UHASSELT

KNOWLEDGE IN ACTION

Faculteit Bedrijfseconomische Wetenschappen

master in de toegepaste economische wetenschappen

Masterthesis

Het succesvol implementeren van CS raamwerken

Tanja Lindekens

Scriptie ingediend tot het behalen van de graad van master in de toegepaste economische wetenschappen, afstudeerrichting accountancy en financiering

PROMOTOR :
Prof. dr. Tensie STEIJVERS

COPROMOTOR :
Prof. dr. Maarten CORTEN

2020
2021

UHASSELT
KNOWLEDGE IN ACTION

www.uhasselt.be
Universiteit Hasselt
Campus Hasselt:
Martelarenlaan 42 | 3500 Hasselt
Campus Diepenbeek:
Agoralaan Gebouw D | 3590 Diepenbeek

UHASSELT

KNOWLEDGE IN ACTION

Faculteit Bedrijfseconomische Wetenschappen

master in de toegepaste economische wetenschappen

Masterthesis

Het succesvol implementeren van CS raamwerken

Tanja Lindekens

Scriptie ingediend tot het behalen van de graad van master in de toegepaste economische wetenschappen, afstudeerrichting accountancy en financiering

PROMOTOR :
Prof. dr. Tensie STEIJVERS

COPROMOTOR :
Prof. dr. Maarten CORTEN

Deze masterproef werd geschreven tijdens de COVID-19 crisis in 2020-2021. Deze wereldwijde gezondheidscrisis heeft mogelijk een impact gehad op het schrijf- en verwerkingsproces, de onderzoekshandelingen en de onderzoeksresultaten die aan de basis liggen van dit werkstuk.

Woord vooraf

Deze eindverhandeling is gericht tot het behalen van de graad van Master in de Toegepaste Economische Wetenschappen: *Accountancy and Finance* aan de Universiteit Hasselt. In het kader van dit onderzoek kreeg ik de kans om de succesvolle implementatie van *cybersecurity* raamwerken te onderzoeken, alsook de factoren die daarbij een rol spelen. Zo kreeg ik meer inzicht in het onderwerp *cybersecurity* en de manier waarop ondernemingen deze risico's aanpakken. Ik wil hiermee ook het belang van *cybersecurity* aankaarten aangezien dit steeds belangrijker wordt voor ondernemingen.

Daarnaast zou ik graag een aantal mensen willen bedanken die mij hebben ondersteund gedurende dit proces. Allereerst wil ik graag mijn promotor Prof. Dr. Tensie Steijvers en copromotor Prof. dr. Maarten Corten bedanken voor hun goede begeleiding, hulp en feedback bij het schrijven van deze studie. Vervolgens wil ik ook de veertien respondenten bedanken die hebben meegewerkt aan het onderzoek. Tot slot wil ik mijn familie en vrienden bedanken voor hun steun en motivatie die ze mij hebben gegeven gedurende mijn opleiding aan de Universiteit Hasselt.

Samenvatting

De opkomst van nieuwe technologie en software hebben het landschap waarin ondernemingen vandaag de dag opereren compleet veranderd. Nieuwe technologische ontwikkelingen hebben niet alleen de manier van werken beïnvloed, maar hebben ook nieuwe opportuniteiten en risico's voor ondernemingen gecreëerd. In onze huidige economie is het belangrijk dat ondernemingen flexibel zijn: ze moeten kunnen inspelen op een veranderende omgeving. Daarom is het cruciaal dat ondernemingen inzetten op *information technology* (IT). Technologische vooruitgang is immers de drijfkracht geworden voor economische groei. Onderzoekers zijn het er ook over eens dat de grootste risico's waar ondernemingen tegenwoordig mee in contact komen, behoren tot de cyberrisico's. Zowel private als publieke ondernemingen worden regelmatig geconfronteerd met geavanceerde cyberdreigingen en -aanvallen. Het is belangrijk dat ondernemingen leren omgaan met deze cyberrisico's.

Cybersecurity raamwerken kunnen ondernemingen ondersteunen in dit proces. In de literatuur worden enkele voorbeelden aangehaald: COSO ERM, COBIT, NIST CSF en de ISO standaarden. Onderzoekers benadrukken in hun studies het belang van deze raamwerken. Raamwerken helpen ondernemingen immers om hun risico's efficiënt en effectief te beheersen en de impact ervan te verkleinen. Hoewel de inhoud van deze raamwerken in de literatuur uitgebreid is beschreven, valt het op dat er weinig onderzoeken zijn die zich hebben toegelegd op het bestuderen van de eigenlijke implementatie van deze raamwerken. Er is met andere woorden nog niet onderzocht hoe deze raamwerken succesvol geïmplementeerd moeten worden. Daarbij lijken deze raamwerken te focussen op grote ondernemingen met volwaardige IT-departementen terwijl cyberrisico's ook groter worden voor KMO's. Het is daarom ook belangrijk om te weten hoe KMO's deze raamwerken kunnen implementeren. Om deze leegte in de bestaande literatuur op te vullen, zal er in deze masterproef een kwalitatieve studie worden uitgevoerd waarmee de volgende onderzoeksvraag wordt beantwoord: '*Hoe implementeren ondernemingen cybersecurity raamwerken op een succesvolle manier en welke factoren spelen hierbij een rol?*'

In dit onderzoek werd er eerst een grondige literatuurstudie uitgevoerd om meer kennis te verwerven over dit onderwerp. Vervolgens werden er veertien kwalitatieve semigestructureerde interviews afgenomen verspreid over negen verschillende ondernemingen. Dit waren experts op vlak van IT, *cybersecurity*, *policy* en audit binnen verschillende sectoren. Het ging om personen met minstens 10 jaar ervaring in hun vakgebied. De data die hierbij naar voren kwam, werd aan de hand van de *grounded theory* methodiek geanalyseerd. Uiteindelijk leverde deze methode zes thema's op die helpen bij het vormen van een antwoord op de onderzoeksvraag.

Hoewel de resultaten grotendeels overeenstemmen met de literatuur, zijn er toch enkele nieuwe bevindingen die uit dit onderzoek naar voren zijn gekomen. Deze nieuwe bevindingen vullen de leegte in de huidige literatuur aan en bieden een houvast voor ondernemingen die zich willen beschermen tegen cyberrisico's. Een eerste bevinding is dat raamwerken vaak een brug te ver zijn voor ondernemingen. In dit onderzoek wordt namelijk aangetoond dat er een zekere maturiteit nodig is vooraleer een onderneming een raamwerk kan toepassen. Maturiteit houdt in dat een onderneming begrijpt wat de raamwerken en de gevaren omtrent *cybersecurity* zijn en dat een onderneming ook een management heeft dat dit allemaal begrijpt. Deze maturiteit gaat gepaard met bewustwording

van het management en de werknemers omtrent cyberrisico's. Ondernemingen waarbij deze maturiteit ontbreekt, zullen niet aan *cybersecurity* raamwerken uit kunnen en het nut er niet van inzien.

Een tweede bevinding betreft de aspecten die belangrijk zijn vooraleer een raamwerk wordt geïmplementeerd. Het is belangrijk dat er enkele basisstappen worden doorlopen vooraleer we bij raamwerken uitkomen. Een eerste stap is de inventarisatie van hardware en software. Ondernemingen moeten namelijk eerst weten wat ze in huis hebben om te weten wat ze moeten beveiligen. Deze eerste stap gaat gepaard met het creëren van *awareness* in een onderneming. Zowel het management als de werknemers moeten goed begrijpen wat de cyberrisico's zijn. Je kan immers niet gaan beveiligen in een onderneming die zich niet bewust is van de risico's. Vervolgens moeten ondernemingen risico's leren identificeren en proactief beveiligen. Dit slaat bijvoorbeeld ook op het trainen van je werknemers, een klassieke antivirus installeren, een goede firewall hebben, regelmatige back-ups doen… Daarnaast moet een onderneming een plan hebben om te reageren op een aanval en tot slot moet er dan ook een herstelplan opgesteld worden.

Eens dat een onderneming een bepaalde maturiteit heeft bereikt en de basisstappen heeft doorlopen, kan ze raamwerken gaan implementeren. Hierbij zijn er verschillende factoren die bepalen dat de implementatie van raamwerken succesvol gebeurt. *People* is de belangrijkste factor. Het management en de werknemers moeten immers bewust gemaakt worden van de cyberrisico's. Ze moeten de gevaren begrijpen en het nut inzien van bepaalde standaarden en raamwerken. Daarnaast heb je de juiste mensen nodig op de juiste plaats. Ondernemingen hebben bijvoorbeeld een IT-manager of iemand van het management nodig die een visie heeft en alles kan overbrengen. Het is belangrijk om iemand intern te hebben die de nodige elementen kan halen uit de raamwerken. Een raamwerk moet immers niet volledig tot op de letter gevolgd worden, een onderneming moet daar de nodige elementen uithalen. Tot slot is het belangrijk dat er na de implementatie regelmatige training van werknemers, risicoanalyses en simulaties van aanvallen worden gedaan. Een onderneming moet blijven werken aan haar beveiliging, dit is een continu proces.

Een laatste bevinding is de oplossing voor KMO's. KMO's hebben vaak het geld en de middelen niet om raamwerken te implementeren. Daarnaast benadrukken respondenten dat KMO's nog niet matuur genoeg zijn. De bestaande raamwerken zijn te zwaar voor zo een kleine onderneming. In dit onderzoek wordt er daarom een aanzet gegeven om een raamwerk te ontwikkelen dat zich toelegt op KMO's en haar cyberrisico's. Hierbij wordt een onderscheid gemaakt tussen KMO's die IT gaan *outsourcen* en KMO's die IT in huis uitvoeren. Voor KMO's die IT volledig gaan *outsourcen* is het belangrijk om met de juiste partners samen te werken. Omdat in onze huidige economie veel ondernemingen beweren dat ze een expert zijn, is dit niet altijd evident. Daarnaast moeten deze KMO's ook *awareness* creëren in hun onderneming. Het is namelijk niet zo dat als een onderneming haar IT gaat *outsourcen*, ze totaal niet meer bezig moet zijn met haar cyberrisico's. KMO's die hun IT in huis doen daarentegen, moeten focussen op andere zaken. Zo moeten zij enkele basisstappen doorlopen. De eerste stap is inventarisatie van hardware en software waarbij er ook moet worden nagegaan of deze nog up-to-date zijn. Respondenten geven immers aan dat oude besturingssystemen kwetsbaar zijn. Gepaard met deze stap gaat ook het creëren van *awareness* en maturiteit. Vervolgens is standaardisatie belangrijk voor KMO's. Wanneer er bijvoorbeeld

verschillende antivirussen gebruikt worden in een onderneming, kan een IT dienst dat immers heel moeilijk beheren. Het is beter om één antivirus te installeren op alle computers. Tot slot is uit de resultaten gebleken dat KMO's die hun IT in huis doen, in de toekomst best hun informatie in de Cloud zetten aangezien deze providers al erg matuur zijn.

Om af te sluiten zijn er nog enkele beperkingen en suggesties voor verder onderzoek. Een eerste suggestie voor verder onderzoek is een kwantitatieve studie die deze theorie kan testen. Het doel van kwalitatief onderzoek is immers het ontwikkelen van een theorie, maar om theorie te veralgemenen dient dit getoetst te worden in een grotere steekproef. Vervolgens beperkt dit onderzoek zich tot België. Internationaal onderzoek zou interessant kunnen zijn om de bestaande raamwerken in verschillende omgevingen en culturen te bestuderen. Afhankelijk van de eigenheid van een onderneming, zijn bepaalde elementen van een raamwerk nuttig en anderen niet. Als we dit op internationale schaal kunnen bekijken kan er meer duidelijkheid geschept worden. Een tweede beperking is dat de steekproef van negen ondernemingen geen IT provider bevatte. Veel kleine KMO's gaan hun IT namelijk *outsourcen* aan een externe IT provider. Hoewel deze beperking deels werd opgevangen door cases te zoeken die zelf in aanraking komen met KMO's en hun IT infrastructuur, mist deze invalshoek in de resultaten. Verder onderzoek dat zich focust op KMO's moet hier zeker rekening mee houden. Tot slot heeft deze studie de aanzet gegeven voor de ontwikkeling van een raamwerk dat zich toelegt op KMO's en haar cyberrisico's. Dit vormt een enorme meerwaarde voor KMO's die niet weten hoe ze *cybersecurity* moeten aanpakken. Het zou interessant zijn voor toekomstige onderzoekers om dit raamwerk verder uit te bouwen zodat ook KMO's een kader hebben dat hen kan ondersteunen in het cyberrisicobeheersingsproces.

Inhoudsopgave

Inleiding

De opkomst van nieuwe technologie en software hebben het landschap waarin ondernemingen vandaag de dag opereren compleet veranderd. Nieuwe technologische ontwikkelingen hebben niet alleen een impact op de manier van werken, maar creëren ook opportuniteiten voor ondernemingen. In onze huidige economie is het belangrijk dat ondernemingen flexibel zijn: ze moeten kunnen inspelen op een veranderende omgeving en tegelijkertijd de reactie van de concurrentie anticiperen. Daarom is het cruciaal dat ondernemingen inzetten op *information technology* (IT) en hun technologie blijven vernieuwen. Technologische vooruitgang is immers de drijfkracht geworden voor economische groei (Ivanova, Holionko, Tverdushka, Olejarz, & Yakymchuk, 2019; Lanz, 2014).

Nieuwe technologieën gaan echter ook gepaard met nieuwe risico's. *Certified Public Accountants* (CPAs) onderzoeken al jaren de informatie- en computerveiligheidsrisico's waarmee ondernemingen van alle groottes geconfronteerd worden (Lanz, 2014). De grootste risico's waar ondernemingen tegenwoordig mee in contact komen, behoren tot de cyberrisico's. Zowel private als publieke ondernemingen hebben de afgelopen jaren te maken gekregen met geavanceerde cyberdreigingen en -aanvallen (Islam, Farah, & Stafford, 2018; Sabillon, Serra-Ruiz, Cavaller, & Cano, 2017). Bovendien bleek uit het jaarlijkse *risk in focus* onderzoek van de ECIIA (European Confederation of Institutes of Internal Auditing) dat cyber- en datasecurity, net zoals in 2019, ook in 2020 het belangrijkste risico voor ondernemingen vormt. 78% van de deelnemende *chief audit excecutives* (CAEs) gaf aan dat *cybersecurity* één van de top vijf risico's is waaraan hun onderneming wordt blootgesteld, waarvan 21% dit zelfs markeerde als het toprisico. Bekende voorbeelden van deze cyberrisico's zijn de ontdekking van de kwetsbaarheden *Spectre* en *Meltdown* die vrijwel alle computerchips beïnvloeden of de datalekken in verband met de privacy schandalen van Facebook (ECIAA, 2019).

Er bestaan verschillende soorten cyberaanvallen waarmee een onderneming geconfronteerd kan worden. Enerzijds zijn er de passieve aanvallen. Deze betreffen het exploiteren van communicatiekanalen om zo tot vertrouwelijke informatie, zoals ID's en wachtwoorden, te komen of het analyseren van dataverkeerspatronen om zo zwaktes in het systeem te achterhalen. Anderzijds zijn er de actieve aanvallen. Bij zo een aanval kan er gebruik gemaakt worden van de verworven informatie bij een passieve aanval. Bij een actieve aanval heeft de aanvaller invloed op de operaties van het bedrijf. Hierbij kunnen de netwerkdiensten bijvoorbeeld worden aangetast of kan de vertrouwelijkheid en/of integriteit van de data in een netwerk in het gedrang gebracht worden (Cayirci & Ghergherehchi, 2011).

Op deze manier kan er een datalek ontstaan. Dit kan schadelijke gevolgen hebben voor de onderneming zelf en brengt hoge kosten met zich mee. Een zwakke *cybersecurity* kan immers de hele organisatie treffen en daarmee de klantenrelaties, de reputatie en de winstgevendheid van een onderneming schaden (Lanz, 2014). Men verwacht dat het aantal datalekken ten gevolge van cyberaanvallen en -dreigingen alleen nog maar verder zal toenemen (Islam et al., 2018). Islam et al. (2018) benadrukken daarom in hun onderzoek het belang van het *cybersecurity risk management*, *information security management* en de interne audit.

Omdat technologie zo verweven zit in onze economie is *cybersecurity* niet meer weg te denken binnen ondernemingen (Lanz, 2014). Deze technologische verwevenheid is vandaag nog groter ten gevolge van de wereldwijde COVID-19 crisis. Fysiek samenkomen is immers niet meer de norm en ondernemingen steunen nu meer dan ooit op technologie. Het is daarom in het belang van alle individuen en ondernemingen om *cybersecurity* centraal te stellen (Cayirci & Ghergherehchi, 2011).

Er bestaan verschillende raamwerken die zich focussen op dit cybersecurityverhaal en ondernemingen ondersteunen in de beveiliging van hun processen en gevoelige informatie. Enkele voorbeelden van deze *cybersecurity* raamwerken zijn: COSO ERM, COBIT, NIST CSF en de ISO standaarden. Hoewel de inhoud van deze raamwerken in de literatuur uitgebreid is beschreven, valt het op dat er weinig onderzoeken zijn die zich hebben toegelegd op het bestuderen van de eigenlijke implementatie van deze raamwerken. Er is met andere woorden nog niet onderzocht hoe deze raamwerken succesvol geïmplementeerd moeten worden. Daarbij lijken deze raamwerken te focussen op grote ondernemingen met volwaardige IT-departementen terwijl cyberrisico's ook groter worden voor KMO's. Het is daarom ook belangrijk om te weten hoe KMO's deze raamwerken kunnen implementeren. Aangezien het belang van *cybersecurity* de laatste jaren enorm is toegenomen, is het relevant om hier dieper op in te gaan. In deze studie zullen we onderzoek doen naar de factoren die meespelen bij de succesvolle implementatie van *cybersecurity* raamwerken. Meer specifiek, hoe pakken ondernemingen de implementatie van raamwerken aan en wat zorgt voor een goede implementatie? Met deze studie kunnen we ondernemingen bijstaan in hun strijd tegen cyberbedreigingen en de leegte in de huidige literatuur opvullen. Op basis een grondige literatuurstudie en gesprekken met experts uit de audit (zowel interne audit als externe audit), *policy*, IT en *cybersecurity* zullen we een antwoord trachten te bieden op de vraag: '*Hoe implementeren ondernemingen cybersecurity raamwerken op een succesvolle manier en welke factoren spelen hierbij een rol?'*

Alvorens deze onderzoeksvraag te beantwoorden, wordt er in het volgend onderdeel een overzicht gegeven van de huidige literatuur omtrent dit onderwerp en worden het onderwerp *cybersecurity* en de bestaande raamwerken verder toegelicht. Vervolgens wordt de gehanteerde onderzoeksmethode geduid, gevolgd door de bevindingen van deze kwalitatieve studie. Tot slot wordt een conclusie gevormd waarin de onderzoeksvraag wordt beantwoord en de terugkoppeling naar de literatuur wordt gemaakt. Daarbij worden de beperkingen van het onderzoek besproken in combinatie met enkele aanbevelingen voor verder onderzoek en implicaties voor de praktijk.

Literatuurstudie

1. Cyberbedreigingen

1.1 Inleiding

Technologie is de bedrijfswereld en de manier waarop we handelen volledig aan het veranderen. Met de continue nieuwe ontwikkelingen binnen IT verwacht men dat deze transformatie de komende jaren zal blijven aanhouden. Aangezien organisaties aanzienlijk meer informatie delen met externe partijen via e-mail of informatiesystemen, worden organisaties meer en meer geconfronteerd met een hogere complexiteit, volatiliteit en afhankelijkheid van die informatiesystemen. Volledige controle ligt niet meer bij de organisatie. Om de veiligheid van informatie te garanderen zijn er daarom controles en vertrouwensbanden opgezet tussen ondernemingen en hun externe partijen (Galligan, Herrygers, & Rau, 2019).

Toch kunnen er zich problemen voordoen, zoals bijvoorbeeld een datalek. Wanneer dit gebeurt, is de onderneming verantwoordelijk en de gevolgen ervan kunnen zeer schadelijk zijn voor de reputatie van een onderneming. *Cyber security breaches* zijn echter geen nieuw fenomeen. Ze bestaan al sinds het ontstaan van informatiesystemen en zullen in de toekomst ook blijven gebeuren omdat aanvallers inspelen op de zwakheden van die informatiesystemen. Het is een risico waarmee ondernemingen van alle groottes geconfronteerd worden. Daarom is het belangrijk dat ondernemingen cyberrisico's efficiënt en effectief leren beheersen (Furnell, Heyburn, Whitehead, & Shah, 2020 ;Galligan et al., 2019).

Het is met andere woorden duidelijk dat de grootste risico's waar ondernemingen tegenwoordig mee in contact komen, behoren tot de cyberrisico's. Zowel private als publieke ondernemingen hebben de afgelopen jaren te maken gekregen met geavanceerde cyberdreigingen en -aanvallen (Islam et al., 2018; Sabillon et al., 2017). Dit betreft ondernemingen van alle groottes. Bovendien stelden Bissell, Lasalle en Dal Chin (2019) in hun onderzoek dat er in het afgelopen jaar een aanzienlijke toename van economische spionage, zoals de diefstal van intellectueel eigendom was.

