Angst als drijfveer van motivatie om meer veiligheidsmaatregelen te nemen tegen cybercriminaliteit bij ondernemers in het MKB

Julian Cammelbeeck (s1002728)
Begeleider: Ferry van de Pol
Radboud Universiteit, Nijmegen
Faculteit der sociale wetenschappen
Master Behaviour Change
Datum: 8-7-2024
Aantal woorden: 7985

Abstract

Ondernemers in het MKB (midden- en kleinbedrijf) onderschatten het gevaar van cybercriminaliteit en voelen zich mede hierdoor niet gemotiveerd om het bedrijf digitaal beter te beveiligen. De huidige studie legt de focus op die lage motivatie van ondernemers om meer veiligheidsmaatregelen te nemen tegen cybercriminaliteit. In totaal vulden 134 ondernemers een online vragenlijst in. De studie onderzocht hiermee ten eerste de onderlinge relaties van de variabelen uit de protection motivation theory (PMT). Resultaten wezen uit dat waargenomen ernst en waargenomen kwetsbaarheid positieve voorspellers zijn van angst en dat motivatie een positieve voorspeller is van de intentie om een handeling uit te voeren om het bedrijf beter te beveiligen. Daarnaast werd gekeken of het vergroten van angst bij ondernemers kan zorgen voor een verhoogde motivatie en intentie. Ondernemers werden hiervoor geheel willekeurig ingedeeld in een conditie (controle/negatief/positief) met een LinkedIn bericht. De resultaten onthulden dat de manipulatie niet het gewenste effect had en dat er geen verschillen waren in angst, motivatie of intentie tussen de drie groepen. Het negatieve LinkedIn bericht maakte gebruik van loss framing, maar werkte tegen de verwachting in niet significant beter dan de gain framing bij het positieve LinkedIn bericht. Toekomstig onderzoek moet uitwijzen wat de beste manier van het communiceren van een fear appeal is om ondernemers gemotiveerd te krijgen voor het beveiligen van hun bedrijf.

Sinds de opkomst van de digitale wereld heeft het zich gemanifesteerd tot een wereldwijd begrip. Hedendaags maken 5,4 miljard mensen gebruik van digitale diensten (Statista, 2024). In Nederland, eind 2022, waren dit 14,7 miljoen mensen van vijftien jaar en ouder (CBS, 2023). In alle facetten van de samenleving is de digitalisering doorgedrongen. Het bedrijfsleven is één van die facetten, waar het bekend staat als informatie- en communicatietechnologieën (ICT). Naar schatting had 92 procent van de Nederlandse bedrijven met tien of meer werknemers een eigen website in 2022 (CBS, 2022). Bedrijven digitaliseren gevoelige en belangrijke gegevens. Dit maakt hen een interessant doelwit voor cybercriminelen om geld los te weken. De meest voorkomende manier hiervoor is ransomware, waarbij criminelen gegevens blokkeren die alleen zijn terug te halen door hiervoor te betalen (Alert Online, 2022). Het rapport van Alert Online toont aan dat ook andere typen cybercriminaliteit veelvuldig gebruikt worden tegen bedrijven, zoals phising, waarbij nepmailtjes trachten betaalgegevens te achterhalen. Het bedrijfsleven heeft dus meerdere gevaren te duchten van cybercriminelen.

Het goed beveiligd zijn tegen cybercriminaliteit is een noodzaak gezien de verwoestende impact die het kan hebben op bedrijven (Ozkan et al., 2021). Zo zijn herstelkosten vaak hoog, met in het ergste geval een faillissement als gevolg. The Global Risk Report (2023) onthult dat cybercriminaliteit op plek vier staat in de lijst van potentiële risico's voor het bedrijfsleven. Dit potentiële risico maakt ook geen onderscheid tussen bedrijfssectoren. Zo zijn er in 2022 en het begin van 2023 onder andere cyberaanvallen uitgevoerd op tandartspraktijken, ziekenhuizen, energiedienstverleners, spoorwegmaatschappijen, woningcorporaties en mobiele providers (CBS, 2022). Tegenwoordig loopt 1 op de 5 bedrijven al het risico om getroffen te worden door een cyberaanval (Eye Security, 2023). Ter vergelijking, voor bedrijven is de kans op een fysieke inbraak 1 op 250 en de kans op een brand 1 op 8000 (Rabobank, 2023). Tóch zijn er veel bedrijven die weinig tot geen veiligheidsmaatregelen nemen tegen cybercriminaliteit (Alert Online, 2022).

Er bestaat een duidelijke discrepantie tussen de grotere en kleinere bedrijven met betrekking tot de genomen hoeveelheid veiligheidsmaatregelen. De tendens is dat grote bedrijven significant beter beveiligd zijn tegen cybercriminaliteit dan midden- kleinbedrijven (MKB) (Alert Online, 2022). Ter illustratie, afspraken over het uitwisselen van bestanden en persoonsgegevens wordt door grote bedrijven in 48% van de gevallen gemaakt, terwijl dit voor het MKB gemiddeld 20% is. Bovendien onderneemt bijna een kwart van de MKB's uit het rapport van Alert Online zelfs geen énkele actie omtrent online veilig gedrag, terwijl dit

slechts 1% is bij de grote bedrijven. Uit data van het CBS blijkt verder dat 50% van het MKB geen risicoanalyse maakte, wat resulteert in onvoldoende inzicht in de kans op incidenten en de daarmee gepaard gaande consequenties (CBS, 2022). Dit percentage neemt sterk toe naarmate bedrijven minder werknemers hebben. Verder wijzen studies uit dat ondernemers van het MKB een lage cyberweerbaarheid hebben en niet voorbereid zijn om cyberaanvallen te voorkomen en te herstellen (Van der Kleij & Leukfeldt, 2019). Daarbovenop wordt alleen een minderheid van de genomen IT-maatregelen correct uitgevoerd (Osborn & Simpson, 2018; Rohn et al., 2016).

Het probleem van de lage genomen hoeveelheid veiligheidsmaatregelen door ondernemers in het MKB lijkt een duidelijke oorzaak te hebben. Recente interviews en studies met ondernemers binnen het MKB, wijzen namelijk uit dat motivatie het hoofdelement is waaraan het ontbreekt (BIC, 2024; Heidt, Gerlach, & Buxmann, 2019). Zo blijk dat ondernemers in het MKB denken dat er bij hun relatief kleine bedrijf toch niks te halen valt en dat zij daardoor geen doelwit zijn. Er heerst dus een optimisme bias. De gedachtegang is dat er niks kan gebeuren, omdat er nog nooit iets is gebeurd. Ondernemers ervaren daarbij de potentiële gevaren als niet ernstig en minimaal in schade (Workman, 2008). Daarnaast blijkt ook uit het rapport van BIC (2014) dat ondernemers het te veel tijd en moeite vinden kosten om het bedrijf beter te beveiligen. Deze voorgaande voorbeelden zijn allemaal redenen waarom ondernemers nauwelijks gemotiveerd zijn. Verder is er nog maar amper onderzoek gedaan naar wat de motivatie en de cognitieve processen van ondernemers zijn om zich te beschermen tegen cybercriminaliteit, zoals ook geconcludeerd wordt in de studie van Bekkers et al. (2023). Meer onderzoek is noodzakelijk om een completer beeld te krijgen van deze processen.

Drijfveren van motivatie voor cyberveilig gedrag

Zoals geschetst is het grote probleem binnen het MKB de lage motivatie om maatregelen te treffen tegen cybercriminaliteit. De gelimiteerde hoeveelheid studies die onderzoek deed naar de psychologie achter de motivatie bij ondernemers, maakte gebruik van de protection motivation theory (PMT) (Rogers, 1975). De PMT is hiervoor een geschikt model omdat hierin de ‘protection motivation’ centraal staat. De protection motivation is de motivatie die een persoon ervaart om zich tegen een specifiek gevaar te beschermen en zal in deze studie verder worden aangeduid als ‘beschermingsmotivatie'. De PMT is in het algemeen ook de meest gebruikte theorie voor het verklaren van cyberveilig gedrag (Alsharida et al., 2023). Daarbij blijkt de theorie binnen dit domein goed stand te houden (De Kimpe et al.,

2022; Martens et al., 2019; Tsai et al., 2016). Dit wil zeggen dat studies bevestiging vinden, aan de hand van significante resultaten, voor het model als verklaring voor het gedrag. De PMT gaat uit van twee hoofdcomponenten, namelijk 'threat appraisal' en 'coping appraisal'. Toepassend op deze studie; threat appraisal gaat om de beoordeling van de ondernemer over het gevaar van cybercriminaliteit voor zijn bedrijf en bij coping appraisal gaat dit om de beoordeling van de ondernemer wat hijzelf kan doen tegen cybercriminaliteit. Beide paden leiden tot motivatie om het bedrijf te beschermen, waardoor aanbevolen veiligheidsmaatregelen sneller worden uitgevoerd. Zo blijkt er uit een meta-analyse naar informatiebeveiliging een significant positief effect van de beschermingsmotivatie op gedrag (Mou et al., 2022). Hoe gemotiveerder een ondernemer is om zijn bedrijf te bewapenen tegen cybercriminaliteit, hoe sneller dit dus kan worden vertaald naar gedrag (**H5, H9**). Het is dus van belang om te begrijpen hoe de PMT het gebrek aan motivatie bij ondernemers kan verklaren.

Een onderdeel van de coping appraisal is de responseffectiviteit. De ***responseffectiviteit*** is de overtuiging van een persoon dat de adaptieve respons zal werken en dat het nemen van een beschermende maatregel henzelf en anderen effectief beschermt tegen een gevaar (Boss et al., 2015; Floyd et al., 2000). Meerdere studies vonden een positief significant effect van de responseffectiviteit op de beschermingsmotivatie (Jansen et al., 2016; Mou et al., 2022). Naarmate een ondernemer de maatregel(en) tegen cybercriminaliteit als effectief beschouwt, zal hij dus gemotiveerder zijn om dit ook daadwerkelijk uit te voeren. Daarbij was het verband tussen responseffectiviteit en beschermingsmotivatie een van de meer robuuste PMT-verbanden in de meta-analyse van Mou et al. (2022) en daarbovenop relatief consistent in het domein van informatiebeveiliging.

Zelfeffectiviteit is de andere determinant die deel uitmaakt van de coping appraisal. Dit is de overtuiging dat je als persoon in staat bent om de juiste handelingen uit te voeren om een gevaar te verminderen (Norman et al., 2005). Uit meerdere studies blijkt dat, uit de originele PMT-variabelen, zelfeffectiviteit de grootste predictor is voor de beschermingsmotivatie (Crossler et al., 2013; Jansen et al., 2016; Mou et al., 2022). Een ondernemer die weet wat te doen tegen cybercriminaliteit, zal gemotiveerder zijn om maatregelen te nemen. Een lage perceptie van zelfeffectiviteit kan resulteren in maladaptief gedrag als het niet opweegt tegen de ernst van het gevaar (Nabi et al., 2008).

