MAB MAANDBLAD VOOR ACCOUNTANCY EN BEDRIJFSECONOMIE

Maandblad voor Accountancy en Bedrijfseconomie 96(7/8) (2022): 221–230
DOI 10.5117/mab.96.90957

Research Article

Cybersecurity en menselijk gedrag: de meerwaarde van games voor een sterkere securitycultuur

Suzanne Janse, Annebeth Erdbrink

Received 27 July 2022 | **Accepted** 7 September 2022 | **Published** 16 September 2022

Samenvatting

Cybersecurity is een steeds belangrijker wordend en hard groeiend vakgebied. Naast technologische vernieuwingen blijft daarbij ook het menselijke aspect belangrijk. Daar waar security experts zich voorheen richtten op bewustwordingscampagnes, krijgt het effect van deze campagnes – de daadwerkelijke gedragsverandering en de impact op de organisatiecultuur – steeds meer aandacht. In dit artikel wordt ingegaan op de wijze waarop de impact van gedragsinterventies mogelijk kan worden versterkt vanuit de gedragspsychologie en de gamewetenschap. De in dit artikel beschreven casestudy laat zien dat games potentie hebben, met name als onderdeel van een groter, breder programma van interventies. Concreet maken welk gedrag wenselijk is, het vooraf en doorlopend meten, analyseren en het aanpassen van het interventieprogramma zijn daarbij belangrijke randvoorwaarden.

Relevantie voor de praktijk

Interne auditors staan voor diverse uitdagingen en dilemma's in de professionele beroepspraktijk. Risico's kunnen nauwelijks nog worden losgezien van het gedrag dat ermee samenhangt en de percepties van de betrokkenen. Dit artikel biedt inzicht in het gebruik van games als onderdeel van gedragsinterventies voor een cyberveiligere organisatiecultuur. De voorlopige uitkomsten van de beschreven casestudy (n = 60) met een cybsersecurity awareness game geven interne auditors inspiratie om gedragsinterventies voor cybersecurity te verkennen en elementen mee te nemen in toetsend onderzoek naar de effectiviteit van awareness- en gedragsbeïnvloedingscampagnes, om cybersecurityrisico's te verlagen.

Trefwoorden

Cybersecurity, menselijk gedrag, serious games, human risk, cultuurverandering

1. Inleiding

1.1. Groot en dynamisch aanvalsoppervlak

Cyberdreigingen zijn permanent en de gevolgen ervan zijn zeer zorgelijk voor onze steeds verder digitaliserende samenleving in Nederland (CSR meerjarenstrategie 2022–2025). Hoewel veel cybersecurityrisico's te beperken zijn met technische maatregelen, blijft ook de menselijke factor belangrijk om de informatiesystemen van organisaties veilig te houden. Regelmatig hebben cybersecurityrisico's hun oorsprong in menselijk gedrag, al dan niet bewust (kiezen van een sterk wachtwoord) of onbewust (klik op een frauduleuze link). Kwaadwillenden maken steeds betere *phishing* e-mails (die nog nauwelijks van echt te onderscheiden zijn) met daarin *malware* die toegang geeft tot systemen. Denk ook aan *vishing* (*voice phishing*) en *smishing* (*sms phishing*) als succesvolle methoden om mensen te bewegen vertrouwelijke informatie te delen of toegang te verkrijgen tot systemen. Criminelen worden steeds slimmer en gebruiken vaker allerlei psychologische beïnvloedingstechnieken, zoals de zeven

overtuigingsprincipes van Cialdini (Cialdini 2017). Daarnaast blijft het ook belangrijk om alert te blijven op onveilige situaties in de fysieke wereld; van onbekende gasten op de werkvloer – een netwerk *sniffer* is zo geplaatst – tot rondslingerende printjes met persoonsgegevens op een bureau en vreemd gedrag van een collega. Kortom: menselijk gedrag blijft voor veel organisaties misschien wel het grootste en meest dynamische aanvalsoppervlak (de verschillende manieren waarop een aanvaller een apparaat of netwerk kan binnendringen en gegevens kan onderscheppen).

1.2. Van opzichzelfstaande (compliance)activiteit naar gewenst gedrag

Veel organisaties houden bewustwordingscampagnes en trainingen voor hun medewerkers, met als doel om hen bewust te maken van cyberrisico's en hun persoonlijke verantwoordelijkheid daarin. Voor de meeste organisaties zijn bewustwordingscampagnes inmiddels een essentieel onderdeel van hun organisatie om de risico's rond menselijk gedrag te managen (SANS 2021). De drijfveer voor die interventies is vaak nog vanuit een 'tick-in-the-box' en opzichzelfstaand. Denk hierbij aan *compliance* gerichte campagnes of trainingen met een beperkte aandacht voor de daadwerkelijke impact op gedrag.

Als er al meer bewustwording wordt gecreëerd, dan betekent dit vaak nog niet dat men zich daadwerkelijk veiliger gaat gedragen. In de praktijk blijkt vaak gemakkelijk te worden gedacht over het 'oplossen' van onveilig gedrag van werknemers. Veelal ontbreekt een gedegen analyse vooraf over waarom medewerkers zich gedragen zoals ze doen (Beris et al. 2015). Een dergelijke analyse vraagt onder andere om gedragskennis vanuit de psychologie en neurowetenschap; vakgebieden die van nature niet veel overlap kennen met die van informatiebeveiligers. Uiteindelijk wordt vaak te ondoordacht voor een bepaalde interventie gekozen, met het risico dat deze onvoldoende aansluit bij de specifieke behoefte van de situatie en/of de doelgroep. Zo'n interventie gaat dan uiteindelijk voorbij aan het beoogde doel ervan; het vergroten van verantwoordelijk, cyberveilig gedrag. Dat is zonde van de kosten en tijd die erin zijn gaan zitten en is bovendien demotiverend voor alle betrokkenen.

1.3. Complexiteit van cybersecurity breder erkennen

Om ervoor te zorgen dat geschikte methoden en instrumenten worden ingezet om op grote schaal gedrag te veranderen, moet allereerst de complexiteit van cybersecurity als maatschappelijk vraagstuk worden onderkend, zoals bij elk *wicked problem* (Conklin 2010). En daarbij is het essentieel om te beseffen dat het niet zomaar in een keer kan worden opgelost en zelfs steeds kan blijven opduiken (Rittel et al. 1973).