1.2 Cybercriminaliteit

Eén van de grootste cyberrisico's is het lekken van data. Jackson, Vanteeva en Fearon (2019) definiëren een datalek als een beveiligingsincident waarbij vertrouwelijke, beveiligde of gevoelige informatie wordt gekopieerd, geobserveerd, gestolen, overgedragen of gebruikt door een onbevoegd persoon. Er zijn verschillende incidenten die een datalek kunnen veroorzaken. We moeten hierbij opletten we dat we termen zoals '*cybercrime*', 'cyberaanval' en 'datalek' niet door elkaar gebruiken. Hoewel deze termen aan elkaar gelinkt kunnen worden, betekenen ze niet hetzelfde. *Cybercrime* betreft het illegaal gebruik van technologie (Chandra & Snowe 2020; Furnell et al., 2020). Een cyberaanval is dus een voorbeeld van een *cybercrime.* Een cyberaanval slaat op een gerichte actie om informatie te bekomen van een andere partij. Deze leidt enkel tot een datalek indien de aanval succesvol is (Furnell et al., 2020).

Er bestaan verschillende soorten cyberaanvallen waarmee een onderneming geconfronteerd kan worden. Enerzijds zijn er de passieve aanvallen. Deze betreffen het exploiteren van communicatiekanalen om zo tot vertrouwelijke informatie, zoals ID's en wachtwoorden, te komen of het analyseren van dataverkeerspatronen om zo zwaktes in het systeem te achterhalen. Anderzijds

zijn er de actieve aanvallen. Bij zo een aanval kan er gebruik gemaakt worden van de verworven informatie uit een passieve aanval. Bij een actieve aanval heeft de aanvaller invloed op de operaties van het bedrijf. Hierbij kunnen de netwerkdiensten bijvoorbeeld worden aangetast of kan de vertrouwelijkheid en/of integriteit van de data in een netwerk in het gedrang gebracht worden (Cayirci & Ghergherehchi, 2011).

Cybercriminelen blijven hun aanvalstechnieken aanpassen en hanteren verschillende middelen en methoden om in hun opzet te slagen. Zo wordt er tegenwoordig veel ingespeeld op mensen als een manier om informatie te bekomen. Bewust of onbewust, werknemers zijn vaak de oorzaak van succesvolle cyberaanvallen. Een duidelijk voorbeeld hiervan zijn de werknemers die slachtoffer worden van het fenomeen *phishing* (Bissell et al., 2019). *Phishing* is een methode die cybercriminelen gebruiken om ondernemingen te infiltreren. Ze gebruiken social engineering-technieken om e-mails van een betrouwbare bron te imiteren waarin er wordt gevraagd om op een link te klikken. Wanneer een werknemer op die link klikt, kunnen cybercriminelen inloggegevens stelen, privégegevens verzamelen of schadelijke software installeren (Jensen, Dinger, Wright & Thatcher, 2017). Deze zaken gebeuren nog omdat werknemers niet altijd uitleg krijgen over de mogelijke cyberrisico's wanneer er binnen de onderneming nieuwe producten, diensten of processen worden ontwikkeld. Het is dus in het belang van alle stakeholders dat werknemers getraind worden omtrent cyberrisico's en beschikken over de nodige informatie. Ze hebben nood aan tools en motivatie om deze risico's te leren herkennen en te adresseren (Bissell et al., 2019). Zo zal ten gevolge van de COVID-19 crisis thuiswerk meer de norm worden en dat zal deze nood aan cybertraining alleen maar vergroten.

Een van de meest gebruikte middelen voor cyberaanvallen is *malware*. *Malware* kunnen we opdelen in vier soorten:

- Virus: Virussen zijn ingebed in uitvoerbare bestanden zoals computerprogramma's. Wanneer deze bestanden worden uitgevoerd, treedt het virus in werking. De werking van een computervirus is gelijkaardig aan de werking van een griepvirus. Een computervirus kan zichzelf naar andere uitvoerbare bestanden kopiëren en verplaatsen wanneer de uitvoerbare bestanden van de ene computer naar de andere worden gekopieerd. Ze zijn in staat om hardware en software te beschadigen of de beschikbare geheugencapaciteit te verminderen.

- *Worm*: *Worms* lijken op computervirussen. Het verschil is dat een *worm* zichzelf kan verspreiden. Een *worm* infecteert namelijk zichzelf en heeft geen uitvoerbare bestanden nodig om van de ene computer naar de andere gekopieerd te worden.

- *Trojan Horse*: Een Trojaans paard is vergelijkbaar met een computervirus. Dit zit vaak verborgen in programma's. Wanneer de gebruiker een Trojaans paard activeert, krijgt de aanvaller toegang tot de computer van de gebruiker.

- Botnet: Botnets zijn netwerken van meer gesofisticeerde *malwares*. Bij deze vorm van *malware* infecteren aanvallers meerdere computers, de bots, om aanvallen te coördineren en samen te werken (Cayirci & Ghergherehchi, 2011).

De opkomst van het internet heeft het verspreiden van botnets aanzienlijk vergemakkelijkt. Enkele bekende voorbeelden van botnets zijn 'gAmeover ZeuS', 'Mirai' en 'ZeroAccess'. Vroeger werden botnets vooral ingezet om spam te verspreiden naar zoveel mogelijk mensen op korte tijd. Vandaag de dag gaan cybercriminelen echter creatiever te werk met botnets. Ze worden onder andere ingezet om *ransomware* te verspreiden, DDoS-aanvallen (*distributed denial of service*) uit te voeren en cryptocurrency te exploiteren (Anderson et al., 2019). *Ransomware* is een vorm van *malware* die documenten in een systeem of netwerk gaan encrypteren om de toegang ertoe te blokkeren. Tegen een betaling van losgeld krijgen ondernemingen vaak terug toegang tot hun systemen (Oberly, 2019). Een DDoS aanval gaat anders in zijn werk. Bij een DDoS aanval gaat een hacker via *bots* zoveel mogelijk verzoeken sturen naar een bepaald systeem om het plat te leggen. Dit kan enorme schade verrichten (Joëlle, Park & Hwang, 2018). Afhankelijk van de middelen die ze hanteren, kunnen cybercriminelen hier veel geld mee verdienen (Anderson et al., 2019).

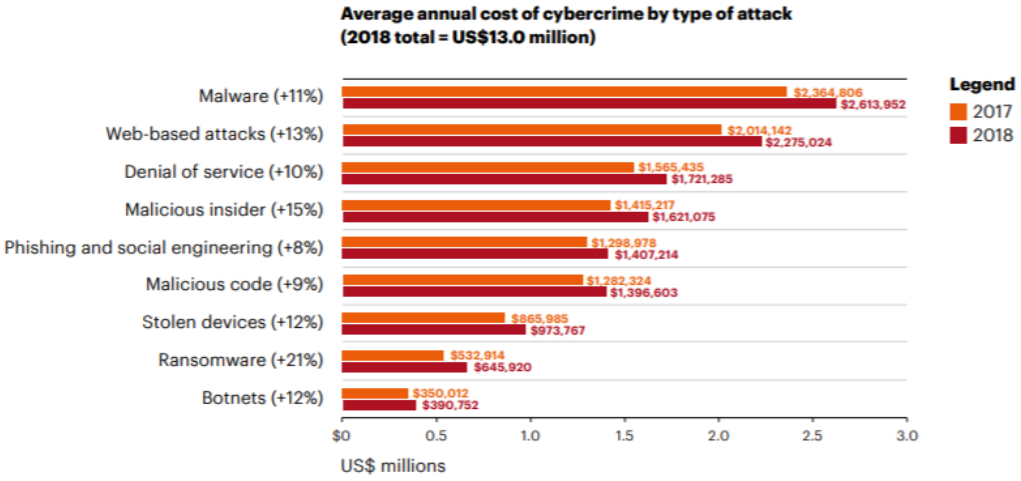
1.3 Kosten van *cybercrime*

Er zijn zoals hierboven beschreven verschillende middelen die cybercriminelen gebruiken om ondernemingen aan te vallen en hoewel veel ondernemingen al inzetten op *cybersecurity*, komen datalekken nog steeds voor. Dit komt doordat het potentiële risico op datalekken alleen nog maar versterkt wordt door onder andere het toenemende gebruik van technologie en de hogere frequentie van cyberaanvallen. Ondernemingen die met datalekken worden geconfronteerd, krijgen al snel een duidelijk beeld van de directe kosten die hierbij komen kijken. Een voorbeeld van zo een directe kost is de kosten die je maakt wanneer je (extra) personeel moet inschakelen om te reageren op een datalek. In zo een situatie moeten werknemers dikwijls overuren presteren om het probleem zo snel mogelijk op te lossen. Wat vaak moeilijker te begrijpen is, zijn de lange termijn en indirecte kosten. Dit kan problemen met zich meebrengen in de toekomst. Een onderneming die de volledige kost van lekken niet kan inschatten, riskeert immers de waarde van *cybersecurity* te onderschatten. Hierdoor wordt er misschien minder tijd en geld gestoken in het ontwikkelen van bepaalde technologische controles, cybertraining en het ontwikkelen van IT-vaardigheden (Furnell et al., 2020).

- Directe en indirecte kosten

Er wordt een onderscheid gemaakt tussen directe en indirecte kosten. Directe kosten zijn kosten die een directe monetaire uitwisseling vereisen. Dit zijn bijvoorbeeld kosten voor de verbetering van *cybersecurity*, compensaties voor de partijen die schade hebben ondervonden van een datalek, overuren van personeel, eventuele boetes die betaald moeten worden… Indirecte kosten daarentegen leiden niet tot een directe monetaire uitwisseling. Verlies van data en software, diefstal van intellectuele eigendom, verlies door stillegging van activiteiten tijdens het datalek… zijn voorbeelden van indirecte kosten (Furnell et al., 2020). Furnell et al. (2020) benadrukken daarom in hun onderzoek dat het cruciaal is om de volledige kosten van *security breaches* te begrijpen. Dit vereist niet alleen erkenning van de werkelijke impact en de omvang van een *security breach,* maar ook het vermogen om de juiste data te verzamelen op een efficiënte manier. Hoe beter de kennis over de kosten van *cybercrime,* hoe meer geïnformeerde beslissingen men kan maken.

- Cyberaanvallen en hun jaarlijkse kost



Figuur 1: gemiddelde jaarlijkse kost van *cybercrime* per aanvalstype (Bissell et al., 2019).

Het aantal cyberaanvallen is doorheen de jaren aanzienlijk blijven toenemen. Hiervan dragen vooral *malware* en web-based aanvallen (figuur 1) de hoogste kosten met zich mee (Bissell et al., 2019). Het onderzoek van Anderson et al. (2019) geeft een verklaring voor de hoge kosten van *malware*: op zich zal een vorm van *malware* in één computer niet veel schade kunnen aanrichten. De hoge kosten ontstaan pas wanneer de *malware* zich gaat verspreiden. *Malware* is immers ontworpen om zich snel te verspreiden en zoveel mogelijk computers en andere toestellen te infecteren (Anderson et al., 2019). Daarnaast maken *ransomware, malicious insider* aanvallen en *phishing* de laatste jaren ook een opmars. De impact van deze cyberaanvallen op ondernemingen is zeer groot. Niet alleen zien we het aantal datalekken groeien, ook stijgt de totale kost van cybercriminaliteit jaarlijks. Zo steeg deze totale kost bijvoorbeeld van US$11.7 miljoen per onderneming in 2017 tot US$13.0 miljoen in 2018. Dit is een stijging van maar liefst 12% (Bissell et al., 2019).

Met de toename in cyberaanvallen zien we ook een groei in dataverlies. Er is daarom nieuwe regelgeving, zoals de *General Data Protection Regulations* (GDPR), uitgebracht om organisaties en hun leidinggevenden meer verantwoordelijk te houden voor de bescherming van informatie en voor het verantwoord gebruik van klantgegevens. Aangezien er boetes worden opgelegd bij dataverlies zullen de financiële gevolgen van cyberaanvallen nog vergroten. Elke onderneming heeft er dus baat bij om te investeren in *cybersecurity* (Bissell et al., 2019).

2. Verantwoordelijken *cybersecurity*

2.1 Drie lijnen van verdediging

Hoewel iedereen binnen een organisatie zijn verantwoordelijkheid dient te nemen inzake *cybersecurity*, zijn er een aantal centrale verantwoordelijken die we hier verder zullen bespreken. Zo vinden we in een onderneming verschillende mensen die focussen op (*cybersecurity) assurance. Assurance* wordt door Bozkus en Caliyurt (2018) gedefinieerd als een middel om vertrouwen te creëren dat beveiligingscontroles de functies uitvoeren die van hen worden verwacht. De mensen die zich toeleggen op (*cybersecurity) assurance* houden zich bezig met risicomanagement, *security assurance* en audit. Er zijn drie principes die centraal staan in dit *cybersecurity assurance* proces:

(i) Betrouwbaarheid: Het is in het belang van alle stakeholders dat informatie confidentieel blijft.
(ii) Integriteit: Een systeem moet werken zoals het hoort te werken.
(iii) Beschikbaarheid: Het informatiesysteem moet functioneren en altijd klaar zijn voor gebruik. (Bozkus & Caliyurt, 2018).

Het belang van deze verantwoordelijken in het *assurance* proces wordt nog eens benadrukt in het drie lijnen model van verdediging (figuur 2). Het drie lijnen model brengt processen in kaart om risicomanagement te faciliteren en is iets wat veel ondernemingen toepassen.

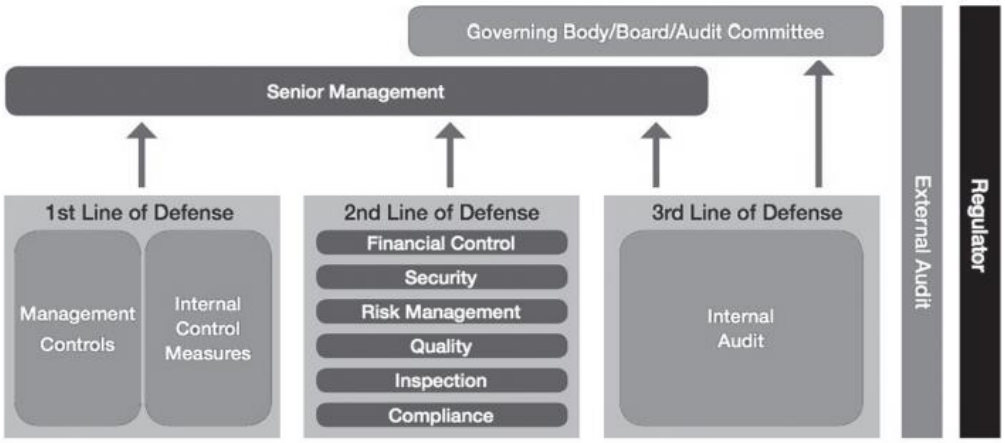
De eerste lijn houdt zich bezig met het identificeren en analyseren van risico's. Hier vindt de risicobeheersing plaats en worden maatregelen genomen (Weatherford, & Ruppert, 2016). De eerste lijn betreft vooral lijnmanagers en het middenmanagement. Zij ontwikkelen en implementeren processen omtrent interne controle en risicomanagement en communiceren dit naar de belangrijkste stakeholders. Hierbij heeft het topmanagement de eindverantwoordelijkheid. Het topmanagement zal daarom bij hoge risico's direct toezien op de lijn- en midden managers of de taken deels zelf uitvoeren (Anderson & Eubanks, 2015).

De tweede lijn staat hoofdzakelijk in voor het continu monitoren van controles en risicomanagementprocessen die zijn geïmplementeerd door de eerste lijn. Ze moet nagaan of de controles en processen wel werken zoals ze zouden moeten werken en rapporteert aan het topmanagement. Daarnaast gaat de tweede lijn regelmatig samenwerken met het operationeel management om hen te helpen met het ontwikkelen van een implementatiestrategie, het implementeren van een nieuw beleid en procedures, het verzamelen van informatie omtrent risico en controle… De tweede lijn is typisch opgedeeld in verschillende departementen die elk een functie voor zich nemen. Deze functies zijn: risicomanagement, *security*, financiële controle, *compliance*, kwaliteit en inspectie. Afhankelijk van de grootte en de eigenheid van een onderneming kan de samenstelling van de tweede lijn verschillen. In grote publieke ondernemingen met een complexe structuur zullen al deze functies afzonderlijk uitgevoerd worden. Binnen kleinere ondernemingen zullen enkele functies samengevoegd of gewoon volledig weggelaten worden (Anderson & Eubanks, 2015).

Tot slot is er de derde lijn. Deze betreft de interne audit functie. Ze is volledig onafhankelijk en beoordeelt zowel de effectiviteit van de interne beheersing als de werking van de eerste en tweede lijn (Weatherford & Ruppert, 2016). De interne audit functie ontwikkelt of implementeert zelf geen

controles en is ook niet verantwoordelijk voor de activiteiten van een onderneming. Ze is echter wel verantwoordelijk om haar bevindingen en aanbevelingen omtrent *governance*, riciso en controle naar de raad van bestuur en het auditcomité te communiceren. De interne audit heeft dus een belangrijke functie en draagt bij aan een effectieve *corporate governance*. In realiteit zien we echter dat kleinere ondernemingen geen interne audit functie hebben (Anderson & Eubanks, 2015).

Naast de drie lijnen van verdediging wordt er in onderstaand model de rol van de externe audit en regulatoren benadrukt (Weatherford & Ruppert, 2016). Wanneer ze effectief gecoördineerd zijn, kunnen externe groepen gezien worden als additionele lijnen van verdediging die belangrijke observaties kunnen communiceren naar de raad van bestuur en het topmanagement. Regulatoren gaan immers regelgeving opleggen om een onderneming haar *governance* en controles te versterken en externe auditors voeren risicoanalyses en controles uit die nieuwe zwakheden op gebied van de financiële rapportering naar voor kunnen brengen. Op deze manier kunnen ze een belangrijke rol spelen en bijdragen aan een effectieve *corporate governance*. Hoewel deze externe partijen een toegevoegde waarde kunnen zijn op dit gebied, kunnen we ze niet beschouwen als substituten voor de interne lijnen van verdediging (Anderson & Eubanks, 2015 ;Weatherford & Ruppert, 2016).



Figuur 2: De drie lijnen van verdediging (Weatherford & Ruppert, 2016).

2.2 De veranderende rol van audit

Zoals hierboven werd besproken, heeft de interne audit functie een belangrijke taak binnen ondernemingen. De laatste jaren ziet men echter een verschuiving gebeuren. Met de continue digitalisering van processen en documentatie wordt tegenwoordig veel van de informatie, waarop auditors zich baseren, geautomatiseerd. Technologische ontwikkelingen zijn met andere woorden de klassieke rol van de interne audit functie aan het veranderen (Fountain, 2019). *Cybersecurity* is hierbij een relatief nieuw onderdeel (Islam et al., 2018). Terwijl interne auditors zich vroeger hoofdzakelijk bezighielden met de controle van fysieke activa, komen er nu veel meer aspecten bij kijken (Liu, 2020). Jarenlang steunde de interne audit functie op IT-specialisten als partners in geïntegreerde audits, maar vandaag de dag kunnen interne auditors die verantwoordelijkheid niet meer volledig delegeren aan de IT-afdeling (Fountain, 2019). Het identificeren van risico's en controles binnen IT is immers geen afzonderlijke evaluatie meer (Liu, 2020).

Het beschermen van gevoelige informatie is een bijkomend doel geworden voor interne auditors. Dit kan interne informatie zijn van de onderneming zelf, maar ook belangrijke informatie over klanten. De interne audit functie is dus verantwoordelijk voor het controleren van *Information Security* (IS) processen en test het vermogen van deze processen om informatie te beschermen. Hierbij is het belangrijk dat de drie principes van *cybersecurity assurance* worden gehanteerd: (i) de integriteit wordt bewaard, (ii) de vertrouwelijkheid van gegevens wordt gegarandeerd en (iii) de toegang en beschikbaarheid van gegevens wordt gecontroleerd (Islam et al., 2018).

Het is daarom belangrijk dat interne auditors evolueren en een grondige kennis ontwikkelen van meer dan alleen algemene en toepassingscontroles. Audits werken namelijk het best wanneer alle auditors controles kunnen uitvoeren vanuit een IT perspectief en zich bewust zijn van de belangrijkste technologische risico's. Met de toename van cyberrisico's is het belangrijk dat auditors zowel de onderliggende drijvers als de oorzaken van deze risico's begrijpen (Bozkus, & Caliyurt, 2018; Fountain, 2019). Niet alleen kennis over IT kan de interne audit verbeteren, maar ook kennis over de IS beveiligingsfuncties (Islam et al., 2018). Door het management in het *cybersecurity* proces te ondersteunen, kunnen interne auditors bijdragen aan de ontwikkeling van effectieve beveiligingsprogramma's. Op deze manier creëren auditors waarde voor het bedrijf en verhogen ze de kwaliteit van de *cybersecurity* (Fountain, 2019; Islam et al., 2018).

Trainingen en het behalen van certificaten kunnen auditors helpen met het ontwikkelen van een brede kennis. Zo zijn er trainingen over: cyber- of fraudedreigingen en op welke manier deze zich kunnen voordoen, hoe procedures in kaart gebracht worden om cyberrisico's in te schatten en of deze binnen het risicoappetijt van de onderneming vallen, verschillende types van *breaches*, diverse methodes om activa te beschermen… (Fountain, 2019). Certificaten zoals CISA of CPA blijken ook wel degelijk een invloed te hebben op de cybersecurity audit (Islam et al.; 2018).

