Vlaanderen
is economie, wetenschap & innovatie

CS-barometer

Maturiteit in cybersecurity bij Vlaamse bedrijven
situatie 2023

ecoom
EXPERTISECENTRUM O&O MONITORING

DEPARTEMENT
ECONOMIE
WETENSCHAP &
INNOVATIE

CS-barometer

Maturiteit in cybersecurity

bij Vlaamse bedrijven

situatie 2023

Cyber Security Vlaanderen

Colofon

CS-barometer – Maturiteit in cybersecurity bij Vlaamse bedrijven – situatie 2023

(Rapport ECOOM-STORE 23-030) is een publicatie in opdracht van het Departement Economie, Wetenschap en Innovatie (EWI) van de Vlaamse overheid uitgevoerd door ECOOM-STORE, UGent.

Verantwoordelijke uitgever

Johan Hanssens, Secretaris-generaal

Vlaamse overheid, Departement Economie, Wetenschap en Innovatie (EWI)

Koning Albert II-laan 35, bus 10

1030 Brussel

Info.ewi@vlaanderen.be

Tel.: 02 553 59 80

Auteurs

Thomas Standaert, Cathy Lecocq, Petra Andries (ECOOM-STORE, UGent)

Tom Evens (Research Group for Media, Innovation & Technology, UGent)

Datum van uitgave

april 2024

Depotnummer

D/2024/3241/141

DEPARTEMENT
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 anno 2023 in kaart

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 9.680 bedrijven, 2.442 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.

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

Dit rapport beoogt om op een wetenschappelijk onderbouwde manier een actuele monitoring van de CS-maturiteit en de frequentie en gevolgen van cyberaanvallen bij Vlaamse bedrijven te voorzien. Het bespreekt daarom in hoofdzaak statistieken die representatief zijn voor een populatie bedrijven uit een breed scala van productie- en dienstensectoren. Waar mogelijk en relevant wordt een vergelijking gemaakt met statistieken uit de editie van vorig jaar.[1]

[1] In de huidige editie werd gebruik gemaakt van een verkorte vragenlijst waardoor bepaalde onderwerpen niet aan bod komen.

De belangrijkste bevindingen van de studie zijn de volgende:

- In vergelijking met de meting in 2022 **is het aandeel bedrijven dat een veelheid van basis- en meer geavanceerde technische maatregelen treft sterk gestegen**. De grootste vooruitgang wordt geboekt op het vlak van de implementatie van meer geavanceerde technische maatregelen. Toch maakt nog steeds minder dan de helft van de bedrijven gebruik van ICT-veiligheidsanalyse (49,7%), ICT-veiligheidstesten (43,7%), encryptietechnieken (33,3%) en biometrische authenticatietechnieken (28,0%). Het **aandeel bedrijven dat opleidingen of activiteiten voor haar medewerkers voorziet (47,1%) is aanzienlijk gestegen** ten opzichte van de vorige meting. De stijging in de adoptie van verschillende CS-maatregelen (i.e., technische maatregelen en opleidingen of activiteiten) is minder uitgesproken bij de microbedrijven in vergelijking met bedrijven uit andere grootteklassen. De achterstand van deze groep bedrijven ten opzichte van bedrijven uit andere grootteklassen wordt dus groter. Ook kleine en middelgrote bedrijven blijven achter op grote bedrijven.
- **Ongeveer een derde (33,7%) van de bedrijven die minstens één CS-maatregel namen, heeft alle vijf procedures van het NIST-kader in zekere mate geïmplementeerd. Daartegenover staat dat één op vijf (19,9%) van de bedrijven die minstens één CS-maatregel namen geen enkele beheerprocedure in voege heeft**. Algemeen geldt: hoe groter het bedrijf, hoe groter het aantal beheerprocedures. Bij micro-, kleine en middelgrote bedrijven bestaat dus nog heel wat groeimarge op het vlak van de implementatie van beheerprocedures.
- In vergelijking met de vorige meting **oefent een groter aandeel bedrijven druk uit op haar leveranciers inzake cybersecurity (33,5%) en krijgt ook een groter aandeel bedrijven eisen opgelegd door haar klanten (25,7%).**
- Het **bewustzijn omtrent cybersecurity bij de werknemers** en de **relevante kennis, vaardigheden en ervaring binnen de onderneming** zijn er in vergelijking met de vorige meting op vooruitgegaan. Deze evolutie houdt vermoedelijk verband met de hogerop genoemde stijging in de voorziening van opleidingen of activiteiten voor medewerkers Toch blijven een gebrek aan bewustzijn en een gebrek aan relevante kennis, vaardigheden en ervaring de twee belangrijkste obstakels bij de invoer en het gebruik van CS-maatregelen.
- Bedrijven met een lage adoptiegraad van CS-maatregelen kampen vaker met obstakels dan bedrijven met een hoge adoptiegraad, ongeacht de aard van het obstakel. Grote bedrijven ondervinden in het algemeen minder vaak obstakels, behalve wanneer ze pogen **nieuwe werknemers met de juiste kennis, ervaring en vaardigheden aan te werven**. Microbedrijven kampen op hun beurt aanzienlijk vaker dan bedrijven in andere grootteklassen met een gebrek aan relevante kennis, vaardigheden en ervaring binnen de onderneming en een **gebrek aan kennispartners of begeleiding**.

- Consistent met de investeringen in additionele CS-maatregelen en beheerprocedures liet ongeveer de helft (45,8%) van de bedrijven een **lichte of sterke stijging in de uitgaven voor cybersecurity** noteren. Gemiddeld spenderen bedrijven naar schatting 19,7% van hun totale IT-budget aan cybersecurity. Dit aandeel is onveranderd ten opzichte van de vorige meting, wat suggereert dat de stijging in de uitgaven voor cybersecurity evenredig was met de stijging in het totale IT-budget.
- **Bijna één op 10 (8,8%) geeft aan het afgelopen jaar het slachtoffer te zijn geweest van een cyberaanval**, waarbij cybercriminelen al dan niet met succes trachtten computersystemen onklaar te maken of persoonlijke of confidentiële gegevens te verkrijgen. In vergelijking met de vorige meting hadden cyberaanvallen **vaker operationele gevolgen** voor bedrijven. Zo kampte 32,2% van de slachtoffers van cyberaanvallen met de onbruikbaarheid van ICT-systemen; 10,3% met de onbruikbaarheid van operationele systemen; 13,4% met de vernietiging of het onbruikbaar maken van bedrijfsgegevens; en 25,2% met diefstal van (confidentiële) bedrijfsgegevens.

Inleiding

Onze maatschappij digitaliseert en automatiseert in een snel tempo. Bedrijven maken in toenemende mate gebruik van 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 beleidsplan Cybersecurity versterkt het bestaande overheidsinstrumentarium om bedrijven te informeren, sensibiliseren, begeleiden én te ondersteunen in het gebruik van cybersecuritytoepassingen[2].

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 actuele monitoring van de maturiteit, obstakels en noden inzake CS te verschaffen en zodanig de impact van het desbetreffende Vlaamse actieplan mee te helpen evalueren. Het voorliggende rapport is gebaseerd op de derde meting die sinds 2021 werd uitgevoerd. Toekomstige meetmomenten bieden de mogelijkheid om het longitudinaal overzicht van de evolutie inzake CS bij Vlaamse bedrijven verder uit breiden.

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.

Bovenstaande principes zijn cruciaal om de vergelijkbaarheid met andere studies die de adoptiegraad van CS-maatregelen bij Vlaamse bedrijven in kaart brengen te evalueren. Indien deze

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

studies niet stoelen op dezelfde methodologische principes inzake representativiteit en vergelijkbaarheid is er weinig tot geen wetenschappelijke grond om de resultaten van diverse studies met elkaar te vergelijken.