Gelukkig lijkt dit steeds meer door te dringen tot het cybersecurityvakgebied, dat ondertussen hard groeit en haar blik steeds meer verruimt naar andere disciplines die kunnen bijdragen aan de effectiviteit van bewustwordingsinterventies. Zo worden bijvoorbeeld inzichten vanuit de gedragseconomie qua besluitvorming over risico's vaker toegepast (Nuijten and Van Twist 2015). Met dit artikel willen we bijdragen aan de huidige ontwikkelingen door inzichten te bespreken vanuit de gedragspsychologie en de gamewetenschap, die de impact van gedragsinterventies mogelijk kunnen versterken.

1.4. Impact op auditors

De psychologisering van het beroep van internal auditor zorgt ervoor dat risico's nauwelijks nog kunnen worden losgezien van het gedrag dat ermee samenhangt (Nuijten and Van Twist 2018). Interne auditors hebben een belangrijke rol bij het beoordelen en signaleren van die gedragsrisico's. In het licht van de veranderende cybersecuritydreigingen en bijbehorende, groeiende kwetsbaarheden en risico's biedt dit artikel inspiratie over de inzet van cybersecurity games als gedragsinterventie. Het biedt praktische inzichten die interne auditors mee kunnen nemen in het doen van toetsend onderzoek naar de effectiviteit van cybersecurity *awareness* en gedragsbeinvloedingscampagnes voor een sterkere securitycultuur, en om cybersecurityrisico's te verlagen.

Dit artikel geeft inzicht in de effectiviteit van games als interventiemiddel voor gedragsverandering ten aanzien van cybersecurity. In deel twee beschrijven we sociaalpsychologische theorieën over gedragsverandering – waarin bewustwording slechts een eerste stap is – om de inhoud van cybersecurityinterventies te verbeteren. Gebruik van games kan daarbij een geschikte vorm zijn. Vervolgens illustreren we in deel drie de voorlopige onderzoeksresultaten van een casestudy met een cybersecurity game, inclusief enkele aanbevelingen voor het gebruik van dit soort games. In het daaropvolgende vierde deel beschrijven we de uit de casestudy volgende inzichten voor een sterkere securitycultuur. In het laatste deel concluderen we dat games potentie hebben, met name als onderdeel van een breder programma van interventies. Daarnaast vraagt het onderwerp een bredere expertise en kijk op gedragsverandering en biedt het een kans voor auditors om bestaande methoden van toetsend onderzoek te verrijken.

2. Inzichten vanuit de gedragspsychologie

2.1. Elementen voor het versterken van een positieve attitude

Zoals gezegd richten veel bestaande cybersecurityinterventies en -campagnes binnen organisaties zich op het bewustmaken van medewerkers. Bewustmaken van cyberrisico's op de werkvloer en wat mensen zelf kunnen doen om deze risico's zo klein mogelijk te houden. Het bewustzijn kan nog nauwelijks aanwezig zijn en moet worden gecreëerd (bij nieuwe dreigingen) óf bestaat

(gedeeltelijk) al en dient 'enkel' versterkt te worden. Het doel van die interventies is uiteindelijk om de attitude (positief versterkte houding) van werknemers ten aanzien van veilig werken te beïnvloeden. Het gaat er dan dus echt om hoe iemand tegenover het onderwerp staat (attitude), en niet alleen om de vraag of men zich bewust is van het onderwerp.

Om de kans te vergroten dat dit ook daadwerkelijk gebeurt, is het interessant om te kijken naar wetenschappelijke kennis over attitudevorming, zoals bijvoorbeeld het bekende *Elaboration Likelihood Model* (Petty and Cacioppo 1986). Dit model uit de sociale psychologie beschrijft hoe waarschijnlijk het is dat personen hun attitudes zullen veranderen op basis van een boodschap die ze gepresenteerd krijgen. Het proces van het doorlopen van voors en tegens van de inhoud van de boodschap wordt hierbij *elaboratie* genoemd. In hoeverre iemand met aandacht op die manier nadenkt over de boodschap is daarnaast afhankelijk van de mate van persoonlijke motivatie die iemand heeft én de praktische mogelijkheid om te elaboreren op het moment dat de boodschap wordt gepresenteerd. Belangrijke aspecten die hierbij vervolgens een rol spelen, en die de mate van motivatie en mogelijkheid beïnvloeden, zijn o.a. de relevantie van de boodschap en de verantwoordelijkheid ervoor (bij motivatie) en kennis en begrip van de boodschap, de hoeveelheid tijd, afleiding en herhaling van de boodschap (bij mogelijkheid) (O'Keefe 2002; Perloff 2008).

Voor een effectieve inhoud van een cybersecurityinterventie die attitudes wil versterken, lijkt het dus van belang om te kijken in hoeverre deze genoemde elementen erin zitten (of juist niet). Het is daarbij belangrijk om een juist evenwicht te hebben; bij een overkill aan informatie of herhaling kan het de ontvanger van de boodschap gaan tegenstaan en averechts werken. Maar met een juiste balans zouden medewerkers gemotiveerd moeten raken en wordt hun de mogelijkheid geboden om de boodschap (zoals bijvoorbeeld '*veilig werken op de werkvloer is cruciaal om de organisatie veilig te houden en je hebt daar een verantwoordelijkheid in'*) met aandacht tot zich te nemen. Dit vergroot de kans dat zij hiervan overtuigd raken.

2.2. Effect meten

Naast een weloverwogen inhoud die kan overtuigen en zoveel mogelijk aansluit bij de functie van een medewerker (qua kennisniveau, relevante voorbeelden, etc.) is het ook waardevol om de effectiviteit meetbaar te maken. Want hoe weet je anders of de interventie iets voor je bedrijf gedaan heeft? Attitudes worden vaak gemeten aan de hand van vragenlijsten. Dus de meest simpele manier zou zijn om zowel voor als na de interventie bij medewerkers een vragenlijst af te nemen die hun attitude over veilig gedrag meet. De eerste vragenlijst fungeert dan als een nulmeting, die vervolgens met de tweede vragenlijst kan worden vergeleken. Bij gedetailleerde en valide vragenlijsten kan zo een goed, genuanceerd beeld worden verkregen van de thema's binnen veilig werken waar al dan niet een versterkte attitude en meer aandacht gewenst zijn. Uiteraard ligt hier het gevaar van sociale wenselijkheid op de loer, door het gevoel dat de baas de antwoorden zou kunnen inzien. Dit kan zelfs ook angst veroorzaken, omdat men bang kan zijn ergens op te worden afgerekend. Belangrijk is dus om deze effectmeting geheel anoniem te laten verlopen en dit duidelijk te communiceren aan de medewerkers.