Dat de brede kennis van interne auditors de kwaliteit van *cybersecuriy* ten goede komt, werd ook bevestigd in andere studies (Bedard & Graham, 2011; Haislip, Peters, & Richardson, 2016). Islam et al. (2018) toonden aan dat er een positieve relatie is tussen *cybersecurity* audit door de interne audit functie en de competentie van de interne audit functie betreffende *governance*, risico en controle. Ook werd er aangetoond dat zowel een uitgebreide risicobeoordeling door de interne audit functie als de kwaliteit van de interne audit een positief effect hebben op de *cybersecurity* van een onderneming (Islam et al., 2018).

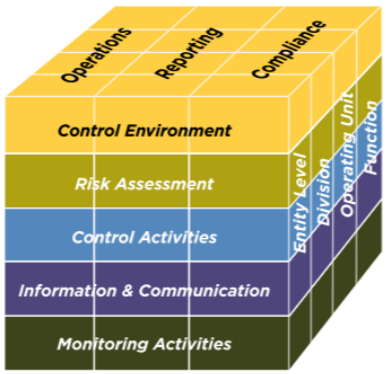
3. Relevante raamwerken

Het beheersen van cyberrisico's is zeer complex omdat het raakt aan bijna elk onderdeel van een onderneming. Daarom dient het beheersen ervan ook op een holistische manier aangepakt te worden. Er werden hiervoor verschillende raamwerken ontwikkeld die ondernemingen kunnen ondersteunen in dit risicobeheersingsproces. Volgens Fountain (2019) is het ook belangrijk om deze raamwerken toe te passen. Op die manier leren bedrijven immers hun risico's efficiënt en effectief te beheersen en de impact ervan te verkleinen (Fountain, 2019). Er bestaan verschillende raamwerken, maar de volgende raamwerken zijn relevant in deze studie omdat ze focussen op de *cyberspace* van een onderneming. Deze raamwerken zijn: (i) COSO en COSO ERM, (ii) *Control Objectives for Information and Related Technology* (COBIT), (iii) *The U.S. National Institute of Standards and Technology's* (NIST) *Cybersecurity Framework* en (iv) de *International Organization for Standardization* standaarden (ISO) (Bozkus & Caliyurt, 2018). Het kiezen van het juiste raamwerk is afhankelijk van verschillende factoren. Zo kunnen bijvoorbeeld de industrie, *compliance*-vereisten en factoren die eigen zijn aan de onderneming zelf deze keuze beïnvloeden (Islam et al., 2018).

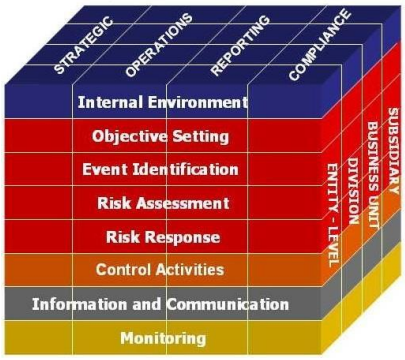
3.1 COSO en COSO ERM

Het COSO en COSO ERM raamwerk werd opgesteld door *The American Institute of Certified Public Accountants.* Naast de COSO raamwerken, heeft de AICPA nog heel wat andere raamwerken ontwikkeld waaronder bijvoorbeeld het SOC *cybersecurity risk management reporting framework.* Het COSO raamwerk werd in 1992 ontwikkeld door AICPA in samenwerking met *the American Accounting Association* (AAA), *Financial Executives International* (FEI), *the Institute of Internal Auditors* (IIA) en *the Institute of Management Accountants* (IMA). COSO (figuur 3) voorziet organisaties van richtlijnen bij het ontwikkelen en implementeren van effectieve interne controleprocessen en ondersteunt daarnaast deze organisaties in het behalen van hun doelstellingen (*operations*, *compliance* en *reporting*). Dit raamwerk wordt traditioneel voorgesteld door een driehoek, maar de alternatieve kubusvorm komt ook voor. Door de jaren heen is het COSO raamwerk regelmatig bijgewerkt en vandaag de dag is het uitgegroeid tot een van de meest gebruikte raamwerken voor interne controle (COSO*,* z.d.).

Naast het COSO raamwerk werd in 2004 ook het COSO ERM raamwerk (figuur 4) ontwikkeld. Terwijl COSO de focust legt op interne controle, gaat COSO ERM dieper in op *enterprise risk management* (ERM). Dit was het eerste raamwerk dat met een duidelijke definitie van risicomanagement kwam, alsook met een uitlijning van het proces en richtlijnen over de juiste implementatie van risicomanagement. Dit raamwerk implementeert het concept van risicoappetijt. De risicoappetijt van een onderneming is de mate van risico die ze wil accepteren om haar doelstellingen te behalen. Daarnaast legt COSO ERM ook de nadruk op strategische doelstellingen, iets waar in het eerdere COSO raamwerk nog geen extra aandacht aan besteed werd (Moeller, 2011).



figuur 3: COSO *framework* (COSO, 2013).



figuur 4: COSO ERM *framework* (Pierce, Goldstein & Pierce, 2016).

Volgens Galligan & Rau (2015) kan het beheersen van cyberrisico's aan de hand van het COSO raamwerk de raad van bestuur en senior executives van de onderneming helpen om de bedrijfsdoelstellingen, de definitie van kritische informatiesystemen en de gerelateerde risicotolerantieniveaus beter te communiceren. Door de informatiesystemen die het meest gevoelig zijn voor aanvallen en de waarschijnlijke aanvalsmethoden te evalueren, kunnen werknemers van een organisatie gedetailleerde cyberrisicoanalyses uitvoeren. Dit stelt ondernemingen in staat om gepaste controleactiviteiten op te zetten voor de cyberrisico's (Galligan & Rau, 2015).

3.2 COBIT

Het COBIT raamwerk is opgesteld door de *Information Systems Audit and Control Association* (ISACA) en is doorheen de jaren regelmatig aangepast. Hoewel COBIT begon als een gidsend raamwerk voor audit met verschillende controledoelstellingen, is het tegenwoordig uitgegroeid tot een omvangrijk IT *governance* raamwerk. De meest recente versie van het raamwerk is COBIT 2019. Hierin worden digitale transformatie-gerelateerde doelstellingen samen met organisatorische structuren besproken. Daarnaast focust COBIT 2019 zich op nieuwe uitdagingen zoals *cybersecurity*. Binnen dit raamwerk wordt nogmaals bevestigd dat de rol van de interne audit aan het veranderen is (Drozdov, 2019). COBIT 2019 is een goed uitgewerkt raamwerk dat door auditors over de hele wereld positief ontvangen wordt. De update van COBIT 5 naar COBIT 2019 heeft immers de praktijken bijgewerkt en gezorgd voor meer duidelijke terminologie en nieuwe sleutelconcepten (Harisaiprasad, 2020).

COBIT 2019 beschrijft zes *governance* principes:

(i) Creëer waarde voor de stakeholders.
(ii) Hanteer een alomvattende aanpak.
(iii) Ontwikkel een dynamisch *governance* systeem.
(iv) Zorg voor een duidelijk onderscheid tussen controle en management.
(v) Stem het systeem af op de noden van de onderneming.
(vi) Bekom een volledig *governance* systeem (Harisaiprasad, 2020).

Deze principes moeten ervoor zorgen dat de behoeften van de stakeholders bevredigd worden en in lijn zijn met de ondernemingsdoelstellingen. Op die manier kunnen ze aan de hand van

prioriteitenstelling en besluitvorming richting geven aan en toezien op de prestaties en naleving van de vastgelegde doelstellingen (Harisaiprasad, 2020).

3.3 NIST cybersecurity framework

Eén van de meest toegepaste raamwerken is *the U.S. National Institute of Standards and Technology's* (NIST's) *Cybersecurity Framework* (CSF) (Fountain, 2019). Dit raamwerk werd in 2014 opgesteld in samenwerking met verschillende ondernemingen en de overheid van de Verenigde Staten. Het doel was om een *cybersecurity* raamwerk te ontwikkelen dat ondernemingen een flexibele, prestatie-gebaseerde en kostenefficiënte aanpak biedt om haar cyberrisico's te beheren (NIST, 2014). NIST CSF beschrijft met andere woorden hoe ondernemingen *cybersecurity* moeten aanpakken en hoe ze moeten reageren op en herstellen van cyberaanvallen (Fountain, 2019). NIST CSF bestaat uit drie delen: de kern, de implementatieniveaus van het raamwerk en de profielen (NIST, 2020).

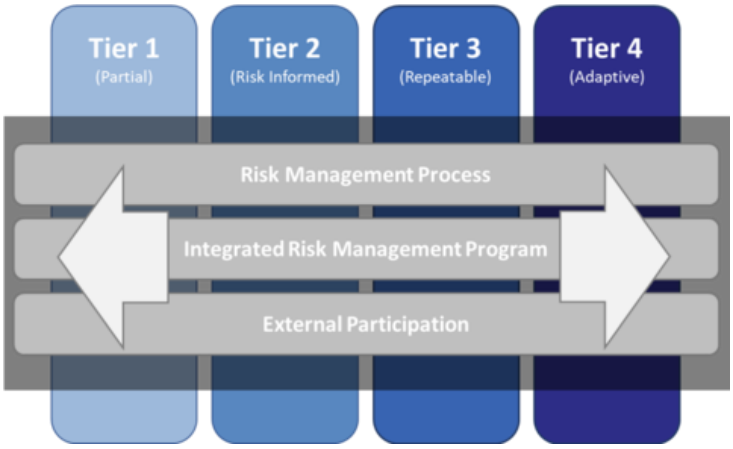
- De kern: De kern van het raamwerk geeft *cybersecurity* activiteiten en gewenste uitkomsten voor ondernemingen weer. Dit kan gaan van industrie standaarden tot richtlijnen of praktijken. De kern wordt opgedeeld in 5 functies, 23 categorieën en 108 subcategorieën. Deze vijf functies zijn: identificeren, beschermen, detecteren, reageren en herstellen. Aan de hand van deze functies worden de onderliggende categorieën en subcategorieën geïdentificeerd. Vervolgens koppelt het raamwerk deze aan voorbeelden van informatieve verwijzingen zoals bestaande normen, richtlijnen en praktijken voor elke subcategorie (figuur 5). Op deze manier kunnen zelfs de meest complexe problemen door de gehele organisatie gecommuniceerd en begrepen worden (NIST, 2014).

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figuur 5: NIST CSF *framework core* (NIST 2021).

- De implementatieniveaus: Dit deel van de CSF beschrijft de mate waarin de *cybersecurity* risicomanagementpraktijken van een onderneming de kenmerken vertonen die in het raamwerk zijn gedefinieerd (*partial, risk informed, repeatable, adaptive*). Meer specifiek, dit geeft aan in welke mate ondernemingen *cybersecurity* in hun beslissingsproces hebben geïntegreerd waarbij *partial* het laagste niveau is en *adaptive* het hoogste (figuur 6). Op deze manier probeert NIST CSF ondernemingen een context te bieden over hoe ze kijken naar *cybersecurity* risicomanagement (NIST, 2020).



Figuur 6: NIST CSF *framework implementation tiers* (NIST 2021).

- Het profiel: Het raamwerkprofiel brengt de vorige delen van het NIST CSF samen en stemt standaarden, richtlijnen en praktijken af op de kern in een bepaald implementatiescenario. Het huidige profiel kan vergeleken worden met een doelproefiel en zo kunnen ondernemingen hun *cybersecurity* verbeteren en opportuniteiten onderscheiden (NIST, 2014).

3.4 ISO

International Organization for Standardization (ISO) is een onafhankelijke, wereldwijde organisatie die experts samenbrengt om kennis te delen en marktrelevante internationale normen te ontwikkelen die innovatie ondersteunen en oplossingen bieden voor wereldwijde uitdagingen. De ISO heeft tot heden dag 23664 internationale standaarden ontwikkeld die betrekking hebben op een heel aantal aspecten van technologie en productie (ISO, z.d.). Binnen deze studie zijn de ISO 27000 en de ISO 9000 standaarden het meest relevant.

Volgens Otero (2015) worden de ISO standaarden gebruikt door ondernemingen om IS controles te introduceren. Niet alleen de ISO standaarden, ook COBIT en ITIL worden genoemd (Otero, 2015). Otero (2015) stelt dat ondernemingen zelf de IS controles moeten identificeren wanneer ze *best practice frameworks* hanteren. Dit vormt een uitdaging voor veel ondernemingen (Otero, 2015). Bovendien stellen Karimi, Cowan en Alencar (2014) dat de ISO 27001/2 standaarden het belang benadrukken van strenge toegangscontroles. Daarbij is het ook belangrijk dat kritische informatie enkel door bevoegde personen geraadpleegd kan worden. In het algemeen accentueren deze standaarden het belang van beveiligingsmechanismen en -processen. Ze gaan ervan uit dat ondernemingen uit alle sectoren het beschermen van vertrouwelijke data beschouwen als een prioriteit (Karimi, Cowan & Alencar, 2014).

4. Besluit literatuurstudie

We kunnen besluiten dat er in de literatuur al heel wat bestudeerd is op gebied van *cybersecurity*. Zo is het duidelijk geworden dat de opkomst van technologie en internet het landschap waarin ondernemingen vandaag de dag opereren compleet heeft veranderd. Dit heeft niet alleen nieuwe opportuniteiten met zich meegebracht maar ook nieuwe risico's, waarvan de grootste risico's behoren tot de cyberrisico's. Ondernemingen van alle groottes worden hiermee geconfronteerd en geen enkele onderneming is volledig veilig voor cyberaanvallen. De soorten aanvallen en middelen die cybercriminelen hanteren werden ook verder toegelicht. Hieruit is gebleken dat *malware* het meeste voorkomt. De literatuur benadrukt ook het belang van *cybersecurity* door de mogelijke gevolgen van een cyberaanval te duiden. Wanneer cyberaanvallen immers succesvol zijn, kunnen ze datalekken doen ontstaan. Dit kan schadelijke gevolgen hebben voor de onderneming zelf en brengt hoge kosten met zich mee. Een zwakke *cybersecurity* kan immers de hele organisatie treffen en daarmee de klantenrelaties, de reputatie en de winstgevendheid van een onderneming schaden. Omdat technologie zo verweven zit in onze economie is *cybersecurity* niet meer weg te denken binnen ondernemingen. Deze technologische verwevenheid is vandaag nog groter ten gevolge van de wereldwijde COVID-19 crisis. Het is daarom in het belang van alle individuen en ondernemingen om *cybersecurity* centraal te stellen.

Gelukkig werden er verschillende raamwerken ontwikkeld die ondernemingen kunnen ondersteunen in de beveiliging van hun processen en gevoelige informatie. In de literatuur werden enkele voorbeelden van deze *cybersecurity* raamwerken aangehaald: COSO ERM, COBIT, NIST CSF en de ISO standaarden. Hierbij is het opgevallen dat onderzoekers vooral hebben gefocust op de inhoud van deze raamwerken. De bestaande raamwerken worden immers *high level* besproken maar de stappen die ondernemingen moeten nemen om deze raamwerken succesvol te implementeren, ontbreken. Het is met andere woorden duidelijk wat ondernemingen kunnen doen om hun cyberrisico's te beheersen, maar nog niet duidelijk hoe ze dat precies moeten doen. Daarbij lijken deze raamwerken te focussen op grote ondernemingen met volwaardige IT-departementen terwijl cyberrisico's ook groter worden voor KMO's. Het is daarom ook belangrijk om te weten hoe KMO's deze raamwerken kunnen implementeren.

In de volgende onderdelen wordt een kwalitatief onderzoek gevoerd naar de factoren die meespelen bij de succesvolle implementatie van *cybersecurity* raamwerken. Meer specifiek, hoe pakken ondernemingen de implementatie van raamwerken aan en wat zorgt voor een goede implementatie? Aangezien de bestaande literatuur naar de implementatie van *cybersecurity* raamwerken beperkt is, zeker in het Belgische KMO-landschap, werd hiervoor de grounded theory methodiek verkozen. Deze wordt verder uitgelegd in het volgend onderdeel.

Onderzoeksmethode

1. Grounded theory

In dit onderzoek wordt een kwalitatieve grounded theory methode toegepast om een antwoord te bieden op de onderzoeksvraag '*Hoe implementeren ondernemingen cybersecurity raamwerken op een succesvolle manier en welke factoren spelen hierbij een rol?'*. Deze methode is vooral gepast wanneer er relatief weinig onderzoek naar een onderwerp is gedaan (Chun, Birks, & Francis, 2019). Aangezien de bestaande literatuur naar de implementatie van *cybersecurity* raamwerken beperkt is, zeker in het Belgische KMO-landschap, werd deze methode verkozen. De grounded theory methode werd in 1967 ontwikkeld door Barney Glaser en Anselm Strauss (Johnson, 2015). Met hun boek 'The Discovery of Grounded Theory: Strategies for Qualitative Research' wilden Glaser en Strauss het idee dat enkel kwantitatieve methodologie een geschikte manier is om data te analyseren en waarheden bloot te leggen, weerleggen (Chun, Birks, & Francis, 2019). De grounded theory methode helpt bij het ontwikkelen van een theorie op een systematische en inductieve wijze en benadrukt hierbij twee aspecten: *purposive sampling* en *constant comparative analysis* (Bryant & Charmaz, 2007; Chun, Birks, & Francis, 2019).

Purposive sampling wijst op het verzamelen van data. De auteur moet doelgericht op zoek naar experts en andere databronnen die een antwoord kunnen bieden op de onderzoeksvraag (Chun, Birks, & Francis, 2019). Zowel Yin (2003) als Eisenhardt en Graebner (2007) stellen dat een theorie het best wordt ontwikkeld aan de hand van case study gegevens. Een case study wordt door Yin (2003) gedefinieerd als: "a qualitative research strategy that involves an empirical investigation of a particular contemporary phenomenon within its real-life context" (Yin, 2003; p. 13). Case studies worden dan ook geselecteerd op basis van hun relevantie en opportuniteit om nieuwe informatie of theoretische inzichten bloot te leggen. Dit noemt men *theoretical sampling* (Eisenhardt & Graebner, 2007).

Een tweede aspect van de grounded theory methode is *constant comparative analysis*. Dit is een iteratief proces dat als doel heeft om verschillen en consistenties tussen verschillende cases te beoordelen. Op deze manier kan de auteur concepten en theoretisch relevante categorieën voortdurend verfijnen (Charmaz, 2006; Chun, Birks, & Francis, 2019). Meer specifiek, via *comparative analysis* worden nieuwe cases vergeleken met eerder bevraagde cases. Hieruit volgt dan ofwel een bevestiging van oorspronkelijke inzichten indien de nieuwe case vergelijkbare resultaten toont ofwel een herformulering van inzichten. Elke nieuwe case geeft duidelijkheid over bestaande inzichten en beïnvloedt toekomstige vragen. Dit iteratieve proces omvat zowel inductief als deductief denken. Hierbij erkent de grounded theory methode ook dat de kwaliteit en de aard van de resultaten niet alleen afhankelijk zijn van de geselecteerde cases, maar ook van de interpretatie van de auteur (Chun, Birks, & Francis, 2019; Johnson, 2015).

Om dit tweede aspect zo goed mogelijk toe te passen, werd er gekozen voor *de multiple case study* methode van Yin (2003). Deze draagt immers het sterkst bij aan het proces van theorieontwikkeling (Eisenhardt & Graebner, 2007).

2. Cases voor dit onderzoek

Vooraleer de cases werden geselecteerd, heeft de auteur dit eerst met haar promotor en copromotor besproken. Uit dit gesprek kwamen enkele potentiële cases naar voren. Vervolgens ging de auteur individueel op zoek naar relevante cases. Om het proces van *theoretical sampling* zo goed mogelijk uit te voeren, waren er enkele belangrijke criteria. Zo moesten de potentiële cases zo veel mogelijk gevestigd zijn in verschillende sectoren om een zo duidelijk mogelijk beeld te krijgen van het Belgische ondernemingslandschap. Daarnaast werd er zowel naar KMO's gezocht als grotere bedrijven. Aangezien veel KMO's IT volledig outsourcen, werd dit gecompenseerd door cases te zoeken die zelf in aanraking komen met KMO's en hun IT infrastructuur. Dit betreft zowel KMO's die hun IT in huis doen als consultancy bedrijven die KMO's als klant hebben. Tot slot was het ook belangrijk om enkele toezichthoudende organen te bevragen om zo de theorie te bekijken vanuit een andere invalshoek. Uiteindelijk bleven er negen cases over voor een uitgebreide analyse. In tabel 1 (pagina 27) worden de negen geselecteerde cases beschreven. Hierbij wordt de anonimiteit en vertrouwelijkheid ten aanzien van de deelnemende bedrijven gerespecteerd.

3. Dataverzameling

De primaire methode voor de dataverzameling was het afnemen van kwalitatieve diepte-interviews. Op deze manier kon de auteur via één op één gesprekken de cases uitgebreid bevragen. Er werden veertien interviews afgenomen uit de negen vooropgestelde cases. Dit gebeurde omwille van de COVID-19 crisis zowel online als telefonisch. De interviews waren semigestructureerd en werden individueel afgenomen. Alleen voor case D en case F (F2 en F3) werden collega's samen geïnterviewd omdat elke collega zijn specialiteit had maar samen vertelden ze een samenhangend verhaal. De collega's vulden elkaar ook aan bij specifieke vragen wat zorgde voor een coherent beeld van de realiteit. De bedoeling van semigestructureerde interviews is dat de geïnterviewde de thema's uit de vragenlijst in zijn eigen woorden gaat concretiseren. De onderzoeker speelt dan in op de antwoorden van de respondent door interesse te tonen en kritische bijvragen te stellen. Op die manier wordt het gesprek verder gestimuleerd (Saunders , Lewis, Thornhill, Booij, & Verckens, 2011).