Ondanks dat de coping appraisel in de literatuur over informatiebeveiliging interessante resultaten oplevert, legt de huidige studie de focus op de 'threat appraisal' kant van de PMT. De reden hiervoor is dat het probleem bij ondernemers vooral zit in het

onderschatten van hoe kwetsbaar hun bedrijf is en hoe ernstig de gevolgen van cybercriminaliteit zijn (BIC, 2024; Workman, 2008). Deze twee elementen vormen samen de threat appraisal uit de PMT. Waar bij de ruime meerderheid van de PMT-studies de 'threat appraisal' hier stopt, kan 'angst' een mogelijk goede toevoeging zijn. De meta-analyse van Mou et al. (2023) onthult namelijk het belang van het toevoegen van de 'angst' variabele. Zo vertoont de waargenomen kwetsbaarheid op zichzelf geen significant effect op de beschermingsmotivatie. Echter, wanneer angst als mediërende variabele tussen de waargenomen kwetsbaarheid en de motivatie wordt toegevoegd, ontstaat er een significant effect van de waargenomen kwetsbaarheid op angst. Hierbij is het effect van kwetsbaarheid op angst zelfs wat groter dan het effect van ernst op angst (H3). Bovendien is er een positief significant effect van angst op de beschermingsmotivatie (Mou et al., 2023) (**H4, H8**). Angst maakt de threat appraisal dus completer en speelt daarmee een cruciale rol in het verklaren van de beschermingsmotivatie van ondernemers.

Een determinant die onderdeel is van de threat appraisal, is de ***waargenomen ernst.*** Hierbij gaat het om hoe erg de ondernemer de schadelijke gevolgen van cybercriminaliteit beoordeelt voor zijn bedrijf. De waargenomen ernst heeft een positief significant effect op de angst die een persoon ervaart (Mou et al., 2022) (**H1, H7**). Naarmate een ondernemer de gevolgen van een cyberaanval als erger beoordeelt, zal de angst hiervoor toenemen. Uit het rapport van BIC (2024) blijkt dus dat ondernemers van het MKB de ernst van de schadelijke gevolgen onderschatten en daarbij denken dat de gevolgen wel zullen meevallen. Dit houdt in dat ondernemers over het algemeen de ernst van cybercriminaliteit als laag beoordelen. Hierdoor zal de angst voor cybercriminaliteit minder zijn. Dit alles leidt tot een lagere motivatie onder ondernemers om maatregelen te treffen.

De tweede determinant die onderdeel is van de threat appraisal is de ***waargenomen kwetsbaarheid.*** Zoals uitgelegd is het MKB zeer kwetsbaar. Het rapport van BIC onthulde dus dat ondernemers in het MKB leiden aan een optimisme bias (2024). Waar zij erkennen dat iedereen risico loopt, schatten zij de kans voor hun eigen bedrijf veel lager in. De waargenomen kwetsbaarheid heeft een positief significant effect op de angst die een persoon ervaart voor een gevaar (Mou et al., 2022) (**H2, H6)**. Hoe kwetsbaarder een ondernemer zijn bedrijf beoordeelt voor cybercriminaliteit, hoe groter de angst. Er is een onderscheid tussen MKB's die hun IT uitbesteden en MKB's die dit niet doen. Wanneer ondernemers hun IT uitbesteden, denken zij dat zij minder kwetsbaar zijn voor cybercriminaliteit (Bekker et al., 2023) (**H10)**. Dit komt door het vertrouwen van de ondernemer in de expertise van het externe bedrijf en het idee dat zijn bedrijf hiermee in goede handen is (Osborn & Simpson,

2018; Van den Berg & Keymolen, 2017). Hiermee bestaat de volledige threat appraisal, die de huidige studie gebruikt, uit de elementen ernst, kwetsbaarheid en angst. .

Omdat angst dus een cruciale rol speelt in de threat appraisal, richt deze studie zich op fear appeals om de angst onder ondernemers te vergroten. Ondanks dat het verband tussen gevaar en angst vanzelfsprekend lijkt, heeft PMT-onderzoek in de informatiebeveiligingsliteratuur fear appeals over het algemeen genegeerd (Boss et al., 2015). Dit is merkwaardig aangezien de fear appeal een fundamentele assumptie is van PMT-onderzoek (Floyd et al., 2000; Rogers, 1975). Zo zijn fear appeals belangrijk voor het motiveren van beveiligingsgedrag (Boss et al., 2015). Bovendien kan een gebrek aan een fear appeal boodschap ervoor zorgen dat de gewenste motivatie zelfs uitblijft vanwege een incomplete threat appraisal (Workman et al., 2009). De auteurs uit de studie van Boss et al. (2015) adviseren PMT-onderzoekers in de informatieveiligheidsliteratuur om idealiter fear appeal manipulaties te gebruiken. Daarbij beargumenteren ze dat wanneer het fear appeal bericht geen gevoel van angst oproept, de kans veel kleiner is dat de persoon zich wil beschermen voor het gevaar. Het niet gebruiken van een fear appeal schendt de PMT als model, met misleidende resultaten tot gevolg. De verwachting van de manipulatie is dat de angst onder ondernemers toeneemt en daarmee, op basis van het PMT-model, de motivatie en intentie tot gedrag ook stijgen (**H11, H12, H13**).

Een fear appeal is een loss frame boodschap die negatieve consequenties benadrukt (Rosoff et al., 2013). Vanuit een theoretisch oogpunt is het interessant om deze loss framing tegenover gain framing te plaatsen. Dit omdat onderzoek aan de ene kant laat zien dat ‘losses’ psychologisch impactvoller zijn dan ‘gains’ (Tversky & Kahneman, 1981). Zo deden Rosoff et al. (2013) onderzoek naar gain en loss frame effecten bij online veiligheidsgedrag. De auteurs vonden dat wanneer de focus meer lag op losses, het waarschijnlijker was dat deelnemers veiligere cyberbeslissingen namen (**H14)**. Dit werd ook gevonden in de studie van Rodriguez-Priego et al. (2020). Aan de andere kant vertelt de economische psychologie dat mensen bij het zien van een bericht met winstframing meer geneigd zijn om zich risicomijdend te gedragen dan bij het zien van een bericht met verliesframing (Kahneman & Tversky, 1979). Een studie in het domein van informatieveiligheid toont bewijs dat mensen risicoavers zijn wanneer gains centraal staan (Arora et al., 2006). Dit zou dus beteken dat mensen sneller maatregelen zouden nemen tegen cybercriminaliteit na het zien van een bericht met winstframing, aangezien het tegenovergestelde gedrag een risico met zich meebrengt. Vanwege deze discrepantie in de literatuur zet het huidige onderzoek een juxtapositie van negative (loss) en positive framing (gain) tegenover elkaar.

De huidige studie zoekt bevestiging of de PMT-variabelen van de threat appraisal van invloed zijn op het gedrag van een ondernemer om zijn bedrijf te beschermen tegen cybercriminaliteit. De lage genomen hoeveelheid veiligheidsmaatregelen en de daarmee gepaard gaande kwetsbaarheid, maakt dat deze studie de focus zal leggen op het verbeteren van cyberveiligheid binnen het MKB. Daarbij focust deze studie zich op ondernemers van het MKB die IT-afhankelijk zijn met een grootte van 1 tot 250 werknemers (de grens tot waar een bedrijf tot MKB behoort). Het doel van de huidige studie is om ondernemers te motiveren om (meer) veiligheidsmaatregelen te nemen tegen cybercriminaliteit. Daarbij is de onderzoeksvraag of het vergroten van angst bij ondernemers resulteert in hogere motivatie om veiligheidsmaatregelen te nemen tegen cybercriminaliteit. Verder worden twee aanvullende vragen behandeld. Ten eerste of ondernemers door de manipulatie ook daadwerkelijk sneller gedrag vertonen dat wijst op (de intentie tot) cyberveilig gedrag. Ten tweede of loss framing beter werkt dan gain framing in het motiveren van ondernemers. Tabel 1 bevat de hypotheses van de huidige studie die gebaseerd zijn op de hiervoor behandelde theorie.

Tabel 1

Overzicht hypothesen

Nummer	Hypothese
1	Angst wordt positief voorspeld door ernst
2	Angst wordt positief voorspeld door kwetsbaarheid
3	Kwetsbaarheid is een sterkere predictor van angst dan ernst
4	Motivatie wordt positief voorspeld door angst
5	Intentie voor gedrag wordt positief voorspeld door motivatie
6	Hogere scores op kwetsbaarheid leidt tot hogere scores op angst
7	Hogere scores op ernst leidt tot hogere scores op angst
8	Hogere scores op angst leidt tot hogere scores op motivatie
9	Hogere scores op motivatie leidt tot hogere scores op intentie
10	Kwetsbaarheid verschilt tussen ondernemers die IT intern hebben geregeld en die IT extern hebben geregeld
11	Angst is hoger in de manipulatieconditie dan de andere condities.

12	Motivatie is hoger in de manipulatieconditie dan de andere condities
13	Intentie is hoger in de manipuatieconditie dan de andere condities
14	Loss framing zorgt voor hogere motivatie dan gain framing
15	Ondernemers in de manipulatieconditie willen meer informatie lezen over cybercriminaliteit dan in andere condities

Note Hier worden de hypothesen weergeven die gebaseerd zijn op theorie uit de introductie. De hypothesen worden in de tekst aangegeven door middel van een dikgedrukte H met het nummer erachter.

Methode

Deelnemers

Een kwantitatief onderzoek werd uitgevoerd om te zien of ondernemers in het MKB te motiveren zijn om meer veiligheidsmaatregelen te nemen tegen cybercriminaliteit. Een a priori poweranalyse voor een one-way ANOVA ($f^2 = 0.29$, $\alpha = .05$, $1\text{-}\beta = .80$, Groepen = 3) wees op een minimale steekproefgrootte van 120 deelnemers. Hierbij zijn de inclusiecriteria gehanteerd dat de ondernemer de eigenaar is van het bedrijf én dat hij of zij daarnaast minimaal 1 tot maximaal 250 medewerkers in dienst heeft.

In totaal hebben 192 ondernemers deelgenomen aan het onderzoek. Deelnemers werden geschrapt als zij niet aan de inclusiecriteria voldeden of onvolledige vragenlijsten invulden. Hierdoor omvat het huidige onderzoek uiteindelijk 134 deelnemers. Van dit aantal ondernemers hebben de meeste een bedrijf in de zakelijke dienstverlening (43,3%) en een hoeveelheid van 6 tot 75 medewerkers (35,8%) of 2 tot 5 medewerkers (34,3%). Van alle deelnemers gaf de meerderheid aan dat IT belangrijk (34.3%) of zelfs zeer belangrijk (38,8%) is voor hun bedrijfsvoering. De volledige percentages zijn te vinden in bijlage A. De werving van deelnemers vond plaats door middel van verschillende kanalen. Zo is er gebruik gemaakt van een extern panelbureau (Norstat), een klantenpanel (Interpolis), brieven, e-mails en sociale media. Deelname aan het onderzoek was vrijwillig en kon op ieder moment worden beëindigd. Voor deelname is geen beloning verstrekt. Het huidige onderzoek is bekeken en beoordeeld door de Ethiek Commissie Sociale Wetenschappen (ECSW) en daarbij waren geen formele bezwaren tegen het onderzoek: ECSW-2024-077.

