DIGITALE VEILIGHEID ALS MAATSCHAPPELIJKE UITDAGING

NAAR EEN SYSTEEMAANPAK VAN CYBER SECURITY

Openbare les
23 april 2026

Dr. Martine Groen

Kenniscentrum Digital Business and Media
Lectoraat Cyber Security

HOGESCHOOL UTRECHT

HIER KOMT ALLES SAMEN

DIGITALE VEILIGHEID ALS MAATSCHAPPELIJKE UITDAGING

NAAR EEN SYSTEEMAANPAK VAN CYBER SECURITY

Openbare les
23 april 2026

Dr. Martine Groen

Kenniscentrum Digital Business and Media
Lectoraat Cyber Security

INHOUD

INLEIDING

Je hoeft het nieuws maar open te slaan, of je leest weer over een nieuw cyber security incident, over onze afhankelijkheid van Big Tech en digitale autonomie, of over kennisspionage en -diefstal vanuit China.[1] Het aantal cyber security aanvallen neemt toe, met als gevolg enorme financiële en maatschappelijke schade en ook reputatieschade.

We zien dat cyber security criminelen zich specifiek richten op bepaalde groepen vanwege hun verhoogde kwetsbaarheid, zoals het Midden en Klein Bedrijf (MKB), Operational Technologie (OT), ouderen en jongeren.[2,3]

De verantwoordelijkheid van de huidige cyber security ligt primair bij bedrijven en publieke instanties. Maar de impact van een hack is veel breder dan het bedrijf dat aangevallen wordt.[4] Burgers kunnen jaren later nog last krijgen van identiteitsfraude, jongeren worden al vanaf jonge leeftijd online benaderd en afgeperst zonder dat ouders of school het doorhebben. Ook is digitaal gedrag niet beperkt tot de afgeschermde veilige omgeving van het werk, maar gebruiken we ook privé veelvuldig allerlei digitale mogelijkheden. Dat maakt cyber security tot een maatschappelijk probleem.

Het steeds grotere aantal aanvallen in combinatie met de verhoogde maatschappelijke impact vereist actie – vanuit bedrijven, overheden en consumenten. In de afgelopen jaren zijn er dan ook verschillende initiatieven opgezet. Vanuit de wetgevende kant, en specifiek vanuit de Europese Unie, wordt binnen de Digital Decade en alle regulering die daaruit voorkomt, met een groot aantal nieuwe wetten gepoogd om bedrijven te dwingen hun cyber security te verhogen tot een minimum niveau, zoals AI act, NIS2 (de Nederlandse implementatie

in de cyberbeveiligingswet), de Cyber Resilience Act en de AVG. Ook zijn er vanuit het werkveld verschillende securitystandaarden opgesteld en wordt er aandacht besteed aan de menselijke factor, door bewustwordingscampagnes aan te bieden.

Tegelijkertijd zie je ook een grote mate van gelatenheid en frustratie in de samenleving ontstaan als het gaat om cyber security.[5] Iedereen wordt weleens gehackt, er is toch niks tegen te doen, twee-factor-authenticatie is vervelend. Ook is een substantieel deel van de bevolking nog van mening: ik ben niet interessant voor hackers. Dit verlamt het accuraat handelen van bedrijven en individuen.

De bestaande initiatieven en tendensen staan veelal los van elkaar en zijn gericht op een specifieke doelgroep. Maar dat gaat voorbij aan het feit dat mensen en organisaties functioneren in een systeem. Cyber security keuzes in het ene veld hebben invloed op cyber security keuzes in het andere veld.

> **Actie is nodig, omdat het aantal cyber security aanvallen steeds groter wordt en ook de maatschappelijke impact ervan.**

EEN INTEGRALE AANPAK VAN DIGITALE ONVEILIGHEID IS NODIG

We kunnen het complexe maatschappelijke probleem van digitale onveiligheid alleen bestrijden met een systeemaanpak. Een integrale aanpak, waarin het probleem als systeem wordt bekeken, om vervolgens door een combinatie van gerichte maatregelen op meerdere fronten tegelijk te worden aangepakt. Met enkel losstaande maatregelen die door een organisatie worden genomen, zie je dat het systeem er gemakkelijk 'omheen gaat', en dat de criminelen vrij spel houden. De noodzaak van een integrale aanpak in cyber security van de toekomst wil ik hieronder graag illustreren met een aantal voorbeelden.