Methodologie

Meetinstrument

Bij de keuze van het meetinstrument werd, net als in de edities van 2021 en 2022, gestreefd naar een maximale vergelijkbaarheid met gelijkaardige Europese vragenlijsten en onderzoeksinitiatieven. De vragenlijst omvat module D (ICT-security) van de *2022 Survey on ICT Usage and E-Commerce in Enterprises* aangewend door Eurostat[3] en Statbel[4], en gepubliceerd in de *Digital Economy and Society Index* (DESI)[5]. Deze module werd aangevuld met bestaande elementen uit andere relevante nationale en internationale studies[6]. Tot slot werden nieuwe elementen inzake de impact van CS op de bedrijfsprestaties en de kennis over beleidsondersteunende maatregelen van de Vlaamse overheid opgenomen.

De ontwikkeling van een stabiel meetinstrument in lijn met de structurele dataverzamelingen van officiële instanties zoals Eurostat en Statbel 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.

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 Tabel 3 in Appendix voor een overzicht van de geselecteerde sectoren). Ten opzichte van de vorige editie van de CS-barometer (situatie 2022) werden geen aanpassingen uitgevoerd aan de lijst van geselecteerde sectoren.[7] Zowel grote, middelgrote, kleine als micro-ondernemingen – opgedeeld in grootteklassen op basis van het werknemersaantal – werden opgenomen. Voor deze laatste grootteklasse werd weliswaar een ondergrens van minstens vijf werknemers gehanteerd.

De Bel-first-databank van Bureau van Dijk werd als vertrekpunt gehanteerd voor de steekproef, die gestratificeerd werd naar economische sectoren en grootteklassen (zie Tabel 1 voor populatie-

[3] https://ec.europa.eu/eurostat/cache/metadata/en/isoc_e_esms.htm
[4] https://statbel.fgov.be/en/themes/enterprises/ict-and-e-commerce-enterprises#documents
[5] https://digital-strategy.ec.europa.eu/en/policies/desi
[6] IPSOS (2022). Cyber Security Breaches Survey 2022 (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022); 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)
[7] Vanaf de tweede editie van de CS-barometer (editie 2022) werd de populatie uitgebreid met bedrijven actief in financiële activiteiten en verzekeringen (NACE 64-66) en menselijke gezondheidszorg en maatschappelijke dienstverlening (NACE 86-88).

en steekproefaantallen, gestratificeerd naar sector en grootteklasse). Alle (i) bedrijven met maatschappelijke zetel in Vlaanderen en (ii) bedrijven met maatschappelijke zetel in Brussel én minstens één vestiging in Vlaanderen werden geselecteerd. Omwille van de hoge mate van ontbrekende waarden voor werknemersaantallen in Bel-first, raadpleegden we de RSZ-databank om bedrijven onder te verdelen in grootteklassen.

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.[8] Van de micro- en kleine bedrijven in de populatie werd in totaal 16% geselecteerd (rekening houdend met de verdeling over de verschillende sectoren). Voor elk micro- of klein bedrijf in de steekproef werd vervolgens een contactpersoon en bijhorend e-mailadres opgezocht. Dit gebeurde in de eerste plaats aan de hand van persoonsgegevens die naar aanleiding van de CS-barometer edities 2021 en 2022 verzameld werden. Deze werden aangevuld met gegevens uit Trends Top, en via manuele opzoekingen op internet en informatie in Bel-first wanneer de informatie uit Trends Top niet beschikbaar of onvolledig was.

Bij voorkeur identificeerden we voor elk bedrijf in de steekproef een contactpersoon voor wie (a) de functietitel wijst op verantwoordelijkheid voor technologische ontwikkelingen binnen het bedrijf en (b) een persoonlijk e-mailadres beschikbaar is. Indien geen contactpersoon met deze functietitel werd gevonden, werd voor een contactpersoon met een meer algemene management- of IT-functie geopteerd.[9] Indien voor een micro- of kleine onderneming geen persoonlijk e-mailadres werd gevonden, werd een algemeen e-mailadres ter attentie van de zaakvoerder geregistreerd. Middelgrote en grote ondernemingen waarvoor een contactpersoon maar géén persoonlijk emailadres gevonden werd, werden per brief gecontacteerd. De totale steekproef bevatte 9.680 bedrijven, waarvan er initieel 9.184 per e-mail en 496 per brief gecontacteerd werden. De dataverzamelingsperiode liep van juni tot september 2023.

[8] Contactinformatie voor relevante contactpersonen tewerkgesteld in middelgrote of grote bedrijven is minder frequent beschikbaar in onze databronnen dan bij kleine of micro-bedrijven.
[9] Binnen het kader van het DESI project richten Eurostat en de nationale partners zich prioritair op deze tweede groep (zie https://circabc.europa.eu/ui/group/89577311-0f9b-4fc0-b8c2-2aaa7d3ccb91/library/0edfd04c-6ac6-49be-98c4-553564bc3407/details). Eventuele afwijkingen in de door ons berekende statistieken en die gegenereerd door andere instellingen zijn bijgevolg mogelijk te wijten aan het verschil in het profiel van de respondenten.

Respons en weging

Van de 9.184 bedrijven die we via e-mail contacteerden, konden we er 8.466 bereiken. 718 e-mails konden niet afgeleverd worden. Voor deze bedrijven werd nieuwe contactinformatie opgezocht en werden de nieuwe contactpersonen gecontacteerd via e-mail of brief, waardoor een extra 187 bedrijven werden bereikt. Van de 496 bedrijven die we per brief contacteerden, konden 9 brieven niet afgeleverd worden. In totaal konden we dus 9.140 bedrijven bereiken. Na het uitsturen van drie herinneringen per e-mail aan de bedrijven die via e-mail bereikt werden, en een doorgedreven telefonische opvolging van alle bedrijven in de steekproef, ontvingen we antwoorden van 3.044 bedrijven. Dit impliceert een responsgraad van 33,3% (3.044/9.140). Van deze antwoorden waren uiteindelijk 2.442 antwoorden bruikbaar (zie Tabel 2). 602 antwoorden vielen uit de responsgroep omdat (a) de vragenlijst werd ingevuld voor een ander ondernemingsnummer dan gevraagd, (b) we voor eenzelfde bedrijf twee antwoorden verkregen, of (c) geen enkele vraag betreffende cybersecurity werd beantwoord. Ontbrekende gegevens werden door middel van de *random hot-deck*-imputatiemethode geïmputeerd.

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 statistieken, die – omwille van deze weging – representatief zijn voor de totale bedrijfspopulatie beoogd in het onderzoek.

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

	NACE 10-33 (maakindustrie)	NACE 35-39 (nutssector)	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 (accommodatie en maaltijden)	NACE 58-63 (informatie en communicatie)	NACE 64-66 (financiële activiteiten en verzekeringen)	NACE 68-75 (onroerend goed; vrije beroepen en wetenschappelijke en technische activiteiten)	NACE 77-82;95.1 (administratieve en ondersteunende diensten; reparatie van computers en communicatieapparatuur)	NACE 86-88 (menselijke gezondheidszorg en maatschappelijke dienstverlening)	**Totaal**
Micro	1.565	76	2.625	4.379	992	1.645	662	754	2.150	930	512	**16.290**
(5-9 werknemers)	*254*	*20*	*446*	*711*	*161*	*267*	*108*	*123*	*346*	*152*	*83*	***2.671***
Klein	2.451	159	2.395	4.667	1.446	907	842	438	1.756	1.038	764	**16.863**
(10-49 werknemers)	*394*	*40*	*385*	*749*	*237*	*148*	*135*	*71*	*287*	*183*	*125*	***2.754***
Middelgroot	838	43	336	692	343	56	192	84	302	411	583	**3.880**
(50-249 werknemers)	*780*	*36*	*306*	*563*	*304*	*45*	*163*	*65*	*251*	*340*	*454*	***3.307***
Groot	230	24	48	146	61	18	30	34	77	140	230	**1.038**
(>= 250 werknemers)	*218*	*21*	*46*	*119*	*54*	*16*	*29*	*34*	*67*	*128*	*216*	***948***
Totaal	**5.084**	**302**	**5.404**	**9.884**	**2.842**	**2.626**	**1.726**	**1.310**	**4.285**	**2.519**	**2.089**	**38.071**
	1.646	***117***	***1.183***	***2.142***	***756***	***476***	***435***	***293***	***951***	***803***	***878***	***9.680***