2.3. Oorzaken uitblijven gewenste gedragsverandering

Als na een effectmeting van een cybersecurity interventie de attitude versterkt blijkt te zijn, is dit in eerste instantie natuurlijk goed nieuws. Dit zou dan betekenen dat medewerkers veilig werken belangrijker zijn gaan vinden. Maar wat betekent dat concreet voor de veiligheid van een bedrijf? In hoeverre resulteert dit ook echt in het nodige gewenste veilige gedrag van medewerkers? Want uiteindelijk is dat tenslotte wat men hoopt te bereiken: een gedragsverandering.

Volgens de vaak aangehaalde *Theory of Planned Behavior* (Ajzen 1991) is de intentie die iemand heeft tot bepaald gedrag de belangrijkste voorspellende factor voor het tonen van dat gedrag. Maar die intentie is vervolgens wel opgebouwd uit drie verschillende onderdelen:

1) de positieve attitude met betrekking tot dat gedrag;
2) de 'subjectieve norm' (wat iemand denkt dat anderen vinden/doen); en
3) de 'waargenomen gedragscontrole' (in hoeverre ervaren wordt dat het gedrag uitvoerbaar is; dat er geen belemmeringen zijn van eigen vaardigheden of van omgevingsfactoren).

Kortom, alleen een positieve attitude ten aanzien van veilig werken lijkt niet voldoende garantie te geven dat medewerkers ook daadwerkelijk veilig gaan werken. De subjectieve norm en de waargenomen gedragscontrole spelen ook een belangrijke rol. Idealiter zouden die twee dus moeten worden meegenomen in het ontwerp van een interventie, naast het feit dat er aandacht aan wordt besteed in de dagelijkse praktijk.

Stel nu dat een interventie ontworpen is, die rekening houdt met bovengenoemde inzichten uit de gedragspsychologie en resulteert in een sterke intentie van de werknemers om veiliger te gaan werken. Dan nog betekent dit niet dat dit gewenste, veiliger gedrag ook daadwerkelijk wordt getoond. Er zijn nog altijd redenen voor mensen om toch níet over te gaan op het voorgenomen gedrag.
Een belangrijke reden hiervoor kan een hoge 'gedoefactor' zijn (De Vries 2020). Veilig werken vraagt vaak meer tijd en aandacht, omdat er bepaalde extra handelingen moeten worden uitgevoerd, die vaak als 'extra gedoe' worden ervaren.

Een andere, meer algemene reden is een gebrek aan *engagement*. Ondanks de juiste intenties tot veilig werken kan een gebrek aan betrokkenheid met het onderwerp (of de organisatie zelf) ervoor zorgen dat er geen gewenste

gedragsverandering optreedt. Een weloverwogen, inhoudelijk 'kloppende' interventie kan hierdoor dan alsnog niet de impact hebben waar men op hoopt. Daarom lijkt het ook zeker van belang om te kijken naar de vorm van de interventie. Hoe kan alle informatie op een aantrekkelijke manier worden aangeboden, op een manier die meer betrokkenheid en *agency* oplevert?

2.4. Cybersecurity games, gamificatie en nudging

Games en gamificatie lijken goed op de hiervoor genoemde factoren in te kunnen spelen. Al jaren zetten bedrijven ze in om bewustwording te creëren en vaardigheden te trainen rondom cybersecurity. Vaak worden bestaande formats gebruikt, die per context (per klant) redelijk eenvoudig kunnen worden aangepast. Games en gamificatie worden overigens vaak gebruikt als inwisselbare termen, maar ze zijn wel degelijk verschillend. In het kort: met games worden aparte speelwerelden bedoeld waar elementen uit de werkelijkheid in zijn verwerkt. Bij gamificatie is het juist net andersom. Daarbij pas je spelelementen toe in de werkelijkheid (Deterding 2011). Ondanks de populariteit van gamificatie, zitten er ook nadelen aan. Want heel mooi dat mensen het gewenste gedrag uitvoeren onder de aanmoediging van scores en ranglijsten, maar in hoeverre houdt het gedrag ook stand zonder deze spelelementen? En kiezen mensen ervoor om zich te gedragen naar de inhoud of doen ze dat slechts vanwege de vorm?

Een meer indirecte manier van beïnvloeden is het populaire *nudging* (het veranderen van de omgeving waarin een keuze plaatsvindt om op onbewust niveau die keuze te beïnvloeden). Over nudging (waar gamificatie een vorm van is) zijn diverse publicaties uitgebracht die de impact, uitdagingen en bruikbaarheid ervan voor de internal auditpraktijk beschrijven (Nuijten and Van Twist 2018). Nudging is nogal subtiel en gevoelig voor de context waarbinnen het gebruikt wordt. Veel onderzoeken over de effectiviteit van nudging gaan daaraan voorbij, waardoor het dus de vraag is wat de daadwerkelijke effectsize is (soms zijn effecten zelfs averechts). Recent onderzoek toont aan dat het effect van nudging als interventie beperkt is, maar dat het wel kan werken in een programma van interventies (Maier et al. 2022).

Voor dit artikel beperken we onze focus tot games, want die lijken goed aan te sluiten op de complexiteit van cybersecurity. Het gebruik daarvan kan van grote waarde zijn (Klabbers 2018). Games bieden namelijk interactieve leeromgevingen waarin de werkelijkheid kan worden gesimuleerd. In de woorden van Richard Duke (schrijver van o.a. *Gaming: the Future's Language*, dat al in de jaren zeventig verscheen): "*Dit stelt de speler in staat om een complex probleem te benaderen vanuit welk perspectief dan ook relevant lijkt, in een context die coherent en logisch is, en om te experimenteren in een omgeving die in principe veilig is*". Dat interactieve karakter maakt games uniek ten opzichte van andere media. Het stelt mensen in staat om keuzes te maken en de gevolgen daarvan te ervaren. Maar de ene game is de andere niet, en lang niet alle games doen wat ze beloven (Soekarjo and Van Oostendorp 2017). Gamewetenschappers buigen zich dan ook over de vraag hoe (cybersecurity)games kunnen worden ontworpen en moeten worden ingezet om hun potentie waar te kunnen maken.

3. Potentie van games als onderdeel van cybersecurityinterventies

3.1. Casestudy met persoonlijke assistenten TU Delft

Games lijken steeds vaker te worden ingezet om attitudes 'spelenderwijs' te versterken en uiteindelijk gedrag te veranderen. Dit soort games worden ook wel *persuasive games* genoemd, omdat ze een overtuigende boodschap willen overbrengen (Bogost et al. 2012). Ze worden toegepast in uiteenlopende gebieden, zoals onder andere het onderwijs, de gezondheidszorg en de reclamewereld. Er bestaat een toenemende belangstelling voor persuasieve games, die spelers de mogelijkheid bieden om te gaan met complexe maatschappelijke vraagstukken (Antle et al. 2014), waaronder ook cybersecurity.

