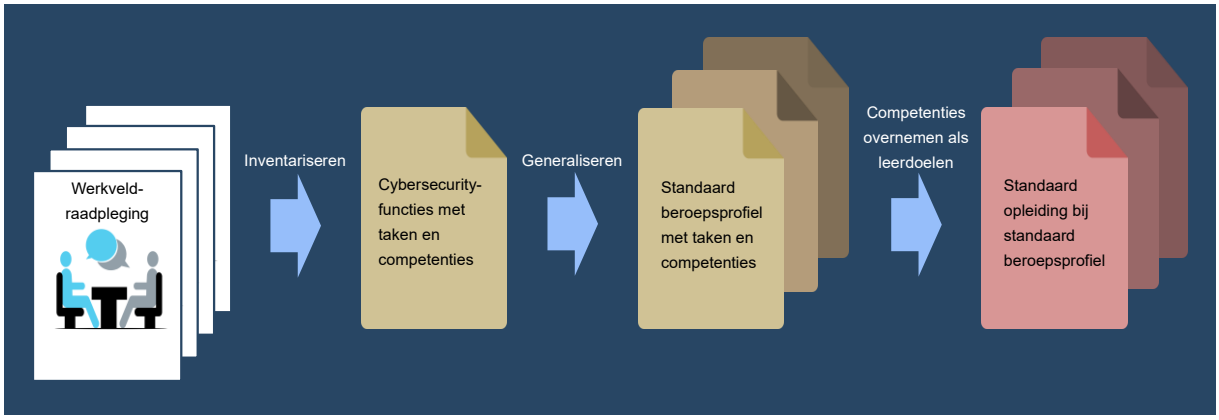
[54] Spruit, M., & Kerpershoek, E. (2022). *Digitale veiligheid van Greenport West-Holland*. Den Haag: De Haagse Hogeschool.

[55] Spruit, M., Kerpershoek, E., Blankers. H., Bertens, H., & Paalman, L. (2023). *Digitale veiligheid van de Life Sciences & Health-sector*. Den Haag: De Haagse Hogeschool.

Inmiddels zien we steeds meer opleidingen op het gebied van cybersecurity ontstaan. Dat is weliswaar een mooie ontwikkeling, maar doordat verschillende partijen zonder afstemming opleidingen ontwikkelen, is een chaotische situatie ontstaan. De chaos wordt nog versterkt doordat verschillende aanbieders verschillende certificaten afgeven en titels die je achter je naam mag zetten. In de tabel staan een paar voorbeelden. Er zijn er nog veel meer. Voor sommige titels moet je jaren studeren en voor andere is een paar dagen ruim voldoende. Het grootste aantal titels wat ik bij één persoon achter zijn naam ben tegengekomen is veertien. Is zo iemand nu goed in z'n vak, of geobsedeerd door titels? Niemand heeft meer het overzicht.

Het werkveld zou geholpen zijn met een beperkt aantal standaard cybersecurityopleidingen waarvan iedereen makkelijk kan nagaan wat erin geleerd wordt. Bijvoorbeeld een opleiding voor Information Security Officer, of ICT-beveiligingsspecialist. Het opleidingenveld wordt daardoor eenduidiger en overzichtelijker. Toekomstige cybersecurityprofessionals kunnen dan beter beoordelen welke opleidingen ze zouden moeten volgen en personeelsfunctionarissen kunnen dan beter bepalen welke opleidingen nodig zijn voor cybersecurityfuncties. Maar wat wellicht nòg belangrijker is, is dat iedere cybersecurityprofessional beter een individueel leerpad uit kan zetten, met goed op elkaar aansluitende standaard opleidingen.

Wat hebben we hiervoor nodig? Ten eerste de specificaties voor de standaard opleidingen.[56] Dan hoeft niet iedere onderwijsinstelling voor elke nieuwe opleiding weer opnieuw een set competenties te bedenken. In plaats daarvan specificeert een vertrouwde partij de competenties voor de standaard opleidingen en houdt die actueel.



Figuur 15: Werkwijze voor de ontwikkeling van standaard cybersecurityopleidingen.

De werkwijze hiervoor is als volgt, zie figuur 15.[57] Om te beginnen wordt op basis van een werkveldraadpleging geïnventariseerd wat voor functies iemand na de standaard opleiding zou kunnen krijgen, welke taken daarbij horen en welke competenties diegene dan zou

[56] Davidovitch, N. (2013). Learning-Centered Teaching and Backward Course Design – From Transferring Knowledge to Teaching Skills. *Journal of International Education Research*, 9 (4), 329-338.