Uit de negen cases kunnen we drie groepen onderscheiden. De eerste groep betreft bedrijven die actief zijn op het gebied van audit, accountancy, belastingadvies en bedrijfsadvies. Het ging hier om personen met minstens tien jaar ervaring binnen verschillende sectoren en bedrijven. De tweede groep omvat adviserende organen en autoriteiten binnen de financiële sector. Tot slot de derde groep, deze betreft de KMO's en grotere bedrijven die hun IT en *cybersecurity* in huis doen. De geïnterviewde personen uit deze laatste groep waren eveneens mensen met minstens tien jaar ervaring en een leidinggevende functie binnen hun vakgebied. In totaal werden er elf diepte-interviews afgenomen met elk een tijdsduur tussen de dertig en zestig minuten. Daarnaast werden de interviews handmatig getranscribeerd. Met gevolg waren er meer dan 60 pagina's aan data om te analyseren. Tabel 2 (pagina 28) geeft een overzicht van de geïnterviewde respondenten.

Tabel 1

Geselecteerde cases

Case A is een wereldwijde professionele dienstenorganisatie met onder andere verschillende vestigingen hier in België. Verspreid over verschillende sectoren biedt dit bedrijf diverse diensten aan op gebied van audit, accountancy, strategie, belastingen, juridisch advies… Hun cliënteel varieert van internationale beursgenoteerde bedrijven tot lokale KMO's.

Case B is een Belgische verzekeringsmaatschappij die verzekerden heeft in verschillende sectoren. Hun klanten zijn voornamelijk de openbare overheden, ondernemingen en particulieren.

Case C is een van de grootste coöperatieve groente- en fruitveilingen van België met verschillende vestigingen in Vlaanderen en Wallonië. Dit bedrijf wordt beschouwd als een van de grotere KMO's hier in België.

Case D is een autonome openbare instelling die instaat voor het toezicht op de Belgische financiële sector. Naast haar toezichthoudende functie heeft deze instelling ook een adviserende rol.

Case E is een globaal accounting en consultancy netwerk. Binnen België heeft dit bedrijf ook verschillende kantoren. Dit bedrijf opereert in diverse sectoren en biedt diensten aan op vlak van audit, accountancy, bedrijfsfinanciering, consulting, belastingen, juridisch advies… Ze werkt vooral met KMO's. Grote internationale klanten komen minder voor, maar zijn niet onbestaand.

Case F is een nationale onafhankelijke autoriteit die allerhande taken uitvoert zoals bijvoorbeeld de bepaling en de uitvoering van het Europese monetaire beleid en het verzamelen, opstellen, analyseren en verspreiden van economische en financiële informatie. Daarnaast staat ook zij in voor het toezicht op de financiële sector.

Case G is een globaal dienstennetwerk dat bestaat uit verschillende organisaties wereldwijd met ook in België heel wat vestigingen. Dit bedrijf biedt diensten aan op gebied van audit, accountancy, consulting, belastingen, juridisch advies… Net zoals case A omvat haar cliënteel alles van internationale beursgenoteerde bedrijven tot lokale KMO's die actief zijn in diverse sectoren.

Case H is een nationale autoriteit van België die zich vooral bezighoudt met de cyberbeveiliging. Ze heeft een toezichthoudende en coördinerende rol.

Case I is een Belgisch advieskantoor met verschillende vestigingen in Vlaanderen. Dit bedrijf specialiseert zich in audit, accountancy, juridisch advies, belastingen, bedrijfsfinanciering… Haar cliënteel bestaat vooral uit KMO's.

Tabel 2

Overzicht data-verzameling

Geselecteerde cases	geïnterviewde respondenten
Case A	**A1:** Director cybersecurity **A2:** Partner
Case B	**B1:** IT manager
Case C	**C1:** IT manager
Case D	**D1:** Senior advisor **D2:** Advisor **D3:** Advisor (policy department)
Case E	**E1:** Partner
Case F	**F1:** Expert in cyberrisico **F2:** Manager **F3:** Manager
Case G	**G1:** Partner
Case H	**H1:** Advisor
Case I	**I1:** IT director

4. Data-analyse

Binnen grounded theory is het belangrijk om aan de hand van *constant comparative analysis* informatie te gaan analyseren en concretiseren. De auteur moet immers concepten en theoretisch relevante categorieën voortdurend verfijnen (Charmaz, 2006; Chun, Birks, & Francis, 2019). Dit samenhangend proces werd doorheen het onderzoek gerespecteerd en de analyse van informatie startte reeds na het eerste interview. Op deze manier konden de onderliggende motieven tussen interviews vergeleken worden. Na het afleggen van de interviews volgde er een grondig codeerproces.

De eerste fase van dit codeerproces noemen we de open codering. Bij open codering is het de bedoeling om de data op te splitsen in afzonderlijke delen. Data wordt dan nauwkeurig bekeken en consistenties en verschillen tussen interviews worden verder onderzocht. Door te focussen op

consistenties en verschillen tussen interviews kunnen er codes onderscheiden worden. Chun, Birk & Francis (2019) gebruiken de definitie van Charmaz in hun onderzoek en beschrijven codes als: "codes rely on interaction between researchers and their data. Codes consist of short labels that we construct as we interact with the data. Something kinaesthetic occurs when we are coding; we are mentally and physically active in the process." (Chun, Birk & Francis, 2019, p4). Hiervoor werd er een lijn-bij-lijn coderingsmethode gehanteerd. De lijn-bij-lijn methode helpt de auteur niet alleen bij het verifiëren van categorieën, maar garandeert ook dat de gevonden codes relevant zijn (Bryant & Charmaz, 2007; Strauss & Corbin, 1999). In tabel 3 (pagina 30) wordt een voorbeeld gegeven van lijn-bij-lijn codering. Er werden in totaal 187 codes geïdentificeerd.

De volgende fase van het coderingsproces was de gerichte codering. In deze fase werd er gefocust op de meest significante codes uit het open codeerproces. De gevonden codes werden gegroepeerd in categorieën om een duidelijker overzicht te bekomen. Zo werd er bijvoorbeeld een categorie 'cybercriminaliteit' gemaakt op basis van de codes die hierop betrekking hadden. Op deze manier kon er dieper ingegaan worden op de gevonden data en zo werd het aantal deelcategorieën herleid tot dertien. In tabel 4 (pagina 31) wordt een voorbeeld van gerichte codering weergeven. De auteur ging op basis van haar interpretatie verder te werk. Zo konden uiteindelijk zes centrale thema's worden onderscheiden die samen de onderzoeksvraag zo goed mogelijk beantwoorden. Deze zijn: belang van *cybersecurity*, cybercriminaliteit, bescherming tegen cyberdreigingen, de financiële sector, de bescherming van KMO's en de implementatie van raamwerken. Deze laatste stap wordt *theoretical coding* genoemd. (Bryant & Charmaz, 2007; Strauss & Corbin, 1999). Het codeerproces werd uitgevoerd met behulp van NVIVO (QRS international).

5. Het omsluiten van de literatuur

De laatste jaren wordt theorievorming op basis van casestudy's meer en meer gezien als een relevante onderzoeksstrategie en deze vorm van theorievorming wordt dan ook meer toegepast in studies (Eisenhardt & Graebner, 2007). Een belangrijk aspect van theorievorming is het vergelijken van de emergent theory met de bestaande literatuur (Eisenhardt, 1989). Daarom werd er in dit onderzoek eerst een grondige literatuurstudie gedaan aan de hand van bestaande academische bronnen omtrent *cybersecurity* raamwerken, de implementatie ervan, cybercriminaliteit, de gevolgen van cyberaanvallen en datalekken enzovoort.

In het volgende onderdeel zullen de resultaten per thema worden besproken aan de hand van quotes van de veertien respondenten. Vervolgens volgt er een conclusie waarin de bestaande literatuur vergeleken zal worden met de belangrijkste resultaten uit dit onderzoek en waar de beperkingen van dit onderzoek worden aangekaart.

Tabel 3

Voorbeeld van open codering

Except 1. Een IT manager spreekt over de uitdagingen in verband met cyberaanvallen en de meest gebruikte middelen.	
Cyberaanvallen zijn moeilijk in te schatten Kennis van hacking tools en programma's beperkt. Hackers zijn expert en jij niet Ransomware wordt veel gebruikt en vormt een grote uitdaging Drijver om te gaan hacken is vaak geld Hackers gaan bedrijven lam leggen om losgeld te vragen → Bitcoin/cyptocurrency (want anoniem) Zoeken naar weak spots Aanvalsbasis is breed want het hele web is ter beschikking van hackers Bijna altijd malware/ransomware	"Als IT manager is dit niet altijd makkelijk in te schatten. Je weet er niet voldoende van, want de specialisten zitten eigenlijk aan de andere kant. Maar als ik zie wat er de laatste jaren gebeurt… Bijvoorbeeld ook nog dit jaar is er een zeer belangrijke IT-speler geraakt geweest door een aanval, een ransomware attack. Ik denk wat er de laatste jaren meer en meer gebeurt, is het verhaal rond ransomware. De uitdaging om te gaan hacken of eerder de reden om te gaan hacken is vandaag vooral geld verdienen. Als je vandaag als hacker een bedrijf kan lam leggen en vragen of ze je betalen in bitcoins of om het even dan kan je op een heel makkelijke manier wat geld gaan verdienen. Ik denk dat de tools die ze gebruiken nog altijd wel hetzelfde zullen zijn. Ik denk dat men altijd de weak spots probeert te vinden in een bedrijf, men gaat daar ook niet meer al te veel tijd insteken omdat men het hele web ter beschikking heeft en eigenlijk nogal vrij breed kan gaan proberen om ergens binnen te geraken. Zodra dat men ergens een zwak punt vindt dan gaat het denk ik bijna altijd over *malware* gaan, die zich gaat nestelen en op een gegeven moment gaat activeren als een soort van ransomware."

Tabel 4

Voorbeeld van gerichte codering

Except 1. Een IT-manager vertelt over de verschillen in aanvallen en cybercriminelen	
Threat actors Bescherming bedrijven Motivatie threat actors	**"**Je hebt aanvallen die gericht naar een bedrijf gaan omdat ze echt een bedrijf willen hebben. Dat is een hele andere aanpak dan wanneer dat het gaat over een individuele hacker die wel iets van computers kent. Het grootste risico voor bedrijven vandaag is dat eerste. Als je echt getarget gaat worden omdat een bepaalde groepering je wil hebben dan ben ik vrijwel overtuigd dat je niet veel kan doen. Die mensen hebben tijd en die kunnen dag en nacht werken en die hebben altijd wel een manier om binnen te geraken. Vandaag de dag moet je ervan uitgaan dat je als bedrijf vooral gaat aangevallen worden omdat ze je willen lam leggen en geld willen verdienen aan jou."
Except 2. *Cybersecurity* & *privacy* partner spreekt over de implementatie van een ISO standaard	
Implementatie van raamwerken en standaarden Bescherming bedrijven	"Wij zijn ook een ISO 27001 implementatie aan het doen voor een software bedrijf van 13 man en dat gaat in totaal een dertigtal mandagen zijn. Maar je moet daar pragmatisch mee omgaan, want je kan je ook snel verliezen in procedures. Ik had onlangs een klant en ze dachten dat ze ISO 27000 aan het implementeren waren maar ze hadden policies opgemaakt om policies up te daten dat ik dacht van nee. Je kan daar zoveel papierwerk rond genereren als je wilt, maar het is heel belangrijk dat je het proportionaliteitsprincipe respecteert en het aanpast aan je organisatie."

Resultaten

Zoals eerder in dit onderzoek werd besproken is het duidelijk dat IT en *cybersecurity* een belangrijke rol hebben gekregen binnen ondernemingen. IT mag dan wel een ondersteunende functie zijn, maar ondernemingen kunnen vandaag de dag niet werken zonder te steunen op technologie. Deze grotere afhankelijkheid van technologie brengt natuurlijk nieuwe risico's met zich mee. Het cyberrisico wordt al jaren als grootste risico en uitdaging gezien voor ondernemingen. Elke onderneming wordt immers wel eens geconfronteerd met cyberdreigingen. Ondernemingen die *cybersecurity* niet als een van hun prioriteiten gaan zien, kunnen hier nadelige gevolgen van ondervinden. In dit onderdeel zullen de belangrijkste bevindingen, die naar voren zijn gekomen bij de analyse van de interviews, uitgebreid besproken worden. Aan de hand van zes thema's zal er een zo duidelijk mogelijk antwoord geschetst worden op de onderzoeksvraag *'Hoe implementeren ondernemingen cybersecurity raamwerken op een succesvolle manier en welke factoren spelen hierbij een rol?'.*

1 Belang van cybersecurity

1.1 Toenemende nood aan cybersecurity

In het kader van dit onderzoek is het essentieel om het belang van *cybersecurity* aan te tonen. *Cybersecurity* is namelijk niet meer weg te denken binnen ondernemingen en wordt alsmaar belangrijker. Dit werd ook bevestigd door alle deelnemende respondenten. Uit de interviews konden hiervoor verschillende verklaringen worden afgeleid. Ten eerste zijn de cyberrisico's er altijd al geweest. Zodra een onderneming een website of een e-mailserver en dergelijke heeft, is ze immers kwetsbaar voor aanvallen maar de laatste jaren ziet men het aantal cyberaanvallen exponentieel toenemen. Dit onder andere doordat we steeds meer afhankelijk worden van IT, wat opportuniteiten creëert voor cybercriminelen. Systemen worden wel veiliger, maar de mens blijft de zwakste schakel en hackers blijven innoveren en nieuwe manieren vinden om systemen binnen te dringen.

> *"Als ik zie, de laatste vijf/zes jaren, de risico's zijn er al altijd geweest. Het komt alleen meer in de media vandaag, maar de gevaren die ken ik al een aantal jaren." (C1)*

> *"Vanaf het moment dat ze een computer hebben, een website een e-mailadres komen ze er eigenlijk mee in aanraking." (E1)*

> *"Ja, maar ik weet niet omdat het omwille van COVID en thuiswerken is maar we zien bijna een exponentiële stijging. Het is echt een enorm probleem en als je van die research leest over incidenten dan ga je zien dat er altijd een stijgende trend in zit." (G1)*

> *"Binnen onze sector, wordt de afhankelijkheid van IT alsmaar belangrijker." (F1)*

> *"Daarnaast is er ook natuurlijk het feit dat er zeer veel technologie wordt geïmplementeerd binnen organisaties. Technologie is allemaal geconnecteerd met internet wat uiteindelijk maakt dat uw aanvalsbasis, van een hacker tegen uw organisatie, alleen maar groter wordt." (A1)*

> *"De systemen worden wel veiliger, maar de mens blijft de zwakke schakel" (F2)*

> *"Het gebruik van internet, computers, Cloud neemt alleen maar toe. Dus ook de criminaliteit op de platformen neemt alleen maar toe en de aanvallen worden steeds hardnekkiger en steeds inventiever" (H1)*

Ten tweede uit het belang aan *cybersecurity* zich ook op de markten zelf. Uit de interviews is gebleken dat meer en meer ondernemingen een bepaald niveau van *cybersecurity* eisen vooraleer ze gaan samenwerken met andere partijen en hen dus toegang verlenen tot hun systemen. Er worden dan meestal bepaalde attesteringen of certificaten gevraagd waarmee bedrijven kunnen aantonen dat ze aandacht besteden aan hun cyberrisico's. Met het aantal cyberincidenten vandaag de dag en de opkomst van *supply chain attacks* gaan ondernemingen zich op deze manier beter proberen te beschermen. Dit in combinatie met de aandacht voor cyberincidenten in de media onder andere heeft ook positieve effecten. Ondernemingen gaan hierdoor meer aandacht besteden aan *cybersecurity* en de cyber- en IT risico's serieus nemen.

> *"We zien vaak, kleinere bedrijven als die nu voor een groot willen werken. De grote beginnen meer en meer due diligence te doen van hun leveranciers. Dus die zeggen 'Ja wij willen wel met je werken maar vooraleer dat wij je gaan toelaten je te connecteren op onze netwerken en systemen willen wij bepaalde garanties'." (G1)*

> *"Ik heb bij mijn vorige job ISO 27001 geïmplementeerd en we zijn dan gecertifieerd geraakt. Daar moest dat omdat onze klanten dat vroegen. De klanten, grote multinationals, die zeiden 'als je niet kan aantonen dat je ISO 27001 certified bent, werken we niet meer samen met jou.'" (C1)*

> *"Wij zijn ook al niet meer de enige partij waar dat ze mee samen werken die ernaar beginnen vragen. We zien daar zelf ook banken en andere belangrijke stakeholders die met die bedrijven werken, die vragen ook gewoon bepaalde attesteringen. 'Wij vertrouwen heel veel informatie aan jullie toe, dat is een groot risico. Jullie moeten kunnen aantonen aan ons dat je aan dat risico iets gedaan hebt.'" (E1)*

> *"Er is ook meer afhankelijkheid van derde partijen" (F1)*

Tot slot gaf de meerderheid van de respondenten aan dat steeds meer regel- en wetgeving het topic van *cybersecurity* aankaart. Regulatoren proberen hiermee het belang van *cybersecurity* te benadrukken en bedrijven in de juiste richting te duwen. In de financiële sector zien we bijvoorbeeld NIS. Respondent A1 verduidelijkte dat NIS eigenlijk gaat over het beschermen van essentiële functies en operatoren van essentiële diensten tegen cyberaanvallen. Het is een wettelijk kader dat geschept is voor enkele kritische sectoren. Aangezien er veel kritiek was op NIS, wordt er gewerkt aan een nieuwe versie van NIS die waarschijnlijk binnenkort op de markt zal komen. Daarnaast is er sinds 2018 van Europa uit de GDPR of de Algemene Verordening Gegevensbescherming om de gegevens van Europese burgers te beschermen.

> *"Een derde reden van groeien aan belang is ook zeker het online gedeelte dus er wordt meer wet- en regelgeving gemaakt richting cybersecurity natuurlijk omdat de regulators het nodig vinden." (A1)*

> *"Cybersecurity wordt nu meer en meer gelinkt ook met GDPR" (B1)*

> *"Binnenkort treedt een nieuwe, de vernieuwde NIS richtlijn, in werking en ik begrijp dat dat bijzonder systeem van kracht zou blijven." (D2)*

"Je hebt dus die ene richtlijn. Als je op internet kijkt dan zie je dat er ook meteen nadat deze in voegen was, dat er al veel kritiek was. Vandaar dat er zo snel die NIS 2 is gekomen, die van toepassing is op 2024." (D1)

1.2 COVID-19 en thuiswerken

Meer dan de helft van de respondenten gaf aan dat de COVID-19 crisis en bijgevolg het thuiswerken een uitdaging hebben gevormd het afgelopen jaar. Zo legden respondenten C1, E1 en F3 verder uit dat met het thuiswerken iedereen digitaal overal moet aankunnen op elk moment en dat ondernemingen zich dus heel flexibel hebben moeten opstellen om de nodige infrastructuren op te zetten. Dit maakt natuurlijk ook dat bedrijven kwetsbaarder zijn geworden. De aanvalsbasis is nu immers groter. Respondent F2 en G1 gaven hier als voorbeeld dat mensen door het feit dat ze thuiswerken ook het bedrijfsnetwerk kunnen besmetten via hun computer thuis. Als je inlogt op het netwerk van je onderneming met een eigen computer en die is gehackt geweest zonder dat je het weet, kunnen cybercriminelen zo het netwerk van je onderneming binnendringen. Het aantal work-from-home infrastructuren heeft het dus af en toe wat vergemakkelijkt voor cybercriminelen. Respondent F3 vulde hier nog op aan dat thuiswerken er is om te blijven en dat we ons dus moeten aanpassen.

"Door corona is het wel zo dat er een nieuwe uitdaging komt en dat is dat er veel meer mensen van thuis werken. Je moet dus niet alleen in de hand houden wat er tussen de vier muren van je bedrijf gebeurt, maar dat je ook in de hand moet houden wat er daarbuiten gebeurt." (C1)

"Iedereen moet overal digitaal aankunnen op elk moment en we zijn dus eigenlijk heel flexibel geworden maar ook veel kwetsbaarder voor aanvallen van buitenaf" (E1)

"Verandering zorgt voor security issues, zeker bij IT, dus de attack surface is toegenomen met thuiswerken." (F3)

"Het aantal cyberaanvallen neemt toe en het thuiswerken heeft het af en toe voor hackers vergemakkelijkt." (G1)

Verschillende respondenten haalden ook aan dat COVID-19 werd gebruikt als pretext voor cyberaanvallen. Zo zijn er bijvoorbeeld tal van *phishing* mails verstuurd die corona als dekmantel gebruikten. Een belangrijke nuance volgens respondent F3 hierbij is dat COVID-19 maar een klein onderdeel is van alle *phishing* mails die gestuurd worden, maar omdat het zo relevant is en nog zo onbekend voor velen, is dit een van de meest succesvolle manieren geweest om mensen toch te doen klikken. Daarnaast verduidelijkte respondent E1 ook dat bepaalde controles tijdens het coronatijdperk zijn weggevallen. Zo was er bijvoorbeeld minder sociale controle wat heeft bijgedragen aan het feit dat er sneller op *phishing* links werd geklikt.