Tabel 2: Respons per stratum

	NACE 10-33 (maakindustrie)	NACE 35-39 (nutssector)	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 (accommodatie en maaltijden)	NACE 58-63 (informatie en communicatie)	NACE 64-66 (financiële activiteiten en verzekeringen)	NACE 68-75 (onroerend goed; vrije beroepen en wetenschappelijke en technische activiteiten)	NACE 77-82;95.1 (administratieve en ondersteunende diensten; reparatie van computers en communicatieapparatuur)	NACE 86-88 (menselijke gezondheidszorg en maatschappelijke dienstverlening)	**Totaal**
Micro (5-9 werknemers)	71	2	85	141	34	27	45	22	86	28	22	**563**
Klein (10-49 werknemers)	97	11	85	182	56	19	50	12	72	52	35	**671**
Middelgroot (50-249 werknemers)	230	13	76	119	73	15	49	21	55	75	166	**892**
Groot (>= 250 werknemers)	67	5	16	31	15	5	9	13	25	39	91	**316**
Totaal	**465**	**31**	**262**	**473**	**178**	**66**	**153**	**68**	**238**	**194**	**314**	**2.442**

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 (distributed 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 kunnen bedrijven *technische maatregelen* nemen, zoals toegangscontrole instellen of cryptografie gebruiken om informatie te beschermen. Ten tweede kunnen bedrijven *beheerprocedures* implementeren waarmee digitale systemen worden gebruikt, bestuurd en onderhouden. Een adequaat CS-beleid is er op gericht cyberrisico's te beperken en de impact van eventuele incidenten zo klein mogelijk te houden. Dit is mogelijk door te beschikken over een set van procedures die op continue basis de risico's identificeren, gegevens en systemen beschermen, cyberaanvallen detecteren en waar nodig beantwoorden, én de situatie opnieuw herstellen. Naast de noodzakelijke technische maatregelen en beheerprocedures vormen medewerkers een derde 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 zowel het management als 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 drie domeinen maatregelen neemt.

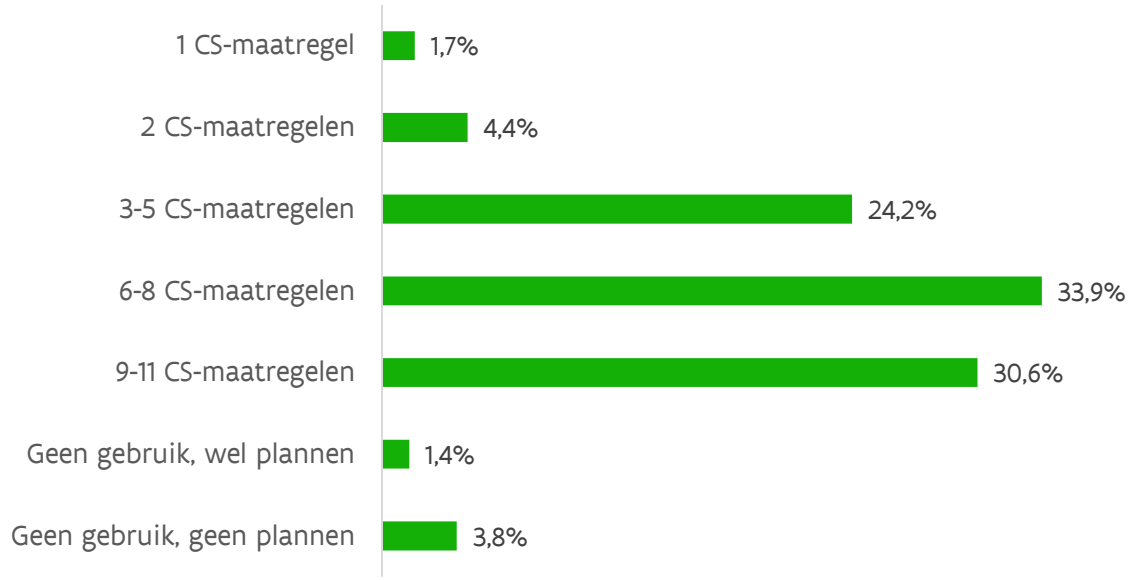
Technische maatregelen en opleidingen

De resultaten uit Figuur 1 geven aan dat de meerderheid van de Vlaamse bedrijven een veelheid aan CS-maatregelen (i.e., technische maatregelen en opleidingen of activiteiten) inzet om zijn cyberveiligheid zo goed als mogelijk te verzekeren. Na het voorleggen van een lijst van elf mogelijke CS-maatregelen (zie verderop) zegt 24,2% van de bedrijven drie tot vijf CS-maatregelen toe te passen. 33,9% past zes tot acht CS-maatregelen toe, terwijl bijna één op drie (30,6%) bedrijven negen of meer van de bevraagde CS-maatregelen toepast. In totaliteit past dus 94,8% van de

Vlaamse bedrijven ten minste één CS-maatregel toe. Dit wijst erop dat slechts een kleine minderheid (5,2%) geen enkele CS-maatregel toepast in de dagelijkse werking. 3,8% van de bedrijven zegt geen plannen te hebben om één of meerdere CS-maatregelen te implementeren in het komende jaar; 1,4% heeft daartoe wel plannen.

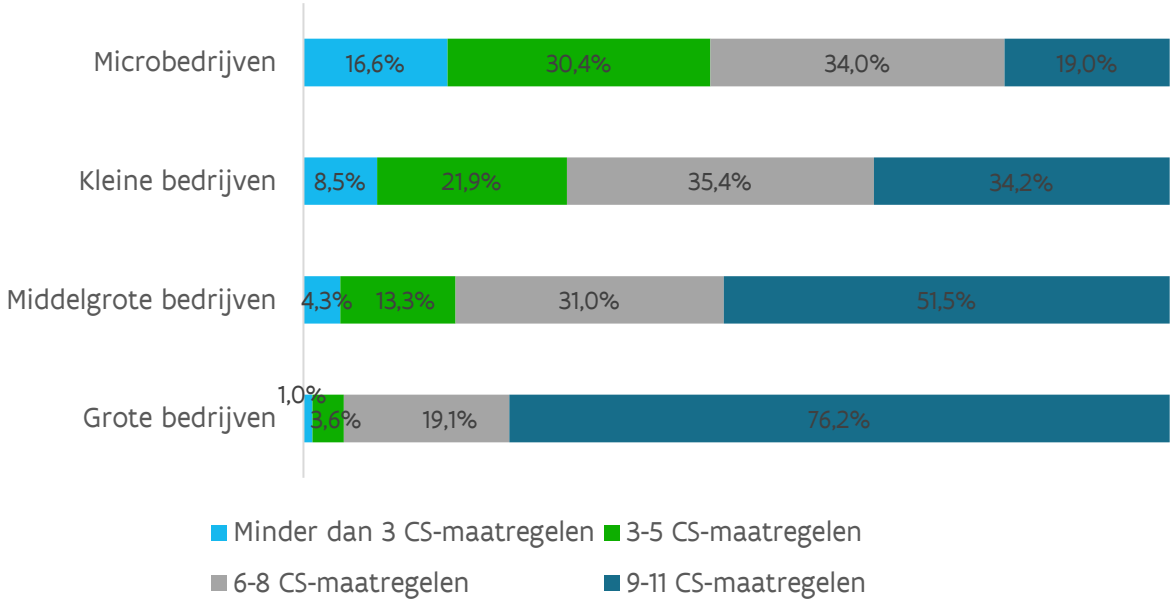
Figuur 18 in Appendix toont dat het aandeel bedrijven in de categorie met 9 tot 11 CS-maatregelen is toegenomen van 19,8% naar 30,6% ten opzichte van de vorige meting. Dit resultaat suggereert dat bedrijven het afgelopen jaar additionele CS-maatregelen hebben geïmplementeerd.