[57] Spruit, M. (2022). Information security education based on job profiles and the e-CF. *Higher Education, Skills and Work-based Learning*, 12 (2), 294-308.

moeten hebben. Aangezien dit voor elke organisatie weer anders is, wordt dit gegeneraliseerd tot een standaard beroep, bijvoorbeeld Information Security Officer. Voor dit standaard beroep is dan bekend welke taken erbij horen en welke competenties daarvoor nodig zijn. Dit wordt dan netjes beschreven in een standaard beroepsprofiel.[58]

Samen met het *Platform voor Informatiebeveiliging*, het PvIB, hebben we in 2017, in overleg met het werkveld, zes standaard cybersecurityberoepen bepaald en hiervoor standaard beroepsprofielen beschreven. Deze zijn toen grondig gereviewd door werkveldpartijen en onderwijsinstellingen.[59]

Bij het Europese agentschap ENISA vond men dat blijkbaar wel een interessant proces en nu onze beroepsprofielen alweer aan de oude kant zijn, wilden ze die exercitie nog een keer dunnetjes overdoen met een tijdelijke werkgroep. Dat heeft geleid tot het *European Cybersecurity Skills Framework*.[60] Als je er even naar kijkt dan zie je dat dat niet goed is gegaan: geen visie, verkeerde keuzes, niet gestandaardiseerd en onvoldoende gereviewd. Daarmee los je dus geen problemen op. Op dit moment lijkt het een reële optie om terug te gaan naar de standaard beroepsprofielen die we samen met de PvIB hebben opgesteld en deze te actualiseren.

Als je een nieuwe opleiding op wil zetten, dan selecteer je eerst het standaard beroep waarvoor de opleiding op gaat leiden, bijvoorbeeld ICT-beveiligingsspecialist 3. Dan zie je in het bijbehorende beroepsprofiel welke competenties nodig zijn. Deze competenties zijn de aan te leren kennis en vaardigheden en dat zijn dus de leerdoelen van de opleiding. De beoogde docenten kunnen daar dan wel een goed lesprogramma voor bedenken.

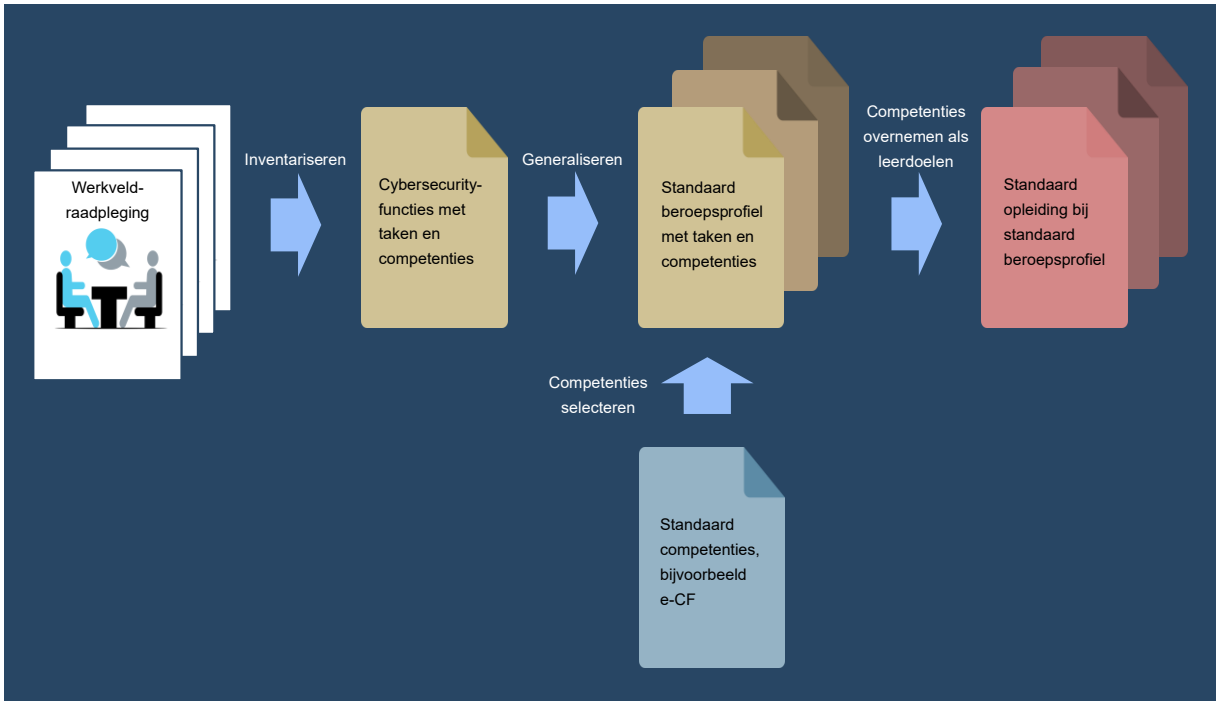
---

58 CEN (2018). *CWA 16458-1: European ICT professionals role profiles - Part 1*. European Committee for Standadization.

59 Spruit, M. & Van Noord, F. (2017). *Beroepsprofielen informatiebeveiliging 2.0*. PvIB.

60 ENISA (2022). *European Cybersecurity Skills Framework (ECSF) User Manual*. The European Union Agency for Cybersecurity (ENISA).