Over het algemeen bestaan er echter nog maar weinig concrete handvatten voor game-ontwerpers om een game te maken die 'werkt' (Visch et al. 2013; Kors et al. 2015; Jacobs 2017). Vaak is het ontwerp gebaseerd op ervaring, intuïtie (Orji 2014) en vele testsessies met de doelgroep. Daarnaast is het verre van simpel om attitudes en gedrag te veranderen; er spelen verschillende factoren een rol die je niet allemaal in de hand kunt hebben. Een voorbeeld van huidig, lopend Nederlands onderzoek naar de impact van cybersecuritygames is dat van promovenda Annebeth Erdbrink aan de TU Delft in samenwerking met Awareways, een organisatie die specialist is op het gebied van gedrags- en cultuurverandering. Ze evalueert hiervoor een bestaande trainingsgame (online, single player), die veelvuldig wordt ingezet door uiteenlopende bedrijven.

3.2. Human Firewall als game thema

In de voornoemde trainingsgame doorlopen de spelers een verhaallijn waarin de eigen organisatie wordt aangevallen door hackers. Alleen als alle medewerkers de opdrachten (aangepast aan de persoonlijke context) tot een goed einde weten te brengen, kan de organisatie worden gered. Zo ontstaat er uiteindelijk een *Human Firewall*, die de organisatie beschermt tegen verdere aanvallen. De opdrachten gaan onder andere over sterke wachtwoorden, dataclassificatie en -minimalisatie, vishing en (spear) phishing, maar ook over fysieke dreigingen. Ze worden steeds ingeleid door filmpjes (waarin spelers persoonlijk worden aangesproken) en stukjes 'theorie'. Na afloop volgt korte feedback waarin wordt toegelicht waarom bepaald gedrag wel of niet goed is. Ook krijgt de speler concrete tips om later mee verder te gaan (zoals het installeren van een wachtwoordmanager).

Los van de speelse vorm, probeert de game het engagement van de werknemers voornamelijk te versterken door het groepsgevoel aan te spreken en spelers te laten inzien dat zij allemaal onderdeel zijn van de veiligheidsketen van de organisatie. Daarnaast is er door de ontwerpers (een team van onder andere een gamedesigner, een psycholoog en een security-expert) bewust aandacht besteed aan de ervaring van een 'subjectieve norm' en 'waargenomen gedragscontrole'. Met haar onderzoek wil Erdbrink kijken hoe dit soort cybersecurity games werken (qua attitude- en gedragsverandering), hoe ze worden ervaren en wat er eventueel kan worden aangepast, zodat hun impact kan worden vergroot. Aan het experiment deden tot nu toe zo'n 60 persoonlijke assistenten van de TU Delft vrijwillig mee. Voorafgaand en na afloop van de game vulden zij vragenlijsten in en daarnaast werden er enkele interviews afgenomen.

3.3. Voorlopige effecten op bewustwording en gedrag

Alhoewel het onderzoek nog loopt en er nog niet naar een attitude-effectmeting kan worden gekeken, leveren de interviews wel al voorlopige resultaten en inzichten op. Veel spelers geven aan dat ze zich door de game meer bewust werden van het belang van veilig omgaan met informatie:

> *"Er waren vragen over het openen van mails waarvan ik dacht – ja, ik kan hier wat mee. Dat heeft mij extra bewust gemaakt. Van ga ik dit openen of niet openen?"*

Zoals verwacht zijn de persoonlijke assistenten er niet zozeer heel anders over gaan denken (want vooraf bleek al dat zij het belangrijk vonden), maar het bewustzijn is wel degelijk versterkt:

> *"Mensen halen toch wel snel hun schouders op en denken: het gaat toch altijd wel goed. Maar het hoeft maar één keer niet goed te gaan. Dus bewustwording is stap één. Dat is wat vooral bij mij is geland."*

Zo gingen spelers tijdens en na de game meer nadenken over hoe ze met vertrouwelijke gegevens omgaan. Er kwamen voor hen niet zozeer nieuwe onderwerpen aan bod in de game, maar spelers realiseren zich dat ze scherper, alerter en consequenter kunnen zijn en hun verantwoordelijkheid vaker moeten nemen. Daarnaast vond men het ook fijn om bevestiging te krijgen van wat men al goed deed:

> "*Het is gewoon even goed om meer met je neus op de feiten gedrukt te worden. De meeste mensen weten het heus wel. Ze weten ook dat het nog steeds actueel is. Je denkt dat je goed bezig bent – en dat is waarschijnlijk ook zo – maar het is fijn als je bevestiging krijgt."*

Concreet werden spelers zich bewust van het belang van een wachtwoordmanager, computerscherm locken en de kwetsbaarheid van een open werkplek:

> "*Mijn vriend heeft altijd een VPN aanstaan en zo'n wachtwoordmanager. Ikzelf tilde er niet zo zwaar aan. Het zijn kleine dingen, maar wanneer je hier geen aandacht voor hebt, kan het enorm misgaan voor een organisatie. Daardoor ben ik me er nu wel bewuster van. En het is vaak een kleine moeite.*"

Eén speler werd zich er door de game van bewust dat het belangrijk is om onveilige situaties te melden en ontdekte voor het eerst (!) waar dat binnen de organisatie dient te gebeuren.

Van woorden naar kleine daden

De toename van awareness is mooi, maar dit zegt nog weinig over het daadwerkelijke gedrag van medewerkers. In hoeverre kon de spelervaring ook bijdragen aan enige gedragsverandering? Om hier een beeld van te krijgen, vroeg Erdbrink een paar weken na de trainingsgame in hoeverre de persoonlijke assistenten hun woorden ook hadden omgezet in daden. Het bleek wel degelijk dat persoonlijke assistenten bepaalde dingen hebben veranderd in hun manier van veilig werken. Weliswaar kleine aanpassingen, maar toch is dit meer dan vooraf werd verwacht.