Figuur 1: Adoptiegraad aantal CS-maatregelen (N=2.442)



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). 76,2% van de grote bedrijven past minstens negen van de vooropgestelde CS-maatregelen toe, een bijkomende 19,1% neemt zes tot acht CS-maatregelen. Bij de middelgrote bedrijven bedraagt het aandeel organisaties met negen of meer CS-maatregelen 51,5%. Dit aandeel ligt beduidend lager bij kleine bedrijven (34,2%) en microbedrijven (19,0%). Van deze laatste geeft 16,6% aan minder dan drie CS-maatregelen te nemen. Bijgevolg bestaat er nog heel wat groeimarge op het vlak van de adoptie van CS-maatregelen, vooral bij de micro-, kleine en middelgrote bedrijven.

Figuur 2: Adoptiegraad aantal CS-maatregelen volgens bedrijfsgrootte (N=2.442)



Bedrijven kunnen een breed spectrum aan technische maatregelen nemen 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).[10] Al naargelang de complexiteit vertoont de adoptie van deze technische 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: 89,0% van de bedrijven geeft aan dit te doen. 77,6% heeft een protocol voor toegangsbeheer tot het ondernemingsnetwerk voor toestellen of gebruikers. Ook een sterke paswoordauthenticatie is met 73,6% stevig verankerd in de bedrijfswerking. Daarnaast beschikt ongeveer twee derde (67,5%) van de bedrijven over een VPN-netwerk. De adoptie van meer geavanceerde, technische maatregelen is minder verspreid. Concreet gaat het hierbij om maatregelen rond het bijhouden van log files om cyberaanvallen te analyseren (53,0%), periodieke ICT-veiligheidsanalyse (49,7%) of ICT-veiligheidstesten (43,7%). Een minderheid van 33,3% past encryptietechnieken toe op data, documenten en/of e-mails; 28,0% gebruikt biometrische technieken ter identificatie en authenticatie van gebruikers (vingerafdrukken, stem- en/of gezichtsherkenning). Daarnaast stellen

[10] Ongeacht de mate van complexiteit is de effectiviteit van een specifieke technische maatregel afhankelijk van de manier waarop deze geïmplementeerd wordt. Zo zijn bijvoorbeeld data back-ups naar een aparte locatie of in de cloud weinig doeltreffend indien deze niet op regelmatige basis gemaakt worden.

we vast dat bijna de helft (47,1%) van de Vlaamse bedrijven zijn werknemers opleidingen of activiteiten aanbiedt om hen bewust te maken van het belang van cybersecurity.[11]

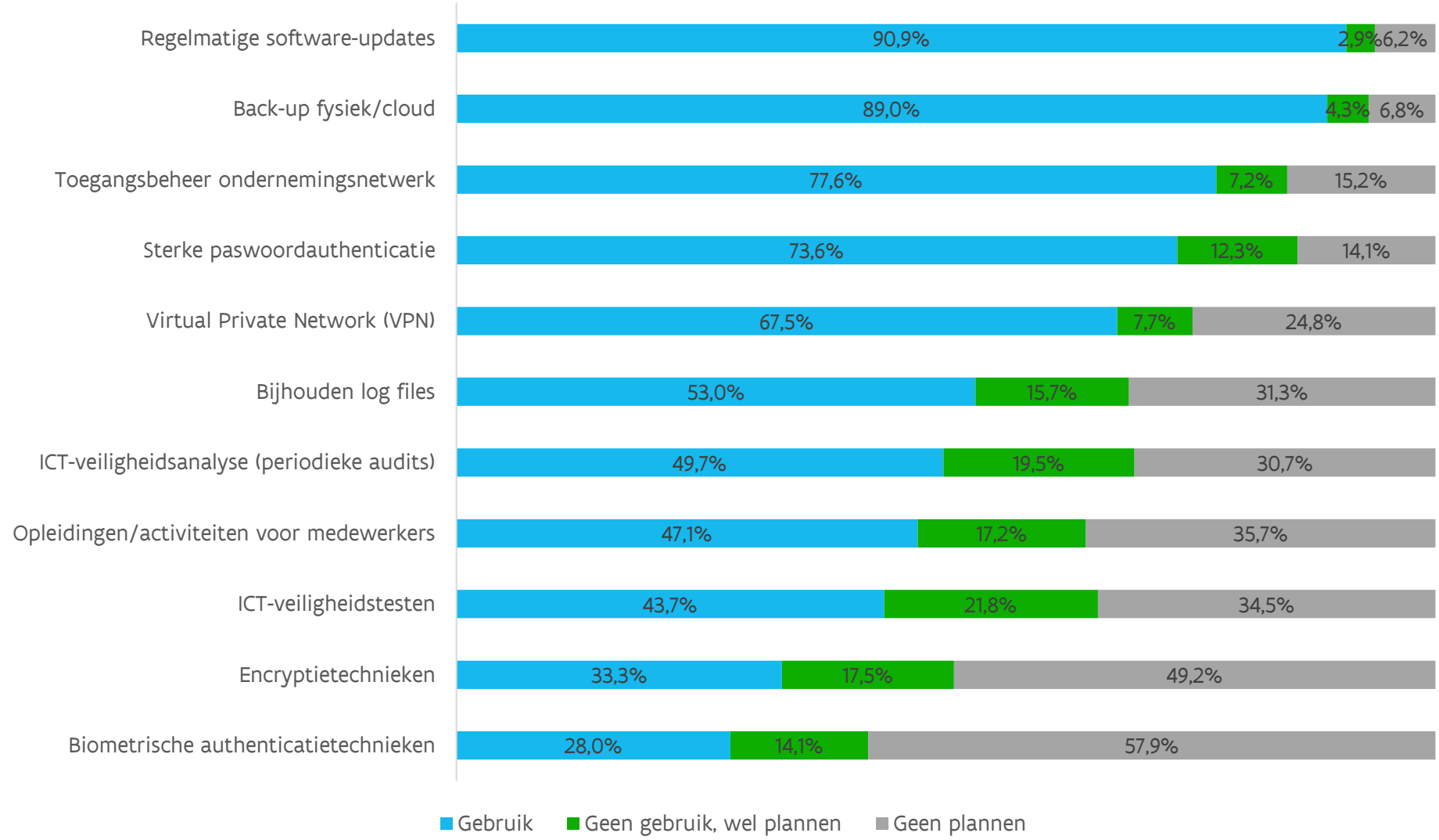
Vergeleken met de meting in 2022 is de adoptiegraad van minder geavanceerde technische maatregelen (data back-ups, VPN-netwerk, protocol voor toegangsbeheer, paswoordauthenticatie) vrijwel onveranderd gebleven (zie Figuur 19 in Appendix). Voor meer geavanceerde technische maatregelen zoals biometrische authenticatietechnieken en periodieke ICT-veiligheidsanalyse of ICT-veiligheidstesten is de adoptiegraad aanzienlijk gestegen. Ook opleidingen of activiteiten worden door een groter aandeel bedrijven voorzien aan hun werknemers. Hoewel deze vergelijking wijst op een positieve evolutie[12], blijft het geheel van ingevoerde technische maatregelen nog te vaak beperkt tot relatieve basistoepassingen.

Bij de interpretatie van deze resultaten moet men er zich van bewust zijn dat een hoge adoptiegraad van deze of gene technische 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 technische maatregelen. Het loutere feit dat bedrijven een aantal technische maatregelen treffen is in die optiek niet automatisch voldoende; de kracht van bescherming ligt immers in de combinatie van technische maatregelen. 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.

[11] Net zoals het geval is bij technische maatregelen is de effectiviteit van opleidingen of activiteiten afhankelijk de implementatie. Zo neemt de effectiviteit van opleidingen of activiteiten toe wanneer hun intensiteit en frequentie stijgt.