Om standaard opleidingen nòg eenduidiger te maken, kunnen we nog een stap verder gaan. We kunnen namelijk ook de competenties standaardiseren tot een soort Lego-blokjes in opleidingsland. Dan hoef je voor een nieuw beroepsprofiel niet steeds opnieuw competenties te bedenken, maar dan selecteer je steeds de geschikte competenties als bouwsteentjes uit een doos. En die neem je dan op in het beroepsprofiel, zie figuur 16.[61]



Figuur 16: Werkwijze voor de ontwikkeling van standaard cybersecurityopleidingen.

Het voordeel van gestandaardiseerde competenties is dat de standaard beroepsprofielen, en daarmee de standaard opleidingen, nog eenduidiger worden. En bovendien kan je gebruik maken van lesmaterialen die hiervoor al zijn ontwikkeld.

Al in 2006 had een groep Europese organisaties zelf ook al bedacht dat gestandaardiseerde competenties wel eens handig zouden kunnen zijn. Onder aanvoering van de Europese standaardisatie-instelling CEN leidde dat tot het opzetten van het Europese *e-Competence Framework*, oftewel e-CF.[62] Dit bevat een set gestandaardiseerde competenties voor het IT-werkveld. Althans, dat was de bedoeling.

Tijdens het opstellen van het e-CF zijn twee cruciale fouten gemaakt, waardoor e-CF uiteindelijk geen oplossing is, maar een probleem.

---

61 Spruit, M. (2022). Information security education based on job profiles and the e-CF. *Higher Education, Skills and Work-based Learning*, 12 (2), 294-308.

62 NEN (2019). *NEN-EN 16234-1 e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all sectors - Part 1: Framework*. NEN.

Foto 8: Bouwen met blokken (Gemaakt met AI).

De eerste fout is dat de ontwerpers het doel uit het oog zijn verloren. Het was de bedoeling om de competenties te standaardiseren tot een soort Lego-blokjes in opleidingsland. Dan moet je natuurlijk wel die Lego-blokjes in je achterhoofd houden en er geen megablokken van maken, zie foto 8. Als de bouwblokken te groot zijn, en dat zijn ze, dan werkt het idee van bouwblokken niet meer.

De tweede fout is dat de standaardisatie is losgelaten. Het was de bedoeling om een verzameling gestandaardiseerde competenties te krijgen die je zelf kan combineren, net zoals je met standaard Lego-blokjes een mooi Lego-kasteel kan maken. Maar nu staat er in de standaard dat je alles naar eigen goeddunken mag wijzigen.[63] Dan is de standaard dus geen standaard meer en het huis op foto 9 een standaard Lego-rijtjeshuis. En als de standaard geen standaard is dan heeft grondig reviewen ook geen zin en dat is dan ook niet gedaan.

Foto 9: Gestandaardiseerd?! (Gemaakt met AI).

Desondanks hebben we het e-CF, zij het zwaar gemodificeerd, gebruikt voor het ontwikkelen van de wetenschappelijke master Cyber Security Engineering. Daarvoor hebben we de competenties in het e-CF eerst opgehakt in compacte hapklare brokken, die geherformuleerd, opnieuw opgedeeld in kennis- en vaardigheidselementen, die voorzien van competentieniveaus en vervolgens alles goed laten reviewen.[64,65,66] Uit de zo verkregen competenties konden we een selectie maken op basis van één

