CS Barometer

Maturiteit in cybersecurity bij Vlaamse bedrijven

Petra Andries (Centre for Entrepreneurship Research, UGent) Tom Evens, Mathias Maes (Research Group for Media, Innovation & Technology, UGent) Jo Reynaerts (VIVES - Research Centre for Regional Economics, KU Leuven) Dimitri Schuurman, Annabel Georges (imec)

CYBERSECURITY VLAANDEREN
BOUWEN AAN JE DIGITALE TOEKOMST
imec
ecoom
Kenniscentrum Data & Maatschappij
STEUNPUNT ECONOMIE & ONDERNEMEN
Vlaanderen is economie, wetenschap & innovatie

Inhoudstafel

Samenvatting

In opdracht van het Departement Economie, Wetenschap en Innovatie (EWI) van de Vlaamse Overheid brengt deze CS-Barometer de maturiteit in cybersecurity (CS) bij Vlaamse bedrijven in kaart. De bedoeling bestaat erin een eerste nulmeting te voorzien om een actuele **monitoring van de maturiteit, drempels en noden inzake CS** te verschaffen en zodanig de impact van het desbetreffende *Vlaamse Actieplan Cybersecurity* mee te helpen evalueren. Toekomstige meetmomenten bieden de mogelijkheid om een longitudinaal overzicht van de evolutie inzake CS bij Vlaamse bedrijven te verwerven en deze als een internationale benchmark te beschouwen.

Deze CS-Barometer schetst een wetenschappelijk onderbouwd beeld van de mate waarin Vlaamse bedrijven CS-maatregelen in hun werking integreren en stoelt op **twee cruciale methodologische principes**. Ten eerste, een grootschalige, aselecte steekproef (steekproefaantal van 14.274 bedrijven, 1.532 bruikbare antwoorden in totaal) representatief voor de populatie van Vlaamse bedrijven volgens bedrijfsgrootte en sector van activiteit. Ten tweede, een gevalideerd meetinstrument in lijn met gelijkaardige Europese vragenlijsten die als benchmark kunnen fungeren.

De mate van CS-maturiteit van bedrijven wordt in belangrijke mate bepaald door een **combinatie van maatregelen**. Ten eerste, bedrijven kunnen *technische maatregelen* nemen, zoals toegangscontrole instellen of cryptografie gebruiken om bedrijfsgegevens te beschermen. Ten tweede, bedrijven kunnen verschillende *beheerprocedures* implementeren waarmee ICT- en operationele systemen worden gebruikt, beheerd en onderhouden. Ten derde, bedrijven kunnen maatregelen nemen om de *kennis en het bewustzijn* omtrent het beschermen van informatie, toestellen, systemen en netwerken bij het management en de medewerkers te verhogen. De CS-maturiteit van een bedrijf neemt toe naarmate het bedrijf op elk van deze aspecten maatregelen neemt.

De belangrijkste bevindingen van de studie zijn:

- **De meerderheid van Vlaamse bedrijven neemt verschillende technische CS-maatregelen.** Bijna een kwart (25,5%) van de bedrijven past 3 tot 5 maatregelen toe, 41,2% 6 tot 9 maatregelen en 20% zelfs 10 of meer maatregelen. In totaal neemt 94,2% van de bedrijven technische maatregelen om de cybersecurity te garanderen; 5,8% neemt vooralsnog geen enkele CS-maatregel. **Het gebruik van CS-maatregelen is daarbij veel vaker een zaak van middelgrote (50-249 werknemers) en grote (meer dan 249 werknemers) bedrijven.** Kleine (10 tot 49 werknemers) en microbedrijven (5 tot 9 werknemers) nemen een opmerkelijk minder aantal CS-maatregelen. De CS-maturiteit neemt toe naarmate bedrijven meer CS-technologieën invoeren.

- **Het nemen van technische CS-maatregelen blijft vaak beperkt tot relatieve basistoepassingen die een minder sterke bescherming bieden.** Zo voert 90,9% geregeld software-updates door; 85,3% maakt data back-ups naar een aparte locatie of in de cloud; 74,5% heeft een protocol voor toegangsbeheer tot het netwerk en 69% heeft een sterke paswoordauthenticatie. **Slechts een minderheid wendt meer geavanceerde CS-maatregelen aan.** Hierbij gaat het onder meer om maatregelen rond het bijhouden van log files om cyberaanvallen te analyseren (46,0%), periodieke ICT-veiligheidsanalyse (44,0%), ICT-veiligheidstesten (37,8%) of encryptietechnieken voor data, documenten of e-mails (28,2%). Minder dan de helft (42,9%) maakt automatisch afspraken met onderaannemers en leveranciers omtrent ICT-veiligheidsvereisten. 41,0% van de Vlaamse bedrijven biedt zijn werknemers opleidingen of activiteiten aan om hen bewust te maken van het belang van cybersecurity.

- **Bedrijven implementeren slechts een beperkt aantal beheerprocedures om zich tegen cyberrisico's te beschermen of om met actuele dreigingen om te gaan.** 71% van de Vlaamse bedrijven implementeren vooral CS-procedures om zich effectief te *beschermen* tegen cyberaanvallen (bijvoorbeeld toegangsbeheer of identificatiemanagement) maar zetten minder in op procedures om gevoelige databronnen of kritieke bedrijfsprocessen die mogelijk doelwit zijn bij een mogelijke cyberaanval te *identificeren* (41,9%). 48,5% heeft procedures om cyberaanvallen te *detecteren* (bijvoorbeeld continue monitoring van veiligheidsrisico's), 38,3% om adequaat op cyberaanvallen te *reageren* (bijvoorbeeld aan de hand van incidentanalyse of crisiscommunicatie) en 50,1% om van een cyberaanval te *herstellen* (zoals herstel van back-ups, her-installeren van systemen of wijzigen van wachtwoorden). De CS-maturiteit neemt toe naarmate bedrijven meer beheerprocedures instellen. Ook hier geldt dat **grote en middelgrote bedrijven (respectievelijk 4,2 en 3,4 procedures) meer beheerprocedures inzetten dan kleine en microbedrijven (respectievelijk 2,5 en 2,1 procedures).**

- **Het gebrek aan kennis, vaardigheden en expertise binnen de onderneming vormt voor 44,9% van de bedrijven de belangrijkste uitdaging bij de implementatie van een CS-beleid.** Bovendien ervaren bedrijven moeilijkheden om werknemers met de vereiste kennis, vaardigheden en expertise te selecteren en aan te werven (30,7%). **Voor 40,7% van de bedrijven vormt een gebrek aan bewustzijn bij de werknemers over de problematiek van cybersecurity een belangrijke drempel.** Dit gebrek aan bewustzijn geldt bovendien zowel voor bedrijven met een lage als hoge CS-implementatiegraad. Eén op vijf (19,8%) ziet een gebrekkige meerwaarde van cybersecurity voor de eigen organisatie als problematisch; 22,1% erkent een gebrek aan prioriteit bij het management als een drempel voor een effectief CS-beleid.

- **De evolutie van het CS-budget bij Vlaamse bedrijven bleef het afgelopen jaar grotendeels onveranderd.** Vlaamse bedrijven spenderen gemiddeld 20,7% van het totale IT-budget aan cybersecurity. Voor de meerderheid (53%) bleef dit budget ongewijzigd, maar 44,7% van de bedrijven liet een – lichte of sterke – stijging noteren. De stijging is het sterkst merkbaar bij grote bedrijven.

- **11,8% van de Vlaamse bedrijven werd het afgelopen jaar slachtoffer van een cyberaanval.** Grote bedrijven (26,8%) zijn het vaakst slachtoffer hiervan, ook middelgrote bedrijven (19,2%) worden bovengemiddeld getroffen. Dit in tegenstelling tot kleine (12,3%) en microbedrijven (8,8%) die in iets minder mate worden geviseerd door cybercriminelen.

- **Kleinere en microbedrijven kennen grotere operationele gevolgen als gevolg van een geslaagde cyberaanval.** Van de geviseerde bedrijven geeft 41,9% aan dat ze als gevolg van een cyberaanval het afgelopen jaar geconfronteerd werden met de *onbruikbaarheid van ICT-systemen*, bijvoorbeeld door hacking, kwaadwillige vergrendeling of DDoS-aanval. Minder prevalent is *onbruikbaarheid van OT-systemen*, zoals machines, gebouwen of andere infrastructuur (10%). 23,5% van de bedrijven kreeg te maken met de *vernietiging of het onbruikbaar maken van bedrijfsgegevens*, bijvoorbeeld door infectie van kwaadaardige software of ongeoorloofde toegang. Tot slot kreeg 13,3% van de bedrijven te kampen met *diefstal van (confidentiële) bedrijfsgegevens*, bijvoorbeeld door infectie van kwaadaardige software of phishingberichten.

- **Bijna een kwart van de Vlaamse bedrijven (22,5%) is verzekerd tegen cyberaanvallen.** Van de grote bedrijven claimt ongeveer de helft (49%) een verzekering afgesloten te hebben tegen cyberaanvallen. Dit aantal ligt een pak lager bij de middelgrote bedrijven (32,90%), de kleine bedrijven (23,9%) en de microbedrijven (16,2%).

1. Inleiding

Onze maatschappij digitaliseert en automatiseert in een snel tempo. Bedrijven maken in toenemende mate gebruik van industrie 4.0-technologieën zoals artificiële intelligentie (AI), robots of Internet of Things om hun concurrentiepositie te versterken. Tegelijkertijd vormt deze toenemende afhankelijkheid van digitale netwerkinfrastructuur een belangrijke bron van kwetsbaarheid en bedreiging. Een adequaat beleid inzake cybersecurity (CS) is van cruciaal belang voor de digitale economie en beschermt bedrijven, overheden en andere organisaties tegen schadelijke cyberaanvallen en kwaadwillige inbreuken op operationele en computernetwerken. Het *Vlaamse Actieplan Cybersecurity* versterkt het bestaande overheidsinstrumentarium om bedrijven te informeren, sensibiliseren, begeleiden én het ondersteunen bij het gebruik van cybersecuritytoepassingen[1].

In opdracht van het Departement Economie, Wetenschap en Innovatie (EWI) van de Vlaamse Overheid brengt voorliggende CS-Barometer **de adoptie van, het gebruik van en de expertise in CS bij Vlaamse bedrijven** in kaart. De bedoeling bestaat erin een eerste nulmeting te voorzien om een actuele monitoring van de maturiteit, drempels en noden inzake CS te verschaffen en zodanig de impact van het desbetreffende Vlaamse actieplan mee te helpen evalueren. Toekomstige meetmomenten bieden de mogelijkheid om een longitudinaal overzicht van de evolutie inzake CS bij Vlaamse bedrijven te verwerven en deze als een internationale benchmark te beschouwen.

Deze CS-Barometer schetst een wetenschappelijk onderbouwd beeld van de mate waarin Vlaamse bedrijven CS-maatregelen in hun werking en aanbod integreren. Om een accuraat beeld van de onderzochte problematiek te bekomen, stoelt deze CS-Barometer op twee cruciale methodologische principes:

1. **Representativiteit:** een grootschalige, aselecte steekproef representatief voor de populatie van Vlaamse bedrijven volgens bedrijfsgrootte en sector van activiteit;
2. **Vergelijkbaarheid:** een gevalideerd meetinstrument in lijn met gelijkaardige Europese vragenlijsten die als benchmark kunnen fungeren.