[12] Een belangrijke vraag is of een *non-responsbias* mogelijk aan de basis van deze stijging zou kunnen liggen. In tegenstelling tot de vorige editie van de bevraging kwamen de vragen rond AI dit jaar vóór die rond CS in de vragenlijst. Dit kan bedrijven zonder interesse in AI hebben afgeschrikt om deel te nemen. Additionele analyses tonen dat er een sterke positieve correlatie bestaat tussen de implementatie van AI en het aantal ingevoerde CS-maatregelen: meer digitaal geavanceerde bedrijven staan sterk op zowel het gebied van cybersecurity als het gebruik van AI. Als vooral digitaal geavanceerde bedrijven mét interesse in AI deelnemen aan de bevraging, zou dit de adoptiegraad van het aantal en dus ook van de meer geavanceerde CS-maatregelen in deze editie positief kunnen beïnvloeden. Figuur 20 in Appendix suggereert echter dat deze non-responsbias naar alle waarschijnlijk zeer beperkt is. Ten gevolge van het vooruitschuiven van de AI-vragen kan men verwachten dat vooral micro- en kleine bedrijven (waarvan we weten dat ze typisch minder bezig zijn met AI) minder geneigd zijn om deel te nemen aan de bevraging. Bijgevolg zou men in deze grootteklasse een grotere non-responsbias verwachten. Figuur 20 in Appendix levert geen bewijs voor deze stelling. Bij de micro- en kleine bedrijven verschillen de verdelingen van het aantal CS-maatregelen voor de bevragingen uitgevoerd in 2022 en 2023 minder dan bij de middelgrote en grote bedrijven.

Figuur 3: Adoptiegraad type CS-maatregelen (N=2.442)



Beheerprocedures en plannen

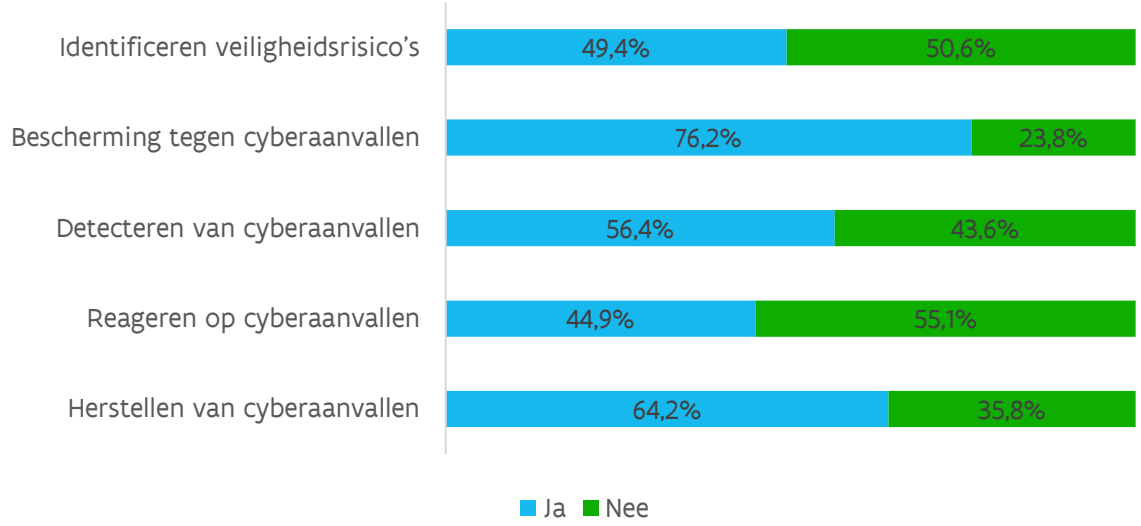
De adoptie van een reeks van technische maatregelen is een noodzakelijke maar geen voldoende voorwaarde voor cyberveiligheid. Ondanks alle mogelijke technische maatregelen kan het risico op een cyberincident nooit tot nul herleid worden. Bedrijven die pas nadenken over te ondernemen acties wanneer het cyberincident reeds heeft plaatsgevonden, lopen hopeloos achter de feiten aan. Aan de hand van beheerprocedures en beleidsplannen denken bedrijven proactief na over hoe cyberincidenten te voorkomen of erop te reageren.

Het NIST-kader biedt een reeks van standaarden, richtlijnen en procedures voor bedrijven om cyberveiligheid te beheren en mogelijke risico's te beperken[13]. 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 bieden om preventief en reactief te antwoorden op cyberaanvallen en er van te herstellen. Net zoals bij het nemen van technische 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 49,4% van de bedrijven die ten minste één CS-maatregel treffen (i.e. 94,8% 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 een mogelijk doelwit zijn bij een eventuele cyberaanval. Ten tweede zegt 76,2% procedures te hebben om zich effectief te beschermen tegen cyberaanvallen, bijvoorbeeld via toegangsbeheer, identificatiemanagement, back-ups, encryptie of regelmatige software-updates. Ten derde heeft 56,4% van de bedrijven die minstens één CS-maatregel namen procedures om cyberaanvallen te detecteren, bijvoorbeeld via continue monitoring van veiligheidsrisico's, technieken en protocollen. Ten vierde zegt 44,9% van deze bedrijven procedures te hebben om adequaat op cyberaanvallen te reageren, bijvoorbeeld aan de hand van incidentanalyses, dreigingseliminatie en/of crisiscommunicatie. Tot slot telt 64,2% van de bedrijven die minstens één CS-maatregel namen 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). In vergelijking met de meting in 2022 is de implementatie voor elk van de beheerprocedures gestegen (zie Figuur 21 in Appendix).

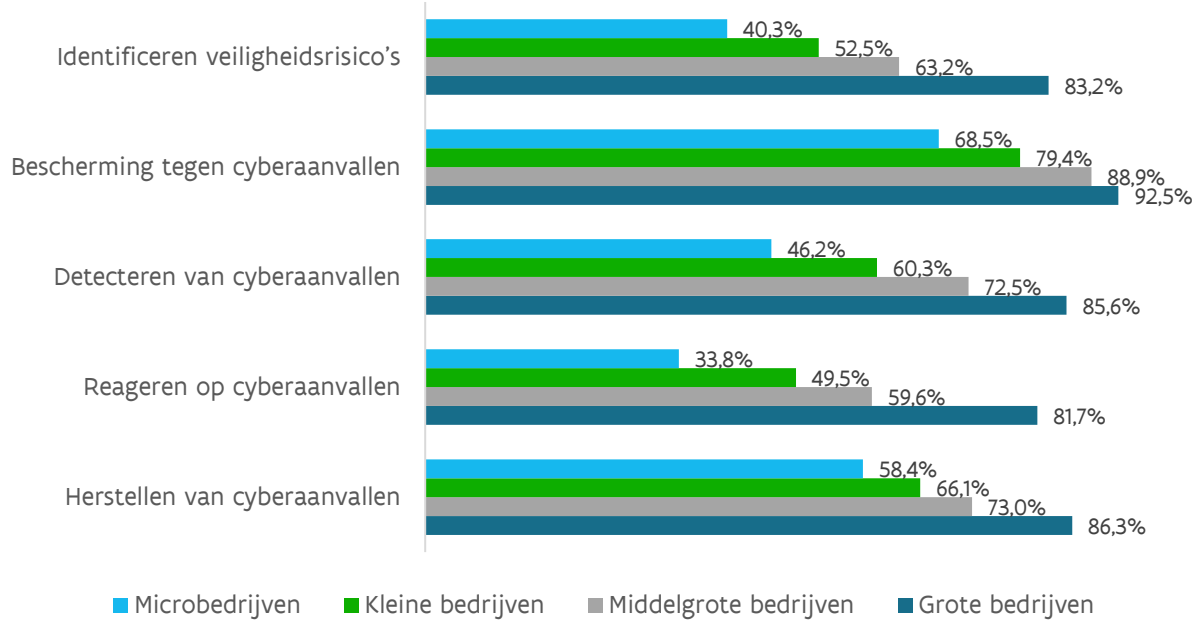
[13] Voor meer informatie, zie https://www.nist.gov/cyberframework