Materialen

Vragenlijst. Het onderzoek maakte hoofdzakelijk gebruik van een vragenlijst (Bijlage B). Het begin bestond uit vragen over de bedrijfsinrichting (branche, aantal medewerkers, IT-afhankelijkheid, IT-inrichting en ervaring met cybercriminaliteit). Om de PMT-variabelen te meten, zijn er zelf geconstrueerde schalen ontworpen. De items uit deze schalen zijn gebaseerd op eerdere studies (Bekkers et al., 2023; Burns et al., 2017). Voor de items van de variabelen waargenomen kwetsbaarheid, ernst, angst en motivatie werd aan de deelnemers gevraagd om een antwoord te selecteren op een 5-punts Likert schaal (1 = Sterk mee oneens, 5 = Sterk mee eens). Voor deze variabelen bestond de schaal uit 3 items. Voor de variabele 'intentie' moesten deelnemers een antwoord selecteren op een 5-punts Likert schaal die opliep in mate van zekerheid (1 = Zeker niet, 5 = Zeker wel). Deze schaal bestond uit 4 items. Als voorbeeld, bij de variabele '*kwetsbaarheid'* was één van de items: "Mijn bedrijf loopt risico op bedreigingen van cybercriminaliteit". Voor '*ernst'* was één van de items: "Als mijn bedrijf slachtoffer zou worden van cybercriminaliteit, dan zal het leiden tot hoge kosten". Bij '*angst*' was dat: "Als ik denk aan de bedreigingen van cybercriminaliteit voor mijn bedrijf, dan voel ik mij angstig". Bij '*motivatie'* was dat: "Ik heb de motivatie om mijn bedrijf te beschermen tegen cybercriminaliteit". En ten slotte bij '*intentie*' was één van de items: "Ik heb de intentie om een adviesgesprek aan te vragen over cyberveiligheid".

Deelnemers kregen ook één van drie LinkedIn berichten te zien (zie 'Interventiemateriaal'). Na het LinkedIn bericht was er een vraag welk rapportcijfer de deelnemer het LinkedIn bericht gaf, gevolgd door zeven stellingen over het LinkedIn bericht. Het rapportcijfer werd gevraagd om te testen hoe de LinkedIn berichten ontvangen werden door de ondernemers. Deze stellingen konden beantwoord worden door een antwoord te selecteren op een 5-punts Likert schaal (1 = Sterk mee oneens, 5 = Sterk mee eens). Voorbeelden van die stellingen zijn: "Ik snap het doel van het LinkedIn bericht" en "Ik vind het LinkedIn bericht heftig". Aan het einde was er een vraag of deelnemers meer informatie wilden lezen over cybercriminaliteit en veiligheidsmaatregelen, die te beantwoorden was met een ja of nee. De functie van de vraag was om een gedragsmaat aan de vragenlijst toe te voegen. De vragen per PMT-variabele zijn terug te vinden in tabel 2.

Interventiemateriaal. Verder maakte deze studie gebruik van drie zelfontworpen LinkedIn berichten (Bijlage C). Er is gekozen voor LinkedIn omdat dit een kanaal is waar ondernemers het makkelijkst te bereiken zijn. De berichten waren verschillend op inhoud in zowel het tekstuele als het visuele aspect. Voor de controleconditie bestond het LinkedIn

bericht uit communicatie door middel van cijfers en feiten. Er werd naar de lezer gecommuniceerd hoe kwetsbaar ondernemers in het MKB zijn voor cybercriminaliteit en dat het kan leiden tot schade in de vorm van kosten. Na onderzoek op LinkedIn bleken dit soort berichten het meest voor te komen en waren daarmee de standaard. Het tweede en het derde LinkedIn bericht zijn, gebaseerd op echte verhalen, geschreven vanuit het perspectief van een ondernemer uit het MKB. In het tweede LinkedIn bericht wordt aan de lezer gecommuniceerd wat er te verliezen (loss frame) valt zónder goede cyberbeveiliging en in het derde LinkedIn bericht wat er te winnen (gain frame) valt mét goede cyberbeveiliging.

De manipulatie zat met name in het tweede LinkedIn bericht waarin het doel was om angst te verhogen door middel van een fear appeal (loss frame). Met het persoonlijke verhaal van de ondernemer is gebruik gemaakt van storytelling. Onderzoek toont namelijk aan dat digitale storytelling menselijk gedrag kan beïnvloeden door het verdiepen van emotionele niveaus (Grindle, 2014). De amygdala, wat het 'angstcentrum' wordt genoemd, wordt gestimuleerd door fictionele representaties van gevaar op exact dezelfde manier als zou gebeuren bij perceptie van gevaar in de echte wereld (Grindle, 2014). Om het gevaar duidelijk te communiceren, bevatte de tekst veel details over wat de ondernemer allemaal kwijt was geraakt. Daarnaast blijkt dat een effectieve fear appeal onder andere moet aantonen hoe de desbetreffende doelgroep risico loopt voor het gevaar (Woon et al., 2005). Door het bericht aan te bieden vanuit een ondernemer in het MKB, wordt hieraan voldaan.

Verder is de tekst in het tweede LinkedIn bericht vergezeld met afbeeldingen die hoogstwaarschijnlijk een gevoel van gevaar en negatieve emoties oproepen, zoals een hacker, een donkere omgeving en een rood gevarenteken. Het LinkedIn bericht in de positieve conditie maakte gebruik van afbeeldingen die waarschijnlijk geassocieerd kunnen worden met veiligheid en positieve emoties, zoals het groene slotje en een lachend persoon. Wanneer mensen een keuze hebben, dan prefereren zij visuele berichten boven tekstuele berichten, wat bekend staat als de 'visual preference heuristic' (Townsend & Kahn, 2014). Afbeeldingen zijn makkelijker om te verwerken en maken de onderliggende tekstuele boodschap meer toegankelijk (Tsohou et al., 2015). De overtuiging is dat visuele risicocommunicatie effectiever is dan tekstuele communicatie in het omzetten van emotionele reacties tot drijfveren van intentie van gedrag (Ancker et al., 2006). Hierdoor is dit een belangrijk uitgangspunt geweest om afbeeldingen in het LinkedIn bericht te implementeren.

Procedure

Deelnemers namen kennis van het onderzoek door middel van verschillende kanalen. De deelnemers kwamen terecht bij de online vragenlijst door middel van het klikken op de link óf door het scannen van de QR-code in de brief. Voordat deelname officieel begon, lazen deelnemers de informatiebrief en gaven zij toestemming voor hun deelname en het verzamelen van hun data. Hierna moesten deelnemers vragen beantwoorden over hun bedrijfsinrichting. Vervolgens werd willekeurig één van de drie LinkedIn berichten toegewezen aan een deelnemer. Hen werd gevraagd om het LinkedIn bericht goed te lezen en de afbeelding aandachtig te bekijken. Er werden daarna namelijk vragen gesteld over het LinkedIn bericht. Hierop volgden de vragen over de PMT-variabelen. Als deelnemers aangaven meer informatie te willen lezen over cyberveiligheid, dan kwamen zij bij een extra blok met de desbetreffende informatie. Als deelnemers dat wilden, was er nog de mogelijkheid om opmerkingen achter te laten over de vragenlijst. Aan het eind werden deelnemers bedankt voor hun deelname en geïnformeerd dat zij de pagina konden sluiten. Alles bij elkaar bedroeg deelname 5 tot 10 minuten.

Data-analyse

Allereerst is tijdens de datapreparatie de data opgeschoond en gestructureerd in SPSS. Er is hierna gekeken naar de betrouwbaarheid van elke schaal van de PMT-variabelen (Tabel 2). Om de betrouwbaarheid van de ‘motivatie’ schaal te verhogen, is het derde item weggelaten. Doordat dit item verwijderd werd, steeg Cronbach’s alpha van .645 naar .769. Verder zijn er voor iedere deelnemer gemiddelde scores berekend voor de PMT-variabelen door de scores van de items van iedere schaal bij elkaar op te tellen en te delen door het aantal items. Vervolgens werden analyses uitgevoerd om een antwoord te krijgen op de hypotheses.

Om te analyseren of ernst en kwetsbaarheid positieve voorspellers zijn van angst, is er gebruik gemaakt van een MLR. Hierbij was angst de kwantitatieve afhankelijke variabele. De kwantitatieve onafhankelijke variabelen bestonden uit ernst en kwetsbaarheid. Er is voldaan aan de assumpties van lineariteit, homogeniteit, geen multicollineariteit, onafhankelijkheid van observaties, en normaliteit. Er bleken drie uitschieters te bestaan in het scatterplot, maar deze zijn niet uitgesloten omdat zij de uitkomst niet beïnvloedden.

Een eenvoudige lineaire regressie is uitgevoerd om te kijken of de onafhankelijke kwantitatieve variabele ‘angst’ een positieve voorspeller is van de afhankelijke kwantitatieve variabele ‘motivatie’. Er is gecontroleerd of werd voldaan aan de assumpties van lineariteit,

homogeniteit, geen multicollineariteit, onafhankelijkheid van observaties, en normaliteit. Om homogeniteit te verbeteren zijn drie uitschieters in het scatterplot buiten beschouwing gelaten. Omdat de assumptie van normaliteit geschonden leek, is ook bootstrapping gebruikt. Daarnaast is de analyse ook uitgevoerd met alle deelnemers en zonder bootstrapping. Uiteindelijk zal de volledige analyse gerapporteerd worden, omdat de uitschieters en bootstrapping geen invloed hadden op het resultaat.

Vervolgens is een tweede eenvoudige lineaire regressie uitgevoerd om te testen of de onafhankelijke kwantitatieve variabele 'motivatie' een positieve voorspeller is van de afhankelijke kwantitatieve variabele 'intentie'. Er is gecontroleerd of werd voldaan aan de assumpties van lineariteit, homogeniteit, geen multicollineariteit, onafhankelijkheid van observaties, en normaliteit. Om homogeniteit te verbeteren zijn vier uitschieters in het scatterplot buiten beschouwing gelaten. Daarna is de analyse ook uitgevoerd met alle deelnemers. De uitschieters hadden geen invloed op het resultaat, waardoor de analyse met alle deelnemers gerapporteerd wordt.

Om te testen of de onafhankelijke kwalitatieve variabele 'conditie' (controle/negatief/positief) het gewenste effect had op de afhankelijke kwantitatieve variabelen angst, motivatie en intentie, is een one-way MANOVA uitgevoerd als manipulatiecheck. Er is gecontroleerd of werd voldaan aan de assumpties van lineariteit, multivariate normaliteit, geen multicolineariteit, homogeniteit en geen multivariate uitschieters. Gebaseerd op de Mahalanobis-afstanden zijn twee deelnemers eerst buiten beschouwing gelaten omdat zij voldeden aan het criterium van een uitschieter. Echter worden zij niet uitgesloten omdat de uitschieters geen invloed hadden op het resultaat. Omdat voor alle drie de afhankelijke variabelen de assumptie van normaliteit geschonden bleek, zijn er additioneel drie Kruskal-Wallistoetsen uitgevoerd. Omdat de MANOVA robuust is voor schendingen van normaliteit, is ook deze analyse uitgevoerd.