Bovenstaande principes zijn cruciaal om de vergelijkbaarheid met andere studies die de adoptiegraad van CS bij Vlaamse bedrijven in kaart brengen te evalueren. Indien deze studies niet stoelen op dezelfde methodologische principes inzake representativiteit en vergelijkbaarheid is

1 Zie https://www.ewi-vlaanderen.be/nieuws/vlaamse-regering-hecht-goedkeuring-aan-onderzoeksprogramma-cybersecurity-initiative-flanders

er weinig tot geen wetenschappelijke grond om de resultaten van diverse studies met elkaar te vergelijken.

Deze onderzoeksopdracht brengt drie partners samen die elk een unieke thematische en/of methodologische expertise inbrengen:

1. Het **Steunpunt Economie en Ondernemen** (STORE) adviseert de Vlaamse overheid op het gebied van clusters, economisch ondersteuningsbeleid, en ondernemen in Vlaanderen. STORE is een samenwerking tussen het Vlaamse Centrum voor Economie en Samenleving (VIVES) van de KU Leuven en het Departement Marketing, Organisatie en Innovatie van Universiteit Gent;

2. **imec-mict-UGent** is een interdisciplinaire onderzoeksgroep van de Universiteit Gent met focus op de veranderende rol van digitale technologie in relatie tot mens en maatschappij. De groep is betrokken bij het Vlaams Kenniscentrum voor Data & Maatschappij dat zich tot doel stelt de ethisch-maatschappelijke en beleidsaspecten van data en AI in kaart te brengen;

3. **imec Vlaanderen** heeft expertise in de ontwikkeling en realisatie van digitale technologieën in Vlaanderen. Als strategisch onderzoekscentrum focust imec ook op het voeren van vraag-gedreven onderzoek en ontwikkeling, in samenwerking met overheden, imec-departementen, kennisinstellingen, bedrijven en burgers. Imec coördineert verschillende 'technologie'-meters zoals Digimeter, eHealth Monitor en Smart City Monitor.

2. Methodologie

2.1 Meetinstrument

Inzake meetinstrument werd een maximale vergelijkbaarheid met gelijkaardige Europese vragenlijsten en onderzoeksinitiatieven nagestreefd. De vragenlijst omvat module E (ICT-security) van de *Survey on ICT Usage and E-Commerce in Enterprises* aangewend door Eurostat [1] en Statbel[2] , en gepubliceerd in de Digital Economy and Society Index (DESI)[3] . Deze module werd aangevuld met bestaande elementen uit andere relevante nationale en internationale studies[4]. Tot slot werden nieuwe elementen inzake de impact van CS op de bedrijfsprestaties en de kennis over beleidsondersteunende maatregelen van de Vlaamse overheid opgenomen.

Tijdens de maanden april en mei 2021 werd de vragenlijst uitvoerig getest middels een serie van diepte-interviews met bedrijven uit de onderzoekspopulatie. In deze interviews werd de vragenlijst samen met deze bedrijven ingevuld via het *think aloud*-protocol en werden mogelijke verbeterpunten geïdentificeerd. Behalve deze interviews werden bedrijven actief binnen de CS-sector en sectororganisaties via e-mail voor feedback gecontacteerd. Daarnaast werden ook onafhankelijke experts betrokken. Deze input werd samen met de opdrachtgever besproken en verwerkt.

De combinatie van de gehanteerde steekproeftrekking en de vergelijkbaarheid van het meetinstrument met ander beleidsvoorbereidend onderzoek inzake CS laat toe voorliggende cijfers als een internationale benchmark te beschouwen. Zodoende kan de positie van Vlaanderen vergeleken en geëvalueerd worden binnen de context van de Europese lidstaten (waaronder België). De ontwikkeling van een stabiel meetinstrument in lijn met de structurele dataverzamelingen van officiële instanties zoals Eurostat en Belstat biedt perspectieven voor het verzamelen van longitudinale gegevens over het gebruik van en expertise in CS bij Vlaamse bedrijven. Op basis van periodieke meetmomenten kan een evolutie ter zake worden geschetst.

1 https://ec.europa.eu/eurostat/cache/metadata/en/isoc_e_esms.htm

2 https://statbel.fgov.be/en/themes/enterprises/ict-and-e-commerce-enterprises#documents

3 https://digital-strategy.ec.europa.eu/en/policies/desi

4 IPSOS (2021). *Cyber Security Breaches Survey* 2021 (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021); Coomans, P.; Callewaert, K.; Codenie, W. & Schellekens, Y. (2021). *Cybersecurity in de maakindustrie* (https://www.digitaletoekomst.be/sites/default/files/2021-04/studie_cybersecurity_maakindustrie_NL.pdf)

2.2 Populatie, steekproeftrekking en contactinformatie

In overleg met de opdrachtgever werd vastgelegd welke economische sectoren en grootteklassen van bedrijven dienden opgenomen te worden in het onderzoek. Het gaat om bedrijven in een breed scala van productie- en dienstensectoren (zie Appendix 1 voor een overzicht van de geselecteerde sectoren). Zowel grote, middelgrote, kleine als micro-ondernemingen werden opgenomen. Voor deze laatste grootteklasse werd wel een ondergrens van minstens vijf werknemers gehanteerd (zie Tabel 1 voor populatie-aantallen, gestratificeerd naar sector en grootteklasse). De Bel-first databank van Bureau van Dijk werd als vertrekpunt gehanteerd.

In lijn met internationaal onderzoek werd een oververtegenwoordiging van middelgrote en grote bedrijven in de finale dataset beoogd. Dit had onmiddellijke implicaties voor de steekproeftrekking. In praktijk werden alle middelgrote en grote bedrijven (in de geselecteerde sectoren) bevraagd waarvoor contactinformatie werd gevonden. Van de kleine bedrijven in de populatie werd in totaal 17% geselecteerd (rekening houdend met de verdeling over de verschillende sectoren). Hierbij werd erover gewaakt geen kleine bedrijven te bevragen die ook al deel uitmaakten van de steekproef van de *Community Innovation Survey*[1] – dit om hen niet bovenmatig te belasten. Ook de microbedrijven mochten ondervertegenwoordigd zijn in de finale dataset. Omdat contactinformatie vrij gemakkelijk beschikbaar was voor deze laatste groep, en telefonische opvolging dan weer zeer duur, werd ervoor gekozen alle microbedrijven die geen deel uitmaakten van de meest recente steekproef voor de *Community Innovation Survey* en waarvoor contactinformatie beschikbaar was, op te nemen in de steekproef, maar hen achteraf minder intensief op te volgen.

Voor elk bedrijf in de steekproef werd een contactpersoon en bijhorend e-mailadres opgezocht in de Bel-first databank. Indien niet beschikbaar, werd deze informatie aangevuld met gegevens uit Trends Top. Indien ook hier geen relevante contactinformatie beschikbaar was, werd deze opgezocht op het internet. Voor microbedrijven werd waar mogelijk de zaakvoerder gecontacteerd. Voor kleine, middelgrote en grote bedrijven werd de voorkeur gegeven aan personen verantwoordelijke voor technologische ontwikkelingen en, in tweede instantie, aan personen met meer algemene management of IT-functies. De totale steekproef bevatte 14.274 bedrijven in Vlaanderen. De dataverzamelingsperiode liep van mei tot augustus 2021.

1 https://ec.europa.eu/eurostat/web/microdata/community-innovation-survey en https://www.ecoom.be/nodes/cisenrd/nl

Tabel 1: Populatie- en steekproefaantallen per stratum (steekproefaantallen schuin gedrukt)

	NACE 10-33	NACE 35-39	NACE 41-43	NACE 45-47	NACE 49-53	NACE 55-56	NACE 58-63	NACE 68-75	NACE 77-82; 95.1[1]	Totaal
Micro (5-9 werknemers)	1.482 *971*	66 *29*	2.257 *1.685*	4.414 *2.825*	747 *451*	1.605 *859*	533 *259*	1.976 *1.198*	710 *458*	**13.790** ***8.735***
Klein (10-49 werknemers)	2.602 *427*	154 *35*	2.391 *393*	5.043 *817*	1.349 *226*	1.914 *317*	751 *131*	1.674 *278*	910 *158*	**16.788** ***2.782***
Middelgroot (50-249 werknemers)	812 *658*	36 *30*	340 *258*	688 *447*	316 *247*	117 *56*	150 *105*	262 *181*	363 *204*	**3.084** ***2.186***
Groot (≥250 werknemers)	227 *183*	23 *17*	50 *44*	156 *95*	62 *45*	22 *13*	36 *26*	69 *54*	145 *94*	**790** **571**
Totaal	**5.123** ***2.239***	**279** ***111***	**5.038** ***2.380***	**10.301** ***14.184***	**2.474** ***969***	**3.658** ***1.245***	**1.470** ***521***	**3.981** ***1.711***	**2.128** ***914***	**34.452** ***14.274***

1 NACE sectoren 77-82 en 95.1 werden samengevoegd, omdat Bel-first voor die laatste sector slechts 11 bedrijven met tewerkstellingscijfers bevatte.

2.3 Respons en weging

Van de 14.274 bedrijven die we een e-mail stuurden, konden we er 12.618 bereiken. 1.656 e-mails konden niet afgeleverd worden. Na het uitsturen van twee herinneringen per e-mail, en een doorgedreven telefonische opvolging, ontvingen we antwoorden van 2.741 bedrijven. Dit impliceert een responsgraad van 22% (2.741/12.618). Van deze antwoorden waren uiteindelijk 1.532 antwoorden bruikbaar (zie Tabel 2). 1.209 antwoorden vielen uit de responsgroep omdat zij, op basis van de antwoorden op de vragenlijst, (a) minder dan 5 werknemers bleken te hebben, (b) niet tot de juiste sector behoorden, (c) geen enkele vraag betreffende cybersecurity hadden beantwoord, of (d) omdat we voor een bedrijf twee antwoorden verkregen (doordat bepaalde respondenten de vragenlijst invulden voor een ander ondernemingsnummer dan gevraagd).

Voor elk bedrijf dat antwoordde, werd nagegaan tot welk stratum het behoorde. Het kreeg vervolgens een gewicht, afhankelijk van het totaal aantal bedrijven in de populatie voor dat stratum en van het totaal aantal bruikbare antwoorden voor dat stratum. Dit rapport presenteert dan ook gewogen cijfers, die – omwille van deze weging – representatief zijn voor de totale bedrijfspopulatie beoogd in het onderzoek.