Waarom een systeemaanpak aan de wieg staat van de oplossing

Als hacks maar openbaar gemaakt zouden worden, zouden bedrijven wel gedreven zijn om digitaal veilige producten te leveren, was heel lang de gedachte. Vanuit die veronderstelling werd ruim tien jaar geleden een meldplicht datalekken vastgelegd in de AVG. Burgers worden gewaarschuwd, het bedrijf leidt reputatieschade, en er kunnen eventueel boetes worden uitgedeeld als mocht blijken dat het bedrijf nalatig met persoonsgegevens is omgegaan.

Maar bedrijven blijken maar zeer beperkt gemotiveerd zijn om hun digitale veiligheid te verhogen boven het minimale. Dat heeft drie oorzaken:

- De reputatieschade vertaalt zich niet of maar beperkt naar een lagere beurswaarde op de lange termijn.[6,7]
- Consumenten en afnemers zijn tot op heden maar zeer beperkt bereid om meer te betalen voor een veiliger product.[8]
- De pijn van een datalek of hack ligt vaak niet bij het bedrijf, maar bij consumenten of toeleveranciers.

Bron: Pexels.

Cyber security volgt dus niet de simpele economische wetten, en er is een gebrek aan incentives om veiliger te worden. Neem bijvoorbeeld de hack bij het bevolkingsonderzoek eind 2025, waarbij de medische gegevens van 485.000 vrouwen openbaar zijn gemaakt.[9] De overheidsinstantie Bevolkingsonderzoek Nederland gaf een externe partij, in dit geval een laboratorium, de opdracht om monsters te verwerken. Dit laboratorium was, naar later blijkt ook herhaaldelijk, kwetsbaar voor aanvallen. De eindverantwoordelijke volgens de wet blijft echter Bevolkingsonderzoek Nederland, en deze organisatie zal wellicht een boete krijgen. De burgers die te goeder

> **Met enkel losstaande maatregelen vanuit organisaties, houden criminelen vrij spel. Een systeemaanpak is noodzakelijk.**

trouw en zonder keuze van aanbieder, hun weefsel en informatie aan Bevolkingsonderzoek Nederland hebben toevertrouwd, zijn echter de dupe. Zij kunnen last krijgen van identiteitsfraude en misbruik van zeer gevoelige medische informatie.[10] Ook zie je dat het vertrouwen en bereidheid om in de toekomst deel te nemen aan het bevolkingsonderzoek afneemt, met potentiële gezondheidsschade tot gevolg.[11]

De oplossing ligt bij een integrale aanpak, zodat de pijn wordt gevoeld bij de verantwoordelijke, en de burger wordt beschermd tegen – of ten minste gecompenseerd wordt voor – leed en schade. Dit zou op eenzelfde wijze kunnen als de automatische vergoeding bij vertraging van vluchten. Maar er kan méér gedaan worden. Denk bijvoorbeeld aan minimum digitale beveiligingseisen, automatische financiële compensatie voor gedupeerden bij een datalek, en de staat van cyber security als output in het financieel jaarverslag van organisaties.

Voorbeeld uit onderzoek – Keten Cyber Security
Een van de projecten van ons lectoraat is Keten Cyber Security, een samenwerking van Hogeschool Utrecht met Avans Hogeschool en de Haagse Hogeschool. We onderzoeken en ontwikkelen methoden om de cyber security van een hele keten van organisaties in te richten, onder andere voor en met de energiesector, om zo maatschappelijke en organisatie-overstijgende cyber security vraagstukken te kunnen adresseren.

CYBER SECURITY IS GEEN TECHNISCH FEESTJE

Traditioneel wordt cyber security opgepakt door IT. Dit heeft impact op diverse manieren:

- Men benadert het probleem eerst en voornamelijk technisch. Eventuele menselijke en organisatorische maatregelen worden vaak pas in tweede instantie opgepakt of over het hoofd gezien, terwijl aanvallen vaak ook via een menselijke schakel gaan.
- De cyber security leider (CISO) is vaak technisch geschoold. Dat resulteert in een technische benadering richting het hoger management, terwijl het hoger management een risicobenadering gewend is. Het gevolg kan zijn een beperkt budget en een gedemotiveerde CISO.[12]
- Veel van de huidige (cyber security) modellen zijn technisch aangevlogen, zoals het 7-laags OSI model. Hierdoor worden keuzes gemaakt op basis van maatregelen, in plaats van de context van het systeem.