Of er een verband is tussen conditie en het willen lezen van extra informatie is geanalyseerd door middel van een chi-square test. In deze analyse was conditie (controle/negatief/positief) de kwalitatieve onafhankelijke variabele en informatie (ja/nee) de kwalitatieve afhankelijke variabele.

Een onafhankelijke t-test uitgevoerd om te zien of de ervaren kwetsbaarheid verschilde tussen de ondernemers die IT intern geregeld hebben en ondernemers die IT extern geregeld hebben. Hierbij was IT (intern/extern) de kwalitatieve onafhankelijke variabele en kwetsbaarheid de kwantitatieve afhankelijke variabele. Er is voldaan aan de assumpties van normaliteit, homogeniteit en geen significante uitschieters.

Ten slotte zijn er nog enkele exploratieve analyses gedaan. Ten eerste is een one-way ANOVA gebruikt om het effect van de onafhankelijke kwalitatieve variabele 'conditie' (controle/negatief/positief) op de beoordeling van de afhankelijke kwantitatieve variabele 'heftigheid' te testen. Er is gecontroleerd of werd voldaan aan de assumpties van lineariteit, normaliteit en homogeniteit. De assumptie voor normaliteit was hierbij geschonden. Aangezien een ANOVA robuust is voor schendingen van normaliteit, heeft de analyse doorgang gevonden. Bootstrapping is niet toegepast omdat dit geen invloed had op het resultaat. Er was één univariate uitschieter, maar deze is niet verwijderd omdat de uitschieter het resultaat ook niet beïnvloedde. Voor statistische zekerheid is nog een Kruskal-Wallistoets uitgevoerd.

Overige exploratieve analyses zijn met Kruskal-Wallistoetsen en Mann-Whitney U testen uitgevoerd. Zo is er gekeken of er verschillen waren voor onder andere de afhankelijke variabelen angst, kwetsbaar, ernst, motivatie en intentie op onder andere de onafhankelijke variabelen kanaal, branche en ervaring.

Tabel 2

Variabelen, items, descriptive statistics en betrouwbaarheid.

Variabele	Items	Betrouwbaarheid
Kwetsbaarheid (*M* = 2.90, *SD* = 1.93)	1. "Mijn bedrijf loopt risico op bedreigingen van cybercriminaliteit" (*M* = 3.25, *SD* = 0.91)	Cronbach's alpha; α = .53
	2. "De kans dat mijn bedrijf slachtoffer wordt cybercriminaliteit is klein" (*M* = 2.71, *SD* = *0.93)*	Matige betrouwbaarheid
	3. "Mijn bedrijfsinformatie is kwetsbaar voor cybercriminaliteit" (*M* = 2.73, *SD* = 0.85)	
Ernst (*M* = 3.61, *SD* = 2.12)	1. "Als mijn bedrijf slachtoffer zou worden van cybercriminaliteit, dan zal het leiden tot hoge kosten" (*M* = 3.27, *SD* = 1.05)	Cronbach's alpha; α = .64
	2. "De gevaren van cybercriminaliteit voor mijn bedrijf zijn ernstig" (*M* = 3.24, *SD* = 0.98)	Acceptabele betrouwbaarheid
	3. "Ik geloof dat cybercriminaliteit iets serieus is" (*M* = 4.31, *SD* =0.73)	
Angst (*M* = 2.70, *SD* = 2.31)	1. "Als ik denk aan de bedreigingen van cybercriminaliteit voor mijn bedrijf, dan voel ik mij angstig" (*M* = 2.61, *SD* = 0.97)	Cronbach's alpha; α = .77
		Acceptabele betrouwbaarheid

	2. “Ik ben bezorgd over de mogelijkheid van cybercrimialiteit bij mijn bedrijf” (*M* = 3.01, *SD* = 0.90) 3. “De dreiging van cybercriminaliteit voor mijn bedrijf maakt mij nerveus” (*M* = 2.49, *SD* = 0.89)	
Motivatie (*M* = 3.88, *SD* =1.59*)*	1. “Ik heb de motivatie om mijn bedrijf te beschermen tegen cybercriminaliteit” (*M* = 3.93, *SD* = 0.85) 2. “Ik heb de motivatie om moeite te doen om mijn bedrijf te beschermen tegen cybercriminaliteit (*M* = 3.84, *SD* = 0.91)	Cronbach’s alpha; α = .77 Acceptabele betrouwbaarheid
Intentie (*M* = 2.83, *SD* = 3.34)	1. “Ik heb de intentie om meer informatie op te zoeken over veiligheidsmaatregelen tegen cybercriminaliteit” (*M* = 3.05, *SD* = 0.97) 2. “Ik heb de intentie om binnen mijn bedrijf te onderzoeken wat de zwakke plekken zijn op het gebied van cyberveiligheid” (*M* = 3.12, *SD* = 1.04) 3. “Ik heb interesse in een product dat mij kan helpen bij het beveiligen van mijn bedrijf (*M* = 2.88, *SD* = 1.05) 4. “Ik heb de intentie om een adviesgesprek aan te vragen over cyberveiligheid” (*M* = 2.25, *SD* = 1.03)	Cronbach’s alpha; α = .84 Goede betrouwbaarheid

Note Een hogere score op kwetsbaarheid betekent dat ondernemers hun bedrijf als kwetsbaarder beschouwen voor cybercriminaliteit. Voor ernst dat ondernemers de gevolgen van cybercriminaliteit voor hun bedrijf als ernstiger beschouwen. Voor angst dat een ondernemer angstiger is voor cybercriminaliteit. Voor motivatie dat een ondernemer gemotiveerder is om zijn bedrijf te beschermen. En voor intentie dat een ondernemer meer intentie heeft om specifieke handelingen uit te voeren om het bedrijf te beschermen.

Resultaten

Een meervoudige lineaire regressie is uitgevoerd om angst te voorspellen uit de variabelen ‘kwetsbaar’ en ‘ernst’. Het model verklaarde 18.3% van de variantie, $R^2 = .18$, $F(2, 131) = 14.62$, $p < .001$. De ‘unstandardized coefficients’, ‘standardized coefficients’ en p-waardes zijn te vinden in tabel 3. Zowel de ervaren ernst als ervaren kwetsbaarheid voorspellen in de huidige studie de ervaren angst van een ondernemer. Hierbij is ‘kwetsbaar’ de sterkste voorspeller van angst.

Tabel 3

Uitkomsten MLR met angst als afhankelijke variabele.

	Unstandardized Coefficients		*Standardized Coefficients*		
Variabele	*B*	Std. error	β	*t*	*p*
Ernst	.25	.10	.23	2.55	.012*
Kwetsbaar	.32	.11	.27	2.96	.004**

Note De significante bevinding van $P < .05$ is aangeduid met één asterisk (*) en die van $p < .01$ met twee asterisken (**).

Een eenvoudige lineaire regressie werd uitgevoerd om motivatie te voorspellen uit angst. De resultaten van de regressie onthulden dat angst 1.5% van de variantie verklaarde, $R^2 = .02$, $F(1, 132) = 2.04$, $p = .156$. Angst was geen statistisch significante voorspeller van motivatie, $b = 0.13$, $p = .156$. De ervaren angst van een ondernemer voorspelt in de huidige studie dus niet de motivatie van een ondernemer. Een andere eenvoudige lineaire regressie werd uitgevoerd om intentie te voorspellen uit motivatie. De resultaten van de regressie onthulden dat motivatie 15% van de variatie verklaarde, $R^2 = .15$, $F(1, 132) = 22.43$, $p < .001$. Motivatie was een statistisch positief significante voorspeller van intentie, $b = 0.40$, $p < .001$. De motivatie van een ondernemer voorspelt in de huidige studie dus de intentie van een ondernemer.

Een one-way MANOVA is uitgevoerd om het effect te bepalen van conditie (controle/negatief/positief) op angst, motivatie en intentie. De descriptive statistics zijn te vinden in tabel 4. Er waren geen statistisch significante verschillen tussen de condities op de afhankelijke variabelen, $F(6, 260) = 0.31$, $p = .933$; Pillai's Trace = .014; partial $\eta 2 = .007$. Additioneel zijn Kruskal-Wallistoetsen uitgevoerd om dezelfde effecten te toetsen. Uit deze resultaten blijkt ook geen significant verschil tussen de condities op de afhankelijke variabelen. Voor angst: (H(2) = .55; $p = .759$). Voor motivatie: (H(2) = .27; $p = .873$) Voor intentie: (H(2) = .14; $p = .931$). Beide analyses (MANOVA en Kruskal-Wallis) onthullen dat de drie condities voor zowel angst, motivatie als intentie niet dusdanig van elkaar verschillen.

Tabel 4
Descriptive statistics voor de manipulatie check MANOVA.

	Angst			Motivatie			Intentie	
	n	*M*	*SD*	*n*	*M*	*SD*	*n*	*M*	*SD*
Controle	47	2.62	0.78	47	3.87	0.92	47	2.78	0.82
Negatief	45	2.78	0.76	45	3.83	0.83	45	2.81	0.91
Positief	42	2.71	0.78	42	3.95	0.60	42	2.89	0.79

Note De onafhankelijke variabele was conditie bestaande uit drie groepen (controle/negatief/positief). De variabelen angst, motivatie en intentie zijn weergeven als de afhankelijke variabelen.

Een chi-square toets is uitgevoerd om te analyseren wat het verband is tussen conditie (controle/negatief/positief) en extra informatie willen lezen (ja/nee). In Tabel 5 zijn de aantallen van de deelnemers weergeven. Er is geen statistisch significant verband tussen de variabelen, χ^2 (2, N = 134) = 3.79, p = .150. Het is voor alle condities dus ongeveer even waarschijnlijk dat ondernemers extra informatie (willen) lezen.

Tabel 5
Aantallen deelnemers van de Conditie x Meer informatie chi-square toets.

		Conditie			
		Controle	Negatief	Positief	Totaal
Meer informatie	Ja	34	25	23	82
	Nee	13	20	19	52
Totaal		47	45	42	134

Note De conditie is hier de onafhankelijke variabele en de ‘meer informatie’ is de afhankelijke variabele.

Een onafhankelijke t-test is uitgevoerd om ervaren kwetsbaarheid te vergelijken tussen ondernemers die IT Intern (N = 25) hebben geregeld en de ondernemers die IT extern (N = 41) hebben geregeld. Er bestond geen statistisch significant verschil voor de scores van ondernemers die IT intern hebben geregeld (M =3.1, SD = 0.7) en ondernemers die IT extern hebben geregeld (M =2.9, SD = 0.6); t(64) = 1.23, p = .222. Ondernemers beoordelen kwetsbaarheid dus gelijkwaardig in de IT extern en de IT intern condities.