Tabel 2: Respons per stratum

	NACE 10-33	NACE 35-39	NACE 41-43	NACE 45-47	NACE 49-53	NACE 55-56	NACE 58-63	NACE 68-75	NACE 77-82; 95.1	Totaal
Micro (5-9 werknemers)	38	1	47	75	19	13	14	66	5	**278**
Klein (10-49 werknemers)	85	3	109	156	52	25	33	86	22	**571**
Middelgroot (50-249 werknemers)	157	9	69	83	40	8	26	46	21	**459**
Groot (≥250 werknemers)	77	8	20	41	26	2	13	24	13	**224**
Totaal	**357**	**21**	**245**	**355**	**137**	**48**	**86**	**222**	**61**	**1.532**

3. Resultaten

Dit onderdeel behandelt het bewustzijn en de aanpak van cybersecurity (CS) bij Vlaamse bedrijven. CS verwijst naar het beschermen van computers, servers, netwerken, mobiele toestellen, software, elektronische systemen en data tegen schadelijke cyberaanvallen. Een cyberaanval is een kwaadwillige inbreuk op de veiligheidssystemen van een onderneming met als motief operationele of computersystemen onklaar te maken, persoonlijke of confidentiële gegevens te los te weken of een losgeldbetaling te verkrijgen. Cyberaanvallen zijn er in diverse gradaties, gaande van phishing (frauduleuze berichten) of malware (kwaadaardige software), tot hacking en DDoS (denial of service) waarbij netwerksystemen worden geïnfiltreerd of zelfs vergrendeld.

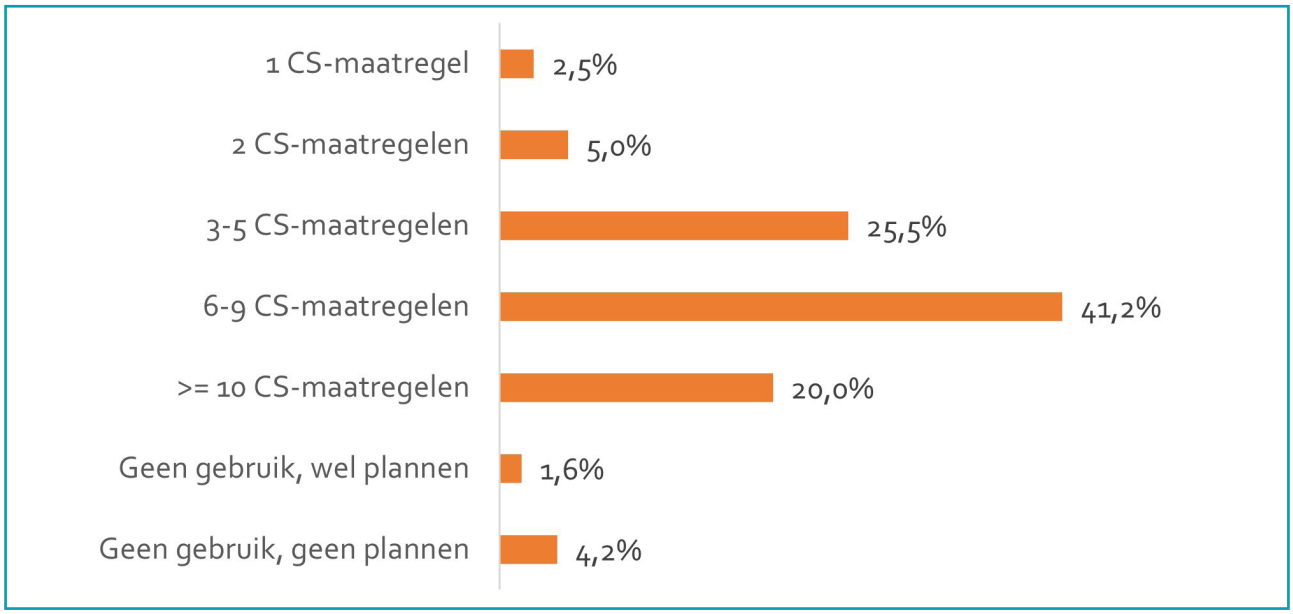
De mate van maturiteit van bedrijven inzake cybersecurity wordt in belangrijke mate bepaald door een combinatie van maatregelen. Ten eerste, bedrijven kunnen *technische maatregelen* nemen, zoals toegangscontrole instellen of cryptografie gebruiken om informatie te beschermen. Ten tweede, bedrijven kunnen *beheerprocedures* implementeren waarmee digitale systemen worden gebruikt, bestuurd en onderhouden. Een adequaat CS-beleid is er op gericht cyberrisico's te identificeren, gegevens en systemen te beschermen, cyberaanvallen te detecteren en te beantwoorden, én de situatie opnieuw te herstellen. Ten derde, medewerkers vormen een belangrijke, en misschien zelfs meest kwetsbare, schakel in de bescherming van bedrijven tegen cyberaanvallen. *Kennis, vaardigheden en bewustzijn* omtrent het beschermen van informatie, toestellen en netwerken bij het management en de medewerkers zijn immers essentieel voor de effectiviteit van technische maatregelen en beheerprocedures. De CS-maturiteit van een bedrijf neemt toe naarmate het bedrijf op elk van deze domeinen maatregelen neemt.

3.1 Technische maatregelen

De resultaten uit Figuur 1 geven aan dat de meerderheid van de Vlaamse bedrijven een veelheid aan technische CS-maatregelen inzetten om hun cyberveiligheid zo goed als mogelijk te verzekeren. Na het voorleggen van een lijst van 12 mogelijke CS-maatregelen (zie verderop) zegt 25,5% van de bedrijven 3 tot 5 CS-maatregelen toe te passen, 41,2% past 6-9 CS-maatregelen toe terwijl één op de vijf van de bedrijven 10 of meer van de bevraagde CS-maatregelen toepast. In totaliteit past dus 94,2% van de Vlaamse bedrijven ten minste 1 CS-maatregel toe. Dit wijst erop dat slechts een kleine minderheid (5,8%) geen enkele CS-maatregel toepast in de dagelijkse werking. 4,2% van de bedrijven zegt geen plannen te hebben om één of meerdere

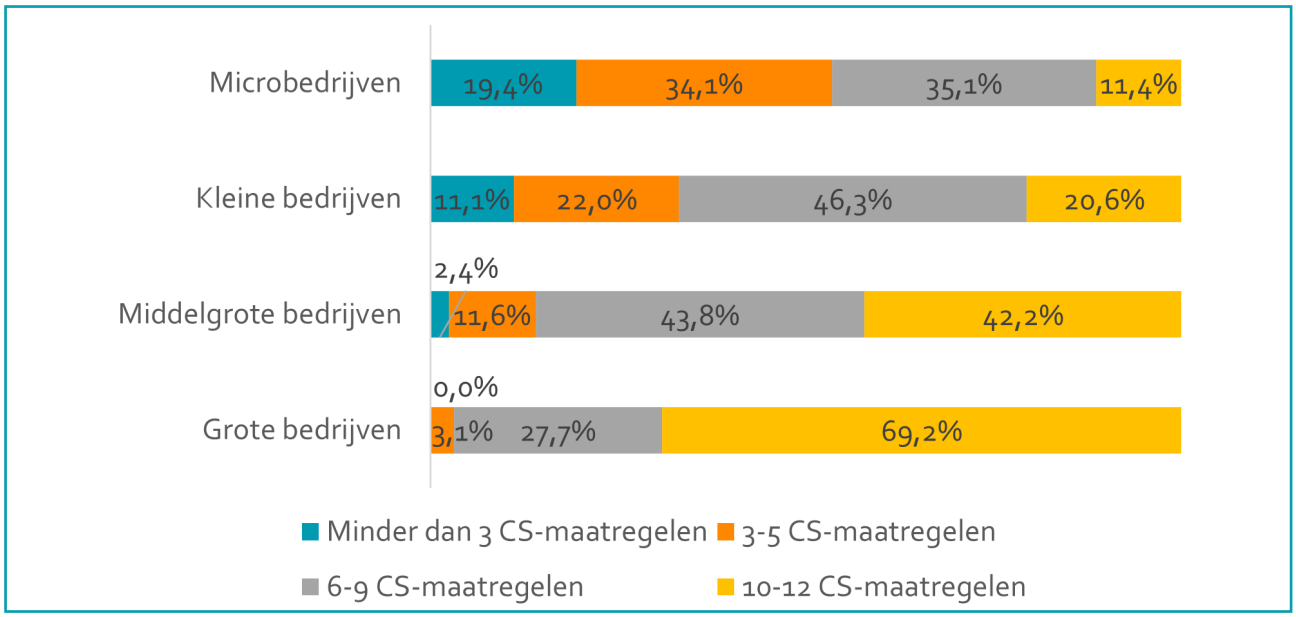
CS-maatregelen te implementeren in het komende jaar; 1,6% heeft daartoe wel plannen.

Figuur 1: Adoptiegraad aantal CS-maatregelen (N=1.532)



Wanneer de bedrijfsgrootte (in termen van aantal werknemers) in beschouwing wordt genomen, is er een duidelijk verband met het aantal geïmplementeerde CS-maatregelen: hoe groter een bedrijf, hoe meer CS-maatregelen het bedrijf neemt (zie Figuur 2). 69,2% van de grote bedrijven past dan meer dan 10 van de vooropgestelde CS-maatregelen toe, een bijkomende 27,7% neemt 6 tot 9 CS-maatregelen. 18,6% van de grote bedrijven geven aan alle bevraagde CS-maatregelen toe te passen in hun werking, terwijl geen enkel van de grote bedrijven aangeeft minder dan 2 CS-maatregelen geïmplementeerd te hebben. Bij de middelgrote bedrijven bedraagt het aantal organisaties met 10 of meer CS-maatregelen 42,2%. Dit aantal ligt beduidend lager bij de kleine (20,6%) en de microbedrijven (11,4%). Van deze laatste geeft 19,9% aan minder dan 3 CS-maatregelen te nemen.