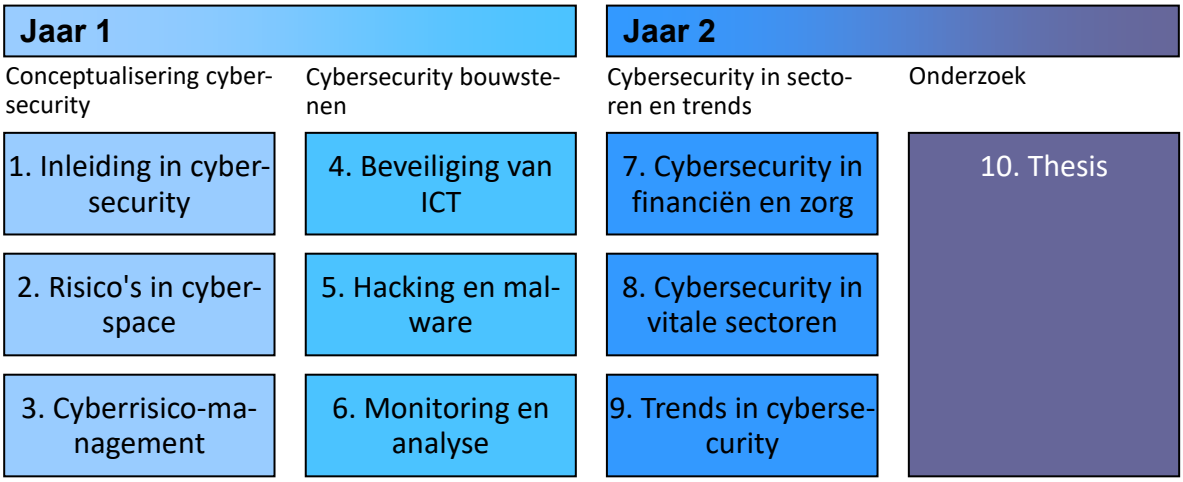
[63] NEN-EN 16234-1 e-Competence Framework (e-CF) - Part 1: Framework, pagina 3, 5, 17 e.v.

[64] Spruit, M. (2022). Information security education based on job profiles and the e-CF. *Higher Education, Skills and Work-based Learning*, 12 (2), 294-308.

[65] EC (2008). *The European Qualifications Framework for Lifelong Learning (EQF)*. European Communities.

[66] Kempers, A. & Petel, F. (2006). Naar een Europees kwalificatiestelsel (EQF). *Examens*, 2006 (4), 19-23.

van de standaard beroepsprofielen. En die selectie konden we gebruiken voor het specificeren van de nieuwe opleiding. De opleidingsstructuur staat in figuur 17.



Figuur 17: Curriculum van de master Cyber Security Engineering.

Door deze zeer gestructureerde aanpak rolde deze master moeiteloos door de verplichte accreditatie. In plaats van de gebruikelijke opbouwende kritiek, kregen we complimenten. En dat lag niet aan het feit dat de commissie weinig kritisch zou zijn, integendeel.

We hebben op deze manier laten zien dat het goed mogelijk is om standaard beroepsprofielen en standaard competenties te formuleren en daarmee succesvol een standaard opleiding te ontwikkelen. Als elke opleiding goed beschreven kan worden in standaard competenties dan is het voor iedereen duidelijk waar de opleiding over gaat en hoe deze aansluit op andere gestandaardiseerde opleidingen en hoe dat weer past in iemands beoogde leerpad.[67,68]

Inmiddels zijn we met ons lectoraat weer verdergegaan en onderzoeken we hoe we de cybersecurityrollen in het mkb kunnen beschrijven als standaard beroepsprofielen met standaard competenties. Vooralsnog gebruiken we daarvoor het door ons aangepaste e-CF. Op basis daarvan kunnen we dan beter onderwijs voor deze cybersecurityrollen ontwikkelen. En dat moet het mkb sterker maken in de strijd tegen cyberdreigingen.

[67] Kaplan, A. (2016). Lifelong learning: Conclusions from a literature review. *International Online Journal of Primary Education*, 5 (2), 43-50.

[68] Baumann, S. & Keimer, I. (2023). Individual Benefits of Continuing Higher Education. The Case of a Swiss Business School. *Journal of Adult and Continuing Education*, 29 (2), 343-359.

5. Ten slotte

Ik nader het eind van mijn presentatie. In de afgelopen jaren ben ik met veel plezier bezig geweest met onderzoek en het ontwikkelen en geven van onderwijs. Het onderwerp cybersecurity blijft me boeien, dus ik zal een aantal vakgenoten vakmatig nog wel tegenkomen, maar dan als emeritus.

Rest mij om iedereen die mijn lectoraat mogelijk en succesvol maakte te bedanken. Dat zijn te veel mensen om hier op te noemen. Het varieert van degenen die het mogelijk maakten om het lectoraat te beginnen tot de onderzoekers uit het lectoraat en de mensen uit het veld waar we mee samenwerkten. En familie en vrienden die me steeds opnieuw energie gaven. Toch wil ik hier nog wel even de altijd onmisbare ondersteuners noemen. Zo hebben Nicole en Maaike ook dit seminar weer georganiseerd. Maar de allerbelangrijkste rol was natuurlijk weggelegd voor mijn vrouw Marian. Zij heeft me gestimuleerd om dit lectorschap op te pakken en was steeds een onmisbare steunpilaar en klankbord voor me. Heel erg bedankt!

Deze publicatie heeft licentie CC BY 4.0
(Creative Commons Naamsvermelding 4.0 Internationaal),
zie https://creativecommons.org/licenses/by/4.0/

let's change
YOU. US. THE WORLD.

DE HAAGSE
HOGESCHOOL