Maar cyber security is geen technisch feestje. We moeten het probleem bekijken vanuit verschillende disciplines. Een systeemaanpak – waarbij alle aspecten (menselijk, organisatorisch en technisch) gelijkwaardig worden meegenomen – zal ertoe leiden dat er een compleet beeld ontstaat, en dat de gekozen maatregelen dekkend en effectief zijn volgens het Defense in Depth-principe.

> **Menselijke, organisatorische en technische aspecten moeten gelijkwaardig worden meegenomen.**

Voorbeeld uit onderzoek – cyber security risico's door het gebruik van shadow IT

In dit promotie-onderzoek van Hogeschool Utrecht in samenwerking met de Radboud Universiteit, kijken we naar welke factoren (menselijk, organisatorisch en technisch) onderliggend zijn aan het gedrag van medewerkers om niet-gecontroleerde IT (shadow IT) te gebruiken, en zo het bedrijf mogelijk kwetsbaar te maken voor cyber security aanvallen. Je ziet dat medewerkers niet bewust onveilig willen werken maar toch shadow IT gebruiken, vanwege een combinatie van menselijke, organisatorische en technische redenen. Ook ontwikkelen we een interventie die specifiek gericht is op deze factoren, zodat het bewustzijn en daarmee ook gedrag van medewerkers kan worden veranderd.[13]

Bron: Pexels.

CYBER SECURITY IS DE VANGRAIL VOOR MENSGERICHTE DIGTIALE INNOVATIE

We leven in een tijd waarin digitale innovaties elkaar in rap tempo opvolgen. Denk aan AI, die door de algemene beschikbaarheid van ChatGPT en dergelijke nu breed toegankelijk is en wordt ingezet voor heel veel toepassingen. Maar ook de ontwikkelingen op het gebied van cryptografie, robotica en Internet of Things (IoT) nemen nu een vlucht (zie Tech Trends-rapport SURF, 2026).[14] Tegelijkertijd groeit de hoeveelheid data die worden verzameld, zowel qua vorm als qua aantal plekken. Sensoren (IoT) worden op veel meer plaatsen toegepast en de data en informatie die daarvandaan komen, zullen een veel breder beeld schetsen dan de tekst- en taaldimensie waar we voornamelijk aan gewend zijn.

Cyber security by design

We moeten in deze tijd van innovatie cyber security niet vergeten. Cyber security by design vormt een belangrijk onderdeel van innovatie. Dat houdt in dat cyber security een integraal onderdeel is van ontwerp, bouw, uitvoering en afbouw. Uit het verleden is immers gebleken dat een cyberlaag toevoegen aan het einde van het ontwikkelproces vanwege tijdsdruk maar in beperkte mate gebeurt. Bovendien is dit minder effectief, het leidt tot een beperkte defense in depth. Hierdoor

> **Cyber security hoort integraal onderdeel te zijn van ontwerp, uitvoering en afbouw.**

blijven er steeds structurele kwetsbaarheden zitten in nieuw ontwikkelde technologie.

Door deze visie op cyber security kan digitale innovatie gefaciliteerd worden vanaf het begin tot eind, van ontwerp tot afbouw. We kunnen duidelijke kaders geven waarbinnen de innovatie op een veilige en ethisch verantwoorde manier kan plaatsvinden. Zo kunnen we veilig mensgericht digitaliseren op basis van principes van digital trust, security en privacy by design. De cyber security professional van de toekomst dient ook integraal te denken en mee te denken tijdens de innovatie. Nee zeggen zonder alternatief te bieden zal alleen maar resulteren in innovatie zonder security.

Voorbeeld uit onderzoek – cyberweerbare gemeentelijke infrastructuren

Dit project is een samenwerking van Hogeschool Utrecht met de Haagse Hogeschool. We kijken hoe gemeenten de digitale veiligheid van hun operationele infrastructuren kunnen borgen. Dat betreft Operational Technology zoals in sluizen en verkeerslichten. De onderliggende technologieën kunnen zowel oud zijn als nieuw. Sluizen gaan tientallen jaren mee, terwijl er tegelijkertijd de laatste jaren veel is geïnnoveerd in sensortechnologie in sluizen. De data en het belang van de beschikbaarheid maken dit tot een urgent vraagstuk. Sluizen hebben veel IoT-sensoren, al dan niet met autonome beslismogelijkheden. En je wilt niet dat een sluis kan worden opengezet van buitenaf. In dit project ontwikkelen we zowel technische als governance oplossingen om de weerbaarheid van gemeentelijke infrastructuren te verhogen.