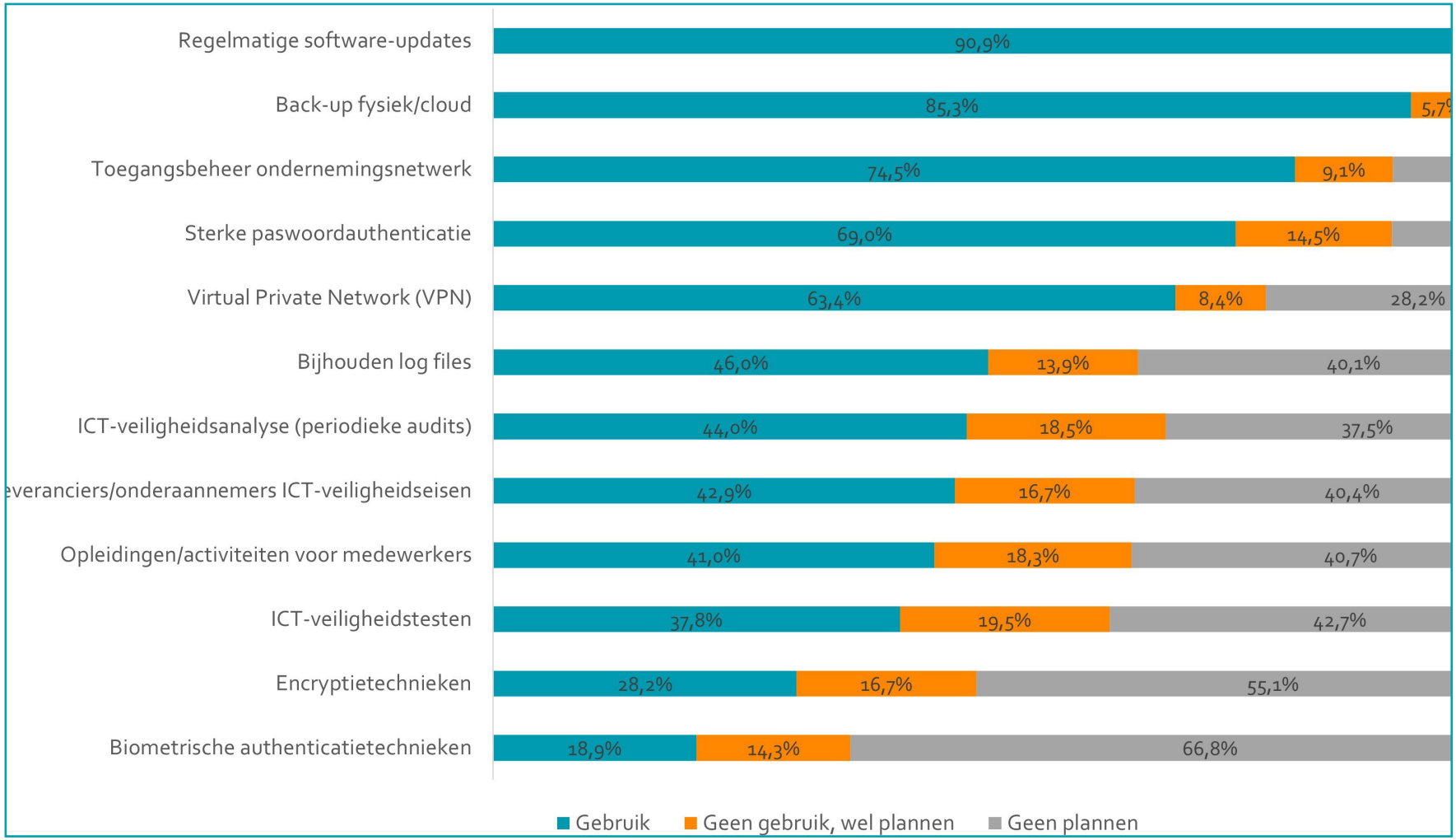
Figuur 2: Adoptiegraad aantal CS-maatregelen volgens bedrijfsgrootte (N=1.532)



Bedrijven kunnen een breed spectrum aan technische maatregelen stellen om een hogere cyberveiligheid te bekomen. Deze maatregelen gaan van eerder basis (zoals paswoordauthenticatie of software-updates) tot vrij geavanceerd (bijvoorbeeld biometrische authenticatie of encryptietechnieken). Al naargelang de complexiteit vertoont de adoptie van deze CS-maatregelen sterke verschillen (zie Figuur 3). Het regelmatig doorvoeren van software-updates, te beschouwen als een basismaatregel, wordt het meest toegepast (90,9%). Een bijna even vaak toegepaste maatregel is het maken van een data back-up naar een aparte locatie of in de cloud: 85,3% geeft aan dit te doen. 74,5% heeft een protocol voor toegangsbeheer tot het ondernemingsnetwerk voor toestellen of gebruikers. Ook beschikt ongeveer twee derden (63,4%) van de bedrijven over een VPN-netwerk. Ook een sterke paswoordauthenticatie met 69% is stevig verankerd in de bedrijfswerking.

Een minderheid van bedrijven neemt andere, vaak meer geavanceerde, technische maatregelen en is zich meer bewust van het belang van cybersecurity. Concreet gaat het hierbij om maatregelen rond het bijhouden van log files om cyberaanvallen te analyseren (46,0%), periodieke ICT-veiligheidsanalyse (44,0%) of ICT-veiligheidstesten (37,8%). Een minderheid van 28,2% past encryptietechnieken toe op data, documenten en/of e-mails; 18,9% gebruikt biometrische technieken ter identificatie en authenticatie van gebruikers (vingerafdrukken, stem- en/of gezichtsherkenning). Minder dan de helft (42,9%) maakt automatisch afspraken met onderaannemers en leveranciers omtrent ICT-veiligheidsvereisten. Bovendien biedt slechts 41,0% van de Vlaamse bedrijven zijn werknemers opleidingen of activiteiten aan om hen bewust te maken van het belang van cybersecurity.

Figuur 3: Adoptiegraad type CS-maatregelen (N=1.532)



Bij de interpretatie van deze resultaten moet men er zich van bewust zijn dat een hoge adoptiegraad van deze of gene CS-maatregelen niet noodzakelijk samengaat met een hoge mate van CS-maturiteit. De meest optimale bescherming tegen cyberaanvallen ligt onder meer in de combinatie van een zo groot aantal van basis- én meer geavanceerde CS-technologieën. Het loutere feit dat bedrijven een aantal technische CS-maatregelen treffen is in die optiek niet automatisch voldoende; de kracht van bescherming ligt immers in de combinatie van CS-technologieën. Bovendien wijzen de resultaten er op dat zelfs vrij elementaire basistoepassingen, zoals regelmatige software-updates, sterke paswoordauthenticatie, toegangsbeheer van het ondernemingsnetwerk en een systematisch beleid rond back-ups niet door alle bedrijven worden toegepast. Het is ook belangrijk er op te wijzen dat slechts een minderheid van bedrijven opleidingen of activiteiten aanbiedt om het bewustzijn en de kennis van zijn medewerkers omtrent cybersecurity te verhogen.

3.2 Beheerprocedures

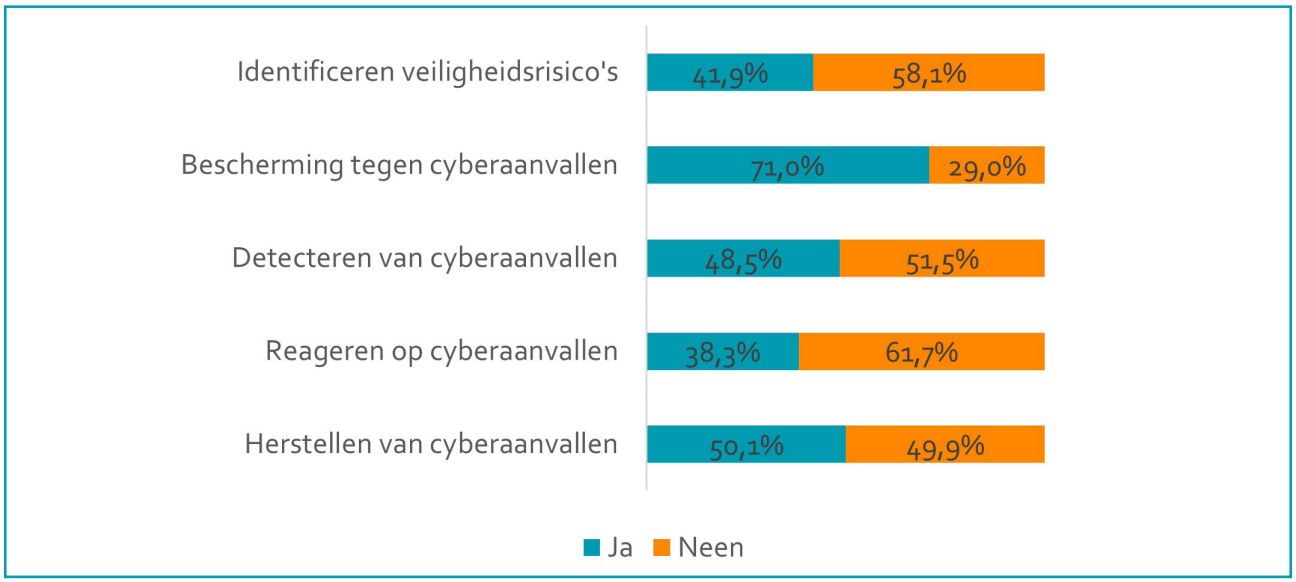
Behalve specifieke CS-maatregelen kunnen bedrijven ook beheerprocedures installeren teneinde zich te beschermen tegen toekomstige cyberrisico's of met actuele cyberaanvallen om te gaan. Zo biedt het NIST-kader een reeks van standaarden, richtlijnen en procedures voor bedrijven om cyberveiligheid te beheren en mogelijke risico's te beperken[1]. NIST bestaat uit vijf elementen van een systematisch cybersecuritybeleid (identificeren, beschermen, detecteren, reageren, herstellen) die cumulatief organisaties helpen cyberaanvallen te identificeren en detecteren, en richtlijnen biedt om preventief en reactief te antwoorden op cyberaanvallen en er van te herstellen. Net zoals bij het nemen van CS-maatregelen volstaat het niet om deze of gene beheerprocedure te hebben, maar ligt een adequate cyberbeveiliging in de toepassing van alle vijf elementen: hoe meer procedures een bedrijf instelt, hoe hoger de CS-maturiteit van dat bedrijf.

Ten eerste claimt 41,9% van die bedrijven die ten minste één technische CS-maatregel treffen (i.e. 94,2% van de Vlaamse bedrijven) beheerprocedures te hebben ingevoerd om veiligheidsrisico's binnen het bedrijf te *identificeren* (zie Figuur 4). Het gaat hierbij bijvoorbeeld om het documenteren van gevoelige databronnen of kritieke bedrijfsprocessen die mogelijk doelwit zijn bij een mogelijke cyberaanval. Ten tweede zegt 71,0% procedures te hebben om zich effectief te *beschermen* tegen cyberaanvallen, bijvoorbeeld via toegangsbeheer, identificatiemanagement, back-ups, encryptie of regelmatige software-updates. Ten derde heeft 48,5% van de bedrijven procedures in plaats om cyberaanvallen te *detecteren*, bijvoorbeeld via continue monitoring van veiligheidsrisico's, technieken en protocollen. Ten vierde zegt 38,3% van de bedrijven