Wat het meest werd genoemd, was het locken van het computerscherm (Windowstoets + L), elke keer als de werkplek werd verlaten. De meesten deden dit eerder wel, maar waren het in de loop van de tijd toch een beetje vergeten:

> *"Wat ik al deed, maar wat ik ook nog wel eens vergat, is mijn scherm locken. Dat doe ik nu weer fanatiek, dus dat was weer een trigger van: wacht even, let op."*

Als tweede werd vaak het installeren van een passwordmanager genoemd. Opvallend is hierbij dat het na de game voor de meesten toch is gebleven bij slechts een intentie; ze geven aan wel van plan te zijn om een passwordmanager te installeren, maar dat ze hiervoor nog geen 'tijd' hebben gehad. Bij doorvragen lijkt hier voornamelijk de 'gedoefactor' een rol te spelen, ondanks het feit dat het relatief snel geregeld is. Toch raakte een enkeling wel overtuigd van het nut ervan:

> *"Wat je zei over die passwordmanager. Ik wist dat zoiets bestaat, maar ik heb er nooit bij stilgestaan of ik dat zou kunnen gebruiken. Dit was net die aanvullende informatie die ik nodig had: zo werkt het en dit is het wachtwoord wat je zou kunnen instellen. Dus dat je een zin of spaties erin zou kunnen verwerken. Dat is fantastisch."*

Ook werden wachtwoorden vervangen of minder vaak dezelfde gebruikt voor verschillende inlogomgevingen:

> *"Ik maakte mijn wachtwoorden altijd al goed. Niet van die voor de hand liggende dingen. Ik had wel bij*

sommige systemen steeds dezelfde wachtwoorden. Dat ben ik aan het veranderen."

Maar, zoals verwacht, is niet iedereen hiervan te overtuigen:

"Ik ben volgende week 54 en dit is niet hoe ik geschoold ben. Ik heb op mijn telefoon dit wachtwoord, voor mijn bank, voor Facebook. En dan vergeet ik er nog tien. Ja weet je, het is wel goed."

Een algemene alertheid werd ook vaak genoemd, dat zich onder andere uit in dingen extra verifiëren (ook aan de telefoon) en vaker onveilige situaties melden bij de IT-afdeling. Tot slot was het veilig houden van de werkplek zelf (clean desk) voor sommigen nieuw gedrag naar aanleiding van de game.

3.4. Ervaring van de game

Naast de vragen over bewustwording en gedrag kwam in de interviews ook aan bod hoe spelers de game überhaupt ervaren hebben. Wat vonden ze van de opdrachten bijvoorbeeld? En hoe werd de spelvorm ervaren?

Inhoud

Voor de meeste spelers was de inhoud van de game voornamelijk herhaling. Er leken weinig echt helemaal nieuwe onderwerpen in te zitten. Maar dit werd niet als storend ervaren, integendeel. De herhaling was juist welkom en werkte goed. Vooral omdat het nu meer een herinnering was van gedrag dat al bekend was of zelfs al eerder eens was uitgevoerd. Daarnaast werkte de extra informatie als goede aanvulling om een thema beter te bevatten. Wat voor sommigen wel nieuw was, was het belang van veilig werken in de fysieke wereld. Dus bijvoorbeeld geen vertrouwelijke informatie op een bureau neerleggen, en goed opletten dat er geen mensen kunnen meekijken op je scherm als je op een openbare plek met vertrouwelijke informatie werkt.

Voor een enkeling was de feedback na afloop van een opdracht niet voldoende om te begrijpen waarom iets niet goed was. Verreweg de meeste indruk maakte een luisteropdracht waarbij de speler een fragment te horen kreeg van een telefoongesprek waarbij de beller naar vertrouwelijke informatie viste:

"Wat ik overigens een hele goeie vond was het stukje van die jongen die belde van: ik ben de schoonzoon van de directeur. Dat je inderdaad bewust wordt. Als iemand veel voorkennis heeft en doet voorkomen alsof hij weet van hoe en wat. Hij was heel amicaal. Daar moet je dus extra alert op zijn. Dat vond ik een heel goede opdracht. Je wordt dan echt ingepakt, en je denkt dan: oh, zo werkt het."

Spelvorm

De afwisseling tussen tekst en uitleg en zelf aan de slag gaan met opdrachten wordt door spelers gewaardeerd. De filmpjes met de acteur werken daarbij extra motiverend, omdat spelers persoonlijk worden aangesproken en het bijdraagt aan een verhaallijn die je wilt volgen:

"Dat die acteur zegt van: 'ik heb jouw hulp nodig' en je echt persoonlijk benadert, dan word je er gewoon in getrokken. Als het gewoon iemand is die weer een verhaaltje houdt over van: 'Nou, we hebben cybersecurity hoor.' Ik denk niet dat je dan lang bij de les blijft."

Door de spelvorm werd het serieuze onderwerp cybersecurity als minder droog ervaren:

"Bij een standaardtraining dwaal je af. Nu moet je gelijk actief meedoen en reageren. Ik vond het op deze manier heel leuk om te doen. Je bent zelf bezig."

Zelfs persoonlijke assistenten die niet alle spelopdrachten begrepen, gaven aan er toch de lol van in te kunnen zien. Een opvallende bevinding is dat geen enkele speler iets opmerkte over punten die je per trainingsonderdeel kon behalen en het behaalde 'certificaat' aan het einde van de game. Wat dit precies betekent, is moeilijk te zeggen. Het lijkt alleen niet per se positief te hebben bijgedragen aan de ervaring en de stimulerende werking te hebben zoals vaak wordt verwacht. Voor één speler werkte de belonende opmerkingen van 'goed gedaan' na afloop van een opdracht in ieder geval averechts. Hierdoor kreeg ze het gevoel dat ze niet serieus genomen werd, waardoor de gehele ervaring ook minder geloofwaardig werd voor haar:

"*Sommige opdrachten waren echt heel simpel. Dan kreeg je van die juichende reacties. Ik had alleen maar ergens op geklikt."*

4. Inzichten voor een sterkere securitycultuur

4.1. Games als aftrap van breder programma

De voorlopige onderzoeksresultaten geven een paar inzichten die een aantal algemene aanbevelingen vormen, zowel voor de makers van dergelijke trainingsgames als de bedrijven die ze inzetten op hun werkvloer. Om alles goed tot zijn recht te laten komen, zijn namelijk niet alleen de inhoud en vorm van de game vorm van belang, maar ook de rol van de game in combinatie met andere interventies die samen tot een sterkere securitycultuur leiden.

Het onderzoek laat zien dat een game niet alleen awareness kan laten toenemen, maar ook tot bepaalde simpele gewenste gedragingen kan leiden. Toch is er daarna de nodige ondersteuning nodig om deze vol te blijven houden, uit te breiden met meer veilige gedragingen en betrokken te blijven bij nieuwe ontwikkelingen op het gebied van veilig werken. Een game inzetten als een losstaand iets, zonder follow-up, lijkt in ieder geval volgens Erdbrink geen duurzame aanpak. Maar als onderdeel van

een breder programma aan interventies zou het een heel geslaagde aftrap kunnen zijn. Het biedt een gedeelde ervaring, waarop mensen gezamenlijk kunnen reflecteren en de concrete realistische scenario's uit het spel kunnen direct worden erkend op de werkvloer.