WAT KAN HET LECTORAAT CYBER SECURITY BRENGEN?

Praktijkgericht onderzoek speelt een essentiële rol om vraagstukken zoals eerder benoemd te kunnen adresseren. Het lectoraat Cyber Security van Hogeschool Utrecht is opgericht in 2022 met als doel deze vraagstukken te beantwoorden. Als lector heb ik gekozen voor een expliciete systeemaanpak: we onderzoeken digitale vraagstukken vanuit verschillende perspectieven, om zo tot duurzame effectieve oplossingen te komen.

Bij deze systeemaanpak past dan ook een divers team, waarbij de leden van het lectoraat ieder een andere achtergrond hebben. Hun expertisegebieden en ervaring op het gebied van onderwijs, onderzoek en praktijk zijn heel verschillend. Dit maakt dat ook de integratie en adoptie van onderzoek bij en met de praktijk en het onderwijs op een natuurlijke manier plaatsvindt. Door producten als systeem gezamenlijk te ontwikkelen, zorgen we voor de creatie van kennis en producten die meteen kunnen worden toegepast door het werkveld en de toekomstige professionals.

Onderzoekslijnen

Om vanuit het lectoraat bij te dragen aan de cyber security van de toekomst, zijn de volgende onderling gerelateerde onderzoekslijnen gedefinieerd:

- *Veilige digitale cultuur.* Mensen, van jong tot oud, maken gebruik van de digitale wereld, op het werk en privé. Hoe kunnen we mensen bewegen om zich veilig digitaal te gedragen zodat ze volledig gebruik kunnen maken van de digitale mogelijkheden?
- *Veilig toegepaste digitale innovatie.* Hoe kunnen we nieuwe technologische ontwikkelingen omarmen, maar wel toepassen op een verantwoorde en veilige manier?

- *Digitale veiligheid binnen gemeenschappen.* Organisaties zijn onderling (digitaal) verbonden, in toevoerketens maar ook in branche-verenigingen. Hoe richt je de digitale veiligheid van de gemeenschap zo in dat organisaties op een veilige manier kunnen samenwerken?

Deze onderzoekslijnen bouwen voort op een breed scala aan expertises aanwezig binnen het lectoraat. Ze betreffen de volgende thema's: digitaal gedrag en gedragsverandering; digitale weerbaarheid van het MKB en de energiesector; Operational Technology (OT); digitale autonomie; TRUST; security architectuur; security governance; security leiderschap; digital identities; AI; netwerk security; en data security.

Cyber security is het meest krachtig als het geïntegreerd wordt met andere expertises, zoals security by design. De deelname binnen het Kenniscentrum Digital Business en Media van Hogeschool Utrecht, alsmede de sterke link met de HU-instituten ICT en Veiligheid en met andere lectoraten, is dan ook essentieel voor het floreren van het lectoraat. Ook externe samenwerkingen zijn essentieel voor het succes.

Projecten en samenwerkingen

Gezamenlijk resulteert dit in de volgende lopende projecten en samenwerkingen:

- Shadow IT – promotie-onderzoek in samenwerking met Radboud Universiteit.
- CISO leiderschap – in samenwerking met Neyenrode Business Universiteit.
- Cyberweerbare gemeentelijke infrastructuren (OT) – in samenwerking met de Haagse Hogeschool.
- Kenniswerkplaats Veiligheid – onder andere MKB startup.
- Digitale Weerbaarheid van het MKB – in samenwerking met Hogeschool Saxion.
- Digital Trust & Digital identities.
- Cyber security over ketens – in samenwerking met Avans Hogeschool en de Haagse Hogeschool.
- Digitale weerbaarheid van reservisten.

AI-event Universiteit Utrecht, 24 maart 2026. Foto Jelmer de Haas.

AI Cyber Security Lab

Ook zijn we per maart 2026 samen met de Universiteit Utrecht het AI Cyber Security Lab begonnen. In dit nieuwe lab zorgen we voor synergie en kruisbestuiving tussen het lectoraat Cyber Security van lector Martine Groen en het AI Lab for Cyber Security van dr. Slinger Jansen van de Universiteit Utrecht, om zo gezamenlijk grotere projecten met het werkveld te kunnen oppakken. Op deze wijze kan ons team samen met de diverse partners toegepast onderzoek met impact uitvoeren en zo de cyber security van de toekomst mede vormgeven.