1Voor meer informatie, zie https://www.nist.gov/cyberframework

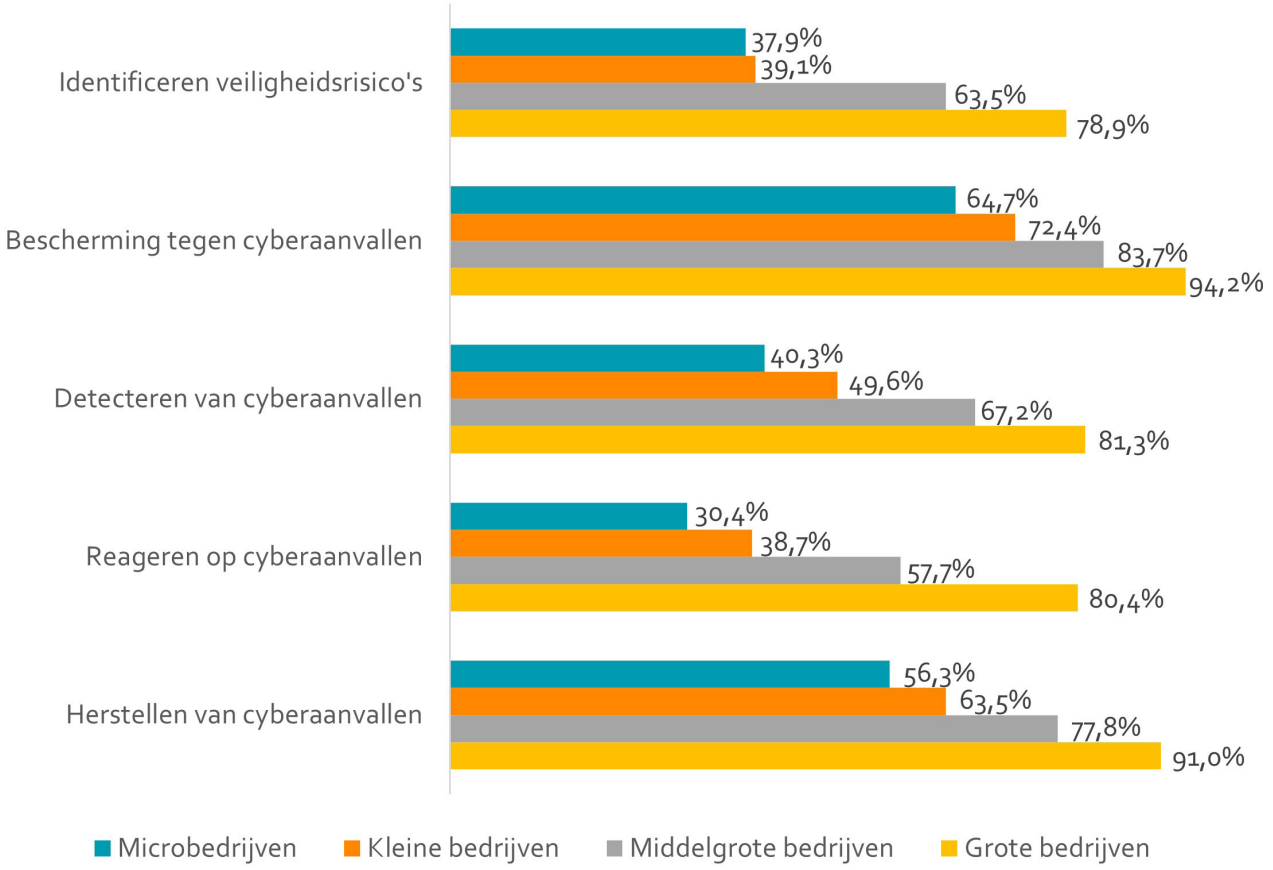
procedures te hebben om adequaat op cyberaanvallen te *reageren*, bijvoorbeeld aan de hand van incidentanalyses, dreigingseliminatie en/of crisiscommunicatie. Tot slot telt de helft van de bedrijven (50,1%) procedures om te *herstellen* van een mogelijke cyberaanval (zoals herstel van back-ups, het her-installeren van systemen, het wijzigen van wachtwoorden of firewalls en dergelijke meer).

Figuur 4: Type beheerprocedures (N= 1.469) - *Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen*



Net zoals bij de CS-maatregelen blijkt er een sterk verband tussen het installeren van gerichte beheerprocedures en de bedrijfsgrootte. Ook hier geldt: hoe groter het bedrijf, hoe vaker de kans dat het bedrijf beheerprocedures heeft geïnstalleerd (zie Figuur 5). Zo heeft 78,9% van de grote bedrijven procedures om veiligheidsrisico's te identificeren terwijl dit bij kleine en microbedrijven respectievelijk 39,1% en 37,9% is. 94,2% van de grote bedrijven heeft procedures om zich te beschermen tegen cyberaanvallen, wat substantieel hoger is dan microbedrijven (64,7%). Procedures om cyberaanvallen te detecteren zijn sterker ingeburgerd bij grote bedrijven (81,3%) wat in groot contrast staat bij de gebrekkige implementatie bij kleine (49,6%) en microbedrijven (40,3%). Deze trend is eveneens waarneembaar inzake procedures om te reageren of cyberaanvallen: 80,4% van de grote bedrijven heeft dergelijke procedures in vergelijking met middelgrote bedrijven (57,7%), microbedrijven (30,4%) en kleine bedrijven (38,7%). Tot slot kent liefst 91,0% van de grote bedrijven procedures om van cyberaanvallen te herstellen terwijl dit bij microbedrijven beperkt blijft tot 56,3%.

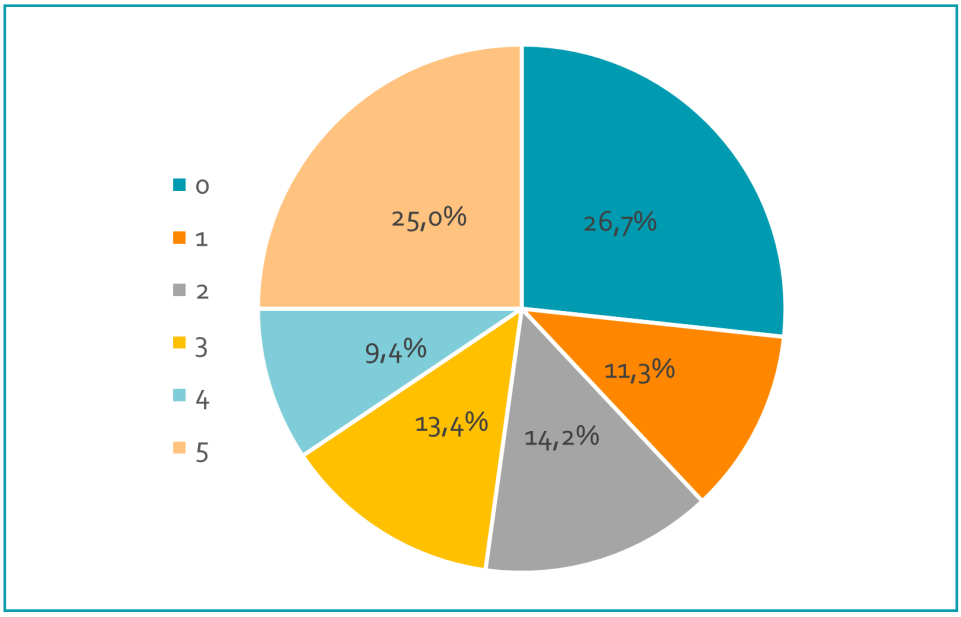
Figuur 5: Type beheerprocedures volgens bedrijfsgrootte (N=1.469) *- Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen*



Opgedeeld volgens het aantal beheerprocedures blijkt dat slechts een kwart van de Vlaamse bedrijven alle vijf procedures van het NIST-kader heeft geïmplementeerd (zie Figuur 6) en dus een hoge mate van CS-maturiteit kent. Terwijl 67,7% van de grote bedrijven en 42,8% van de middelgrote bedrijven het NIST-kader toepast, is dit slechts voor 20,2% van de microbedrijven en 23,6% van de kleine bedrijven het geval. Vooral de sectoren actief in administratieve en ondersteunende diensten (NACE 77-82; 95.1), informatie- en communicatie (NACE 58-63) en onroerend goed, vrije beroepen en wetenschappelijke en technische activiteiten (NACE 68-75) scoren hier goed in (respectievelijk 51,5%, 45,0% en 35,9%). Omgekeerd heeft maar liefst 26,7% van de bedrijven geen enkele beheerprocedure om zich te beschermen tegen toekomstige cyberrisico's of met actuele cyberaanvallen om te gaan. Dit geldt voor 32,5% van de microbedrijven en 26,1% van de kleine bedrijven; slechts 10,2% van de middelgrote en 3,6% van de grote bedrijven valt hieronder. Bedrijven actief in accommodatie en maaltijden (NACE 55-56) en bouwnijverheid (NACE 41-43) vertonen minimale CS-maturiteit, met respectievelijk 53,7% en 36,7% actief in die sector.

Het belang van bedrijfsgrootte met betrekking tot CS-maturiteit blijkt opnieuw duidelijk uit het gemiddeld aantal beheerprocedures dat de verschillende bedrijfstypes installeren: microbedrijven hebben gemiddeld 2,1 procedures, kleine bedrijven 2,5, middelgrote bedrijven 3,4 en grote bedrijven 4,2. Grote bedrijven hebben met andere woorden een hogere mate van CS-maturiteit, terwijl kleine en microbedrijven opmerkelijk minder goed beschermd zijn tegen cyberaanvallen.

Figuur 6: Aantal beheerprocedures (N=1.469) *- Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen*



3.3 Drempels

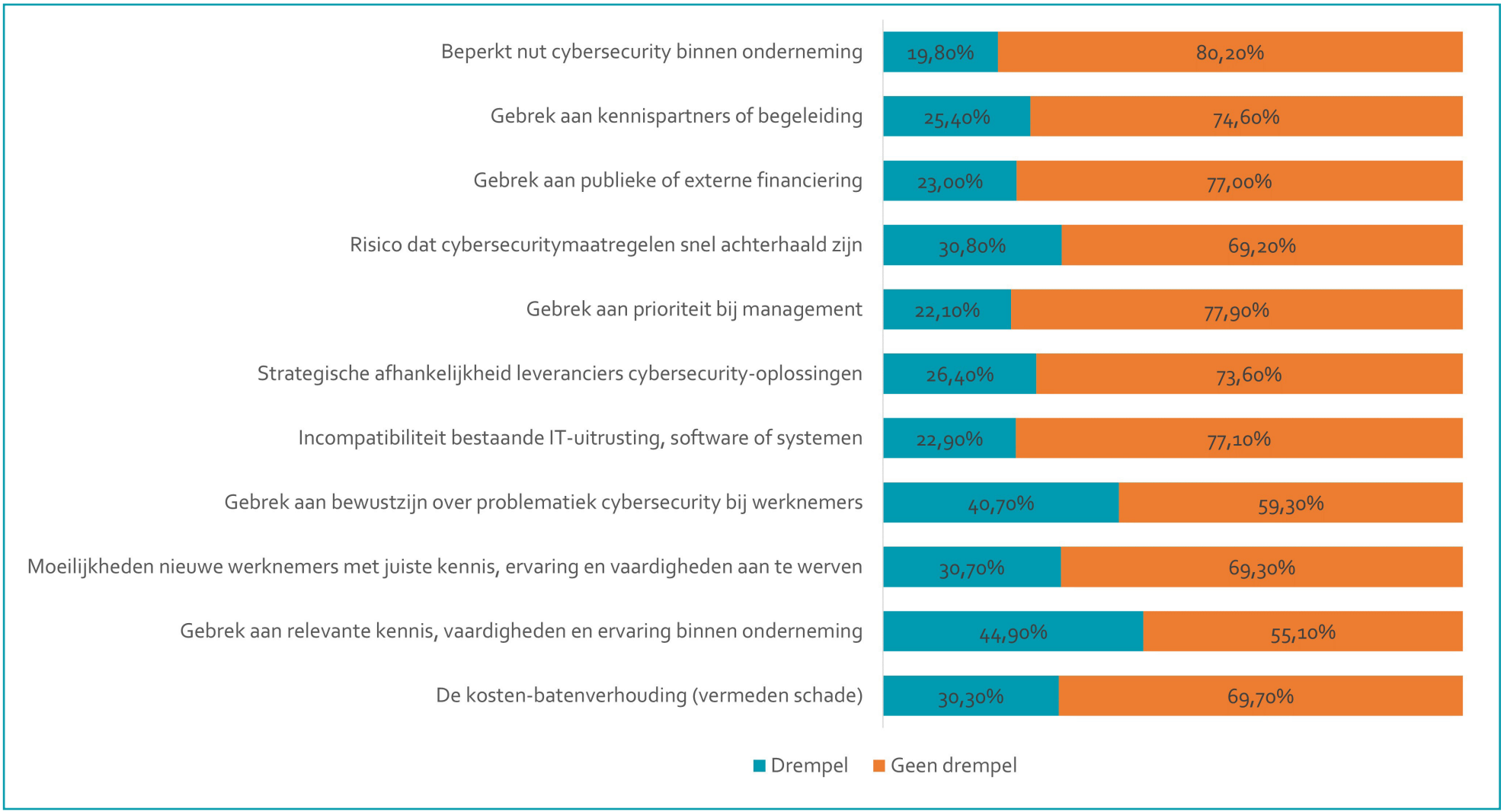
Het invoeren van CS-technologieën en beheerprocedures stelt bedrijven voor de nodige uitdagingen, die van operationele, financiële, technische of nog andere aard kunnen zijn. Figuur 7 toont welke moeilijkheden bedrijven ondervinden bij het opzetten en handhaven van een CS-beleid. 44,9% identificeert het gebrek aan relevante kennis, vaardigheden en ervaring bij de huidige werknemers als de belangrijkste drempel tot een adequaat CS-beleid; 30,7% ondervindt moeilijkheden om deze nieuwe werknemers met deze kennis, vaardigheden en ervaring aan te werven. Behalve kennis en vaardigheden erkent 40,7% van de bedrijven eveneens een gebrek aan bewustzijn omtrent cybersecurity bij de werknemers. Bedrijven zien het gebrek aan kennis, vaardigheden en bewustzijn met andere woorden als dé belangrijkste drempel bij het invoeren van een CS-beleid. Nochtans vormt deze menselijke component – naast technische maatregelen