Exploratieve analyses

Een one-way ANOVA is uitgevoerd om te kijken naar het effect van conditie (controle/negatief/positief) op de beoordeling van heftigheid van het LinkedIn bericht. De descriptive statistics zijn te vinden in tabel 6. Uit de resultaten blijkt een statistisch significant verschil tussen de condities op de beoordeling van heftigheid van een LinkedIn bericht, $F(2, 130) = 7.11$, $p = .001$. Een Scheffe post hoc test onthulde dat de ervaren heftigheid van het LinkedIn bericht statistisch significant lager was voor de controlegroep (2.5 ± 0.9, $p = .025$) en de positieve groep (2.3 ± 1.0, $p = .002$) in vergelijking met de negatieve groep (3.1 ± 1.0). Uit de Kruskal-Wallistoets bleek ook een significant verschil tussen de condities op heftigheid ($H(2) = 11.47$; $p = .003$). Ook hier waren de verschillen tussen de negatieve groep en de controlegroep/positieve groep significant, respectievelijk $p = .014$ en $p = .001$. Beide analyses tonen aan dat ondernemers in de negatieve conditie het bericht als heftiger beoordeelden dan in de andere twee condities.

Tabel 6
Descriptive statistics voor de Conditie x Heftigheid ANOVA.

	n	*M*	*SD*
Controle	47	2.53	0.93
Negatief	45	3.09	0.97
Positief	42	2.33	1.00

Note De onafhankelijke variabele was conditie (controle/positief/negatief). Heftigheid is de afhankelijke variabele.

Daarnaast bleek uit een Mann-Whitney U test dat ondernemers die aangaven al ervaring te hebben met cybercriminaliteit, significant hogere scores rapporteerden bij zowel motivatie ($U = 1442$, $p = .020$) als ernst ($U = 1370$, $p = .009$), dan ondernemers die nog geen ervaring hadden met cybercriminaliteit. Ervaring met cybercriminaliteit resulteerde dus in hogere scores op ernst en motivatie.

Discussie

Deze studie onderzocht of de motivatie en/of intentie bij ondernemers te vergroten was door middel van het inspelen op angst in een LinkedIn bericht. Hierbij werden zowel de verbanden tussen de PMT-variabelen getest als de effectiviteit van de manipulatie. Daarnaast is gekeken of loss framing beter werkt om te motiveren dan gain framing. Een overzicht van de beslissingen over de hypothesen is te vinden in tabel 7. De beslissingen worden hierna besproken.

Tabel 7
Beoordeling van hypothesen

Nummer	Hypothese	Beslissing
1	Angst wordt positief voorspeld door ernst	Aangenomen*
2	Angst wordt positief voorspeld door kwetsbaarheid	Aangenomen**
3	Kwetsbaarheid is een sterkere predictor van angst dan ernst	Aangenomen
4	Motivatie wordt positief voorspeld door angst	Verworpen
5	Intentie wordt positief voorspeld door motivatie	Aangenomen***
6	Hogere scores op kwetsbaarheid leidt tot hogere scores op angst	Aangenomen
7	Hogere scores op ernst leidt tot hogere scores op angst	Aangenomen
8	Hogere scores op angst leidt tot hogere scores op motivatie	Verworpen
9	Hogere scores op motivatie leidt tot hogere scores op intentie	Aangenomen
10	Kwetsbaarheid verschilt tussen ondernemers die IT intern hebben geregeld en die IT extern hebben geregeld	Verworpen
11	Angst is hoger in de negatieve conditie dan de andere condities.	Verworpen

12	Motivatie is hoger in de negatieve conditie dan de andere condities	Verworpen
13	Intentie is hoger in de negatieve conditie dan de andere condities	Verworpen
14	Loss framing zorgt voor hogere motivatie dan gain framing	Verworpen
15	Ondernemers in de negatieve conditie willen meer informatie lezen over cybercriminaliteit dan in de andere condities	Verworpen

Note De aangenomen hypothese gebaseerd op een significantie van $p < .05$ is gemarkeerd met één asterisk (*), de aangenomen hypothese gebaseerd op een significantie van $p < .01$ is gemarkeerd met twee asterisken (**) en de aangenomen hypothese gebaseerd op een significantie van $p < .001$ is gemarkeerd met drie asterisken (***). Hypothese 3 bevat geen asterisk omdat deze niet gebaseerd is op een *p*-waarde. Hypothese 6, 7, 8 en 9 bevatten geen asterisk omdat deze gebaseerd zijn op de uitkomst van hypothese 1, 2, 4 en 5

De huidige studie heeft bij het onderzoeken van de PMT-variabelen meerdere resultaten gerepliceerd uit de meta-analyse van Mou et al. (2023). Zo vond de huidige studie, net als in de meta-analyse, dat ervaren ernst en ervaren kwetsbaarheid positieve voorspellers zijn van de hoeveelheid angst die iemand ervaart. Daarbij blijkt in beide studies dat kwetsbaarheid een sterkere predictor is van angst. Hiermee zijn hypotheses 1 tot en met 3 bevestigd. Voor het meest cruciale verband van de PMT voor deze studie, angst als positieve voorspeller van motivatie, is er geen bevestiging gevonden. Dit verband is het meest cruciaal aangezien de manipulatie in deze studie om dit verband draait. Hypothese 4 werd dus verworpen. Wél heeft de huidige studie bevestiging gevonden voor hypotheses 5, dat motivatie een positieve voorspeller is van intentie. Hierbij gaat het om de intentie voor een handeling (gedrag). Dit is ook weer in lijn met de studie van Mou et al. (2023).

Om tot een verklaring te komen voor het niet gevonden verband tussen de PMT-variabelen angst en motivatie, is het van belang om in te zoomen op de PMT als theoretisch model. Hoewel de PMT is gebruikt in meerdere onderzoeken naar informatiebeveiliging, blijken de resultaten in de literatuur inconsistent. Zo zijn er studies die erin slaagden om delen van het PMT-model te bevestigen (De Kimpe et al., 2022; Tsai et al., 2016), en studies die hier niet in slaagden (Ogbanufe et al., 2023; Posey et al., 2015). De oorzaak hiervoor ligt mogelijk in het feit dat de PMT origineel ontworpen is voor onderzoek in de medische wereld (Crossler et al., 2013). In het gebruik van de PMT bij de medische wereld wordt een gevaar toegeschreven aan de eigen persoon, aangezien het om de gezondheid van een persoon gaat. Het gevaar is dus direct gerelateerd aan de persoon en dit maakt dat hij/zij het gevaar als

relevant beschouwd. In de huidige studie is de gevareninformatie gericht op organisatieniveau, zoals bestanden en informatie van het bedrijf. Zoals Jamil et al. (2024) beweren, kan er hierdoor een paradox ontstaan tussen de motivatie om deze informatie te willen beschermen en de persoonlijke relevantie om daadwerkelijk veiligheidshandelingen uit te voeren. Dit betekent dat ondernemers waarschijnlijk het bedrijf niet als onderdeel van zichzelf zien, waardoor het gevaar niet aan het individu wordt toegeschreven. Dit idee wordt versterkt doordat individuen in het bedrijfsleven weinig 'psychological ownership' ervaren, waardoor relevantie tot het gevaar vermindert (Menard et al., 2017).

De studie van Crossler et al. (2013) bewijst dat die persoonlijke relevantie (relatedness) een belangrijke toevoeging is aan het PMT-model in de literatuur rondom informatiebeveiliging. De auteurs beargumenteren dat het toevoegen van 'relatedness' in het model, vanuit de self-determination theory (SDT), zorgt voor meer intrinsieke motivatie en daarbij een positief significant effect heeft op de kwetsbaarheid en ernst. Door in te spelen op de persoonlijke connectie van de ondernemer met een element in zijn bedrijf, zal intrinsieke motivatie ontstaan en hierdoor de situatie als persoonlijk relevanter worden beschouwd. Uit onderzoek blijkt dat persoonlijke relevantie cruciaal is voor de emotionele impact van gevareninformatie (Shen & Dillard, 2007). In de huidige studie bleek het communiceren van het verhaal vanuit het perspectief van een MKB'er niet genoeg om deze persoonlijke relevantie bij alle ondernemers op te roepen. Uit de huidige studie bleek namelijk dat van de 45 ondernemers in de negatieve conditie, slechts 18 mensen het LinkedIn bericht als relevant of zeer relevant ervaarden. Dit betekent dat 27 mensen (60%) dit niet zo ervaarden. Op basis van deze informatie zou dit een verklaring kunnen zijn waarom er geen effect gevonden is van de manipulatie en zal toekomstig onderzoek moeten uitwijzen welke elementen gebruikt moeten worden om het gevaar van cybercriminaliteit persoonlijk relevanter te maken bij ondernemers.

Een verdere mogelijke verklaring voor het niet gevonden verband tussen angst en motivatie, en de mislukte manipulatie (hypothese 11, 12, 13 en 15), ligt wellicht bij de inhoud van de gebruikte fear appeal. De huidige studie is een van de eerste, dan wel niet de eerste, die het element 'angst' in de PMT gebruikt bij ondernemers op het gebied van cybercriminaliteit. De vraag is dan ook wat de meest effectieve manier is voor het gebruik van een fear appeal bij deze doelgroep. Hoewel het bericht in de negatieve conditie als significant heftiger beoordeeld werd, lag de gemiddelde angst in die conditie niet heel hoog. De mogelijkheid bestaat dat het LinkedIn bericht te laagdrempelig was als angstopwekkend element. Met andere woorden, de fear appeal was niet sterk genoeg om als manipulatie effectief te zijn.

Boss et al. (2015) beargumenteren namelijk dat wanneer de sterkte van de fear appeal in het bericht niet hoog genoeg is, dit kan leiden tot onverklaarde variantie. Dit leidt vervolgens tot het ondermijnen van PMT-voorspellingen. Zo bleek in die studie dat sommige PMT-verbanden in de lage fear appeal conditie niet significant waren, terwijl een sterke fear appeal het kernmodel van de PMT juist kon bevestigen. Een sterke fear appeal verdubbelde zelfs de invloed op intentie.

In die studie van Boss et al. (2015) gebruikten ze, net als in de huidige studie, digitale berichten met een fear appeal. Het verschil met de huidige studie is dat bij het sterke bericht een échte onverwachte situatie nagebootst werd van het krijgen van een virus, waarbij het hoogst mogelijke gevarenniveau (catastrofaal) werd aangegeven. De fear appeal liet deelnemers daadwerkelijk denken dat zij te maken hebben met een virus. De hoeveelheid angst zoals die in de praktijk ervaren wordt, is moeilijk na te bootsen in een online studie. De auteurs beargumenteren dat wanneer personen onverwacht een bericht te zien krijgen met gevareninformatie, zonder vooraf te weten wat het onderwerp is, de angst als veel groter wordt ervaren. Doordat deelnemers in de huidige studie een LinkedIn bericht kregen met informatie over cyberaanvallen in plaats van het zelf te ervaren, bestond er geen direct gevaar. Hierdoor zal de angst ook niet zo hoog zijn geweest als in de studie van Boss et al. waar angst wel een significante voorspeller was van motivatie. Bovendien bleek uit exploratieve analyses in de huidige studie dat ondernemers die aangaven eerdere ervaring te hebben met cybercriminaliteit, significant hogere motivatie en ernst rapporteerden dan ondernemers die geen ervaring hadden met cybercriminaliteit. Pas wanneer een ondernemer cybercriminaliteit écht ervaart, blijken ondernemers cybercriminaliteit als ernstiger te zien en zijn daardoor gemotiveerder om gevaren af te wenden.