4.2. Aandachtspunten voor ontwerp en inzet van cybersecurity games

Op basis van de voorlopige resultaten komt Erdbrink met een aantal aandachtspunten voor ontwikkelaars van vergelijkbare games:

- Denk allereerst goed na over wat je concreet wilt bereiken. Wat wil je dat medewerkers weten en doen (gewenst gedrag) na afloop van de game? Pas je ontwerp van de game daarop aan. Hoe meer doel en ontwerp op elkaar aansluiten, hoe groter de kans dat er daadwerkelijk enige gedragsverandering plaatsvindt. Verwacht daarbij niet te veel in één keer.
- Houd het bij kleine tastbare gedragingen die je wilt bereiken. Zo wordt het niet te overweldigend en blijft het leuk en haalbaar. Later op de werkvloer kan daar dan weer iets bij komen.
- Je kunt nooit iets maken voor 'iedereen', dus probeer zoveel mogelijk homogene groepen te trainen. Pas zo nodig de inhoud aan de functie van werknemers aan. De kans op succes wordt vergoot als de scenario's in het spel voor de speler realistische simulaties zijn. Op die manier kan de brug naar de werkelijkheid namelijk makkelijker worden gemaakt.
- Benadruk het groepsgevoel en de eigen verantwoordelijkheid (sociale norm) in de game. Dit zorgt niet alleen voor meer betrokkenheid van mensen bij het spel, maar ook daarbuiten.
- Pas om met te veel punten, badges, etc. toekennen. Dit kan een spel zeker leuker maken om te spelen, maar het moet niet de overhand krijgen. Op basis van eerdere casestudies met games ontdekte Erdbrink dat spelers vaak aangeven dat een 'serieus' onderwerp ook best serieus mag worden gebracht. Anders kan het soms als kinderachtig worden ervaren. Een spel kan een meer blijvende indruk maken als de speler zich serieus genomen voelt.

Ook voor wat betreft de manier waarop de game wordt ingezet zijn een aantal aandachtspunten te noemen:

- Denk goed na over hoe je de game vooraf presenteert aan medewerkers. Dit schept namelijk (onbewust) bepaalde verwachtingen. Erdbrink ervaarde bij eerdere studies dat het woord 'game' niet iedereen zal aanspreken. Als de game niet verplicht is, kunnen medewerkers afvallen. Deze medewerkers denken dat het niet serieus zal zijn en 'niet voor hen' is, omdat ze niet van 'spelletjes' houden. Een alternatieve term zou bijvoorbeeld 'interactieve training' kunnen zijn.
- Na afloop van de game kan er een (verplichte) fysieke *debrief* worden georganiseerd. Dit biedt medewerkers de mogelijkheid om vragen te stellen over dingen die onduidelijk waren. Ervaringen kunnen vergeleken worden, belangrijke lessen kunnen nog eens worden herhaald en verbeteringen in beleid kunnen worden geïnitieerd. Bovendien kan er met elkaar bekeken worden hoe de 'gedoefactor' (die veilig werken in de weg kan zitten) zoveel mogelijk kan worden bestreden in de praktijk.
- Tot slot, misschien een open deur, maar laat als bedrijf (dagelijks) duidelijk zien aan werknemers hoeveel waarde er aan veilig werken wordt gehecht. Geef dus ook zelf het goede voorbeeld (zonder met vingertjes te wijzen). Als sommige zaken onduidelijk zijn, niet werken of ontbreken, dan kan dat werknemers demotiveren om ook zelf hun best te doen.

4.3. Breder programma aan interventies

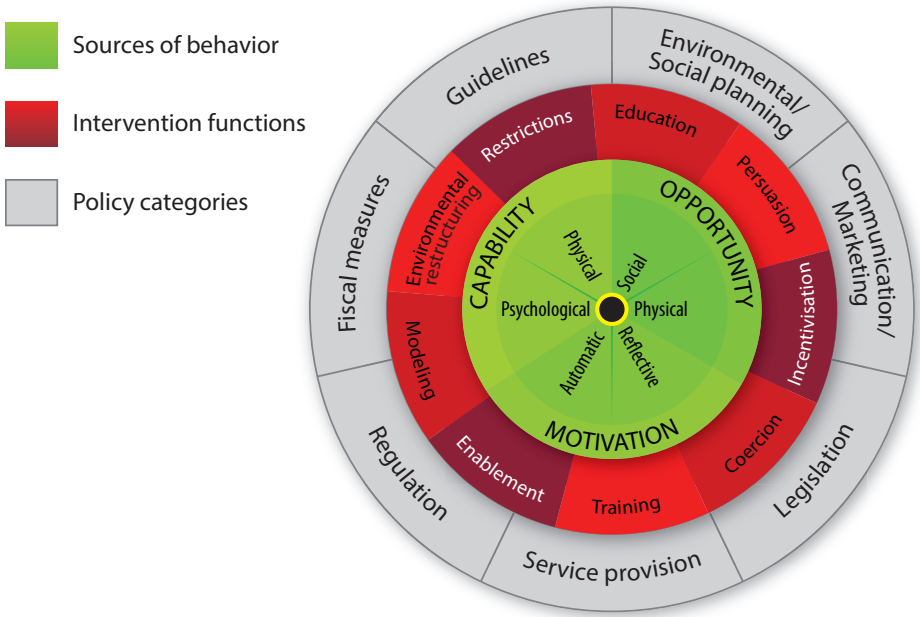
Awareness blijft een belangrijke eerste stap in een breder programma van interventies. Of uiteindelijk gedragsverandering plaatsvindt, is afhankelijk van verschillende onderliggende factoren, die kunnen worden onderverdeeld in drie voorwaarden: capaciteit, gelegenheid en motivatie (Michie et al. 2011). Hoe consistenter deze worden ingevuld, des te groter de kans dat de gedragsinterventies effect hebben. Games kunnen *Capaciteit* (kennis en vaardigheden) en *Motivatie* (emoties, geloof en waarden) positief beïnvloeden. Voor een succesvolle algehele aanpak (programma van interventies) zou je dan ook nog de *Gelegenheid* willen beïnvloeden met een interventie. Een handig, praktisch hulpmiddel bij het vormgeven van die algehele aanpak is het zogenaamde *Behaviour Change Wheel* (Michie et al. 2011).