Figuur 4: Type beheerprocedures (N=2.360) – 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 hoger de kans dat het bedrijf beheerprocedures heeft geïnstalleerd (zie Figuur 5). Zo heeft 83,2% van de grote bedrijven die minstens één CS-maatregel namen ook effectief procedures om veiligheidsrisico's te identificeren terwijl dit bij kleine en microbedrijven respectievelijk 52,5% en 40,3% is. 92,5% van de grote bedrijven die minstens één CS-maatregel namen heeft procedures om zich te beschermen tegen cyberaanvallen, wat substantieel hoger is dan bij microbedrijven (68,5%). Procedures om cyberaanvallen te detecteren zijn sterker ingeburgerd bij grote bedrijven (85,6%) dan bij kleine (60,3%) en microbedrijven (46,2%). Deze trend is eveneens waarneembaar inzake procedures om te reageren op cyberaanvallen: 81,7% van de grote bedrijven die minstens één CS-maatregel namen heeft dergelijke procedures; dit is aanzienlijk hoger dan bij middelgrote bedrijven (59,6%), kleine bedrijven (49,5%) en microbedrijven (33,8%). Tot slot kent 86,3% van de grote bedrijven die minstens één CS-maatregel namen procedures om van cyberaanvallen te herstellen terwijl dit bij microbedrijven beperkt blijft tot 58,4%.

Figuur 5: Type beheerprocedures volgens bedrijfsgrootte (N=2.360) – Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen



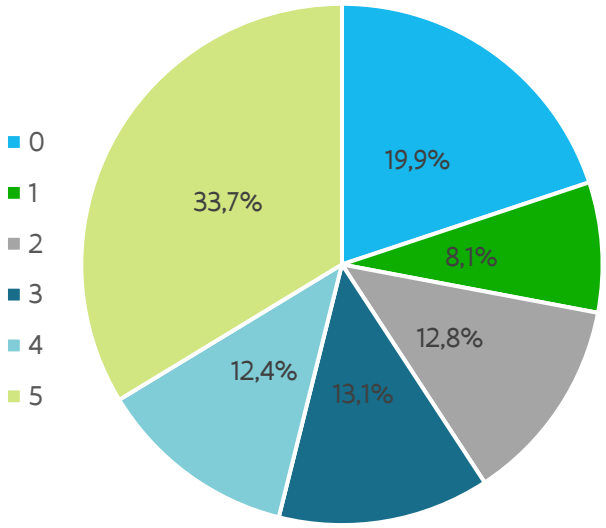
Ongeveer een derde (33,7%) van de Vlaamse bedrijven die minstens één CS-maatregel namen, heeft alle vijf procedures van het NIST-kader in zekere mate geïmplementeerd (zie Figuur 6). Terwijl 72,0% van de grote bedrijven met CS-maatregelen en 47,6% van de middelgrote bedrijven met CS-maatregelen alle vijf procedures van het NIST-kader toepast, is dit slechts voor 36,9% van de kleine bedrijven en 24,1% van de microbedrijven met CS-maatregelen het geval. Net zoals in meting in 2022 noteren de sectoren informatie en communicatie (NACE 58-63) en financiële activiteiten en verzekeringen (NACE 64-66) de hoogste scores op dit gebied, met aandelen van respectievelijk 59,2% en 42,6%.[14]

Omgekeerd heeft maar liefst 19,9% van de bedrijven die minstens één CS-maatregel namen geen enkele beheerprocedure om zich te beschermen tegen toekomstige cyberrisico's of met actuele cyberaanvallen om te gaan. Dit geldt voor 26,6% van de microbedrijven en 17,6% van de kleine bedrijven die minstens één CS-maatregel namen; slechts 7,3% van de middelgrote en 4,7% van de grote bedrijven valt hieronder. Consistent met de meting in 2022 vertonen bedrijven actief in accommodatie en maaltijden (NACE 55-56) en de bouwnijverheid (NACE 41-43) minimale CS-maturiteit; respectievelijk 41,1% en 29,6% van de bedrijven actief in die sector en met minstens één CS-maatregel heeft geen enkele beheerprocedure. In vergelijking met de meting in 2022 is bij de bedrijven die minstens één CS-maatregel namen het aandeel bedrijven met vijf beheerprocedures

[14] In vergelijking met andere sectoren zijn deze twee sectoren door de Europese wetgeving (i.e., NIS- en NIS-2-richtlijn) aan strengere verplichtingen inzake technische maatregelen en beheerprocedures onderworpen.

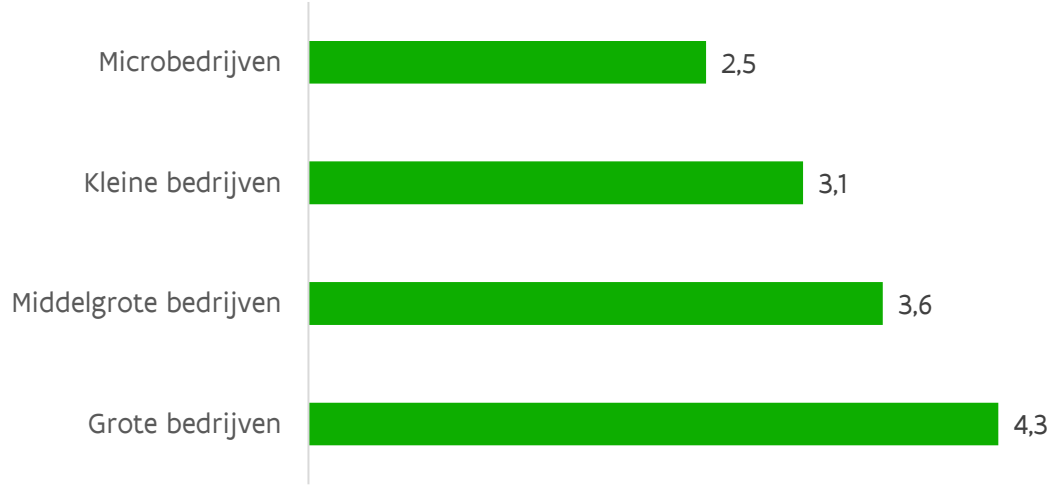
sterk gestegen (zie Figuur 22 in Appendix). Het aandeel bedrijven zonder enige beheerprocedure is daarentegen constant gebleven. Dit wijst erop dat bedrijven die eerder reeds minstens één beheerprocedure toepasten ingezet hebben op een uitbreiding van het aantal beheerprocedures.

Figuur 6: Aantal beheerprocedures (N=2.360) – Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen



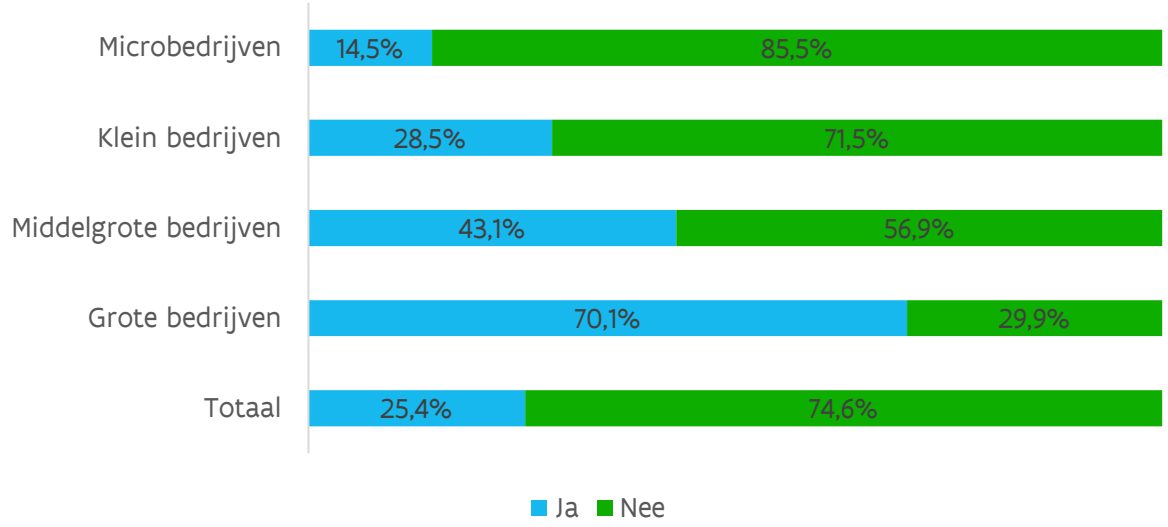
Het belang van bedrijfsgrootte met betrekking tot CS-maturiteit blijkt opnieuw duidelijk uit het gemiddeld aantal beheerprocedures dat bedrijven met CS-maatregelen uit verschillende grootteklassen installeren: microbedrijven hebben gemiddeld 2,5 procedures, kleine bedrijven 3,1, middelgrote bedrijven 3,6 en grote bedrijven 4,3 (zie Figuur 7). Grote bedrijven hebben met andere woorden een hogere mate van CS-maturiteit, terwijl kleine en microbedrijven opmerkelijk minder goed beschermd zijn tegen cyberaanvallen. In vergelijking met de meting in 2022 is het aantal beheerprocedures voor alle grootteklassen licht gestegen (zie Figuur 23 in Appendix).