In tegenstelling tot Bekker et al. (2023), heeft de huidige studie geen verschil gevonden tussen de ervaren kwetsbaarheid bij ondernemers die IT intern hebben geregeld en ondernemers die hun IT hebben uitbesteed (extern). Hypothese 10 werd dus niet bevestigd. In de huidige studie waren er 25 ondernemers die hun IT intern regelen en 41 mensen die IT uitbesteden. Ondanks het niet gevonden significante effect, blijkt wel dat ondernemers die IT hebben uitbesteed een lagere ‘mean rank’ (32.0) hadden dan ondernemers die IT intern regelen (36.0). Dit houdt in dat de IT-extern groep lager scoort op ervaren kwetsbaarheid dan de IT-intern groep. Hier zit een mogelijke indicatie dat met meer ondernemers in beide groepen het effect uit de studie van Bekker et al. (2023) gerepliceerd kan worden.

Voor de hypothese (14) dat loss framing beter werkt in het motiveren dan gain framing, zoals in de studie van Rosoff et al. (2013), is geen bevestiging gevonden. Aangezien

de loss framing onderdeel is van de niet gelukte fear appeal manipulatie, is het lastig vast te stellen wat loss framing ten opzichte van gain framing doet voor de motivatie van ondernemers. Ondernemers gaven het loss framing bericht gemiddeld een 6.2 en in de gain framing een 5.8. De gemiddelde motivatie lag heel iets hoger in de positieve conditie (3.95) dan in de negatieve conditie (3.83). Hieruit blijken dus geen opvallende verschillen. Over het algemeen blijkt loss framing beter te werken in de informatiebeveiligingsliteratuur. Zeker omdat 'losses' psychologisch impactvoller zijn dan 'gains' (Tversky & Kahneman, 1981). Hierbij is het belangrijk dat de gevareninformatie niet te algemeen is omdat het dan een averechts effect kan hebben waarbij ondernemers minder beschermingsgedrag vertonen. (Junger et al., 2017; Boss et al., 2015). Daarnaast falen loss berichten wanneer zij puur het gevaar communiceren, maar zijn ze effectief als het wordt vergezeld met een duidelijk idee wat mensen kunnen doen om het verlies af te wenden (Van Bavel et al., 2019).

Generaliseerbaarheid en limitaties

Kijkend naar de generaliseerbaarheid van de resultaten, kan het volgende gezegd worden. De ondernemers die deelnamen aan de huidige studie zijn waarschijnlijk grotendeels representatief voor alle ondernemers uit het MKB in Nederland. Wel is het de vraag of mensen van het klantenpanel en het panelbureau helemaal representatief zijn. Het kan namelijk dat ondernemers bij zo'n panel aansluiten omdat zij sowieso al gemotiveerder zijn om mee te doen aan dit soort onderzoeken. Er zijn echter geen verschillen gevonden op de PMT-variabelen tussen de verschillende kanalen. Wel bevatte het huidige onderzoek met name ondernemers uit de branche van de zakelijke dienstverlening (N = 58, 43%). De resultaten zijn dus vooral door deze branche gevormd. Het is niet duidelijk of deze resultaten van het onderzoek ook vertaalt kunnen worden naar andere branches binnen het MKB.

Aangezien motivatie het grote probleem is bij ondernemers, kan het zo zijn dat vooral ondernemers deelnamen die wél gemotiveerd waren in plaats van de groep die deze studie eigenlijk trachtte te veranderen. Dit lijkt nog waarschijnlijker door de hoge gemiddelde motivatie van de deelnemers in de huidige studie. Een limitatie van de huidige studie is dus dat een voormeting ontbreekt om dit te kunnen vaststellen. Een andere limitatie is dat niet gevraagd is naar demografische gegeven zoals leeftijd en geslacht (vanwege privacy redenen). Deze gegevens kunnen wellicht een verklaring zijn voor het resultaat. Zo vonden Rosoff et al. (2013) in een van hun studies dat vrouwen meer risicomijdend waren dan mannen. Als het huidige onderzoek ingevuld is door veel mannen, dan kan het zo zijn dat de ondernemers minder onder de indruk waren van het LinkedIn bericht dat gericht is op losses, dan wanneer

meer vrouwen hadden deelgenomen. Zo laat de studie van Milne et al. (2009) zien dat mannen een grotere neiging hebben om risicogedrag te vertonen online.

Al met al is de huidige studie een bevestiging voor het overgrote deel van het PMT-model, toegepast op de sector van informatieveiligheid. Daarbij vergroot het de kennis over een nog weinig onderzochte theorie onder ondernemers in het MKB. De manipulatiecheck in de praktijk leverde geen significante resultaten op. Zolang de motivatie laag blijft onder ondernemers, zullen er nog veel ondernemers in het MKB slachtoffer worden van cybercriminelen. Het is dus cruciaal dat toekomstig onderzoek zich richt op wat de beste manier van het communiceren van een fear appeal is, om motivatie onder ondernemers omtrent digitale veiligheidsmaatregelen te verhogen.

Referentielijst

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, 1-13. doi: https://doi.org/10.1016/j.techsoc.2023.102258

Ancker, J. S., Senathirajah, Y., Kukafka, R., & Starren, J. B. (2006). Design features of graphs in health risk communication: A systematic review. *Journal of the American Medical Informatics Association*, *13*(6), 608-618. doi: https://doi.org/10.1197/jamia.M2115

Arora, H., Steinbart, P., & Shao, B. (2006). Looking at information security through a prospect theory lens. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1715&context=amcis2006

Bekkers, L., van't Hoff-De Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security*, *127*, 1-12. https://doi.org/10.1016/j.cose.2023.103099

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly*, *39*(4), 837-864. doi: https://doi.org/10.25300/MISQ/2015/39.4.5

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209. doi: https://doi.org/10.1016/j.chb.2016.11.018

Centraal bureau voor de statistiek. (2022). *ICT-gebruik bij bedrijven*. https://longreads.cbs.nl/ict-kennis-en-economie-2022/ict-gebruik-bij-bedrijven/#:~:text=Nederlandse%20bedrijven%20hebben%20sneller%20internet,(figuur%204.1.2).

Centraal bureau voor de statistiek. (2023, Mei 11). *Online veiligheid en criminaliteit 2022*. https://www.cbs.nl/nl-nl/longread/rapportages/2023/online-veiligheid-en-criminaliteit-2022/2-internetgebruik

Conradie, M., & Doms, B. (2022). Cybersecurity onderzoek Alert Online 2022. I&O Research. Geraadpleegd op 18 februari 2024, van https://open.overheid.nl/documenten/ronl-f9dabadc3e7b330da895c60b98cf4db8ae54c95d/pdf

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101. doi: https://doi.org/10.1016/j.cose.2012.09.010

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, *41*(8), 1796-1808. doi: https://doi.org/10.1080/0144929X.2021.1905066

Eye security. (2023, Januari 12). *Eye security slaat alarm – kans op een hack is 1 op 5*. https://www.eye.security/nl/blog/eye-security-slaat-alarm-kans-op-een-hack-is-1-op-5

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407-429. doi: https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Grindle, M. (2014). The Power of Digital Storytelling to Influence Human Behaviour. https://www.storre.stir.ac.uk/bitstream/1893/21800/5/MG-PhD-Final.pdf

Heidt, M., Gerlach, J., & Buxmann, P. (2019). A holistic view on organizational IT security: The influence of contextual aspects during IT security decisions. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/93778cc4-5d44-4234-9fb8-de6ae73ad24c/content

Jamil, H., Zia, T., Nayeem, T., Whitty, M. T., & D'Alessandro, S. (2024). Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. *Information and Computer Security*, Vol. ahead-of-print. 1-28. doi: https://doi.org/10.1108/ICS-10-2023-0176

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology*, *35*(5), 368-379. doi: https://doi.org/10.1080/0144929X.2016.1160287

Junger, M., Montoya, L., and Overink, F. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, *66*, 75–87. doi: https://doi.org/10.1016/j.chb.2016.09.012

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139-150. doi: https://doi.org/10.1016/j.chb.2018.11.002

Menard, P., Bott, G.J. and Crossler, R. E. (2017), User motivations in protecting information security: Protection motivation theory versus self-determination theory, *Journal of Management Information Systems*, *34*(4), 1203-1230. doi: https://doi.org/10.1080/07421222.2017.1394083.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, *43*(3), 449-473. doi: https://doi.org/10.1111/j.1745-6606.2009.01148.x

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022) A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems*, *23*(1), 196-236. doi: https://doi.org/10.17705/1jais.00723

Nabi, R. L., Roskos-Ewoldsen, D., & Dillman Carpentier, F. (2008). Subjective knowledge and fear appeal effectiveness: Implications for message design. *Health Communication*, *23*(2), 191–201. doi: https://doi.org/10.1080/10410230701808327

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. https://ris.utwente.nl/ws/portalfiles/portal/5574462/K469____%5B1%5D.pdf

Ogbanufe, O., Crossler, R. E., & Biros, D. (2023). The valued coexistence of protection motivation and stewardship in information security behaviors. *Computers & Security*, *124*, 1-12. doi: https://doi.org/10.1016/j.cose.2022.102960

Osborn, E., & Simpson, A. (2018). Risk and the small-scale cyber security decision making dialogue—a UK case study. *The Computer Journal*, *61*(4), 472-495. doi: https://doi.org/10.1093/comjnl/bxx093

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214. doi: https://doi.org/10.1080/07421222.2015.1138374

Rabobank. (2024). *Kan je bedrijf door na een hack?* https://www.rabobank.nl/bedrijven/verzekeren/verzekeringsnieuws/bescherm-je-tegen-cyberincidenten

Rodríguez-Priego, N., Van Bavel, R., Vila, J., & Briggs, P. (2020). Framing effects on online security behavior. *Frontiers in Psychology*, *11*, 1-11. doi: https://doi.org/10.3389/fpsyg.2020.527886

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93-114. doi: https://doi.org/10.1080/00223980.1975.9915803

Rohn, E., Sabari, G., & Leshem, G. (2016). Explaining small business InfoSec posture using social theories. *Information & Computer Security*, *24*(5), 534-556. doi: https://doi.org/10.1108/ICS-09-2015-0041

Rosoff, H., Cui, J., & John, R. S. (2013). Heuristics and biases in cyber security dilemmas. *Environment Systems and Decisions*, *33*, 517-529. doi: https://doi.org/10.1007/s10669-013-9473-2

Shen, L., & Dillard, J. P. (2007). The influence of behavioral inhibition/approach systems and message framing on the processing of persuasive health messages. *Communication Research*, *34*(4), 433-467. doi: https://doi.org/10.1177/0093650207302787

Statista. (2024, April). *Number of internet and social media users worldwide as of april 2024*. https://www.statista.com/statistics/617136/digital-population-worldwide/