> **Cyber security is het meest krachtig als het geïntegreerd wordt met andere expertises, zoals security by design.**

WAT KUN JE ZELF DOEN VOOR DE CYBER SECURITY VAN DE TOEKOMST?

Zoals eerder betoogd is een systeemaanpak essentieel voor een duurzame en effectieve cyber security van de toekomst. Maar wat kun je als organisatie, beleidsmaker of consument zelf doen? Wetenschappelijk onderzoek van het lectoraat Cyber Security en anderen, heeft op deze vraag al wat antwoorden gevonden.

Verandering van mindset

Allereerst vereist dit van alle betrokken spelers een verandering van mindset:

- Kijk niet alleen naar je eigen stukje van de puzzel, maar doe een stap terug, bekijk de puzzel, en beslis dan wat er nodig is voor het geheel.
- Betrek alle spelers inclusief de maatschappij. Samen zijn jullie sterker en de meer ervaren spelers kunnen de kleintjes onder hun hoede nemen.
- Adopteer een gecombineerde gezamenlijke aanpak. Wanneer een speler een nieuwe securitylaag implementeert, zoekt het systeem automatisch de volgende zwakke schakel bij een van de andere spelers. Een systeemaanpak zorgt voor een duurzame verbetering van de cyber security.

> **Streef naar digitale autonomie.**

Acties door cyber security management

Naast deze drie generieke basisprincipes van systeemaanpak, hebben zeker ook de individuele spelers een handelingsperspectief. Het hoofd van security, vaak de CISO, kan daarnaast de volgende acties ondernemen:

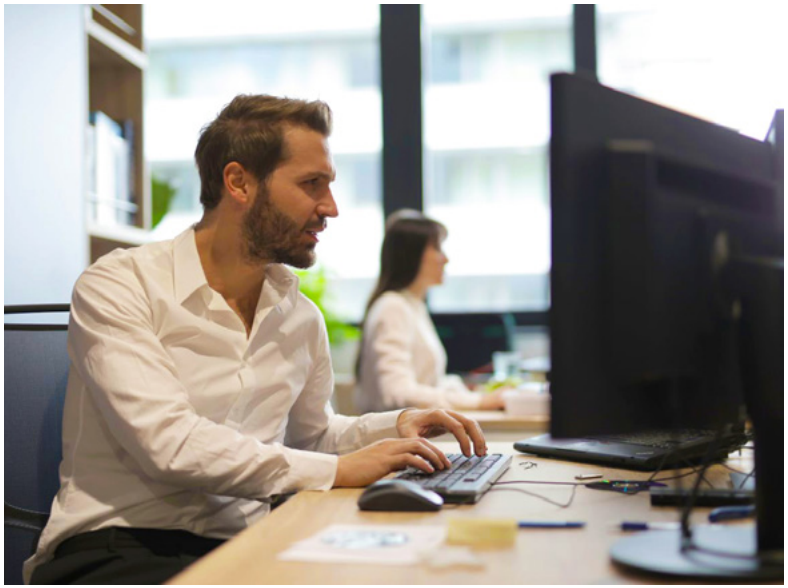
- Participeer in een cyber security community – per branch of per sector – met hetzelfde cyber security doel en dezelfde visie op security. Onderzoek van het lectoraat naar MKB-weerbaarheid en ketensecurity toont aan dat communities een essentiële rol kunnen spelen in het versterken van de digitale weerbaarheid. Dit zorgt ervoor dat je eerder op de hoogte bent van de actuele dreigingen en daar sneller op kunt acteren. Tegelijkertijd krijg je een compleet beeld van de staat van cyber security van het systeem, zoals de toeleveringsketen, en kun je gericht systematisch je eigen cyber security inrichting hierop aanpassen.
- Neem in je team actief mensen aan met een verschillende achtergrond, zoals ICT, veiligheidskunde, economie, psychologie en rechten, in plaats van mensen die op jezelf lijken. Een divers team zal zorgen voor een compleet beeld van je cyber security landschap en leiden tot evenwichtige, effectieve keuzes qua maatregelen.