en beheerprocedures – een belangrijke verdedigingsgordel tegen cyberaanvallen.

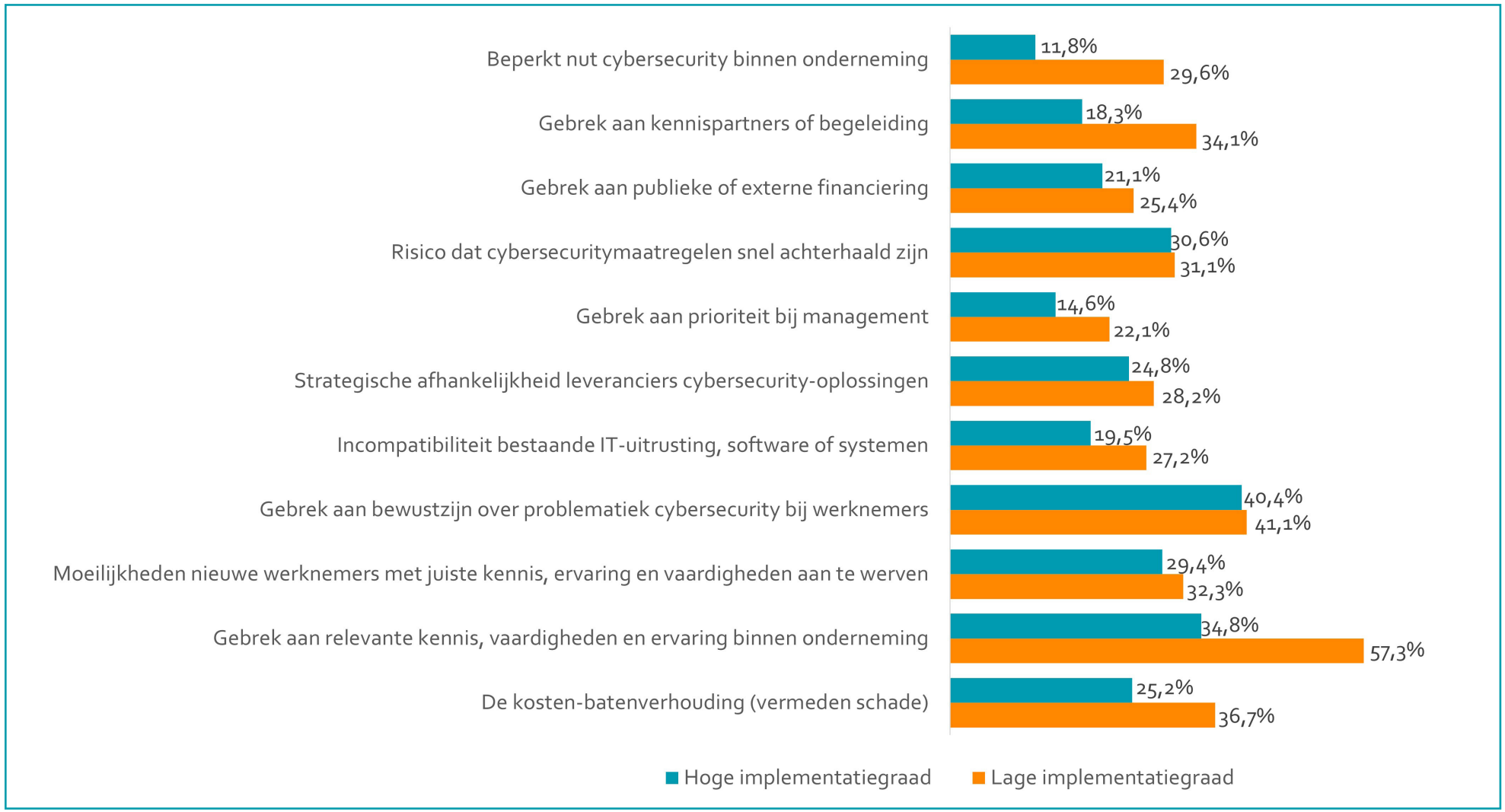
Een derde van de bedrijven (30,3%) wijst de kosten-baten (investeringen tegenover de vermeden schade) als negatief aan; 23,0% wijst een gebrek aan publieke of externe financiering als drempel aan. 22,1% erkent een gebrek aan prioriteit bij het management als een drempel voor een effectief CS-beleid. Bedrijven zien nochtans duidelijk de meerwaarde in van het voeren van een CS-beleid voor hun organisatie: 'slechts' 19,8% zegt dat ze weinig nut zien in een degelijk beleid.

Omdat slechts 42 bedrijven geen enkele CS-maatregel stellen, bleek het niet opportuun om een vergelijking tussen zogenaamde adopters en niet-adopters uit te voeren. Daarom werden bedrijven met een lagere implementatiegraad (aantal genomen CS-maatregelen kleiner of gelijk aan 6) (N = 439) en een hogere implementatiegraad van adoptie (aantal genomen CS-maatregelen groter dan 6) (N = 971) met elkaar vergeleken. Figuur 8 wijst uit dat bedrijven met een lage implementatiegraad meer drempels ervaren bij de uitrol van CS-maatregelen dan bedrijven met een hoge implementatiegraad. Deze ervaren drempels zijn daarom wellicht ook de redenen van de lage implementatiegraad. Bedrijven met een lage implementatiegraad (57,3%) worstelen opmerkelijk vaker met een gebrek aan kennis, vaardigheden en ervaring binnen de organisatie dan bedrijven met een hoge implementatiegraad (34,8%). Bedrijven met een lage implementatiegraad ervaren een groter gebrek aan kennispartners of begeleiding, zien een negatievere kosten-batenverhouding en schatten het nut van een CS-beleid voor hun organisatie als minder waardevol in dan bedrijven met een hogere implementatiegraad. Eveneens zien we een groter gebrek aan prioriteit bij het management bij bedrijven met een lagere implementatiegraad. Enigszins verrassend is dat beide categorieën van bedrijven een hoog gebrek aan bewustzijn over de problematiek van cybersecurity bij werknemers ervaren. Dit toont nogmaals het belang van de menselijke component van cybersecurity aan. Het hebben van gedegen technische maatregelen of adequate beheerprocedures zijn niet noodzakelijk afdoende als medewerkers onbewust of onwetend zijn over hoe met cyberrisico's om te gaan.

Figuur 7: Drempels implementatie CS-maatregelen (N= 1.419)



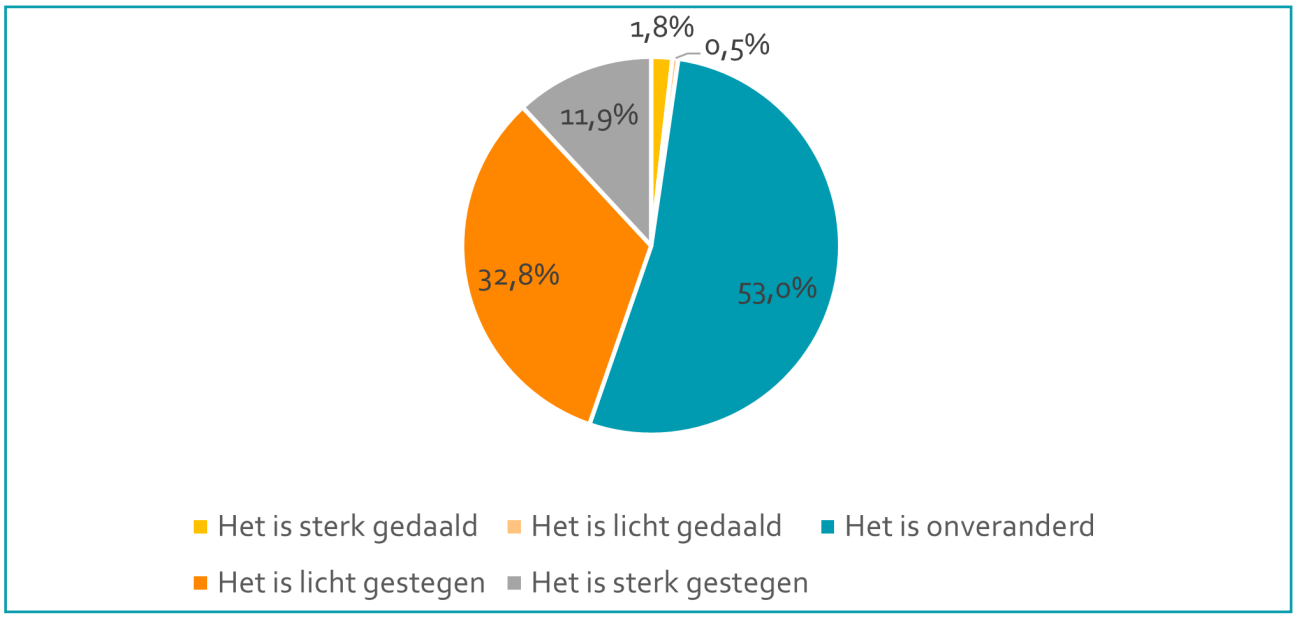
Figuur 8: Drempels implementatie CS-maatregelen volgens adoptiegraad (N= 1.410)



3.4 Budget

De evolutie van het budget van Vlaamse bedrijven om CS-technologieën te gebruiken en CS-procedures uit te werken, is het afgelopen jaar vrijwel onveranderd gebleven (zie Figuur 9). Voor de meerderheid (53%) bleef dit budget ongewijzigd, bij amper 2,3% van de Vlaamse bedrijven daalde het budget voor CS-maatregelen het afgelopen jaar. In totaal 44,7% van de bedrijven liet een – lichte of sterke – stijging in de uitgaven voor CS-maatregelen noteren. De stijging is het sterkst merkbaar bij grote bedrijven; in die groep geeft 46,8% aan dat het budget licht gestegen is terwijl nog eens 32,8% van een sterke toename spreekt. Ook bij middelgrote bedrijven is een stijging waarneembaar: 43% voerde een lichte stijging in het CS-budget door, 19,5% spreekt zelfs van een sterke stijging.