Townsend, C., & Kahn, B. E. (2014). The "visual preference heuristic": The influence of visual versus verbal depiction on assortment processing, perceived variety, and choice overload. *Journal of Consumer Research*, *40*(5), 993-1015. doi: https://doi.org/10.1086/673521

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. doi: https://doi.org/10.1016/j.cose.2016.02.009

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, *52*, 128-141. doi: https://doi.org/10.1016/j.cose.2015.04.006

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, *211*(4481), 453-458. doi: https://doi.org/10.1126/science.7455683

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29-39. doi: https://doi.org/10.1016/j.ijhcs.2018.11.003

Van den Berg, B., & Keymolen, E. (2017). Regulating security on the Internet: Control versus trust. *International Review of Law, Computers & Technology*, *31*(2), 188-205. doi: https://doi.org/10.1080/13600869.2017.1298504

Van der Kleij, R., & Leukfeldt, R. (2020). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. doi: https://doi.org/10.1007/978-3-030-20488-4_2

Van Grinsven, B., Ruis, L., & Riedijk, K. (2024). *Cybermaatregelen en het MKB bedrijf: Een eerste blik op drijvers & barrières*. Behavorial Insights Company. Geraadpleegd op 1 mei 2024, op te vragen bij Interpolis

Woon, I., Tan, G., & Low, R. (2005), A protection motivation theory approach to home wireless security. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1237&context=icis2005

Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security*, *16*(5), 463-483. doi: https://doi.org/10.1108/09685220810920549

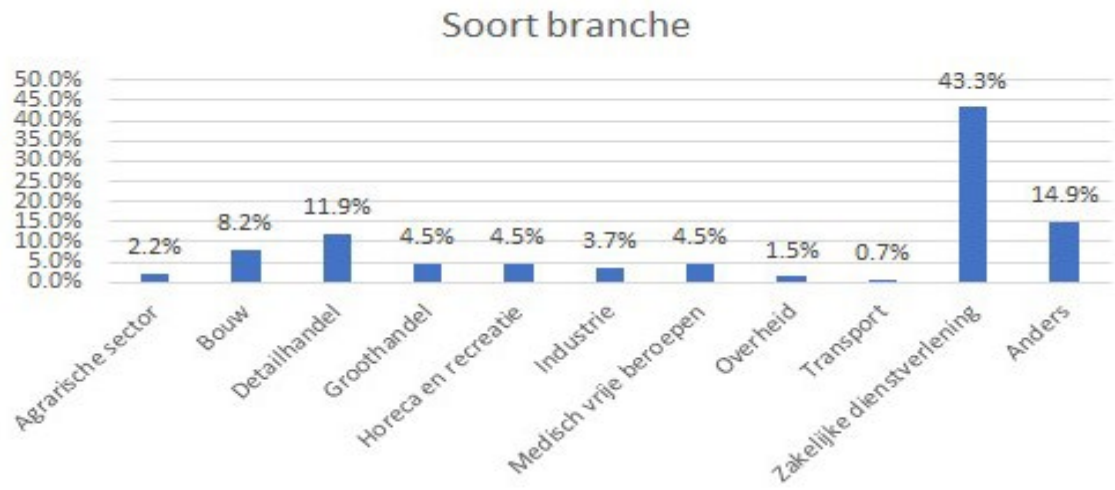
Workman, M., Bommer, W. H., & Straub, D. (2009). The amplification effects of procedural justice on a threat control model of information systems security behaviours. *Behaviour & Information Technology*, *28*(6), 563-575. doi: https://doi.org/10.1016/j.chb.2008.04.005

World Economic Forum. (2023). The Global Risks Report 2023. World Economic Forum. Geraadpleegd op 18 februari 2024, van https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

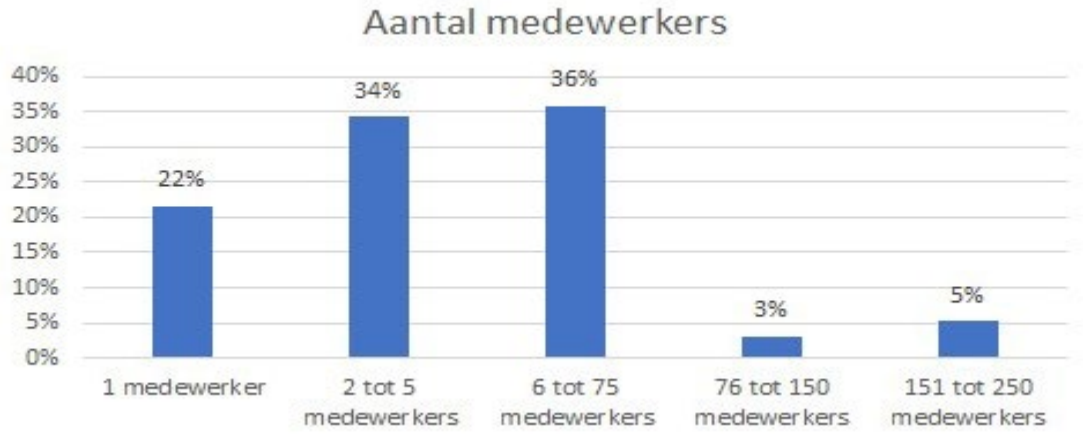
Yigit Ozkan, B., van Lingen, S., & Spruit, M. (2021). The cybersecurity focus area maturity (CYSFAM) model. *Journal of Cybersecurity and Privacy*, *1*(1), 119-139. doi: https://doi.org/10.3390/jcp1010007

BIJLAGE A (Percentages)

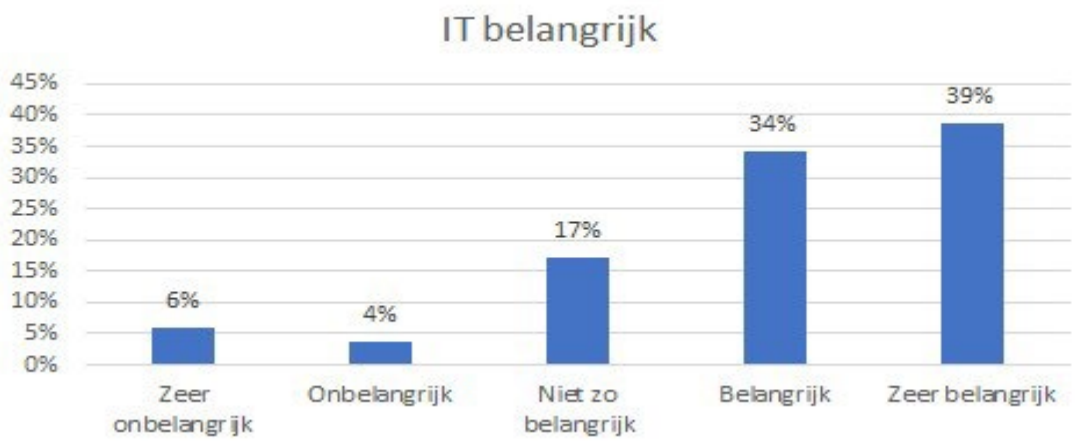
Branches van ondernemers in het onderzoek



Aantal medewerkers in het bedrijf van ondernemers in het onderzoek



Hoe belangrijk vinden de ondernemers IT



BIJLAGE B (vragenlijst)

MKB Cyberveiligheid

Beste ondernemer,

Bedankt dat je de vragenlijst invult! Ik ben Julian en dit onderzoek wordt uitgevoerd voor mijn afstudeeropdracht aan de Radboud Universiteit. De vragenlijst gaat over cyberveiligheid binnen het MKB. Jouw antwoorden zijn heel waardevol!

In deze vragenlijst krijg je een LinkedIn bericht te zien. De tekst in het LinkedIn bericht zou mogelijk als schokkend kunnen worden ervaren. Na het lezen van dit bericht, krijg je enkele vragen en stellingen over het bericht, jouw bedrijf en cyberveiligheid in het algemeen. Het invullen van de vragenlijst duurt ongeveer 5 tot 10 minuten. Jouw deelname aan dit onderzoek is geheel vrijwillig en je kunt op ieder moment stoppen zonder gevolgen. Hiervoor hoef je geen reden op te geven.

Dit onderzoek is onafhankelijk getoetst door de Ethiek Commissie Sociale Wetenschappen (ECSW) van de Radboud Universiteit en er is geen formeel bezwaar tegen dit onderzoek.

Alle gegevens worden anoniem verwerkt en zijn puur ter doeleinden voor de afstudeeropdracht. Er wordt niet naar persoonlijke gegevens gevraagd. Niks uit dit onderzoek zal dus terug te leiden zijn naar jou of jouw bedrijf. Door mee te doen aan dit onderzoek geef je toestemming dat jouw antwoorden worden opgeslagen en gebruikt. De data van het onderzoek wordt in verband met wetenschappelijke integriteit 10 jaar anoniem bewaard op beveiligde servers van de Radboud Universiteit. Alleen mijn supervisor, coördinatoren van de opleiding en ikzelf hebben toegang tot deze data.

Mocht je vragen of opmerkingen hebben over het onderzoek of de vragenlijst, dan mag je altijd contact opnemen door een e-mail te sturen naar julian.cammelbeeck@ru.nl of naar mijn supervisor ferry.vandepol@ru.nl

TOESTEMMINGSVERKLARING

voor deelname aan het wetenschappelijke onderzoek: Cyberveilig MKB

Ik bevestig dat:

- ik voldoende over het onderzoek geïnformeerd ben;
- ik de informatie goed heb gelezen;
- ik de kans heb gehad om vragen over het onderzoek te stellen;
- mijn eventuele vragen goed zijn beantwoord;
- ik goed over deelname aan het onderzoek heb kunnen nadenken;
- ik uit vrije wil mee doe aan het onderzoek.

Ik begrijp dat:

- ik het recht heb om op elk moment te stoppen zonder dat ik daarvoor een reden hoef te geven en zonder dat dit negatieve gevolgen voor mij heeft.

Ik stem in dat:
- mijn onderzoeksgegevens binnen dit onderzoek worden verzameld en gedurende 10 jaar opgeslagen worden voor controle, hergebruik en replicatie.

Toestemming Ik ga akkoord met bovenstaande informatie en bevestig mijn deelname aan het onderzoek.

- ○ Ja, ga verder met de vragenlijst
- ○ Nee, einde vragenlijst

Bedrijfsinrichting Je krijgt nu enkele vragen over jouw bedrijf. Selecteer het antwoord dat voor jouw bedrijf van toepassing is.

Medewerkers Hoeveel medewerkers heeft jouw bedrijf? (Tel jezelf als eigenaar niet mee).

- ○ Geen medewerkers of ik heb geen bedrijf (einde vragenlijst)
- ○ 1 medewerker
- ○ 2 tot 5 medewerkers
- ○ 6 tot 75 medewerkers
- ○ 76 tot 150 medewerkers
- ○ 151 tot 250 medewerkers

Branche Tot welke branche behoort jouw bedrijf?

- ○ Agrarische sector
- ○ Bouw
- ○ Detailhandel
- ○ Groothandel
- ○ Horeca en recreatie
- ○ Industrie
- ○ Medisch vrije beroepen
- ○ Overheid
- ○ Transport
- ○ Visserij
- ○ Zakelijke dienstverlening
- ○ Anders, namelijk: _____

Verantwoordelijk Wie is verantwoordelijk voor de IT (informatietechnologie) van jouw bedrijf? Denk bijvoorbeeld aan software, cloudservices en beveiliging.