"Vorig jaar in april hebben wij op een bepaald moment vastgesteld dat er op twee weken tijd 50000 domain names geregistreerd waren die verband hielden met COVID. Dus hackers hebben enorm geprobeerd om daarop in te spelen: verkoop van mondmaskers, verkoop van ontsmettende gel… allemaal fake sites om te proberen aan je user-ID en login te komen en proberen op verwarring in te spelen om toch maar credentials te harvesten." (G1)

Of COVID-19 in het algemeen de oorzaak is geweest voor de exponentiële toename in cyberdreigingen, daar is men niet zeker over. De meningen zijn wat verdeeld. Zo wees respondent F1 op het feit dat er een toename van cyberdreigingen is geweest, vooral tijdens COVID-19 crisis, maar deze hebben niet geleid tot een hoger aantal incidenten. Volgens respondent F1 is er dus geen aanleiding om te denken dat aanvallen meer gesofisticeerd zijn geworden tijdens de COVID-crisis. Respondent A2 sloot zich hier deels bij aan en legde uit dat door COVID-19 bepaalde vormen van cybercriminaliteit exponentieel zijn toegenomen. Ook respondenten F2 en F3 legden uit dat er een verschuiving te zien is, maar maakten duidelijk dat de toename van cyberdreigingen die COVID-19 als pretext gebruiken maar een klein aandeel is van het totaal. Respondent G1 daarentegen gaf aan dat het onduidelijk blijft of de toename van cyberdreigingen te wijten is aan COVID-19.

"Ja, maar ik weet niet omdat het omwille van COVID en thuiswerken is maar we zien bijna een exponentiële stijging." (G1)

"Ja ik denk zeker door de coronacrisis en het thuiswerken een bepaalde vormen van cybercriminaliteit exponentieel zijn toegenomen" (A2)

2 Cybercriminaliteit

2.1 threat actors

Er zijn verschillende soorten cybercriminelen, ook wel threat actors genoemd, waar ondernemingen vandaag de dag mee geconfronteerd worden. Uit de interviews kwam naar voren dat deze opgedeeld kunnen worden in vijf groepen. Al deze groepen hebben verschillende capaciteiten en verschillende doelen voor ogen. Ten eerste zijn er *nation state actors* of NSA. Een NSA gaat in een netwerk proberen dringen en proberen ongedectecteerd te blijven. *Nation state actors* gaan meestal op zoek naar gevoelige informatie en worden vervolgens vooral ingezet voor industriële spionage. Verder heb je de *organised crime groups* (OCG). Enkele respondenten gaven aan dat OCG eerder gaan hacken om zelf geld te verdienen. Dat is hun grootste drijver. Een OGC gaat daarom bijna altijd *ransomware* uitvoeren. Respondenten I1 en F2 geven hier ook aan dat deze groepen en hun aanvallen het meest in de media komen omdat OCG meestal grote campagnes doen en het kan deze groepen ook niet veel schelen dat ze gedetecteerd zijn. Hun doel is immers geld verdienen.

"Er zijn verschillende soorten threat actors. Je hebt nation state actors, nation sponsored actors. Dan heb je OCG (Organised Crime Groups). Die gaan het meeste ransomware doen. Dan heb je kleinere groepen of individuele hackers. En tot slot heb je ook hacktivisten. Dat zijn dus activisten die hacken voor de natuur of voor bepaalde financiële onafhankelijkheid." (F2)

"Wij hebben bijvoorbeeld ook bij een bedrijf gewerkt, een heel groot ransomware incident, waar dat we niet weten wie erachter zat maar je kan ook niet uitsluiten dat daar een nation state achter zat die eerst industriële spionage gedaan heeft en dan vervolgens zelf de ransomware losgelaten heeft of de manier om binnen te raken doorverkocht heeft op the dark web zodanig dat iemand anders de ransomware heeft losgelaten." (G1)

"Hackers die proberen eigenlijk non-stop aan te loggen op je omgeving. Ik ben dat eens een tijd geleden gaan bekijken. Ik weet niet meer exact hoeveel dat we er hadden, maar we hadden

dagelijks ik denk een 30-tal log-ons buiten Europa, failed log-ons, op onze omgeving. Dat zijn geen mensen van onze onderneming, dat zijn gewoon organisaties, ook zelfs geen mensen, computers die trachten aan te loggen." (C1)

"Passief wil eigenlijk zeggen dat ze echt onopgemerkt willen blijven, onder de radar willen blijven, en iets heel belangrijk mis willen doen natuurlijk. Als ze uiteindelijk met je company secrets gaan lopen zonder dat je het weet, dat is natuurlijk een ramp omdat ze in je productieproces zitten of ik zeg maar iets in een productieproces knoeien met de parameters van een productielijn ofzo en hetgeen dat je produceert is daardoor niet goed. Dat is natuurlijk rampzalig en dat zijn allemaal cyberaanvallen die onder de radar blijven en die je soms pas na twee jaren ontdekt. Dat zijn volgens mij de gevaarlijkste." (A1)

"Er zijn verschillende types van bedreigingen en van personen die erachter zitten. Alles hangt ervan af wat de bedoeling is van de hacker. Zijn ze erop uit om bepaalde informatie van een bepaald bedrijf te gaan halen en zijn ze dan nog eens gesponsord door een of andere overheid? Ja dan zijn de middelen quasi ongelimiteerd en dan zullen ze er wel op een of andere manier in slagen om die informatie te achterhalen. Al dan niet via hacking samen met het laten rekruteren van bepaalde mensen om middelen in die organisatie te zetten." (A2)

Een derde soort van *threat actor* is de individuele hacker. Dit kan iedereen zijn aangezien je vandaag de dag niet veel nodig hebt om een hacker te worden. Alles is beschikbaar op *the dark web*. Zo zijn er cybercriminelen die tools maken en verder verkopen als een *service* op *the dark web* en anderen die zelf aanvallen uitvoeren. Cybercriminaliteit is als het ware uitgegroeid tot een hele industrie. De volgende soort van *threat actor* wordt een hacktivist genoemd. Dit zijn volgens respondent F2 activisten die hacken voor de natuur of voor bepaalde financiële onafhankelijkheid. Een voorbeeld hiervan is Anonymous. Dit internationaal collectief is gekend voor haar cyberaanvallen op grote bedrijven en verschillende overheden wereldwijd. Een hacktivist gaat met andere woorden hacken om bepaalde informatie te stelen of netwerken plat te leggen uit protest. Hacktivisten kunnen bijvoorbeeld politieke motivaties hebben en het publiek bewust willen maken van geheimen die de overheden achterhouden. Ze zijn meestal erg gedreven door hun doel maar hun capaciteiten zijn laag. Ze zullen misschien een DDoS doen of een website *defacement*. Tot slot haalden respondenten F2 en F3 nog een laatste soort aan, namelijk de *ethical hackers*. Deze worden ook wel *white hats* genoemd en dat zijn hackers of computerbeveiligingsexperts die gespecialiseerd zijn in penetratietesten. E*thical hackers* gaan effectief aanvallen uitvoeren op organisaties om hun zwakheden bloot te leggen. Op deze manier kunnen ondernemingen de veiligheid van hun informatiesystemen verbeteren.

"Als je vandaag geld wilt verdienen dan kan je in elk land ter wereld iedereen gaan aanvallen. Je kan 16 jaar zijn en niks voorstellen op straat, geen stoere jongen of meisje. Je moet gewoon wat kennen van code en dan ben je vertrokken." (C1)

"Er wordt heel veel zelf gemaakt, dat gaat over honderden tools maar misschien in die context nog wel vermelden dat dat eigenlijk een industrie is he cybercriminaliteit. Je moet niet persé zelf een tool maken, je kan er downloaden en dergelijke meer. Maar je kan eigenlijk zelf ook gehackte systemen kopen en dat je bij voorbeeld zegt 'oké ik koop nu 100 gehackte systemen en met die

100 gehackte systemen doe ik nu een aanval richting dat bedrijf'. Ja kan dat gewoon op de zwarte markt kopen." (A1)

"Dus ja, daar zit echt een industrie achter. Af en toe boeken de gerechtelijke diensten wel eens een overwinning maar het is een gigantisch probleem. Ik heb ooit statistieken gelezen dat het groter is dan drugs en dat het de 4de grootste economie in de wereld zou zijn." (G1)

"Je hebt nu zelfs op het internet ransomware as service dus bedrijven die zich helemaal gespecialiseerd hebben zowel in de software als de infrastructuur en zij nemen uiteindelijk van wat er wordt betaald een steek op fee basis." (D1)

De meerderheid van de respondenten vertelde ook dat het aantal *threat actors* blijft toenemen, maar dat de grootste uitdaging nog altijd de OCG en NSA zijn. Het vergt immers tijd vooraleer *threat actors* gedetecteerd worden en uit het systeem gedreven kunnen worden. Respondent A1 benadrukte dit hierboven ook al en zei dat het jaren kan duren voordat men hackers in het systeem opmerkt. Daarnaast haalde zowel respondent F1 als F2 hierbij het voorbeeld van SolarWind aan waarvan een *supply chain attack* minstens een half jaar ongedetecteerd is gebleven.

2.2 Meest gebruikte middelen en methoden

Respondenten zijn het erover eens dat *malware* en *ransomware* tegenwoordig de grootste problemen vormen voor ondernemingen. Hackers gebruiken vaak *phishing* of *supply chain attacks* om netwerken binnen te dringen en de *malware* of *ransomware* uit te voeren. *Phishing* is een van de meest gebruikte manieren om bedrijven te infiltreren en ook door zo goed als iedereen gekend. Respondent F1 vertelde hierbij ook dat er steeds nieuwe vormen van *phishing* optreden. Zo is er nu ook *spear phishing* en CEO- of CIO-phishing. Bij dit laatste voorbeeld gaan hackers proberen een *high impact target* te isoleren. *Spear phishing* werkt gelijkaardig, alleen tracht men hier geen individu te isoleren maar een hele organisatie. Dit benadrukt nog maar eens dat cybercriminelen blijven innoveren en creatiever worden. *Supply chain attacks* daarentegen zijn nu vooral aan het opkomen. Dit zijn aanvallen waarbij hackers bedrijven infiltreren die software leveren aan anderen. De opkomst van *supply chain attacks* verklaart waarom veel ondernemingen nu ook meer aandacht gaan besteden aan dat *third party* risico. Respondenten A2, G1 en F3 benadrukten hierbij dat *supply chain attacks* en *ransomware* niet noodzakelijk losstaan van elkaar. Meer concreet, s*upply chain attacks* zijn een manier waarop cybercriminelen toegang krijgen tot hun doelwit en *ransomware* is dan meer het doel dat ze voor ogen hebben. Dit doel is geld verdienen. Dezelfde analogie geldt voor *phishing* en *ransomware*.

"Ook in de rapporten van CCB, Cert en Safeonweb, zal je zien dat phishing een heel belangrijke methode is. Ook ransomware die via mail verspreid wordt is een grote boosdoener…" (H1)

"Zodra dat men ergens een zwak punt vindt dan gaat het denk ik bijna altijd over malware gaan, die zich gaat nestelen en op een gegeven moment gaat activeren als een soort van ransomware." (C1)

"De grootste schadepost en de meest gebruikte manier is phishing via mail. Er zijn zelfs technieken om zonder te klikken binnen te raken, ze noemen dat zero-click spyware." (D1)

"Ransomware is één van… momenteel eigenlijk het grootste probleem. Nu, je ziet daar ook trends in. In het begin was het ja echt de data encrypteren. Nu proberen ze eerst de data te stelen en dat is ook om je onder druk te zetten om te betalen anders dreigen ze je data te publiceren." (G1)

"Nog iets wat we heel hard zien opkomen, is ransomware." (F2)

"Ja dat zijn echt de klassiekers en ze horen ook voor een stuk samen, want phishing maakt ook heel vaak gebruik van malware. Op een bepaald moment ga je op een link klikken en geef je toegang tot je systeem en kunnen ze bepaalde informatie van je achterhalen en gaan misbruiken om je te benaderen, om bepaalde contacten te leggen of om bepaalde vragen te stellen. Of rechtstreeks natuurlijk om informatie te gaan stelen." (A2)

Hoewel er af en toe enkele zeer grote ransomware groepen worden opgedoekt, zien respondenten dat anderen heel snel die plaats innemen. Het is met andere woorden moeilijk onder controle te houden en bedrijven moeten zich daarom ook gaan beveiligen.

3 Beschermen tegen cyberdreigingen

3.1 Raamwerken

Hoe beschermen ondernemingen zich nu het best tegen al deze cyberrisico's? Er zijn verschillende manieren waarop ondernemingen dit kunnen doen. Veel respondenten verwezen naar het nut van bestaande raamwerken zoals NIST CSF, COBIT, ITIL, de ISO standaarden,… Respondenten gaven aan dat raamwerken structuur bieden en richting geven. In België zal je echter niet veel *cybersecurity* raamwerken tegenkomen. Dit heeft te maken met het feit dat het ondernemingslandschap in België hoofdzakelijk uit KMO's bestaat. Daarnaast zien respondenten dat er een lage maturiteit is in België. Maturiteit houdt in dat een onderneming begrijpt wat raamwerken en de gevaren omtrent *cybersecurity* zijn en dat een onderneming ook een management heeft dat dit allemaal begrijpt. Zoals de meerderheid van de respondenten ook uitlegde, is deze lage maturiteit te verklaren door het feit dat KMO's niet de middelen en het geld hebben om grote raamwerken te implementeren.

"Ik vind het heel goed om frameworks te volgen, maar ook weer daar, als je niet matuur bent dan is zo een framework onbegonnen werk. Je kan daar dan niet aan uit. Je hebt daar de middelen niet voor, je snapt daar het nut niet van en daar heb je het geld ook niet voor." (C1)

"Er is weinig geweten van geïmplementeerde frameworks in België. 99% van bedrijven is KMO, met een zeer beperkt gebruik van frameworks, zoals we gemerkt hebben in contact met de verschillende organisaties en regios (VL/Wall/Brussel)…" (H1)

"Dus ik zie heel weinig bedrijven cybersecurity transformatieprocessen opzetten. Die krijgen daar heel moeilijk budgetten voor los tot als er eens een incident gebeurt dan wordt er over kosten niet meer gediscussieerd en wordt er ineens een veelvoud gespendeerd. Maar ja de maturiteit blijft vaak nog laag." (G1)

"En ik denk zeker in België dat de bedrijven echt nog niet genoeg bezig zijn met die dreiging. We zijn daar een beetje naïef in." (A2)

"Ik denk als je gewoon nog maar België bekijkt en je zou een gemiddeld maturiteitsniveau van cybersecurity nemen. Gemiddeld dus als 0 het minste is en 100 het maximum. Als je dan gaat kijken hoeveel mensen er op die 50 zitten, dat zijn er volgens mij heel weinig in België omdat er nog altijd niet genoeg begrip van is. Waarom is dat ook vaak? De grotere bedrijven die gaan daar heel goed in mee zijn, want die hebben geld om IT-managers in dienst te nemen en om mensen aan te nemen die kennis hebben. Kleinere bedrijven hebben gewoon de middelen niet om daar in die mate mee bezig te zijn." (C1)

Het werd al snel duidelijk dat *cybersecurity* raamwerken bij veel ondernemingen niet geïmplementeerd kunnen worden omdat niet voldaan is aan de basisvereisten voor het implementeren van dergelijke raamwerken. Vooraleer ondernemingen iets aan hun *cybersecurity* kunnen gaan doen, is het volgens respondenten belangrijk dat er een zekere maturiteit is. Dit gaat gepaard met *awareness* omtrent cyberrisico's. Ondernemingen die het nut van *cybersecurity* niet inzien, gaan ook niet begrijpen dat ze daar aandacht aan moeten besteden. Eens dat die maturiteit er is en de gehele onderneming het belang van *cybersecurity* inziet dan kan er iets aan gedaan worden. Naast die maturiteit zijn er nog enkele basisvereisten vooraleer we bij de grote raamwerken uitkomen. Respondenten gaven aan dat het belangrijk is voor ondernemingen om enkele basisstappen te nemen. Zo noemde respondent G1 dit *getting the basics right*. Respondent C1 vulde hier nog op aan dat als je de basis niet mee hebt je geen verdere stappen kan ondernemen. Je infrastructuur en processen moeten georganiseerd zijn vooraleer je bijvoorbeeld NIST gaat implementeren.

Een eerste stap die ondernemingen moeten nemen, is de inventarisatie van hardware en software. Ondernemingen moeten weten wat ze in huis hebben om te weten wat ze moeten beschermen. Een ISO 27001 en ISO 27002 standaard of bijvoorbeeld de top 20 CSC kunnen volgens respondenten C1 en G1 ondernemingen hierbij sturen. Beiden standaarden geven goed aan dat de inventarisatie de eerste stap is voor ondernemingen.

"Start al eens met inventariseren van alles wat je hebt in je bedrijf van IT materiaal. Als je niet weet wat je hebt dan weet je ook niet wat je moet/kunt beveiligen." (C1)

"Daarom ook in de top 20, nummer 1 is een inventaris van je hardware, nummer 2 is een inventaris van je software. Als je geen volledig zicht hebt op je hardware en software dan moet je ook niet dromen dat je ze kan beschermen tegen aanvallen. Daar begint het." (G1)

Wanneer je als onderneming op hoogte bent van wat je in huis hebt, is het ook belangrijk om te gaan kijken of je computers nog up-to-date zijn. Zo gaven respondenten aan dat oudere besturingssystemen kwetsbaar zijn. Het is met andere woorden nodig om je hardware en software tijdig te vernieuwen. Respondent C1 duidde hierbij nog eens het belang aan door het voorbeeld van WannaCry aan te halen. WannaCry is een *ransomware* hacker die een paar jaar geleden actief was. Deze maakte gebruik van een fout (Eternalblue) in Windows om systemen binnen te dringen. Deze fout is ondertussen uit de nieuwe besturingssystemen van Windows gehaald, maar benadrukt het belang van deze stap.

"We hadden heel wat oude hardware. Dat hebben we dan ook gezien met die WannaCry aanval, die is ook al die oude hardware gaan aanvallen dus reden te meer om te vernieuwen." (C1)

"De meer traditionele bedrijven zitten vaak nog met oudere infrastructuur en zijn dus kwetsbaarder. Er is dan ook enorme druk om te innoveren." (F1)

"Want het was ook, ze hadden nog bepaalde pc's die nog op Windows XP draaiden waarvan je zegt 'daar beginnen we zelfs niet aan'. Maar bij Windows 2007 dachten wij ook te zeggen van 'komaan mannen dat doen we niet meer'." (G1)

Als je die basis mee hebt dan kan je pas verder gaan. Respondenten A1, B1 en I1 gaven hier ook aan dat je er als onderneming vanuit moet gaan dat je gehackt zal worden. Je moet daarop voorbereid zijn. Je moet dus risico's kunnen identificeren en je moet proactief beveiligen. Dit laatste slaat bijvoorbeeld ook op het trainen van je werknemers, een klassieke antivirus installeren, een goede firewall hebben, regelmatige back-ups… Alle respondenten gaven ook aan dat je daarom als onderneming gericht moet gaan werken. Je kan onmogelijk alles volledig beveiligen en je moet dus rekening houden met de eigenheid van je onderneming. Respondent C1 gaf hier als voorbeeld dat een fruitveiling niet veel gevoelige informatie heeft. Het gevaar is daar vooral wanneer hackers het productieproces kunnen bevuilen of stilleggen. Een advocatenkantoor daarentegen heeft wel veel gevoelige informatie. Zij heeft de verantwoordelijkheid om die informatie van haar klanten te beschermen. Je moet dus goed de gevaren begrijpen.

"Ervaring leert me dat je het beste ervan uit kunt gaan dat je gehackt wordt en dat je ermee moet kunnen omgaan in de situatie als je gehackt wordt. Dus daarop voorbereid zijn." (A1)

"Dus heel gericht te werk gaan in plaats van proberen alles 100% waterdicht te krijgen. Dat is gewoon onmogelijk. Gaan werken met één systeem dat extreem beveiligd is voor bepaalde types informatie." (A2)

"Je moet altijd gaan kijken naar wat zijn de gouden eieren die je wilt gaan beschermen." (C1)

Daarnaast moet je ook een plan hebben om te reageren op een aanval en tot slot moet er dan ook een herstelplan opgesteld zijn. Respondenten gaven hierbij aan dat ondernemingen het evenredigheidprincipe moeten respecteren. Je moet niet gaan beveiligen om te gaan beveiligen of *policies* blijven opstellen. Alles wat je implementeert of opzet moet met andere woorden evenredig zijn met je risico's.