Figuur 9: Evolutie CS-budget (N= 1.412) *- Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen*

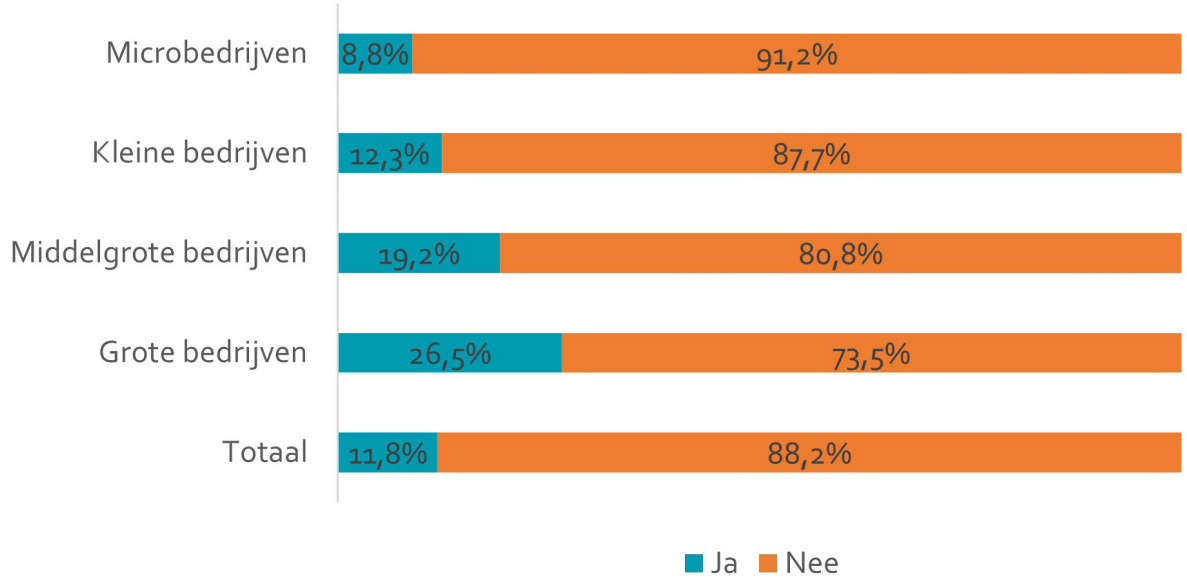


Gemiddeld schatten de Vlaamse bedrijven 20,7% van hun totale IT-budget te spenderen aan cybersecurity. Bij de grote bedrijven ligt dit gemiddelde lager op 14,1%, bij microbedrijven bedraagt dit gemiddeld 22,7%. Daarbij moet uiteraard gewezen worden op het feit dat eerstgenoemde bedrijven over een groter IT-budget beschikken en het CS-budget dus een groter absoluut bedrag representeert dan de uitgaven van microbedrijven voor CS-maatregelen.

3.5 Impact

De dreiging van cyberrisico's is de afgelopen jaren sterk gestegen. Dit vertaalt zich dan ook in een hoge frequentie van cyberaanvallen op Vlaamse bedrijven: 11,8% van de Vlaamse bedrijven geeft aan het afgelopen jaar het slachtoffer te zijn geweest van een cyberaanval (zie Figuur 10). Grote bedrijven (26,8%) zijn het vaakst slachtoffer hiervan, ook middelgrote bedrijven (19,2%) worden bovengemiddeld getroffen. Dit in tegenstelling tot kleine (12,3%) en microbedrijven (8,8%) die in iets minder mate worden geviseerd door cybercriminelen. Bedrijven actief in nutsectoren, en vervoer en opslag worden opmerkelijk vaker getroffen (respectievelijk 25,8% en 16,8%).

Figuur 10: Slachtoffer van cyberaanval (N= 1.507)



Een dergelijke cyberaanval kan verstrekkende gevolgen hebben voor het getroffen bedrijf. Uit Figuur 11 blijkt dat kleinere en microbedrijven kwetsbaarder zijn en grotere operationele gevolgen kennen als gevolg van een geslaagde cyberaanval. Mogelijks is dit te wijten aan de mate van bescherming tegen cyberrisico's die in positieve zin samenhangt met de bedrijfsgrootte (hoe groter het bedrijf, hoe sterker de bescherming tegen cyberrisico's).

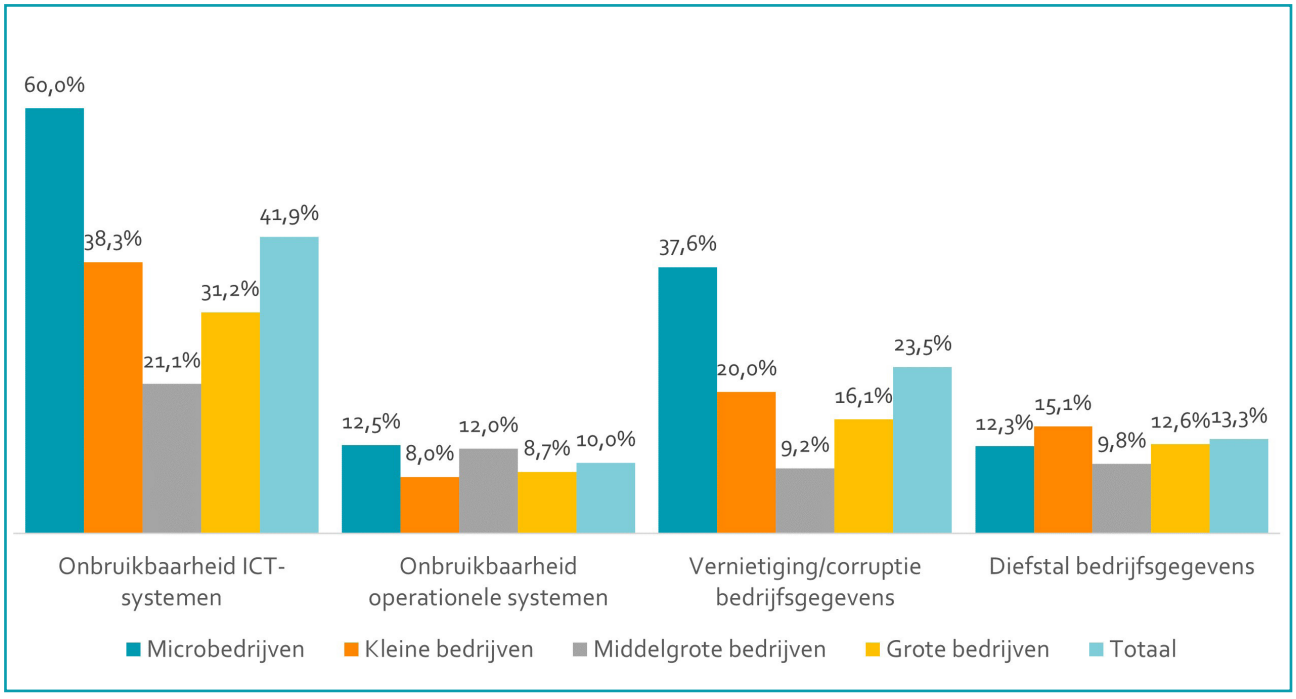
Van de geviseerde bedrijven geeft 41,9% aan dat ze als gevolg van een cyberaanval het afgelopen jaar geconfronteerd werden met de *onbruikbaarheid van ICT-systemen*, bijvoorbeeld door hacking, kwaadwillige vergrendeling of DDoS-aanval. Dit is in bijzondere mate het geval voor kleine (60,0%) en microbedrijven (38,3%), voor bedrijven actief in accommodatie en maaltijden (76,9%), informatie en communicatie (57,1%), nutsector (55,6%) en bouwnijverheid (53,4%).

Minder prevalent is de *onbruikbaarheid van OT-systemen*, zoals machines, gebouwen of andere infrastructuur (10,0%). Vooral bedrijven actief in onroerend goed, vrije beroepen en wetenschappelijke en technische activiteiten (18,3%) blijken hier kwetsbaar, net zoals bedrijven in administratieve en ondersteunende diensten (16,5%) en groot- en detailhandel (14,8%). De maakindustrie (8,7%) scoort hier relatief goed.

Ongeveer een kwart (23,5%) van de bedrijven kreeg te maken met de *vernietiging of het onbruikbaar maken van bedrijfsgegevens*, bijvoorbeeld door infectie van kwaadaardige software of ongeoorloofde toegang. Ook hier ervoeren kleine en microbedrijven de grootste impact van een cyberaanval. In verhouding tot andere sectoren kregen de nutsector (71,3%), bedrijven actief in accommodatie en maaltijden (56,7%) en de bouwnijverheid (48,9%) opmerkelijk vaker met vernietiging van bedrijfsgegevens te maken.