Acties door beleidsmakers en Justitie

Beleidsmakers en Justitie kunnen naast het volgen van de basisprincipes, ook de volgende acties ondernemen:

- Betrek actief alle doelgroepen die deelnemen in de digitale wereld, en dat is nu bijna iedereen. Een groot deel van deze groepen is niet of nauwelijks bekend met cyber security. Ons onderzoek naar reservisten laat tevens zien dat digitaal gedrag niet ophoudt als de werkdag voorbij is, maar dat ook privésituaties relevant zijn.
- Naast het versterken van het bewustzijn is het belangrijk om in te zetten op onbewust automatisch gedrag en de verandering daarvan. Creëer een omgeving, zowel maatschappelijk als via wetgeving, waarin veilige keuzes automatisch en zonder veel moeite genomen worden. Bijvoorbeeld: data die niet standaard worden verzameld, of automatische schadevergoeding bij een datalek.

- Geef zelf het goede voorbeeld. Burgers verwachten impliciet van de overheid dat veilig omgegaan wordt met hun data. Helaas is dit nog niet in alle gevallen terecht.
- Geef digitale criminaliteit dezelfde prioriteit als fysieke criminaliteit. Burgers en organisaties hebben recht op een veilige digitale omgeving, en waar nodig vervolging.
- Neem cyber security actief mee in besluitvorming en handelen, ook in niet cyber security-specifieke situaties. De keuze voor een bepaalde externe dienst kan ook gevolgen hebben voor de staat van cyber security en de afhankelijkheid en integriteit van data: streef naar digitale autonomie.



Bron: Pexels.

Acties van consumenten

Ook consumenten van digitale technologie kunnen bijdragen:

- Ga bewust om met je persoonlijke data. Deel alleen het noodzakelijke.
- Ga bewust om met wachtwoorden. Gebruik twee-factor-identificatie, vermijd hergebruik, en vervang wachtwoorden wanneer er kans is geweest op een datalek.
- Neem cyber security mee in je keuze voor een product of dienst. Een veilig product met data in de Europese Unie is een kwaliteitskenmerk.
- Vertrouw op je onderbuikgevoel. Uit ons onderzoek blijkt dat mensen vaak waarschuwingssignalen niet vertrouwen en dan toch doorgaan. Iemand constateert bijvoorbeeld: ik krijg vragen over betalingen nooit via email van deze collega, hij loopt altijd langs. Zeker met de grootschalige toepassing van AI, inclusief het gebruik van deepfakes en voice cloning, zijn zulke omgangsvormen en persoonlijke en unieke kennis essentieel in het herkennen van verdachte activiteiten.

Conclusie

Een gezamenlijke systeemaanpak is dus essentieel voor het oplossen van de cyber security vraagstukken van de toekomst. Er is nog veel onderzoek nodig om de maatschappelijke vraagstukken te begrijpen en oplossingen te ontwikkelen. Maar je kunt ook zelf al vandaag aan de slag. Gezamenlijk, als systeem, kunnen en moeten we zorgen voor een mensgerichte veilige digitale omgeving.

NOTEN

1. *ENISA threadlandscape 2025 (2025). European Union Agency for Cyber Security.*

2. *Digitale Risico's sterk onderschat meer incidenten dan gedacht (2025).* Klein bedrijf Index 16e editie.

3. *Cyber Security Monitor 2024 (2025).* Centraal Bureau voor de Statistiek.

4. Pattnaik, N., Nurse, J.R.C., Turner, S., Mott, G. , MacColl, J., Huesch, P., Sullivan, J. (2023). *It's more than just money: the real world harms from ransomware attacks:* International Symposium on Human Aspects of Information Security and Assurance.

5. Pattnaik, N., Li, S. & Nurse, J.R. (2023). Perspectives of non-expert users on cyber security and privacy: An analysis of online discussions on twitter. *Computers & Security*, 125, 103008.

6. Kvochko, E. and Pant, R. (2015). "Why Data Breaches Don't Hurt Stock Prices". Harvard Business Review.

7. Cobos, E.V., Cakir, S., Straub, S., Qiang, C.Z. & Torgusson, C. (2024). *A review of the economic costs of cyber incidents.* World Bank, Washington, DC, USA, Rep, 193919.

8. Mmango, N., & Gundu, T. (2024, July). Cyber security as a competitive advantage for entrepreneurs. In *Annual Conference of South African Institute of Computer Scientists and Information Technologists* (pp. 374-387). Cham: Springer Nature Switzerland.