Dus dat is de basisregel van risicobeheersing. Je mag eigenlijk nooit meer investeren dan het risico dat je loopt. (B1)

"…et un principe de proportionnalité qui est prévu c'est-à-dire que plus on est grand, plus q'on a des activités risquées ou complexes, plus il faut évidemment respecter une règle, c'est un principe classique en alimentation financière." (D3)

"Maar de maatregelen die ze treffen moeten proportioneel zijn met het risico dat ze lopen. De kaders moeten daarom gebaseerd zijn op het evenredigheidsprincipe." (F1)

"Het is heel belangrijk dat je het proportionaliteitsprincipe respecteert en het aanpast aan je organisatie. En sommige raamwerken zijn waarschijnlijk meer geschikt voor grotere ondernemingen en anderen meer voor kleinere." (G1)

3.2 De rol van audit

Het is belangrijk dat alle personen in een onderneming hun rol zo goed mogelijk gaan vervullen om cyberrisico's te leren beheersen. Dit betreft niet alleen het topmanagement en de IT managers die deze basisstappen moeten nemen, alle werknemers zijn betrokken in dit cyberverhaal. Zoals eerder werd besproken in het drie lijnen model, heeft de audit functie ook een belangrijke verantwoordelijkheid. Zowel interne als externe audit dragen bij aan een effectieve *corporate governance*. Echter zal je deze enkel tegenkomen in grote ondernemingen. KMO's daarentegen komen vaak niet in aanraking met de audit functie

3.2.1 De interne audit

De interne audit is volgens respondenten een belangrijke drijver voor *cybersecurity*. Zij staat namelijk in voor het communiceren van cyberrisico's naar het auditcomité en de raad van bestuur op een onafhankelijke wijze. Respondent A1 verduidelijkte dit door te zeggen dat de interne audit vaak zal moeten gaan uitzoeken of een onderneming haar cyberrisico wel degelijk onder controle heeft. Daarnaast benadrukte ook respondent F1 het belang van de interne audit door het drie lijnen model van verdediging aan te halen. Volgens respondent F1 moet er voldoende uitdaging zijn binnen de drie lijnen. De interne audit heeft volgens deze respondent dus een cruciale rol in het cyberverhaal. Zowel respondent A2 als G1 vertelden dat de interne audit in haar rol ook IT en *cybersecurity* audits moet laten uitvoeren. Hier nuanceerde respondent A2 dat de interne audit zich hiervoor best laat bijstaan door experts. Een interne auditor moet immers alles kunnen auditeren van business processen tot IT en veel interne auditors zitten niet specifiek in dat IT domein. Respondent A1 benadrukte hierbij dat een interne auditor met IT kennis een toegevoegde waarde kan zijn en al sneller de brug naar *cybersecurity* kan maken.

> *"De rol van een interne auditor, die doet wat aan risicobeheer. Het is aan hem om op een onafhankelijke wijze aan het auditcomité en een raad van bestuur te rapporteren over de stand van zaken van cybersecurity in een organisatie. Dat is vaak een heel belangrijke drijver" (A1)*

> *"Nu, een organisatie met een zekere maturiteit heeft een interne audit afdeling en ja dan vind ik dat die ook wel zeker eens al IT audits moeten doen en ook eens gaan kijken naar cybersecurity." (G1)*

> *"Als je een interne audit hebt dan kunnen die mee gaan kijken of dat de personen die verantwoordelijk zijn voor cyber, die een aantal richtlijnen en een aantal guidances volgen voor de beveiliging, dan kunnen die gaan nakijken of dat effectief gebeurt en dat heeft wel een meerwaarde aan zich. Maar meestal, ofwel werken ze met gespecialiseerde mensen en kunnen ze echt gaan kijken of je beveiliging toch op zekere hoogte waterdicht is ofwel is het weeral afvinken van een aantal checklist om jezelf dan een medaille te geven en te zeggen we zijn goed bezig terwijl dat dat misschien niet altijd het geval is." (A2)*

> *"We kijken dus of het 3 Lines of Defence (LoD) model correct werkt. Dat de 1e LoD, die eigenaar is van de controlemaatregelen, voldoende in vraag wordt gesteld door de 2e LoD (risicomanagement en controle), en dat de 3e LoD (Interne Audit) een voldoende onafhankelijke review doet van de controlemaatregelen en het risicobeheersingsmodel." (F1)*

3.2.2 De externe audit

De meerderheid van de respondenten gaf aan dat ook de externe audit een belangrijke rol speelt in het cyberverhaal. Bedrijfsrevisoren nemen dit mee in hun *assurance*. Het is immers hun taak om de risicoanalyse van hun klanten zo correct mogelijk te doen. Respondent E1 ging hier nog op verder en vertelde dat een externe auditor ervoor moet zorgen dat zijn klanten de cyberrisico's kennen en er ook iets mee gaan doen. Afhankelijk van de sector en de grootte van het bedrijf wordt daar meer aandacht aan besteed. Bij kleine ondernemingen bijvoorbeeld is dit eerder een kleine check. Volgens respondenten A2 en E1 moet er een stap verder worden gegaan bij ondernemingen die werken op basis van technologie. Een voorbeeld hiervan is een onderneming die databanken beheert die gevoelige data bevatten. Wanneer zo een onderneming niet bezig is met *cybersecurity* dan kan ook de jaarrekening niet goedgekeurd worden. Als er mogelijk iets zou gebeuren met die databanken dan kan dat immers zo een impact hebben dat de continuïteit van die onderneming in het gedrang gebracht wordt. Daar moeten bedrijfsrevisoren dan ook een stap verder gaan. Er wordt in dat geval een externe *cybersecurity* audit besteld.

> *"Een externe audit, het aandeel daar is, zij moeten daar uiteindelijk ook aandacht aan besteden, zaken afstemmen, financiële gegevens… Zij gaan dat onder de aandacht brengen en meenemen in hun assurance." (A1)*

> *"Ik vind het heel positief dat ze dat meenemen in een audit, want dat rapport gaat ook naar je aandeelhouders. Dat maakt ook dat die mensen ook wel wat op de hoogte zijn. Dat betekent ook dat dat binnen het bedrijf, doorheen heel het bedrijf, een belangrijk onderwerp is." (C1)*

> *"Wij zijn externe auditors en heel onze audit gebeurt eigenlijk ook vanuit risicoanalyse. Het is onze taak eigenlijk om die risicoanalyse zo correct mogelijk te doen en de topic cybersecurity die komt naar voren. 10 jaar geleden was dat eigenlijk nooit een risico en nooit een topic die naar boven zou zijn gekomen, nu moet je het in elk bedrijf hebben uitgesproken." (E1)*

> *"Externe audit, afhankelijk van het type bedrijf zal externe audit ook een rol moeten spelen daarin. Bedrijven die echt werken op basis van technologie die zullen natuurlijk moeten zien dat ze heel goed beveiligd zijn want anders kan dat een enorme impact hebben op de werking en de continuïteit van het bedrijf." (A2)*

3.2.3 De waarde van certificaten

Er bestaan verschillende certificaten die auditors kunnen behalen om zich meer te specialiseren op vlak van IT en *cybersecurity*. Maar wat zijn deze certificaten nu waard? Respondenten hebben hier verschillende meningen over. Respondenten A1 en C1 zien een certificaat zoals CISA en CPA als een meerwaarde. Daar tegenover staan respondenten G1 en E1 die daar niet veel toegevoegde waarde in zien. Ze redeneren namelijk dat een certificaat zoals CISA makkelijk te halen is op het internet. Je moet als auditor maar een dag leren en je kan dan dat examen online afleggen. Wanneer je dat certificaat hebt gehaald, ben je in theorie in staat om een ISO 27001 audit te doen. Respondent C1 gaf hier wel een belangrijke nuance door te zeggen dat een CISA een mooie basis geeft. Het is een certificaat dat je in staat stelt om de terminologie en belangrijkste concepten te leren, maar het blijft een basis. Respondenten G1 en E1 gaven ook aan dat je tegenwoordig kritisch moet omgaan met certificaten. Er is namelijk zo een wildgroei aan certificaten dat het moeilijk is om te onderscheiden

welke nu daadwerkelijk gewicht hebben. E1 haalde hierbij aan dat de overheid hier duidelijkheid zou kunnen scheppen door een lijst met waardevolle certificaten te publiceren. Dat hoeft geen exhaustieve lijst te zijn. Er kunnen bijvoorbeeld nieuwe certificaten bijkomen, maar het zou voor auditors een meerwaarde zijn om hier meer duidelijkheid over te krijgen.

"*Ja uiteraard! Maar ervaring leert me dat er heel weinig interne auditors zijn die specifiek op dat domein zitten." (A1)*

"Nee (lacht). Om het even welke online cursus dat jij vandaag gaat volgen daar geven ze een certificaat. Dus er zijn maar een handvol certificaten waar dat ik aandacht aan besteed. Waarvan ik weet dat die echt moeilijk zijn om te halen en die hebben echt een zeker gewicht en al de rest is rommel. Een CISSP heeft nog wel een zeker gewicht en wij hebben ook een groot team van pen testers en in die wereld zijn er ook bepaalde certificaten die een stuk meer gewicht hebben dan anderen. Maar certificaten vindt je overal en het is heel moeilijk om het kaf van het koren te scheiden." (G1)

"Die CISA, SCI… op den duur weet je ook al niet meer waarover het gaat en het is voor vele aanbieders van die certificaten al een sport geworden om zoveel mogelijk van die erkenningen te hebben. De vraag is: wat is het waard? Dat zijn ook examens die je kan doen.. ik kan daar morgen aan beginnen he, ik kan dat examen online afleggen en als ik het juist heb ingevuld dan krijg ik mijn certificaat en zou ik zogezegd capabel zijn om die audit te gaan doen. Ik geloof dat niet. Dus is die meerwaarde er? Dat zou kunnen. Het geeft een kader en het zou kwaliteit moeten waarborgen, maar de wildgroei aan verschillende kanalen die dat kunnen doen, schept gewoon ook heel veel onduidelijkheid over de effectieve kwaliteit erachter " (E1)

"Ja absoluut! Een mooie basis, zo een CISA. Een mooie basis dat moet niet echt doorgedreven zijn. Dat is zeker, ook voor die mensen zelf. Als auditor, krijg je ineens een heel ander profiel. Je kan plots misschien ook ISO 27001 audits gaan doen he. Dus ja, toch zeker een goeie basiskennis en inderdaad als je een certificaat daarachter kan steken, nog beter." (C1)

4 De financiële sector

Opvallend wordt er binnen de financiële sector meer aandacht besteed aan cyberrisico's. Dit is deels te verklaren door de nationale autoriteiten. Binnen de financiële sector wordt er namelijk toezicht gehouden door de FSMA en de Nationale Bank van België (NBB). Daarnaast heb je de *Center for Cybersecurity Belgium* (CCB) en deze heeft een coördinerende rol. Respondenten D3, F2, F3 en I1 vertelden dat de wet- en regelgeving binnen de financiële wereld meer aandacht besteedt aan *cybersecurity,* ook omdat dit soms richtlijnen en verordeningen vanuit Europa betreft. Zo zijn er de *guidelines* van EBA, EIOPA en ESMA. Hoewel de *guidelines* van EBA bijvoorbeeld wel complementair zijn aan ISO standaarden en dergelijke, zijn deze niet onderling substitueerbaar.

"In de financiële sector wordt het toezicht uitgeoefend door de FSMA en zij moeten zorgen dat de banken en verzekeringsmaatschappijen in België de nodige richtlijnen of wettelijke verplichtingen toepassen." (B1)

"Voor het toezicht in is het misschien belangrijk om te weten dat het in een federaal systeem is met de ccb (center for cybersecurity belgium) die eigenlijk een coördinerende rol heeft en die eigenlijk beroep doet op verschillende sectorale autoriteiten die verantwoordelijk zijn voor het toezicht op de bedrijven in hun eigen sectoren." (D2)

"Dus voor wat de financiële wereld betreft zijn de bevoegdheden eigenlijk verdeeld tussen de FSMA en de nationale bank van België. De rol van de FSMA is nog extra beperkt omdat enkel de exploitanten van markten in hun bevoegdheid vallen." (D2)

"Les guidelines EBA, ESMA ou EIOPA. Ce sont des choses un peu différent. Ce sont des choses complémentaires mais c'est pas substituables, ça je penses que c'est important de savoir." (D3)

Uit de interviews is gebleken dat de financiële sector op de hoogte is van de bestaande raamwerken zoals NIST, ITIL, COBIT… Banken en verzekeringsmaatschappijen zullen bijvoorbeeld ook op deze raamwerken steunen, maar ze baseren zich vooral op de wetgeving en richtlijnen uit de financiële wereld. Een voorbeeld hiervan is de NIS *directive*. NIS is volgens respondent D2 van toepassing in de financiële wereld op banken, verzekeringen, beursvennootschappen maar ook op de mensen die een beurs uitbaten zoals Euronext. Zoals ook al eerder werd vermeld, komt er binnenkort een tweede versie van NIS die van toepassing zal zijn op 2024. Daarnaast vertelden respondenten D3, F2 en F3 meer over DORA (Digital Operation Resilience Act). Dit initiatief komt vanuit Europa uit, maar is nog niet definitief en zal van toepassing zijn op de financiële sector. Het is ontworpen om ervoor te zorgen dat alle instellingen in de financiële sector onderworpen zijn aan een gemeenschappelijke reeks van normen om de ICT-risico's voor hun activiteiten te beperken. DORA behandelt vier aspecten: (i) Voor financiële instellingen die groot genoeg zijn TAPT (*Threat And Penetration Testing*), (ii) *incident reporting*, (iii) *third party oversight* en (iv) *risk management*. Tot slot is er ook TIBER BE (Threat Intelligence Based Ethical Red teaming). TIBER is een raamwerk voor gecontroleerde en op maat gemaakte cyberaanvaltests. Dit is eigenlijk een raamwerk dat gehanteerd wordt nadat bedrijven een bepaald niveau van maturiteit hebben gehaald. Eerst ga je zorgen dat je infrastructuur goed is opgebouwd en voldoende veilig is volgens de theorie. Daarna volgt er pas een TIBER test om te testen of de veiligheid wel is zoals verwacht.

"Ce texte DORA est toujours en cours de discussions à ce stade-ci au niveau du conseil." (D3)

"We hebben gesproken over C-best wat dat er aan de oorsprong lag en TIBER NL, TIBER EU en TIBER BE en dan heb je DORA in de toekomst. En de bedoeling is altijd harmonisatie." (F2)

"Een TIBER test is geen alternatief bijvoorbeeld voor een certificaat dat zegt dat je COBIT of ITIL compliant bent. TIBER is iets dat daarna komt." (F3)

"TIBER, dat betekent echt dat we gaan kijken naar de echte threats en geen theoretische threats vanuit wat dat de malicious actors effectief zouden doen" (F2)

5 Bescherming van KMO's

Zoals hierboven al werd toegelicht, zal je in België niet snel *cybersecurity* raamwerken tegenkomen. Dit heeft te maken met het feit dat het ondernemingslandschap in België hoofdzakelijk uit KMO's bestaat. Zoals de meerderheid van de respondenten ook uitlegde, is deze lage maturiteit te verklaren door het feit dat KMO's niet de middelen en het geld hebben om grote raamwerken te implementeren. Daarnaast merkten de meeste respondenten ook op dat KMO's gewoon niet bezig zijn met *cybersecurity*. Ondernemingen die niet bezig zijn met *cybersecurity*, zijn het meest kwetsbaar.

> *"Het hangt er ook van af hoe matuur je eigenlijk bent. Een organisatie waar dat de leidinggevenden zeggen van oke ja cybersecurity ja voor ons is dat een non-issue. Dat zijn natuurlijk organisaties die het kwetsbaarste zijn, want die gaan daar geen middelen en aandacht aan besteden. Wanneer een organisatie er geen prioriteit van gaat maken, dan ben je als organisatie kwetsbaar." (A1)*

De KMO's die wel willen inzetten op *cybersecurity* weten vaak niet hoe ze eraan moeten beginnen en de moeilijke terminologie uit raamwerken schrikt ze af. Daarnaast blijken raamwerken ook gewoon een brug te ver te zijn, de meeste ondernemingen in België zijn nog niet zo ver dat deze raamwerken toegevoegde waarde kunnen creëren. De raamwerken lijken eerder nuttig voor grote mature organisaties. Verder is het duidelijk kleine ondernemingen meer sturing nodig hebben. Daarom zal er in dit onderdeel een aanzet worden gegeven voor een apart raamwerk dat zich specifiek toelegt op KMO's (illustratie 1).

> *"De meeste mensen zie ik het risico wel erkennen, maar ze weten gewoon niet hoe ze eraan moeten mee omgaan. Waarschijnlijk zoeken ze dat dat op op het internet en dan kom je allemaal moeilijke terminologie tegen, framework links, dat… mensen kennen dat verschil niet en je hebt dan zoveel verschillende soorten certificaten of vergunningen (ISA's vb), allemaal van die Amerikaanse begrippen en dat is niet op maat van onze bedrijven in Vlaanderen. En bedrijven krijgen daar zo wat schrik van." (E1)*

> *"De frameworks zijn voor een KMO gewoonweg veel te zwaar" (I1)*

Hierbij moeten we een onderscheid maken tussen KMO's die hun IT *outsourcen* en KMO's die hun IT in huis doen. Uit de interviews is gebleken dat veel KMO's hun IT volledig gaan *outsourcen* aan een IT provider. Vooral de kleinere KMO's hebben het geld niet om IT in huis te doen. Dat zou niet rendabel zijn. Respondenten benadrukten daarom dat het belangrijk is dat KMO's zich gaan omringen met de juiste partijen. Verschillende respondenten gingen hierop verder en vertelden dat vandaag de dag bijna iedereen expert is en dat het een uitdaging is geworden om goede partners te vinden. Ondernemingen moeten dus kritisch zijn in hun keuze van provider. Respondent I1 gaf hierbij als opmerking dat ondernemingen daarom goed moeten focussen op wat de IT providers in hun contracten vermelden en verschillende contracten onderling moeten gaan vergelijken. Daarnaast gaven respondenten E1 en A2 aan dat die interne kennis, die vaak bij KMO's ontbreekt, wel belangrijk is om *awareness* binnen je bedrijf te creëren. Dit sluit aan bij het concept van maturiteit. Ondernemingen die de gevaren niet inzien, kunnen ook niet beveiligen. Die *awareness* is met andere woorden even belangrijk voor KMO's die hun IT volledig *outsourcen*. Het is namelijk niet zo dat als een onderneming haar IT gaat *outsourcen*, ze totaal niet meer bezig moet zijn met haar cyberrisico's.

"Een bedrijf van 30 man kan zich dat niet permitteren om een eigen ICT-dienst te hebben. Dat is ook niet meer rendabel. Ik denk dat het daar gewoon een mix is van gezond verstand en uiteraard goede partijen om mee samen te werken." (E1)

"Je moet het bij de juiste zetten en iedereen is wel zo een expert als je er als KMO niks van kent. Het bedrijf van achter de hoek zal je misschien aanspreken, die zullen er iets van kennen want dat zijn IT'ers, en je vertrouwt die alles toe…Maar als je in de verkeerde vertrouwen legt, als je je door de verkeerde laat adviseren, dat is nog gevaarlijker zelfs. Je moet er dus inderdaad wel iets van kennen zelf hoor. Als je er niks van kent dan moet je toch zeer kritisch kunnen zijn en aan een bedrijf kunnen zeggen misschien van kijk, een bedrijf dat je wilt helpen, 'heb je referenties of kunnen wij eens praten met klanten van jou?'. Dat is wel belangrijk." (C1)

"Dus het volledig outsourcen aan een externe firma is nooit een oplossing. Je moet gewoon zien dat dat ingebakken is in je bedrijf." (E1)

"Het hangt ervan af aan wie dat ze outsourcen." (G1)

"Ik denk zeker dat dat een voordeel is want als je gebruik gaat maken van externe partijen die je informatie gaan beveiligen en beheren dan ga je altijd veel beter af zijn dan als je het zelf probeert te doen. Maar inderdaad, die awareness is enorm belangrijk al was het maar om je medewerkers er steeds opnieuw op te wijzen op de gevaren van phishing." (A2)

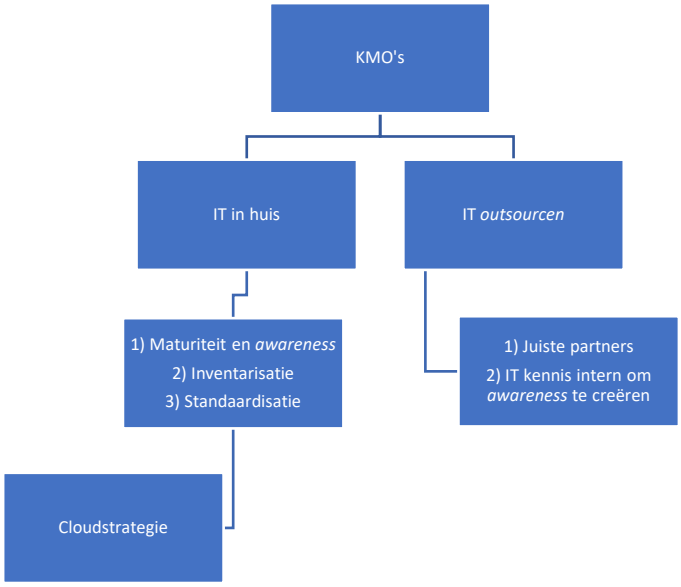
KMO's die IT in huis gaan doen, moeten op andere zaken letten. Zo moeten zij zoals beschreven in onderdeel drie ook enkele basisstappen doorlopen om zich te beschermen. De eerste stap is inventarisatie van hardware en software waarbij er ook moet worden nagegaan of deze nog up-to-date zijn. Respondenten geven immers aan dat oude besturingssystemen kwetsbaar zijn. Gepaard met deze stap gaat ook het creëren van *awareness* en maturiteit. Het trainen van het management en werknemers is hier een belangrijk onderdeel van. Dit is iets waar ondernemingen continu werk in moeten steken. Vervolgens geeft respondent C1 aan dat standaardisatie belangrijk is voor KMO's. Hoewel dit voor grotere ondernemingen een evidentie is, is dit voor KMO's niet altijd zo. Wanneer er bijvoorbeeld verschillende antivirussen gebruikt worden in een onderneming, kan een IT dienst dat heel moeilijk beheren. Het is daarom beter om één antivirus te kiezen die op alle computers geïnstalleerd zal worden. Hetzelfde geldt voor firewalls: een KMO heeft beter één sterke firewall.