Figuur 7: Aantal beheerprocedures volgens bedrijfsgrootte (N=2.360) – Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen



De effectiviteit van CS-maatregelen en beheerprocedures kan verder verhoogd worden door een doordachte aanpak inzake cybersecurity te formuleren. Het geschikte instrument hiervoor is een beleidsdocument of plan waarin bedrijven een coherent geheel van acties en procedures inzake cybersecurity uitwerken. Ongeveer een kwart (25,4%) van de bedrijven die ten minste één CS-maatregel treffen beschikt over een beleidsdocument inzake cybersecurity (zie Figuur 8). Dit aandeel ligt opmerkelijk hoger bij grote bedrijven (70,1%). 55,9% van de bedrijven actief in informatie en communicatie (NACE 58-63) en 45,9% van de bedrijven in financiële activiteiten en verzekeringen (NACE 64-66) die minstens één CS-maatregel namen heeft effectief een beleidsplan, in tegenstelling tot 7,3% van de bedrijven met CS-maatregelen in accommodatie en maaltijden (NACE 55-56) en 13,4% van de bedrijven met CS-maatregelen in de bouwnijverheid (NACE 41-43). In vergelijking met de meting in 2022 is het gebruik van een beleidsdocument inzake cybersecurity gestegen voor de grote, middelgrote en kleine bedrijven. Ondanks de stijging in het gebruik van een beleidsdocument bestaat er nog heel wat groeimarge bij de kleine en middelgrote bedrijven. Bij de microbedrijven valt er geen positieve trend te bespeuren. Hun achterstand t.o.v. bedrijven in andere grootteklassen is bijgevolg enkel toegenomen.

Figuur 8: Plan/beleidsdocument inzake cybersecurity volgens bedrijfsgrootte (N=2.360) – Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen

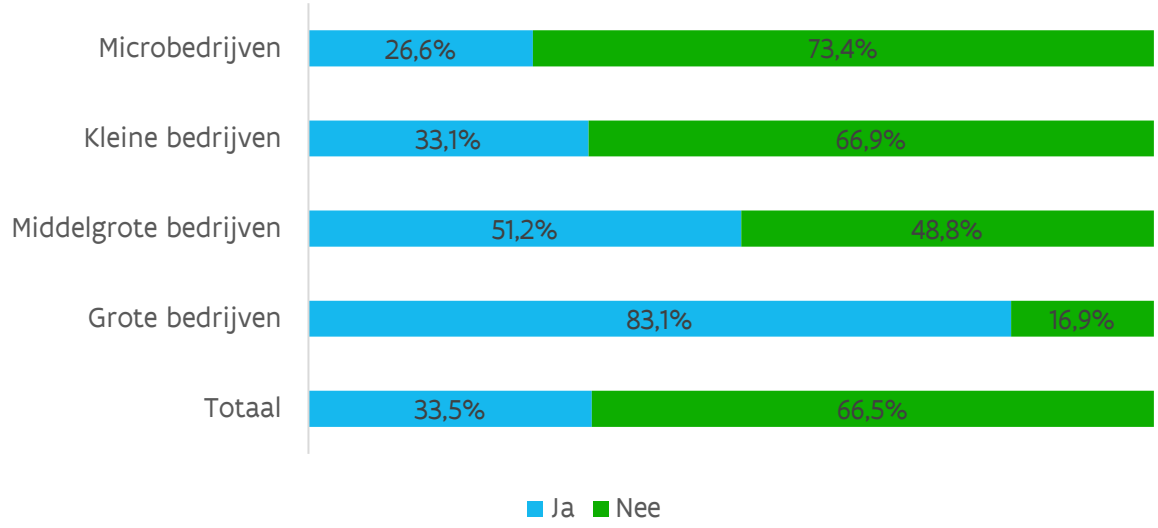


Druk op en vanuit de waardeketen

Als gevolg van de toenemende automatisering en integratie van waardeketens worden elektronische systemen en data almaar vaker gedeeld met leveranciers en klanten. Het directe gevolg hiervan is dat de uiteindelijke mate van bescherming van deze systemen en data bepaald wordt door het bedrijf met de laagste cybersecuritymaturiteit. Een ketting is nu eenmaal net zo sterk als de zwakste schakel. Slechts een derde (33,5%) van de bedrijven in Vlaanderen stelde het afgelopen jaar eisen aan bepaalde of alle leveranciers of onderaannemers inzake cybersecurity (zie Figuur 9).

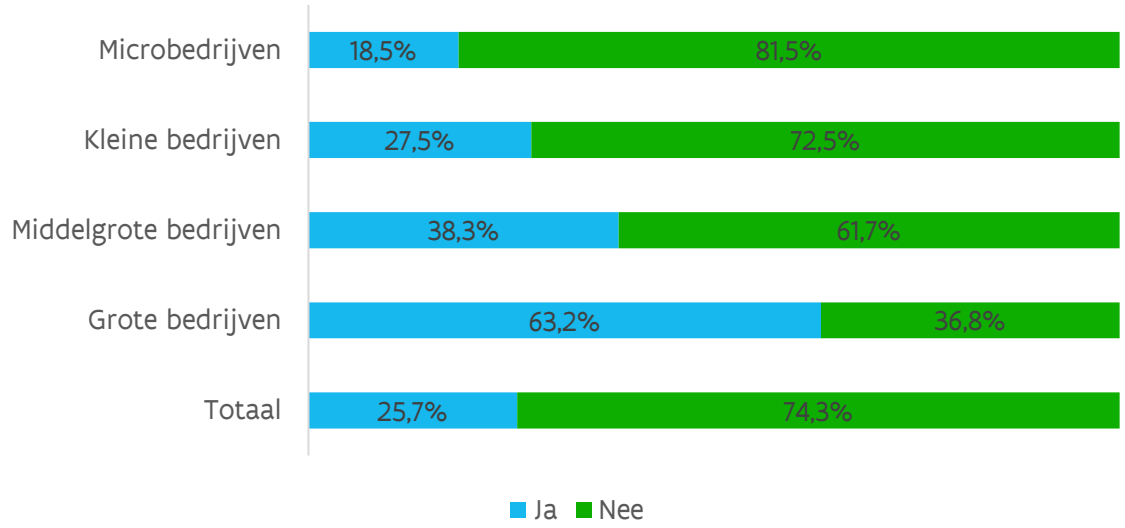
Dit aandeel ligt wel een pak hoger bij grote (83,1%) en middelgrote (51,2%) bedrijven dan bij kleinere ondernemingen. Terwijl meer dan de helft van de bedrijven actief in informatie en communicatie (NACE 58-63) en financiële activiteiten en verzekeringen (NACE 64-66) eisen oplegt aan leveranciers of onderaannemers, is dit slechts het geval voor 19,7% van de bedrijven actief in accommodatie en maaltijden (NACE 55-56) en 17,5% van de bouwbedrijven (NACE 41-43).