9. Datalek met ruim 485.000 deelnemers bevolkingsonderzoek baarmoederhalskanker na hack bij extern laboratorium (2025). *Bevolkingonderzoek Nederland.*

10. Zaeem, R.N., Barber, K.S. (2025). Economics of Cybercrime: Identity Theft and Fraud. In: Jajodia, S., Samarati, P., Yung, M. (eds), *Encyclopedia of Cryptography, Security and Privacy.* Springer, Cham.

11. Na hack twijfelt 1 op 3 Nederlanders aan deelname bevolkingsonderzoek (2025): *Hart van Nederland.*

12. Sahin, Z. & Vance, A. (2025). What do we need to know about the Chief Information Security Officer? A literature review and research agenda. *Computers & Security,* 148, 104063.

13. Van der Schoot, R.M.E. (2025) Managing Shadow IT: from bans to benefitis. IB Magazine #5 2025.

14. SURF Tech-Trends 2026.

CURRICULUM VITAE

Dr. Martine Groen heeft nadrukkelijk gekozen voor praktijkgericht onderzoek in cyber security door een niet-traditionele weg te kiezen.

Ze begon haar wetenschappelijke carrière met fundamenteel onderzoek naar de hersenen. Voortbouwend op een Bachelor Medische Natuurwetenschappen (cum laude afgestudeerd aan de VU) en een Master Neuroscience (with honours afagestudeerd aan VU en Erasmus MC), rondde ze in 2013 aan de VU haar promotieonderzoek af naar het geheugen van individuele hersencellen. Daarin combineerde ze computationele datamodellen met experimenteel onderzoek. Dit onderzoek werd gevolgd door een postdoc op het University College London. Neuronale netwerken, de basis voor het hedendaagse AI, waren daar een belangrijk onderzoeksthema voor haar.

Na deze solide basis in fundamenteel onderzoek, besloot Martine Groen de overstap te maken naar de toepassing van datawetenschapen, als consultant bij Capgemini. Hier kwam ze ook voor het eerst in aanraking met het vakgebied cyber security. Dit maakte ze zich vervolgens in een rap tempo eigen, terwijl ze parallel doorgroeide naar managing consultant. In deze rol was zowel gedegen vakkennis nodig, als inzicht in stakeholders, projectmanagement en people management skills. Dit scherpte de noodzaak van een systeemvisie, het motto van het lectoraat. Ook bouwde ze hier een uitgebreid netwerk op binnen de praktijk van cyber security in binnen- en buitenland. Ze was tevens verantwoordelijk voor het managen van de divisie New Business Enabling Security Services, waar onder andere IoT en OT onder vielen, een belangrijk thema binnen het huidige lectoraat. Als docent was ze ook al betrokken bij het opleiden van nieuwe professionals.

In 2022 richtte Hogeschool Utrecht een nieuw lectoraat Cyber Security op. In samenwerking met de vorige lector bouwde dr. Martine Groen als hogeschoolhoofddocent dit lectoraat op, met de nieuwe onderzoekslijn ‘Cyber security en gedrag’, alsmede de succesvolle oprichting van de Master Digital Security. Per 1 september 2025 staat dr. Martine Groen aan het roer van dit lectoraat. Met een divers team van docenten, onderzoekers en promovendi met verschillende achtergronden, heeft ze een lijn ingezet die de huidige en toekomstige vragen van cyber security kunnen beantwoorden vanuit een systeemblik.

COLOFON

Titel
Digitale veiligheid als maatschappelijke uitdaging
Naar een systeemaanpak van cyber security

Auteur
Dr. Martine Groen
Openbare les
23 april 2026
Lectoraat Cyber Security

ISBN
978-90-8928-173-9

Eindredactie
Mariek Hilhorst Tekstredactie en Productiebegeleiding

Fotografie
Cover: Femke van den Heuvel

Vormgeving
RAAK Grafisch Ontwerp, Utrecht

Hogeschool Utrecht
Kenniscentrum Digital Business and Media

Bezoekadres
Heidelberglaan 15, 3584 CS, Utrecht

Postadres
Postbus 85029, 3508 AA, Utrecht

Email
Martine.groen@hu.nl

Website
www.hu.nl/onderzoek/cyber-security

HIER KOMT ALLES SAMEN