"Een antivirus hadden we, maar we hadden zo wat verspreiding. In vestiging X hebben we heel wat andere oplossingen dan in vestiging Y. Dat is heel moeilijk te beheren als IT-dienst als je verschillende oplossingen hebt dus mijn volgende stap was standaardiseren in die antivirus oplossing en misschien nog eens gaan kijken 'hebben we wel een goede oplossing?'." (C1)

Tot slot gaven enkele respondenten aan dat de oplossing voor KMO's een Cloudstrategie is. Aangezien raamwerken te zwaar zijn voor zo een onderneming, is het voordelig om met Cloud te gaan werken. De Cloud is heel matuur en is ook vrij snel opgezet aan een basis kost. Dit garandeert natuurlijk niet dat KMO's hierdoor 100% waterdicht beveiligd zijn, maar het is een alternatief voor ondernemingen die minder middelen en geld hebben. Daarnaast geven respondenten C1 en G1 aan dat als je dat goed opzet dat je als onderneming vrij gerust mag zijn dat je informatie veilig is.

"Nu ik denk, voor veel KMO's gaat de oplossing zijn van naar de Cloud te gaan. De Cloud providers zijn heel matuur. Nu, let op he, Cloud is ook niet veilig out-of-the-box. Je moet nog altijd goed nadenken hoe je de boel opzet, maar als je dat deftig opzet dan ben je eigenlijk wel gerust." (G1)

"Als je alles in de Cloud zet dan mag je al wel zeker zijn. Dat wil niet zeggen dat je laptop niet aan een ransomware aanval onderhaven kan zijn, dat kan nog altijd gebeuren, maar je data zit nog veilig. Je bedrijfsvoering zit daar nog. Je pakt een andere laptop en je bent opnieuw vertrokken. Dus als KMO heb je het voordeel dat je dat kan, ale als kleinere KMO. Als grotere KMO, zoals wij, kan je onmogelijk alles in de Cloud zetten." (C1)



Illustratie 1: aanzet voor apart KMO raamwerk

6 De implementatie van raamwerken

Wanneer ondernemingen raamwerken gaan implementeren, zijn er enkele belangrijke aspecten die bepalen of dat succesvol gebeurt of niet. In het derde onderdeel van deze resultaten sectie werd al besproken dat een onderneming enkele basisstappen moet nemen vooraleer ze raamwerken kan toepassen. Eens dat er aan die basisvoorwaarden is voldaan, kunnen ondernemingen de volgende stap nemen. Respondenten haalden aan dat ondernemingen tijdens het implementeren ook op bepaalde dingen moeten letten.

6.1 People

Een eerste belangrijk aspect is zoals respondent F2 het noemde: *people*. Dit gaat samen met een van de eerder vermelde aspecten: *awareness* en maturiteit. Alle respondenten gaven aan dat *awareness* een cruciale factor is voor het succesvol implementeren van raamwerken. Dit betreft dus eerst en vooral je management. Het management moet een zekere kennis hebben van IT- en cyberrisico's, ze moet begrijpen wat de gevaren zijn en ook het nut inzien van raamwerken. Respondent C1 vulde hierop aan dat als *management commitment* ontbreekt, de IT manager die *commitment* moet gaan creëren. Heb je immers je management niet achter je staan dan zal het ook

niet mogelijk zijn om budgetten los te krijgen voor *cybersecurity*. Een IT manager zou eigenlijk een plaats moeten hebben aan de directietafel om zijn job goed te kunnen uitvoeren. Enkele respondenten gaven ook aan dat de media hier een hulp is. Wanneer je het management niet kan overtuigen, is het nuttig om actuele voorbeelden van cyberincidenten aan te halen. Een IT manager moet immers duidelijk kunnen maken dat niet investeren in *cybersecurity* later veel meer kosten met zich zal meebrengen. Actuele voorbeelden geven de argumenten van een IT manager meer bewijskracht en benadrukken het belang van *cybersecurity*.

> *"Het begint altijd bij het management. Als er geen management commitment is dan loopt het fout af, maar het is natuurlijk de rol van de IT man om die commitment te gaan creëren. Ook al zijn dat je bazen, heb jij die adviserende rol om die mensen mee te trekken in het verhaal." (C1)*

> *"De top van het bedrijf moet betrokken zijn ook he. Dat is heel belangrijk he." (B1)*

> *"Tone at the top, er is een grote samenhang tussen de IT-expertise bij board/directiecomité en de inschatting van het inherente risico. Als er IT-expertise is binnen het directiecomité dan gaan ze het inherente risico van IT zwaarder inschatten. Dit heeft een invloed op de kwaliteit van een controleomgeving." (F1)*

> *"Het eerste is executive support. Als dat op board level niet deftig wordt gedragen dan heeft dat weinig kans van slagen." (F2)*

> *"Dus de IT manager rapporteerde aan een directeur die er totaal geen verstand van had en ja dan is het heel moeilijk om je ding verkocht te krijgen. Die IT manager zit niet in het directiecomité en de governance van IT zat daar al mis van in het begin eigenlijk. Dus tone at the top speelt altijd een grote rol." (G1)*

Vervolgens zijn de werknemers heel belangrijk. Ook zij moeten volgens respondenten bewust gemaakt worden van het belang van *cybersecurity*. Dit kan soms een hele uitdaging zijn omdat niet iedereen goed met technologie om kan gaan en niet iedereen mee wil in het cyberverhaal. Respondent C1 legde uit dat je een goede afweging moet maken tussen gebruiksvriendelijkheid en veiligheid. Hoe veiliger je systemen, hoe minder gebruiksvriendelijk. Daar moet je als onderneming een balans tussen vinden. Respondenten A2 en C1 gaven ook het advies om zo praktisch mogelijk je werknemers het belang van *cybersecurity* uit te leggen. Volgens respondent A1 moet je herkenbare voorbeelden aanhalen zodat werknemers het kunnen relateren aan hetgeen dat ze zelf kennen. Hierbij sluit volgens de meerderheid van de respondenten *user training* aan. Dat is volgens velen het belangrijkste. Je kan namelijk niet beginnen beveiligen binnen een omgeving die zich van niks bewust is. De medewerkers moeten ook achter je staan en je moet ze blijven trainen.

> *"Een bepaald framework integreren. Dat werkt niet, heel simpel gezegd, als je je mensen niet bewust maakt van die feiten. Dus dat begint eigenlijk gewoon met preventief mensen te informeren." (E1)*

> *"Er zijn heel veel medewerkers die technologie beginnen te gebruiken, maar die uiteindelijk daar niks van snappen maar die zo gebruiksvriendelijk zijn geworden en dat uiteindelijk een leek het kan gebruiken. Die leek moet je natuurlijk kunnen opvoeden rond cyberrisico's en dat is inderdaad niet evident, maar je moet dat down-to-earth houden, heel praktisch, heel toegespitst op de rollen*

en de functie dat die personen hebben en ook vaak het kunnen relateren aan hetgeen dat ze zelf persoonlijk kennen." (A1)

"Een ander aspect is awareness. Dat de werknemers van het bedrijf ook op de hoogte zijn, dat cybersecurity wel serieus genomen moet worden." (F3)

"Regelmatige training en sensibilisering van alle medewerkers. Dus je moet bijvoorbeeld ook, ze noemen dat security om awareness te creëren." (B1)

"Nu, op dat vlak heel simpel he, de belangrijkste in mijn ogen is de awareness van je mensen. Want het begint bijna altijd met phishing dus hoe meer gebruikers dat je bewust kan maken van de gevaren ervan hoe beter." (G1)

Tot slot heb je de juiste mensen op de juiste plaats nodig. Ondernemingen hebben bijvoorbeeld een IT-manager of iemand van het management nodig die een visie heeft en alles kan overbrengen. Zo maakten C1 en F1 duidelijk dat je iemand nodig hebt die de nodige elementen kan halen uit de raamwerken. Een raamwerk moet niet volledig tot op de letter gevolgd worden, een onderneming moet daar de nodige elementen uithalen. Respondent G1 ging hier ook op verder en vertelde dat er geen slechte raamwerken zijn en dat je je vooral moet baseren op de noden van je onderneming. Daarnaast kwam er uit de interviews naar voren dat ondernemingen zich bij de implementatie van raamwerken moeten laten ondersteunen door experts als de ze de nodige kennis of middelen zelf niet in huis hebben.

"Je hebt iemand nodig met een visie. Er zijn een paar key components. Iemand met een visie, dat moet zeker management zijn maar als dat het management niet is en dat is ook vaak niet, dan moet dat een IT verantwoordelijke zijn die die visie wel kan brengen." (C1)

"Het moeten echt technische mensen zijn die kennis hebben van systemen en beveiliging." (E1)

"Dan heb je de juiste mensen nodig die dat aan de man kunnen brengen en de juiste processen kunnen tekenen." (F2)

"Dus ik heb echt ervaring ook bij dat implementeren en ik heb gemerkt ook bij die implementatie dat dus heel die zwart op wit bijbel dat daar heel wat zaken voor interpretatie vatbaar zijn, dat sommige zaken afhankelijk van de context van je bedrijf niet nuttig zijn, anderen veel nuttiger." (C1)

"Er wordt gevolgd of ze bepaalde raamwerken hebben, maar dat kiezen ondernemingen zelf. Ze bepalen zelf welke aspecten ze eventueel gaan implementeren en dat moet ook op een proportionele manier gebeuren." (F1)

"ISO is eerder procedureel, top 20 eerder technisch, NIST is behoorlijk comprehensief…" (G1)

6.2 Na de implementatie

Na het implementeren van een raamwerk is het belangrijk om je werknemers te blijven trainen. Dat is een continu proces. Respondenten wezen erop dat je ook aanvallen moet simuleren. Hier zijn twee redenen voor. Eerst en vooral draagt dit bij aan de training van je werknemers. Zo gaf respondent C1 als voorbeeld dat ondernemingen *phishing* mails uitsturen naar hun medewerkers. Achteraf gaan

ze de personen aanspreken die op de link hebben geklikt en gaan ze bespreken hoe dit in het vervolg voorkomen kan worden. Een tweede reden is dat het zwakheden blootlegt. Zelfs na het implementeren van een raamwerk en het opzetten van een sterke infrastructuur, ben je als onderneming niet 100% veilig. Een onderneming moet blijven werken aan haar beveiliging en regelmatig een risicoanalyse doen. Zoals respondent G1 aangaf: je bent nooit klaar met *cybersecurity*, dit is een continu proces.

> *"Ik denk dat je ook moet weten: the goal posts keep moving. Dus je moet je risicoanalyse geregeld refreshen en je moet nooit denken dat je klaar bent. Er gaat altijd een roadmap zijn. Net zoals je altijd een IT strategie en een IT roadmap hebt, ga je altijd een cyberstrategie en -roadmap moeten hebben. Je gaat nooit zeggen 'Nu is het af, nu heb ik alles geïmplementeerd.'" (G1)*

> *"Zoiets is eigenlijk een continu proces, je moet dat blijven doen. Microsoft helpt je daarbij. We hebben een Microsoft 365 abonnement waar dat we heel wat dingen kunnen doen, waaronder zo van die attacks gaan simuleren. Je kan dan zeggen, de boekhoudafdeling we geven die eens eentje met valse facturen, bij de IT-afdeling doen we weer iets anders en je kan dat eigenlijk non stop laten doen." (C1)*

Een extra opmerking die G1 hierbij gaf is dat een certificatie zoals ISO of ITIL natuurlijk geen garantie is dat een onderneming goed beveiligd is. Dit beaamde respondent F1 ook. Het is pas als een onderneming al jaren gecertifieerd is dat je er een beetje gerust in kan zijn omdat ze een plan-do-check-act cycle moeten doorlopen. Dan kan je erop vertrouwen dat een onderneming aan *continuous improvement* doet.

> "Zo kunnen bedrijven zeggen "wij zijn ISO gecertificeerd" maar dat is niet altijd voldoende." (F1)

6.3 Meest voorkomende raamwerken in België

Uit de interviews is gebleken dat ISO 27001, ISO 27002, ISO 9001 zeer veel geïmplementeerd worden. De ISO standaarden zijn zeer bekende standaarden die niet alleen op vlak van *cybersecurity* gebruikt worden. De ISO 27000 standaarden worden volgens respondent G1 ook regelmatig aangevuld met de top 20 CSC. Daar is een achtste versie van die momenteel eigenlijk een top 18 betreft. De top 18 CSC geeft aan welke technische controles een onderneming moet implementeren en is een goede aanvulling op de ISO standaarden die vooral nog gericht zijn op processen en procedures. Respondent H1 wees er ook op dat de NIS wetgeving verwijst naar de ISO 27001 standaard als basis. Ook de CCB heeft zijn c*ybersecurity* gids gebaseerd op deze standaard. Deze ISO standaard komt dus ook in de financiële sector regelmatig voor.

> *"En bijvoorbeeld binnen onze onderneming zijn wij ISO 9001 gecertificeerd, dat is dan alles rond processen enzoverder." (C1)*

> *"Ik denk dat in België eigenlijk bij de KMO's die ISO's, dat is herkenbaar. Die worden niet alleen op gebied van cybersecurity gebruikt. Dat geeft vertrouwen bij mensen en dat is ook gewoon een kwaliteitslabel." (E1)*

> *"En het CCB heeft zijn CyberSecurity Gids ook op de ISO27001 aanpak gebaseerd." (H1)*

ITIL en COBIT werden minder genoemd tijdens de interviews. Respondent G1 legt uit dat ITIL begint met een CMDB. Dat is een Configuration Database waar dat al je items (hardware en software) inzitten en dat is de basis van alles. Zoals eerder in dit onderzoek werd vermeld: inventarisatie is de basis.

> *"Dat weten we nu heel goed, want onze IT-dienst is zeer georganiseerd. Wij hebben een heel uitgebreid systeem, een beetje ITIL gebaseerd." (C1)*

> *"Ik kan vanuit mijn werkverleden wel zeggen van ITIL is zeker de moeite waard om te implementeren, maar er is maar één klein aspect dat gaat over cybersecurity." (F2)*

Vervolgens gaven respondenten G1 en I1 aan dat een kleine minderheid voor NIST CSF kiest, maar beiden zijn een voorstander van dit raamwerk omdat het zeer makkelijk te begrijpen is. Tot slot gaf geen enkele respondent aan dat COSO ERM werd gehanteerd. Respondent G1 heeft dit verduidelijkt door uit te leggen dat COSO ERM bijzonder high level is. Dat is een voorbeeld dat ze vooral tegenkomen in de audit wereld. Respondent G1 vertelde dat je COSO raamwerk echt moet zien op organisatieniveau, de algemene opzet van je controleraamwerk en *cybersecurity* is daar maar een subset van. Daarnaast is *cybersecurity* zelf al een onderdeel van IS dus COSO ga je niet snel tegenkomen voor *cybersecurity*.

> *"Je hebt er tal van anderen, je hebt daar NIST CSF ook aangehaald. NIST is zeer belangrijk denk ik ook, maar soit je moet een beetje kiezen" (C1)*

> *"De meeste van onze klanten werken wel met bepaalde frameworks en dan is er eigenlijk een minderheid die kiest voor NIST." (G1)*

> *"Ik ben voorstander van het NIST framework, dat is een zeer comprehensief framework." (I1)*

Conclusie

1. Discussie

De opkomst van nieuwe technologie en software hebben het landschap waarin ondernemingen vandaag de dag opereren compleet veranderd. Nieuwe technologische ontwikkelingen beïnvloeden niet alleen de manier waarop we werken, maar creëren ook nieuwe opportuniteiten en risico's voor ondernemingen. Het belang van IT blijft met andere woorden toenemen en ondernemingen worden meer afhankelijk van technologie. Onderzoekers zijn het erover eens dat het daarom belangrijk is voor ondernemingen om in te zetten op *information technology* (IT). Technologische vooruitgang is immers de drijfkracht geworden voor economische groei (Ivanova et al., 2019; Lanz, 2014). Dit wordt ook beaamd door verschillende respondenten. Zo zegt respondent G1 bijvoorbeeld dat je zonder IT tegenwoordig geen business meer doet. Anderen geven aan dat ondernemingen steeds meer technologie gaan implementeren en meer afhankelijk worden van technologie. *Cybersecurity* en IT zijn daarom niet meer weg te denken binnen ondernemingen. Uit de interviews is het duidelijk geworden dat het toenemende belang van *cybersecurity* verschillende verklaringen heeft. Een eerste verklaring is, zoals de literatuur het beschrijft, de grotere afhankelijkheid van technologie. Vervolgens zien respondenten dat andere partijen een bepaald niveau van *cybersecurity* eisen van hun partners vooraleer ze samenwerken. Tot slot werd er in de interviews gesteld dat meer wet- en regelgeving het belang van *cybersecurity* aankaart.

De literatuur stelt dat de grootste risico's waar ondernemingen tegenwoordig mee in contact komen, behoren tot de cyberrisico's. Zowel private als publieke ondernemingen krijgen regelmatig te maken met geavanceerde cyberdreigingen en -aanvallen (Islam et al., 2018; Sabillon et al., 2017). Het is hierbij opvallend dat cybercriminelen hun aanvalstechnieken blijven aanpassen. Zo wordt er tegenwoordig veel ingespeeld op mensen als een manier om informatie te bekomen. Bewust of onbewust, werknemers zijn vaak de oorzaak van succesvolle cyberaanvallen (Bissell et al., 2019). Hackers hanteren verschillende middelen en methoden om in hun opzet te slagen (Bissell et al., 2019). Een van de meest gebruikte middelen voor cyberaanvallen is *malware* (Cayirci & Ghergherehchi, 2011). Daarnaast stellen Bissell et al. (2019) dat er de laatste jaren een opmars is van *ransomware, malicious insider* aanvallen en *phishing*. Uit de interviews kwam dit ook naar voren. Respondenten noemen *ransomware* en *malware* in combinatie met *phishing* of *supply chain attacks* de grootste problemen voor ondernemingen vandaag de dag. De meerderheid van de respondenten geeft aan dat *phishing* een van de meest succesvolle manieren is voor hackers om bedrijven te infiltreren. Respondent F2 legt ook uit dat de mens de zwakste schakel blijft en dat heel wat hackers hebben ingespeeld op de COVID-19 crisis om bijvoorbeeld hun *phishing* mails geloofwaardiger te maken. Bovendien zien respondenten het aantal cyberaanvallen exponentieel toenemen. Enkelen verklaren dit fenomeen door uit te leggen dat we meer afhankelijk worden van IT, wat de aanvalsbasis voor hackers vergroot. Anderen zien ook een link met COVID-19 en thuiswerken, maar hierover is geen consensus bereikt.

Daarnaast benadrukken onderzoekers het belang van raamwerken. In de literatuurstudie worden COSO ERM, COBIT, NIST CSF en de ISO standaarden besproken (Bozkus, & Caliyurt, 2018). Daarbij stellen Islam et al. (2018) dat het kiezen van het juiste raamwerk voor een onderneming afhankelijk is van verschillende factoren. Zo kunnen bijvoorbeeld de industrie, *compliance*-vereisten en factoren

die eigen zijn aan de onderneming zelf deze keuze beïnvloeden (Islam et al., 2018). Volgens Fountain (2019) is NIST CSF een van de meest toegepaste raamwerken. Galligan & Rau (2015) benadrukken het belang van COSO in hun onderzoek. Volgens hen kan het beheersen van cyberrisico's aan de hand van het COSO raamwerk de raad van bestuur en senior executives van een onderneming helpen om de bedrijfsdoelstellingen, de definitie van kritische informatiesystemen en de gerelateerde risicotolerantieniveaus beter te communiceren (Galligan, & Rau, 2015). Respondenten geven aan dat raamwerken richting kunnen geven en structuur bieden, maar wijzen op het feit dat raamwerken geen waarde gaan creëren voor bedrijven die nog niet voldoende matuur zijn op vlak van *cybersecurity*. Dit is vooral bij KMO's het geval. Eens dat die maturiteit er is en het gehele bedrijf het belang van *cybersecurity* inziet dan kan er iets aan de cyberrisico's gedaan worden. Respondent G1 benadrukt ook het belang van *getting the basics right*. Ook respondent C1 beaamt dit en vult aan dat als je de basis niet mee hebt je geen verdere stappen kan ondernemen. Wanneer een onderneming deze basisstappen heeft doorlopen, kan ze afhankelijk van de eigenheid van het bedrijf een geschikt raamwerk gaan kiezen. Respondenten C1, F1 en G1 maken ook duidelijk dat je iemand intern nodig hebt die de nodige elementen kan halen uit de raamwerken. Een raamwerk moet immers niet volledig tot op de letter gevolgd worden, de nodige elementen moeten eruit gehaald worden. Daarnaast kan er uit de interviews afgeleid worden dat NIST SCF in België niet veel gebruikt wordt. Ook COSO ERM wordt niet toegepast op vlak van *cybersecurity*.