- ○ Interne IT-medewerker(s)
- ○ Externe IT-dienstverlener(s)
- ○ Ikzelf
- ○ Niemand specifiek
- ○ Anders, namelijk: _____

Belangrijk Hoe belangrijk is IT voor jouw bedrijfsvoering?

- ○ Zeer onbelangrijk
- ○ Onbelangrijk
- ○ Niet zo belangrijk
- ○ Belangrijk
- ○ Zeer belangrijk

Ervaring Welk van onderstaande gebeurtenissen heb jij wel eens meegemaakt **bij jouw bedrijf?** Je kunt meerdere antwoorden selecteren.

- ☐ Een virus (E-mail of bericht met een bijlage dat een virus bevatte)
- ☐ Phishing (Via E-mail of telefoon deed iemand zich voor als een betrouwbare organisatie en vroeg om bijvoorbeeld persoonlijke gegevens)
- ☐ Hacking (Iemand is zonder toestemming een apparaat binnengekomen en heeft gegevens gestolen, veranderd of beschadigd)
- ☐ Ransomware (Gegevens en/of computer werden geblokkeerd en er werd geld gevraagd om deze weer terug te krijgen)
- ☐ Identiteitsfraude (Iemand heeft persoonlijke informatie gestolen en zich als jou of iemand van het bedrijf voorgedaan)
- ☐ Pinpasfraude (Iemand heeft om bankgegevens gevraagd om hiermee geld van de bedrijfsrekening te halen)
- ☐ Anders, namelijk: _____
- ☐ ⊗Ik heb geen van deze gebeurtenissen meegemaakt

Controle Hieronder zie je een LinkedIn bericht. Het bedrijf is verzonnen. De rest is op waarheid gebaseerd. Lees de tekst goed door en bekijk de afbeelding. Hierna worden enkele vragen over het LinkedIn bericht gesteld.

Positief Hieronder zie je een LinkedIn bericht. Het bedrijf en de persoon zijn verzonnen. De rest is op waarheid gebaseerd. Lees de tekst goed door en bekijk de afbeelding. Hierna worden enkele vragen over het LinkedIn bericht gesteld.

Negatief Hieronder zie je een LinkedIn bericht. Het bedrijf en de persoon zijn verzonnen. De rest is op waarheid gebaseerd. Lees de tekst goed door en bekijk de afbeelding. Hierna worden enkele vragen over het LinkedIn bericht gesteld.

Rapportcijfer Welk rapportcijfer tussen 1 (Slecht) en 10 (Goed) geef jij het LinkedIn bericht?

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ 7
- ○ 8
- ○ 9
- ○ 10

Redencijfer Waarom geef je dit cijfer?

_____

Meningpost Je krijgt nu enkele vragen over het LinkedIn bericht. Selecteer het antwoord dat het beste jouw mening weergeeft.

	Sterk mee oneens	Oneens	Neutraal	Eens	Sterk mee eens
Ik snap het doel van het LinkedIn bericht	○	○	○	○	○
De tekst van het LinkedIn bericht is duidelijk	○	○	○	○	○
Ik vind het LinkedIn bericht relevant	○	○	○	○	○
De afbeelding in het LinkedIn bericht is duidelijk	○	○	○	○	○
Ik vind het LinkedIn bericht aantrekkelijk	○	○	○	○	○
Ik vind het LinkedIn bericht heftig	○	○	○	○	○
Ik vind het LinkedIn bericht realistisch	○	○	○	○	○

Variabelen_1 Hieronder staan enkele uitspraken. Selecteer bij iedere uitspraak het antwoord dat het beste jouw gedachte of gevoel weergeeft.

	Sterk mee oneens	Oneens	Neutraal	Eens	Sterk mee eens
Als ik denk aan de bedreigingen van cybercriminaliteit voor mijn bedrijf, dan voel ik mij angstig	○	○	○	○	○
Als mijn bedrijf slachtoffer zou worden van cybercriminaliteit, dan zal het leiden tot hoge kosten	○	○	○	○	○
Ik heb de motivatie om mijn bedrijf te beschermen tegen cybercriminaliteit	○	○	○	○	○
Mijn bedrijf loopt risico op bedreigingen van cybercriminaliteit	○	○	○	○	○

Variabelen_2 Hieronder staan enkele uitspraken. Selecteer bij iedere uitspraak het antwoord dat het beste jouw gedachte of gevoel weergeeft.

	Sterk mee oneens	Oneens	Neutraal	Eens	Sterk mee eens
De kans dat mijn bedrijf slachtoffer wordt van cybercriminaliteit is klein	○	○	○	○	○
Ik ben bezorgd over de mogelijkheid van cybercriminaliteit bij mijn bedrijf	○	○	○	○	○
Ik heb de motivatie om moeite te doen om mijn bedrijf te beschermen tegen cybercriminaliteit	○	○	○	○	○
De gevaren van cybercriminaliteit voor mijn bedrijf zijn ernstig	○	○	○	○	○

Variabelen_3 Hieronder staan enkele uitspraken. Selecteer bij iedere uitspraak het antwoord dat het beste jouw gedachte of gevoel weergeeft.

	Sterk mee oneens	Oneens	Neutraal	Eens	Sterk mee eens
De dreiging van cybercriminaliteit voor mijn bedrijf maakt mij nerveus	○	○	○	○	○
Mijn bedrijfsinformatie is kwetsbaar voor cybercriminaliteit	○	○	○	○	○
Het is onwaarschijnlijk dat ik (meer) veiligheidsmaatregelen ga nemen tegen cybercriminaliteit	○	○	○	○	○
Ik geloof dat cybercriminaliteit iets serieus is	○	○	○	○	○

Handelingen Hieronder staan de laatste stellingen van de vragenlijst. Selecteer bij iedere uitspraak het antwoord dat het beste jouw gedachte weergeeft. De schaal loopt op in mate van zekerheid vanaf 1 (zeker niet) tot 5 (zeker wel).

	1 (Zeker niet)	2	3	4	5 (Zeker wel)
Ik heb de intentie om (meer) informatie op te zoeken over veiligheidsmaatregelen tegen cybercriminaliteit	○	○	○	○	○
Ik heb de intentie om binnen mijn bedrijf te onderzoeken wat de zwakke plekken zijn op het gebied van cyberveiligheid	○	○	○	○	○
Ik heb interesse in een product dat mij kan helpen bij het beveiligen van mijn bedrijf	○	○	○	○	○
Ik heb de intentie om een adviesgesprek aan te vragen over cyberveiligheid	○	○	○	○	○

Meerinfo Tot slot hebben we wat meer informatie over cybercriminaliteit en mogelijke veiligheidsmaatregelen. Wil je deze informatie lezen?

○ Ja

○ Nee

Wat is cybercriminaliteit?

Cybercriminaliteit is een criminele activiteit die gericht is op een netwerk of een computer. Het doel van cybercriminelen is meestal geld verdienen. Daarnaast zijn er ook andere redenen, zoals het ontregelen van een bedrijf of vanuit een persoonlijk motief. Er zijn vele typen cybercriminaliteit. Voor het bedrijfsleven zijn dit vooral ransomware, e-mailfraude (phishing) en de diefstal en verkoop van bedrijfsgegevens. Criminelen kunnen computers met malware infecteren om ze te ontregelen of om gegevens te verwijderen en stelen.

Wat kan jij doen?
Er zijn gelukkig genoeg handelingen die jij kunt doen om als bedrijf goed beveiligd te zijn. We geven je hieronder graag enkele tips!

1. Gebruik sterke wachtwoorden. Gebruik niet dezelfde wachtwoorden en zorg dat een wachtwoord genoeg verschillende tekens bevat met speciale karakters. Gebruik een wachtwoordmanager om je wachtwoorden op te slaan en te beheren.
2. Open nooit links in spam-mails. Controleer het adres van de afzender, kijk goed naar de domeinnaam (alles achter het @-teken), controleer of het e-mailadres overeenkomt met het websiteadres en wees je ervan bewust dat een nep e-mailadres op maar één lettertje kan schelen van het echte e-mailadres.
3. Zorg voor antivirussoftware en houdt deze up-to-date. Hierdoor heb jij altijd de beste beveiliging voor jouw bedrijf.
4. Update altijd je software en besturingssysteem.
5. Maak meerdere back-ups. Zo kan je altijd bij je bedrijfsgegevens en hoef je niet te vrezen voor een verlies van gegevens.

Naast deze maatregelen zijn er nog meer effectieve maatregelen. Op internet zijn veel tips en adviezen te vinden om jouw bedrijf goed te beveiligen.

Dit was de extra informatie. Je kunt nu door met het einde van de vragenlijst.

Opmerkingen
Heb je nog opmerkingen of tips over de huidige vragenlijst? Die kun je hieronder achterlaten.

Deze tekst bevat informatie over het onderzoek. Ga hierna naar de volgende pagina om de vragenlijst af te ronden.

In dit onderzoek werd gedrag rondom cyberveiligheid onderzocht. Deelnemers kregen één van de drie LinkedIn berichten te zien. We bekeken welk bericht het meest motiverend is om in actie te komen tegen cybercriminaliteit. We zijn hierbij benieuwd of ondernemers vaker informatie over cyberveiligheid willen lezen en vaker cyberveiligheidshandelingen willen doen, nadat zij een van deze LinkedIn berichten lazen.

Er zijn drie verschillende versies van het LinkedIn bericht getoetst.
Versie 1 is een standaard bericht met informatie over cyberveiligheid. Versie 2 bevat een persoonlijk verhaal over wat er te winnen valt met goede cyberveiligheid. Versie 3 bevat een persoonlijk verhaal over wat er te verliezen valt zonder goede cyberveiligheid. In alle drie de LinkedIn berichten is het bedrijf verzonnen en in versie 2 en 3 is de persoon ook verzonnen. Maar het verhaal was iedere keer op waarheid gebaseerd. Deze gebeurtenissen komen in de realiteit voor.

Maak jij je naar aanleiding van dit onderzoek zorgen over de cyberveiligheid van je bedrijf?
Er zijn genoeg handelingen die jij kunt doen om jezelf en je bedrijf te beveiligen. Voor meer informatie over cyberveiligheid kun je onder andere deze website van het Ondernemersplein van de overheid bekijken: https://ondernemersplein.kvk.nl/bescherm-uw-bedrijf-tegen-cybercrime/ Hierin staat hoe je cybercriminaliteit kunt herkennen en wat je kunt doen om het te voorkomen. Er zijn daarnaast op internet veel tips en adviezen te vinden.

Heb je daarnaast nog vragen of opmerkingen over dit onderzoek? Dan kun je een e-mail sturen naar: julian.cammelbeeck@ru.nl of naar mijn supervisor: ferry.vandepol@ru.nl

BIJLAGE C (Posts) – Controleconditie

BIJLAGE C (Posts) – Negatieve/loss conditie

BIJLAGE C (Posts) – Positieve/gain conditie