4.4. Overige randvoorwaarden voor meer effect

Een belangrijke voorwaarde is onder andere om te starten met een goede nulmeting, om goed aan te kunnen sluiten bij de volwassenheid van de huidige securitycultuur. Uitvoerig onderzoek naar de redenen waarom medewerkers zich gedragen zoals ze doen en zich wel of niet aan de richtlijnen houden, biedt al vaak veel inzichten voor het opzetten van een programma. Scenario-based vragenlijsten (waarin wordt onderzocht hoe een respondent zich gedraagt in praktijkgerichte situaties) lijken daarvoor een geschikte methode. Daarmee kunnen grote aantallen gegevens over gedrag en attitude worden verzameld in de praktijk. Zelfs dusdanig uitgebreid dat er verschillen tussen groepen van profielen te onderkennen zijn (Beautement et al. 2016). Ook is er steeds meer securitysoftware die gegevens verzamelt over gedrag van gebruikers, waar met data-analyse inzichten uit kunnen worden verkregen over het gedrag. Het Behaviour Change Wheel helpt vervolgens bij het kiezen en ontwerpen van interventies voor de beoogde gedragsverandering.

Naast een nulmeting is het meten van de effectiviteit van de verschillende interventies belangrijk. Om vervolgens het programma bij te kunnen sturen en interventies eventueel aan te vullen of te veranderen al naar gelang de

Figure 1. Behaviour Change Wheel (Michie et al. 2011).



behoeftes van de organisatie rond het gewenste gedrag. De uitdaging daarbij is de vraag welk ambitieniveau de organisatie nastreeft. Welk gewenst gedrag is afdoende en hoe verhoudt zich dat bijvoorbeeld tot de *risk appetite* van het management? Voor cybersecurityrisico's is dit een extra uitdaging, omdat aanvallen steeds geavanceerder worden en steeds meer gericht zijn op de zwakste schakel in het systeem. En laat die schakel nu vaak gerelateerd zijn aan menselijk gedrag.

Met behulp van data-analysemethodes kan nieuw inzicht worden geven in de effectiviteit van interventies op grote schaal, in de praktijk. Ook het groeiend aantal digitale securityoplossingen dat gegevens verzamelt over gedrag van gebruikers om veiligheidscultuur te kunnen meten, draagt bij aan de mogelijkheid om sneller mensgerelateerde kwetsbaarheden in kaart te brengen en oplossingen te bedenken (Sas et al. 2021).

5. Conclusie en aanbevelingen

5.1. De meerwaarde van games voor een sterkere securitycultuur

In dit artikel hebben we geprobeerd inzicht te geven in de effectiviteit van games als interventiemiddel voor gedragsverandering van medewerkers wat betreft cybersecurityrisico's. Theorieën over gedragsverandering vanuit de psychologie kunnen bruikbaar zijn om de inhoud – en daarmee het succes – van cybersecurityinterventies te verbeteren. Maar een weloverwogen, inhoudelijk 'kloppende' interventie kan alsnog niet de impact hebben die men hoopt, zonder de juiste betrokkenheid van de medewerkers. Games kunnen als interventievorm hierbij helpen, omdat ze de informatie op een aantrekkelijke manier presenteren door onder andere de spelers *agency te* geven. Games stellen mensen in staat om keuzes te maken en de gevolgen daarvan te ervaren. Dit maakt games ook juist voor een complex onderwerp als cybersecurity zo interessant. De beschreven casestudy in dit artikel laat zien dat games potentie hebben als cybersecurity-gedragsinterventie. Ze kunnen niet alleen bewustzijn versterken, maar ook aanzetten tot kleine veranderende handelingen. Voor meer duurzame gedragsverandering zou een game idealiter onderdeel zijn van een groter geheel; een breder programma aan interventies. Een handig, praktisch hulpmiddel bij het vormgeven van zo'n programma is het al genoemde Behaviour Change Wheel (Michie et al. 2011). Een nulmeting, het continu meten van de effectiviteit van de verschillende interventies, het aanpassen ervan en goed voorbeeldgedrag lijken in ieder geval belangrijke voorwaarden voor een succesvol programma aan interventies.

5.2. Wicked problem dat brede expertise vraagt

Cybersecurity blijft een wicked problem, waarbij het altijd belangrijk blijft om in de '*problem space*' te duiken. Want juist het verkennen waarom medewerkers zich gedragen zoals ze doen en het analyseren van de root-cause kan een startpunt zijn voor een sterkere securitycultuur (Kirlappos et al. 2014). De casestudy laat zien dat het afnemen van persoonlijke interviews met werknemers hierbij een waardevolle rol kan spelen. Die geven heel belangrijke inzichten en input voor goede (vervolg)interventies (wat speelt er precies en waarom voelt men zich niet betrokken?). Daarnaast voelen zij zich bovendien ook gehoord en gezien en ervaren zij het als een gezamenlijke effort, in plaats van iets dat van de organisatie (of vanuit algehele wetgeving) moet.

De behoefte aan een sterkere securitycultuur vraagt ook om een nieuw soort expertise in het vakgebied van securityprofessionals (Nuijten and Van Twist 2018). Vanuit specialisaties als psychologie, (digitale) marketingcommunicatie en educatie. Gezamenlijk kan de complexiteit van de gewenste gedragsverandering in kaart worden gebracht en kunnen de behoeftes van de doelgroep goed worden begrepen en gemeten.

5.3. Kans voor de internal auditor

De rol van Internal Audit verandert met de digitalisering en levert nieuwe uitdagingen en dilemma's in de professionele beroepspraktijk. Risico's kunnen nauwelijks nog worden losgezien van het gedrag dat ermee samenhangt. Onderwerpen als bewustwording en gedrag zijn minder concreet (zacht) en de impact ervan is doorgaans moeilijk meetbaar voor organisaties. Voor internal auditors zijn deze onderwerpen ver van het bed en gaan ze over langetermijnsucces (Nuijten and Van Twist 2018). Internal auditors kunnen met de inzichten vanuit dit artikel aansluiten bij: a) de potentie en de impact van games als gedragsinterventie; en b) het beter meetbaar krijgen van de effectiviteit van een breder programma van gedragsbeïnvloedingsinterventies, om uiteindelijk de mensgerelateerde cybersecurityrisico's te verlagen.

- **Suzanne Janse** (1974) studeerde Bedrijfskunde, IT Auditing & Advisory en Sustainability Accounting aan de Erasmus Universiteit. Na een loopbaan van 18 jaar als adviseur en externe IT auditor, is zij momenteel Cybersecurity Transformation lead bij ING. Haar nevenactiviteiten richten zich op het continue vernieuwen van de beroepsgroep, organiseren van meer samenwerking en zo bij te dragen aan een veiligere samenleving.