De literatuur benadrukt het belang van training van de werknemers. Zo stellen Bissell et al. (2019) dat datalekken vaak voorkomen omdat werknemers niet altijd voldoende uitleg krijgen over de mogelijke cyberrisico's wanneer er binnen de onderneming nieuwe producten, diensten of processen worden ontwikkeld. Het is dus in het belang van alle stakeholders dat werknemers training krijgen omtrent cyberrisico's en beschikken over de nodige informatie. Ze hebben nood aan tools en motivatie om deze risico's te leren herkennen en te adresseren (Bissell et al., 2019). Uit de interviews blijkt dit een zeer belangrijke bevinding te zijn. Respondenten stellen dat *user training* en *awareness* cruciaal zijn. Dit betekent dat een onderneming niet alleen haar werknemers, maar ook haar management bewust moet maken van cyberrisico's. Daarnaast geven respondenten aan dat werknemers regelmatig getraind moeten worden. Respondent C1 haalt aan dat ze dit kunnen doen door aanvallen te simuleren op de onderneming zelf. Deze training en bewustmaking zijn volgens respondenten zeer belangrijke factoren. Wanneer werknemers en het management immers zelf de cyberrisico's niet begrijpen, zal een goede software of een sterk raamwerk geen toegevoegde waarde zijn.

Daarnaast wordt er in de literatuurstudie gesproken over verantwoordelijken voor *cybersecurity*. Niet alleen het management en de werknemers spelen een belangrijke rol in het cyberverhaal, maar de audit functie ook. Dit wordt benadrukt in het drie lijnen model (Weatherford & Ruppert, 2016). Zo dragen interne auditors op vlak van *cybersecurity* bij aan de ontwikkeling van effectieve beveiligingsprogramma's door het management in het *cybersecurity* proces te ondersteunen. Op deze manier creëren auditors waarde voor het bedrijf en verhogen ze de kwaliteit van de *cybersecurity* (Fountain, 2019; Islam et al., 2018). Ook de externe audit, wanneer ze effectief gecoördineerd is, kan bijdragen aan *corporate governance* door belangrijke observaties te communiceren naar de raad van bestuur en het topmanagement (Anderson & Eubanks, 2015 ;Weatherford & Ruppert, 2016). Respondenten geven ook aan dat de interne audit een belangrijke

drijver is voor *cybersecurity*. Zo vertelt respondent A1 dat de interne audit instaat voor het communiceren van cyberrisico's naar het auditcomité en de raad van bestuur op een onafhankelijke wijze. Daarbij benadrukt respondent F1 het belang van het drie lijnen model. Ook het belang van de externe audit wordt in de interviews beaamd.

Vervolgens stellen zowel Fountain (2019) als Liu (2020) dat de rol van de interne audit aan het veranderen is. Vandaag de dag is immers er meer druk op de interne audit om IT risico's te begrijpen. Vroeger steunde de interne audit functie hierbij op IT-specialisten, maar tegenwoordig kunnen ze die verantwoordelijkheid niet meer volledig delegeren aan de IT-afdeling (Fountain, 2019). Het is daarom belangrijk dat interne auditors evolueren en een grondige kennis ontwikkelen van meer dan alleen algemene en toepassingscontroles. Audits werken namelijk het best wanneer alle auditors controles kunnen uitvoeren vanuit een IT perspectief en zich bewust zijn van de belangrijkste technologische risico's. (Bozkus, & Caliyurt, 2018; Fountain, 2019). Trainingen en het behalen van certificaten kunnen auditors hiermee helpen (Fountain, 2019). Certificaten zoals CISA of CPA blijken ook wel degelijk een invloed te hebben op de *cybersecurity* audit (Islam et al.; 2018). Respondent A1 gaat hiermee akkoord en stelt dat een interne auditor alles moet kunnen auditeren van business processen tot IT. Er wordt verwacht dat een interne auditor een brede kennis heeft om zijn taak te vervullen. De interne audit laat zich daarom beter bijstaan door experts volgens respondenten A2 en G1. Deze experts kunnen hen ondersteunen door IT of *cybersecurity* audits uitvoeren. Daarnaast benadrukt respondent A1 dat een interne auditor met IT kennis een toegevoegde waarde kan zijn en al sneller de brug naar *cybersecurity* kan maken. Over de waarde van certificaten zijn de meningen van de respondenten verschillend. Respondenten A1 en C1 zien een certificaat zoals CISA en CPA als een meerwaarde. Daar tegenover staan respondenten G1 en E1 die daar niet veel toegevoegde waarde in zien. Ze redeneren namelijk dat een certificaat zoals CISA makkelijk te halen is op het internet en niet veel gewicht heeft. Respondent C1 geeft hier een belangrijke nuance door te zeggen dat een CISA een mooie basis geeft. Het is een certificaat dat je in staat stelt om de terminologie en belangrijkste concepten te leren, maar het blijft een basis. Vervolgens blijkt uit de interviews dat er zo een wildgroei aan certificaten is dat het tegenwoordig moeilijk is om te onderscheiden welke nu daadwerkelijk gewicht hebben. Respondent E1 geeft aan dat het beter zou zijn als de overheid duidelijkheid kan scheppen over de meest waardevolle certificaten.

2. <u>Nieuwe bijdragen</u>

Hoewel de resultaten grotendeels overeenstemmen met de literatuur, zijn er toch enkele nieuwe bevindingen die uit dit onderzoek naar voren zijn gekomen. Deze nieuwe bevindingen vullen de leegte in de huidige literatuur aan en bieden een houvast voor ondernemingen die zich willen beschermen tegen cyberrisico's. Een eerste bevinding is dat raamwerken vaak een brug te ver zijn voor ondernemingen. In dit onderzoek wordt namelijk aangetoond dat er een zekere maturiteit nodig is vooraleer een onderneming een raamwerk kan toepassen. Maturiteit houdt in dat een onderneming begrijpt wat de raamwerken en de gevaren omtrent *cybersecurity* zijn en dat een onderneming ook een management heeft dat dit allemaal begrijpt. Deze maturiteit gaat gepaard met bewustwording van het management en de werknemers omtrent cyberrisico's. Ondernemingen waarbij deze maturiteit ontbreekt, zullen niet aan *cybersecurity* raamwerken uit kunnen en het nut er niet van

inzien. Hierbij kaarten respondenten aan dat de maturiteit in België nog zeer laag ligt omdat de meerderheid van het Belgisch ondernemingslandschap bestaat uit KMO's.

Een tweede bevinding betreft de aspecten die belangrijk zijn vooraleer een raamwerk wordt geïmplementeerd. Het is belangrijk dat er enkele basisstappen worden doorlopen vooraleer we bij raamwerken uitkomen. Een eerste stap is de inventarisatie van hardware en software. Ondernemingen moeten namelijk eerst weten wat ze in huis hebben om te weten wat ze moeten beveiligen. Deze eerste stap gaat gepaard met het creëren van *awareness* in een onderneming. Zowel het management als de werknemers moeten goed begrijpen wat de cyberrisico's zijn. Je kan immers niet gaan beveiligen in een onderneming die zich niet bewust is van de risico's. Vervolgens moeten ondernemingen risico's leren identificeren en proactief beveiligen. Dit slaat bijvoorbeeld ook op het trainen van je werknemers, een klassieke antivirus installeren, een goede firewall hebben, regelmatige back-ups… Daarnaast moet een onderneming een plan hebben om te reageren op een aanval en tot slot moet er dan ook een herstelplan opgesteld worden.

Eens dat een onderneming een bepaalde maturiteit heeft bereikt en de basisstappen heeft doorlopen, kan ze raamwerken gaan implementeren. Hierbij zijn er verschillende factoren die bepalen dat de implementatie van raamwerken succesvol gebeurt. *People* is de belangrijkste factor. Het management en de werknemers moeten immers bewust gemaakt worden van de cyberrisico's. Ze moeten de gevaren begrijpen en het nut inzien van bepaalde standaarden en raamwerken. Daarnaast heb je de juiste mensen nodig op de juiste plaats. Ondernemingen hebben bijvoorbeeld een IT-manager of iemand van het management nodig die een visie heeft en alles kan overbrengen. Het is belangrijk om iemand intern te hebben die de nodige elementen kan halen uit de raamwerken. Een raamwerk moet immers niet volledig tot op de letter gevolgd worden, een onderneming moet daar de nodige elementen uithalen. Tot slot is het belangrijk dat er na de implementatie regelmatige *user training*, risicoanalyses en simulaties van aanvallen worden gedaan. Een onderneming moet blijven werken aan haar beveiliging, dit is een continu proces.

Een laatste bevinding is de oplossing voor KMO's. KMO's hebben vaak het geld en de middelen niet om raamwerken te implementeren. Daarnaast benadrukken respondenten dat KMO's nog niet matuur genoeg zijn. De bestaande raamwerken zijn te zwaar voor zo een kleine onderneming. In dit onderzoek werd er daarom een aanzet gegeven om een raamwerk te ontwikkelen dat zich toelegt op KMO's en haar cyberrisico's. Hierbij werd een onderscheid gemaakt tussen KMO's die IT gaan *outsourcen* en KMO's die IT in huis uitvoeren. Voor KMO's die IT volledig gaan *outsourcen* is het belangrijk om met de juiste partners samen te werken. Omdat in onze huidige economie veel ondernemingen beweren dat ze een expert zijn, is dit niet altijd evident. Daarnaast moeten deze KMO's ook *awareness* creëren in hun onderneming. Het is namelijk niet zo dat als een onderneming haar IT gaat *outsourcen*, ze totaal niet meer bezig moet zijn met haar cyberrisico's. KMO's die hun IT in huis doen daarentegen, moeten focussen op andere zaken. Zo moeten zij enkele basisstappen doorlopen. De eerste stap is inventarisatie van hardware en software waarbij er ook moet worden nagegaan of deze nog up-to-date zijn. Respondenten geven immers aan dat oude besturingssystemen kwetsbaar zijn. Gepaard met deze stap gaat ook het creëren van *awareness* en maturiteit. Vervolgens is standaardisatie belangrijk voor KMO's. Wanneer er bijvoorbeeld verschillende antivirussen gebruikt worden in een onderneming, kan een IT dienst dat immers heel

moeilijk beheren. Het is beter om één antivirus te installeren op alle computers. Tot slot is uit de resultaten gebleken dat KMO's die hun IT in huis doen, in de toekomst best hun informatie in de Cloud zetten aangezien deze providers al erg matuur zijn.

3. Beperkingen en suggesties voor verder onderzoek

Deze kwalitatieve studie onderzoekt hoe ondernemingen *cybersecurity* raamwerken kunnen implementeren op een succesvolle manier. Het doel van kwalitatief onderzoek is het ontwikkelen van een theorie, maar om theorie te veralgemenen dient nader onderzoek te worden gedaan in een grotere steekproef. Een eerste suggestie voor verder onderzoek is met andere woorden een kwantitatieve studie die deze theorie kan testen. Vervolgens beperkt dit onderzoek zich tot België. Internationaal onderzoek zou interessant kunnen zijn om de bestaande raamwerken in verschillende omgevingen en culturen te bestuderen. Afhankelijk van de eigenheid van een onderneming, zijn bepaalde elementen van een raamwerk nuttig en anderen niet. Als we dit op internationale schaal kunnen bekijken kan er meer duidelijkheid geschept worden. Ondernemingen met gelijke structuren en businessactiviteiten kunnen gelijkaardig te werk gaan in de strijd tegen cybercriminaliteit.

Een tweede beperking is dat de steekproef van negen ondernemingen geen IT provider bevatte. Veel kleine KMO's gaan hun IT namelijk *outsourcen* aan een externe IT provider. Hoewel deze beperking deels werd opgevangen door cases te zoeken die zelf in aanraking komen met KMO's en hun IT infrastructuur, mist deze invalshoek in de resultaten. Verder onderzoek dat zich focust op KMO's moet hier zeker rekening mee houden.

Een volgende beperking is dat het onderwerp van *cybersecurity* erg breed is waarbij ook het antwoord op deze onderzoeksvraag verschillende subsets ervan aankaart. Zo is er bijvoorbeeld het thema cybercriminaliteit. Enkele respondenten gaven al aan dat dit is uitgegroeid tot een hele industrie en er zijn nog heel wat onduidelijkheden omtrent dit thema. Het is iets wat onverdeelde aandacht verdient, maar juist omdat deze expertise vooral bij hackers ligt is het moeilijk om onderzoek te doen vanuit dat perspectief.

Tot slot heeft deze studie de aanzet gegeven voor de ontwikkeling van een raamwerk dat zich toelegt op KMO's en haar cyberrisico's. Dit vormt een enorme meerwaarde voor KMO's die niet weten hoe ze *cybersecurity* moeten aanpakken. Het zou interessant zijn voor toekomstige onderzoekers om dit raamwerk verder uit te bouwen zodat ook KMO's een kader hebben dat hen kan ondersteunen in het cyberrisicobeheersingsproces.

Referenties

Anderson, D. J., & Eubanks, G. (2015). Leveraging COSO across the three lines of defense. *Committee of Sponsoring Organizations of the Treadway Commission*, 1-32.

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., ... & Vasek, M. (2019). Measuring the changing cost of cybercrime.

Bedard, J. C., & Graham, L. (2011). Detection and severity classifications of Sarbanes-Oxley Section 404 internal control deficiencies. *The Accounting Review*, *86*(3), 825-855.

Bissell, K., Lasalle, R. M., & Dal Chin, P. (2019). Ninth Annual Cost of Cybercrime Study, Accenture and the Ponemon Institute.

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal, 33*(4), 360–376. https://doi-org.bib-proxy.uhasselt.be/10.1108/MAJ-02-2018-1804

Bryant, A., & Charmaz, K. (Eds.). (2007). *The Sage handbook of grounded theory*. Sage.

Cayirci, E., & Ghergherehchi, R. (2011, December). Modeling cyber attacks and their effects on decision process. In *Proceedings of the 2011 Winter Simulation Conference (WSC)* (pp. 2627-2636). IEEE.

Chandra, A., & Snowe, M.J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems 38*: 100467. https://www.sciencedirect.com/science/article/pii/S1467089520300348

Charmaz, K. (2006). Constructing grounded theory: A practical guide through qualitative research. London: Sage.

Chun Tie, Y., Birks, M., & Francis, K. (2019). Grounded theory research: A design framework for novice researchers. *SAGE open medicine*, *7*, 2050312118822927.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control-integrated framework.

COSO (z.d.). Welcome to COSO. Geraadpleegd op 27/01/2020 via https://www.coso.org/Pages/default.aspx

Drozdov, A. (2019). Impressions From Delivering COBIT 2019 Foundation Training for Auditors. *COBIT Focus*, 1–4.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, *14*(4), 532-550.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of management journal*, *50*(1), 25-32.

Fountain, L. (2019). INTERNAL AUDIT'S EVOLVING CYBERSECURITY ROLE: Auditors need to become involved in helping their organizations address cyber risks. *Internal Auditor, 76(1)*, 19–21.

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, *2020*(12), 6-12.

Galligan, M. E., & Rau, K. (2015). COSO in the cyber age. *Deloitte Global*.

Galligan, M. E., Herrygers, S., & Rau, K. (2019). CYBER RISK IN A DIGITAL AGE.

Haislip, J. Z., Peters, G. F., & Richardson, V. J. (2016). The effect of auditor IT expertise on internal controls. *International Journal of Accounting Information Systems*, *20*, 1-15.

Harisaiprasad, K. (2020). COBIT 2019 and COBIT 5 Comparison. *COBIT Focus*, 1–5.

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*, 33(4), 377-409. doi:10.1108/MAJ-07-2017-1595

ISO. (z.d.). *About us*. Geraadpleegd op 17 februari 2021 van https://www.iso.org/about-us.html

Jackson, S., Vanteeva, N., & Fearon, C. (2019). An Investigation of the Impact of Data Breach Severity on the Readability of Mandatory Data Breach Notification Letters: Evidence From U.S. Firms. *Journal of the Association for Information Science & Technology*, *70*(11), 1277–1289. https://doi-org.bib-proxy.uhasselt.be/10.1002/asi.24188

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems*, 34(2), 597–626. https://doi-org.bib-proxy.uhasselt.be/10.1080/07421222.2017.1334499

Joëlle, M. M., Park, Y.-H., & Hwang, S. O. (2018). Strategies for detecting and mitigating DDoS attacks in SDN: A survey. *Journal of Intelligent & Fuzzy Systems*, 35(6), 5913–5925. https://doi-org.bib-proxy.uhasselt.be/10.3233/JIFS-169833

Johnson, J. S. (2015). Qualitative sales research: an exposition of grounded theory. Journal of Personal Selling & Sales Management, 35(3), 262–273. https://doi-org.bib-proxy.uhasselt.be/10.1080/08853134.2014.954581

Karimi, V. R., Cowan, D. D., & Alencar, P. S. (2014). An approach to correctness of security and operational business policies. *International Journal of Accounting Information Systems*, *15*(4), 323-334.

Liu, L. Y. (2020). *Do Auditors Help Prevent Data Breaches?* (Doctoral dissertation, The University of Chicago).

Moeller, R. R. (2011). *COSO enterprise risk management: establishing effective governance, risk, and compliance processes* (Vol. 560). John Wiley & Sons.

NIST (21 mei 2021). *An introduction to the components of the framework*. Geraadpleegd van https://www.nist.gov/cyberframework/online-learning/components-framework

NIST, (12 februari 2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Geraadpleegd van https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

NIST, (23 september 2020). *New to Framework* [website]. Geraadpleegd op 06/12/2020 via https://www.nist.gov/cyberframework/new-framework#basics

Oberly, D. J. (2019). Best Practices for Effectively Defending Against Ransomware Cyber Attacks. *Intellectual Property & Technology Law Journal*, 31(7), 17–20.

Otero, A. R. (2015). An information security control assessment methodology for organizations' financial information. *International Journal of Accounting Information Systems*, *18*, 26-45.

Pierce, E. M., Goldstein, J., & Pierce, E. (2016, October). Moving from enterprise risk management to strategic risk management: examining the revised COSO ERM framework. In *14th Global Conference on Busness and Economics,(October).* Geraadpleegd van https://www. researchgate. net/publication/308890946_Moving_From_Enterprise_Risk_Management_to_Strategi c_Risk_Management_Examining_the_Revised_COSO_ERM_Framework.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017, November). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In *2017 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 253-259). IEEE.

Saunders, M., Lewis, P., Thornhill, A., Booij, M., & Verckens, J. P. (2011). Methoden en technieken van onderzoek. Pearson Education.

Strauss, A., & Corbin, J. (1999). Basics of qualitative research: Techniques and procedures for developing grounded theory. doi:0-80395939-7 hardcover

Weatherford, D., & Ruppert, M. P. (2016). Auditing and Monitoring: A Closer Look at the Second of the Three Lines of Defense. *Journal of Health Care Compliance, 18*(1), 51–54.

Yin, R. K. (2003). Design and methods. *Case study research*, *3*(9.2).

Appendix

Interviewprotocol

1. Kan u uzelf kort voorstellen?

2. Wat is uw functie en hoe lang doet u deze functie?

3. In welke mate is er meer nood aan *cybersecurity*? Zijn hier bepaalde verklaringen voor?

4. Hoe heeft COVID-19 hier een invloed op gehad?

5. Als we nu echt spreken over hackers, wat zijn daar de grootste risico's? Welke soort aanvallers komen voor?

6. In welke mate worden KMO's geconfronteerd met gelijke risico's?

7. Welke middelen gebruiken hackers het meeste? Welke zijn het gevaarlijkste?

8. Hoe komt het dat het zo moeilijk is om te achterhalen wie achter deze aanvallen zit?

9. Hoe gaan ondernemingen zich hier het beste tegen beschermen? Geldt dit ook voor KMO's?

10. Hoe kunnen *cybersecurity* raamwerken zoals NIST CSF, COBIT, ISO standaarden… toegevoegde waarde bieden? Is dit voor ondernemingen van alle groottes zo?

11. Hanteren jullie zelf een bepaald raamwerk?

12. Waarom kozen jullie voor dit bepaald raamwerk?

13. Zijn er enkele raamwerken beter dan anderen?

14. Welke factoren zijn belangrijk om zo een raamwerk succesvol te implementeren?

15. In welke mate bent u zelf al geconfronteerd geweest met raamwerken die niet succesvol werden geïmplementeerd? Wat was de oorzaak daarvan?

16. Wanneer medewerkers bewust gemaakt moeten worden van bepaalde risico's en inzicht moeten verkrijgen in die systemen, is dat een uitdaging? Hoe gaan jullie om met mensen die geen IT achtergrond hebben en daardoor niet kunnen volgen?

17. Wat gebeurt er als het management niet achter je staat?

18. Veel KMO's gaan hun IT volledig outsourcen omdat ze het geld en de middelen niet hebben om IT in huis te doen. Hoe kijkt u hiernaar? Is dit een goede oplossing?

19. Hoe ziet u de rol van de audit functie, zowel intern als extern? Wat is haar aandeel in heel dit cyberverhaal?

20. Uit de academische literatuur is er naar voren gekomen dat bepaalde certificaten zoals CISA en CPA waardevol kunnen zijn. Wat is uw mening hierover?

21. Welke certificaten zouden nog waardevol kunnen zijn voor auditors op dat vlak?

22. Zijn er nog andere zaken die niet besproken zijn maar u wel belangrijk vindt en wilt toevoegen?