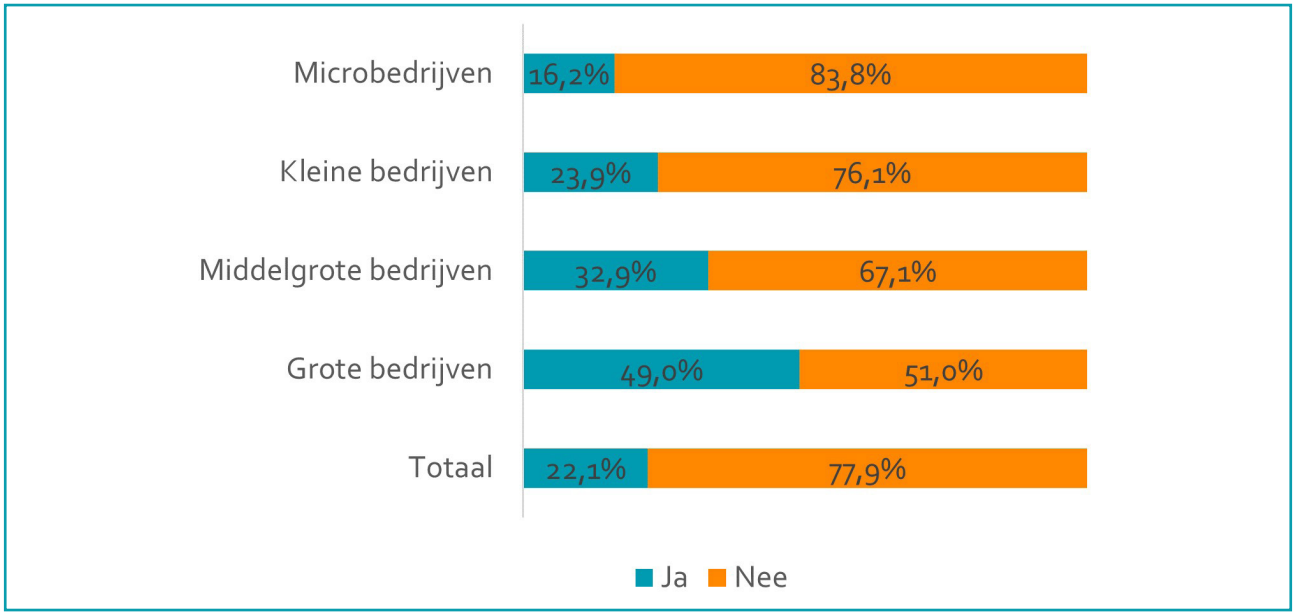
Tot slot kreeg 13,3% van de bedrijven te kampen met *diefstal van (confidentiële) bedrijfsgegevens*, bijvoorbeeld door infectie van kwaadaardige software of phishingberichten. Vooral bedrijven actief in informatie en communicatie (30,4%), accommodatie en maaltijden (20,2%) en de bouwnijverheid (19,9%) werden het meeste getroffen.

Figuur 11: Gevolgen cyberaanval volgens bedrijfsgrootte (N= 232) *- Deze vraag werd enkel gesteld aan bedrijven die het slachtoffer werden van een geslaagde cyberaanval*



Bijna een kwart van de Vlaamse bedrijven (22,5%) is verzekerd tegen cyberaanvallen (zie Figuur 12). Een dergelijke verzekering dekt (gedeeltelijk) de financiële schade van een cyberaanval (zoals bijvoorbeeld losgeld of schade bij derden) maar neemt uiteraard het cyberrisico niet weg. Bedrijven blijven ondanks een verzekering tegen cybercrime even kwetsbaar bij gebrek aan andere CS-maatregelen. Van de grote bedrijven claimt ongeveer de helft (49%) een verzekering afgesloten te hebben tegen cyberaanvallen. Dit aantal ligt een pak lager bij de middelgrote bedrijven (32,90%), de kleine bedrijven (23,9%) en de microbedrijven (16,2%). Terwijl bedrijven uit de informatie- en communicatiesector opmerkelijk vaker verzekerd zijn (37,5%), geldt het omgekeerde voor de nutsector (5,6%).

Figuur 12: Verzekering tegen cybercrime volgens bedrijfsgrootte (N= 1.460)



4. Conclusies

In deze CS-Barometer werd geprobeerd een betrouwbaar overzicht te bieden van de maturiteit in cybersecurity bij Vlaamse bedrijven. De mate van CS-maturiteit wordt bepaald door een combinatie van maatregelen: technische maatregelen, beheerprocedures, en kennis en bewustzijn binnen het bedrijf. Deze maturiteit neemt dan ook toe naarmate het bedrijf op elk van deze aspecten gepaste maatregelen neemt. Hoewel 94,2% van de Vlaamse bedrijven één of meerdere technische maatregelen neemt om de cybersecurity te verhogen, vertoont slechts een kwart van deze bedrijven voldoende maturiteit als het op beheerprocedures aankomt. Ook op het vlak van kennis en bewustzijn bij management en medewerkers valt het met die maturiteit bij een grote proportie bedrijven nogal tegen.

De meest optimale bescherming tegen cyberrisico's schuilt immers in de combinatie van zo veel mogelijk CS-maatregelen. Het louter updaten van software of het instellen van een paswoordauthenticatie zijn uiteraard noodzakelijk, maar allerminst voldoende om op redelijke wijze beschermd te zijn tegen cyberrisico's of -aanvallen. Het toepassen van enkele van deze technische maatregelen biedt met andere woorden een vals veiligheidsgevoel. Dit geldt evenzeer voor het instellen van diverse procedures om alle elementen van een systematisch CS-beleid uit te rollen. Met de toename van cyberrisico's volstaat het voor bedrijven niet langer om enkel beheerprocedures in te stellen om zich effectief te beschermen tegen cyberaanvallen, maar moet er blijvend gewerkt worden aan een holistische benadering inclusief het identificeren van kritieke databronnen of ondernemingsprocessen, cyberaanvallen te detecteren, adequaat te reageren op en te herstellen van cyberaanvallen.

Hoewel een dergelijk beleid cruciaal is voor alle bedrijven vormt de kwetsbare situatie van kleine en microbedrijven een belangrijk aandachtspunt voor de industrie, overheden en sectororganisaties. Uit de studie blijkt dat het voeren van een doordacht CS-beleid recht evenredig is met bedrijfsgrootte. Kleine bedrijven nemen een lager aantal en minder geavanceerde CS-maatregelen en implementeren minder CS-procedures om zich tegen cyberrisico's te beschermen. Hoewel grote bedrijven vaker het slachtoffer zijn van een cyberaanval, blijken kleine bedrijven meer kwetsbaar aan cyberaanvallen en ondervinden ze grotere operationele gevolgen door dergelijke aanvallen. Het is dan ook cruciaal om te blijven inzetten op de vele drempels die kleinere bedrijven ervaren bij het implementeren van CS-maatregelen.

Ondanks de toegenomen risico's ontbreekt bij een grote proportie Vlaamse bedrijven nog steeds de vereiste kennis, vaardigheden en expertise over cybersecurity binnen de organisatie. Daarnaast vormen het gebrekkige bewustzijn omtrent cybersecurity bij management en werknemers, en het gepercipieerde gebrek aan meerwaarde van CS-maatregelen voor de organisatie kritieke pijnpunten bij het uitrollen van een doordacht CS-beleid. Een dergelijk beleid noodzaakt performante technologie én werknemers die op een bewuste én voorzichtige manier met technologie, informatie en data omgaan. De Vlaamse overheid heeft tal van initiatieven opgestart om bedrijven te inspireren, sensibiliseren, adviseren, informeren of op te leiden inzake het belang van cybersecurity. Het is evident dat dit soort initiatieven het bewustzijn van onze Vlaamse bedrijven verder moeten ontwikkelen, vaker wel dan niet met krachtige, laagdrempelige voorbeelden over waarom cybersecurity cruciaal is voor de gezondheid van elk bedrijf in elke sector.

Daarbij is het cruciaal om de vele voordelen van, of tenminste de vermeden schade door een systematisch CS-beleid te blijven beklemtonen. Een geslaagde cyberaanval kan verstrekkende gevolgen hebben voor het getroffen bedrijf. Geviseerde bedrijven kampen hoofdzakelijk met onbruikbaarheid van ICT-systemen waardoor het toegangsnetwerk en andere IT-infrastructuur voor bepaalde duur onbruikbaar wordt. Daarnaast kampen getroffen bedrijven met onbruikbare operationele systemen, vernietigde of gestolen bedrijfsgegevens. Geslaagde cyberaanvallen brengen verlies van inkomsten, reputatieschade, productiviteitsverlies, extra kosten voor herstel en eventueel losgeld met zich mee. Een verzekering tegen cybercrime is daarbij zeker aan te raden, maar ontslaat het bedrijf niet van de verplichting om gerichte maatregelen te nemen om zich optimaal te beschermen tegen de toenemende cyberdreiging.

5. Reflectie

“Volgens deze CS-Barometer werden meer dan één op tien bedrijven het slachtoffer van een cyberaanval en alhoewel ze het minst vaak werden aangevallen, voelden kleinere bedrijven hiervan de meeste impact. Oorzaak hiervan is het kleine aantal CS-maatregelen samen met het gebrek aan beheerprocedures bij kleinere bedrijven. Externe IT-leveranciers kunnen een grotere rol spelen om het bewustzijn te vergroten. Zes op de tien bedrijven heeft geen plan om te reageren op een aanval. Dit heeft tot gevolg dat het heropstarten van het bedrijf langer zal duren en er gedurende vele dagen tot meerdere weken paniek heerst. Hoewel grotere bedrijven meer CS-maatregelen nemen, blijven ze kwetsbaar als kleinere bedrijven deel uitmaken van hun toeleveringsketen. Grotere bedrijven moeten hun toeleveranciers meer bewust maken.

Daarnaast moet er verder worden ingezet op de CS-maturiteit van het personeel. Naargelang de job of functie in het bedrijf werkt men op andere bedrijfsprocessen en moet men dan ook een aangepaste training krijgen om de kwetsbaarheden verbonden aan deze processen te kunnen zien, begrijpen en op te lossen. De systemen van kleine bedrijven zijn minder complex, zeker niet altijd uitgebreid en kunnen dus zonder groot budget beschermd worden. Ransomware blijft de grote boeman maar deze malware kan ook dienen om diefstal van bedrijfsdata te maskeren. Een vijfde van het IT-budget wordt gespendeerd aan cybersecurity wat een goede tendens is gezien men meer digitaal werkt, er veel van thuis uit wordt gewerkt en er meer toestellen (IoT, OT, enz.) aan het internet worden gekoppeld. Het uitvallen van een OT-netwerk (industrieel netwerk) kan voor grote onkosten zorgen. Deze netwerken vallen niet altijd onder de cybersecurityverzekering. De digitale transformatie die bij de meeste bedrijven op de planning staat, zal de volgende maanden en jaren echter een positieve rol spelen in het verhogen van de cyberveiligheid. Cybersecurity wordt in deze transformatie meestal standaard meegenomen. Dit was vroeger immers zeker niet het geval bij vroegere automatisatie en invoering van nieuwe IT-systemen.”

Kurt Callewaert (expert cybersecurity, Howest)

Appendix

Tabel 3: Geselecteerde sectoren

NACE-codes	Omschrijving
NACE 10-33	Industrie
NACE 35-39	Productie en distributie van elektriciteit, gas, stoom en gekoelde lucht; distributie van water; afval- en afvalwaterbeheer en sanering
NACE 41-43	Bouwnijverheid
NACE 45-47	Groothandel en detailhandel; reparatie van auto's en motorfietsen
NACE 49-53	Vervoer en opslag
NACE 55-56	Verschaffen van accommodatie en maaltijden
NACE 58-63	Informatie en communicatie
NACE 68-75	Exploitatie van en handel in onroerend goed; vrije beroepen en wetenschappelijke en technische activiteiten
NACE 77-82	Administratieve en ondersteunende diensten
NACE 95.1	Reparatie van computers en communicatieapparatuur

Colofon

Deze studie werd uitgevoerd in opdracht van het Departement Economie, Wetenschap en Innovatie (EWI) van de Vlaamse overheid

Contactpersonen:

Petra.Andries@UGent.be

Tom.Evens@UGent.be