- **Annebeth Erdbrink** (1984) studeerde Sociale Psychologie en Information Studies (track Game Studies) aan de Universiteit van Amsterdam. Momenteel rondt zij haar promotieonderzoek *Game Design for Sustainable Societies* af aan de TU Delft.

Literatuur

- Ajzen I (1991) The theory of planned behavior. Organizational Behavior and Human Decision Processes 50: 179–211. https://doi.org/10.1016/0749-5978(91)90020-T
- Antle AN, Tanenbaum J, Macaranas A, Robinson J (2014) Games for Change: Looking at Models of Persuasion Through the Lens of Design. Gaming Media and Social Effects. Springer Science + Business Media, Singapore. https://doi.org/10.1007/978-981-4560-96-2_8
- Beautement A, Becker I, Parkin S, Krol K, Sasse A (2016) Productive Security: A scalable methodology for analysing employee security behaviours, SOUPS.
- Beris O, Beautement A, Sasse MA (2015) Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. Proceedings of the 2015 New Security Paradigms Workshop, 73–84. https://doi.org/10.1145/2841113.2841119
- Bogost I (2010) Persuasive Games: The Expressive Power of Videogames. MIT Press, Cambridge, USA.
- Cialdini R (2017) Pre-Suasion, A Revolutionary Way to Influence and Persuade. [ISBN9781847941435]
- Conklin J (2005) Dialogue Mapping: Building Shared Understanding of Wicked Problems. UK Wiley, Chichester.
- Cyber Security Raad (2022) MEERJARENSTRATEGIE 2022–2025.
- De la Hera Conde-Pumpido T (2013) Conceptual Model for the Study of Persuasive Games. DiGRA 2013 - DeFragging Game Studies.
- Deterding S, Dixon D, Khaled R, Nacke L (2011) From Game Design Elements to Gamefulness: Defining Gamification. Proceedings of the 15th International Academic MindTrek Conference Envisioning Future Media Environments, 9–15. https://doi.org/10.1145/2181037.2181040
- De Vries G, Rietkerk M, Kooger R (2020) The hassle factor as a psychological barrier to a green home. Journal of Consumer Policy 43(2): 345–352. https://doi.org/10.1007/s10603-019-09410-7
- Edmondson A, Chamorro-Premuzic T (2020[, October 19]) Today's Leaders Need Vulnerability, Not Bravado.
- Jacobs RS (2017) Play to Win Over: Effects of Persuasive Games. Erasmus University Rotterdam, The Netherlands.
- Kirlappos I, Parkin S, Sasse MA (2014) Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. In: (Proceedings) Workshop on Usable Security, 1–10. https://doi.org/10.14722/usec.2014.23007
- Klabbers JHG (2018) On the architecture of game science. Simulation & Gaming 49(3): 207–245. https://doi.org/10.1177/1046878118762534
- Kors MJL, van der Spek ED, Schouten BAM (2017) A foundation for the persuasive gameplay experience. Proceedings of the 10th Annual Foundations of Digital Games Conference Foundations of Digital Games.
- Maier M, Bartoš F, Stanley TD, Shanks DR, Harris AJL, Wagenmakers E-J (2022) No evidence for nudging after adjusting for publication bias. PNAS 119(31): e2200300119. https://doi.org/10.1073/pnas.2200300119
- Michie S, Van Stralen MM, West R (2011) The behaviour change wheel: A new method for characterising and designing behaviour change interventions. Implementation Science 6: e42. https://doi.org/10.1186/1748-5908-6-42
- Nuijten A, Van Twist M, Van der Steen M (2015) Auditing interactive complexity: challenges for the internal audit profession. International Journal of Auditing 19(3): 195–205. https://doi.org/10.1111/ijau.12049

- Nuijten A, Van Twist M (2018) Bewust omgaan met het onbewuste: Over de relevantie van gamification voor internal audit. Speciale uitgave IIA Nederland.
- O'Keefe DJ (2002) Persuasion: Theory and research, 2nd edn. Sage Publications, Thousand Oaks, California.
- Orji R, Vassileva J, Mandryk RL (2014) Modelling the efficacy of persuasive strategies for different gamer types in serious games for health. User Modelling and User-Adapted Interaction 24: 453–498. https://doi.org/10.1007/s11257-014-9149-8
- Perloff R (2008) The dynamics of persuasion: Communication and attitudes in the 21st century. 3rd edn. Lawrence Erlbaum Associates, New York.
- Petty RJ, Cacioppo JT (1986) The elaboration likelihood model of persuasion. Advances in Experimental Social Psychology 19: 123–205. https://doi.org/10.1016/S0065-2601(08)60214-2
- Renaud K, Zimmermann V (2018) Ethical guidelines for nudging in information security & privacy. International Journal of Human-Computer Studies 120: 22–35. https://doi.org/10.1016/j.ijhcs.2018.05.011
- Rittel H, Webber M (1973) Dilemmas in a General Theory of Planning, Policy Sciences 4. Elsevier Scientific Publishing, 155–159. https://doi.org/10.1007/BF01405730
- Rothrock RA, Kaplan J, Van Der Oord F (2018) The board's role in managing cybersecurity risks. MIT Sloan Management Review 59(2): 12–15.
- SANS Security Awareness Report™ (2021) Managing Human Cyber Risk.
- Sas M, Hardyns W, Van Nunen K, Reniers G, Ponnet K (2021) Measuring the security culture in organizations: a systematic overview of existing tools. Security Journal 34: 340–357. https://doi.org/10.1057/s41284-020-00228-4
- Schein E.H (2010) Organizational culture and leadership, vol. 2. John Wiley & Sons.
- Soekarjo M, van Oostendorp H (2015) Measuring Effectiveness of Persuasive Games Using an Informative Control Condition. International Journal of Serious Game 2(2): 37–55. https://doi.org/10.17083/ijsg.v2i2.74
- Visch V, Vegt N, Anderiesen H, Van der Kooij K (2013) Persuasive Game Design: A model and its definitions. CHI'13. Paris, France.
- Yazdanmehr A, Wang J, Yang Z (2020) Peers matter: The moderating role of social influence on information security policy compliance. Information Systems Journal 30(5): 791–844. https://doi.org/10.1111/isj.12271
- Yukl G (2012) Effective leadership behaviour: What we know and what questions need more attention. Academy of Management Perspectives 26(4): 66–85. https://doi.org/10.5465/amp.2012.0088
- Zimmermann V, Renaud K (2019) Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. International Journal of Human-Computer Studies 131: 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005