Figuur 9: Eisen aan leveranciers/onderaannemers inzake cybersecurity volgens bedrijfsgrootte (N=2.442)



Iets meer dan een kwart (25,7%) van de bedrijven kreeg op zijn beurt eisen opgelegd van bepaalde of alle klanten (zie Figuur 10). Opnieuw ligt dit aandeel beduidend hoger bij grote (63,2%) en middelgrote (38,3%) bedrijven. Maar liefst 79,6% van de bedrijven in informatie en communicatie (NACE 58-63) kreeg eisen opgelegd van klanten.

Figuur 10: Eisen van klanten inzake cybersecurity volgens bedrijfsgrootte (N=2.442)



Alhoewel nog steeds vrij beperkt, oefent een groter aandeel bedrijven druk uit op haar leveranciers inzake cybersecurity en krijgt ook een groter aandeel bedrijven eisen opgelegd door haar klanten in vergelijking met de meting in 2022 (zie Figuur 24 in Appendix).

Obstakels

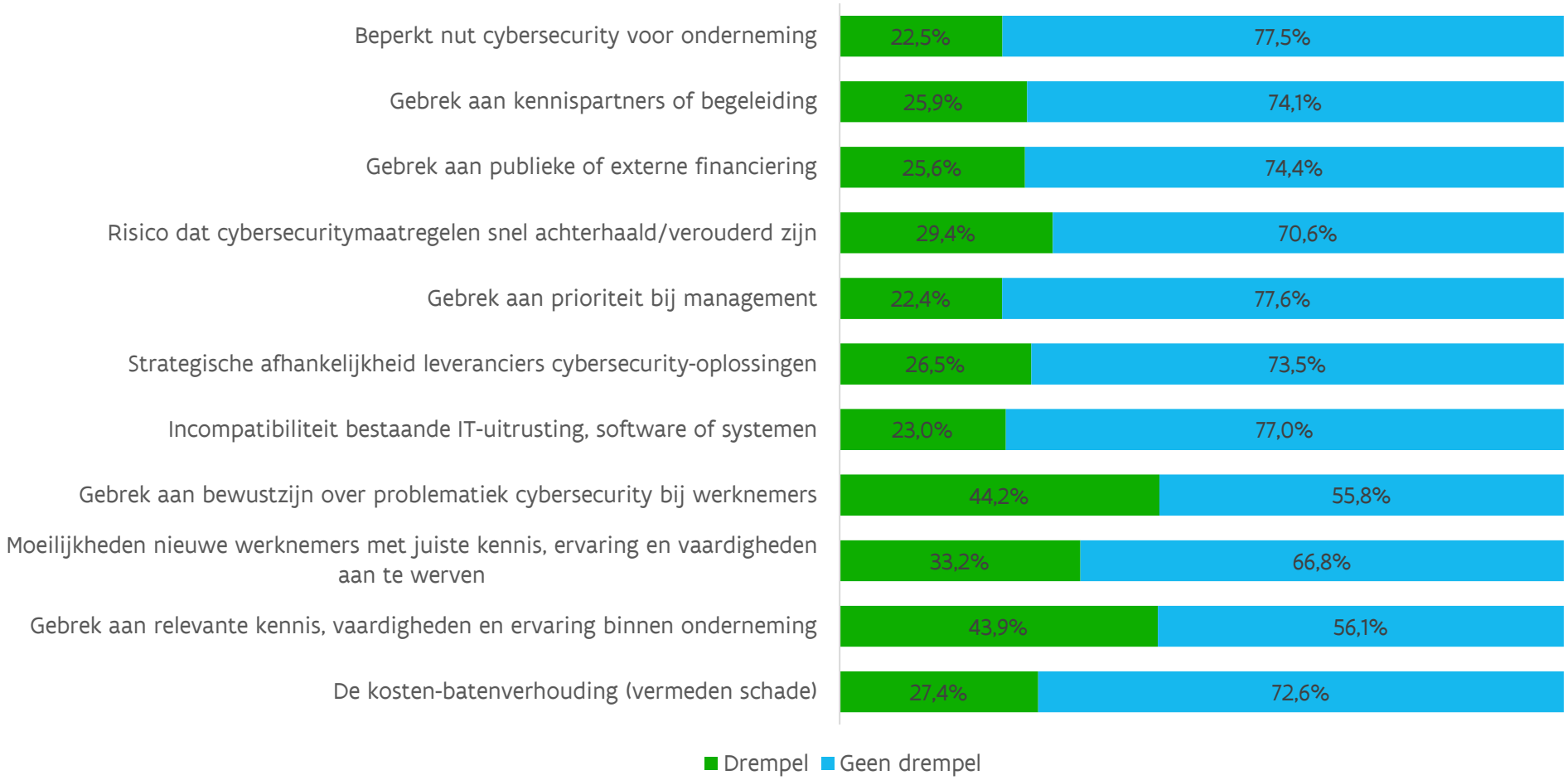
De invoer en het gebruik van CS-maatregelen en beheerprocedures stelt bedrijven voor de nodige uitdagingen, die van operationele, financiële, technische of nog andere aard kunnen zijn. Figuur 11 toont welke obstakels bedrijven voornamelijk ondervinden. 43,9% van de ondernemingen die minstens één CS-maatregel invoerden, identificeert het gebrek aan relevante kennis, vaardigheden en ervaring bij de huidige werknemers als een obstakel voor een adequaat CS-beleid; 33,2% ondervindt bovendien moeilijkheden om nieuwe werknemers met deze kennis, vaardigheden en ervaring aan te werven. Behalve kennis en vaardigheden erkent 44,2% van de bedrijven die CS-maatregelen namen eveneens een gebrek aan bewustzijn omtrent cybersecurity bij de werknemers. Daarnaast ziet 25,9% een gebrek aan kennispartners of begeleiding. Bedrijven zien het gebrek aan kennis, vaardigheden en bewustzijn met andere woorden als hét belangrijkste obstakel bij de invoer en het gebruik van CS-maatregelen. Nochtans vormt deze menselijke component – naast technische maatregelen en beheerprocedures – een belangrijke verdedigingsgordel tegen cyberaanvallen.

Bijna drie op tien (29,4%) van de bedrijven die minstens één CS-maatregel toepassen wijst het risico dat CS-maatregelen snel achterhaald of verouderd zijn als obstakel aan. Een effectief CS-beleid vereist immers continue aanpassingen en daardoor periodieke investeringen. Deze investeringen worden afgezet tegen de verwachte voordelen, ofwel de vermeden schade in het geval van een cyberaanval. Voor 27,4% van de bedrijven die minstens één CS-maatregel invoerden wegen de kosten van een adequaat CS-beleid zwaarder dan de baten (i.e., vermeden schade). Een gelijkaardig aandeel (25,6%) ondervindt een gebrek aan publieke of externe financiering.

Hoewel het minst vaak beschouwd als obstakels, blijken de perceptie dat het invoeren van een CS-beleid weinig nut biedt voor de organisatie en het gebrek aan prioriteit bij het management toch nog een probleem bij respectievelijk 22,5% en 22,4% van de ondernemingen die minstens één CS-maatregel toepassen.

In vergelijking met de meting in 2022 is de mate waarin Vlaamse bedrijven obstakels ondervinden bij de invoer en het gebruik van CS-maatregelen gedaald. De daling is het meest uitgesproken voor het gebrek aan kennis, vaardigheden en bewustzijn en het gebrek aan bewustzijn omtrent cybersecurity bij werknemers (zie Figuur 25 in Appendix).

Figuur 11: Obstakels bij de invoer en het gebruik van CS-maatregelen voor bedrijven die minstens één CS-maatregel toepassen (N=2.360)



Omdat slechts 82 bedrijven in de bevraging geen enkele CS-maatregel hanteerden, bleek een vergelijking tussen zogenaamde adopters en niet-adopters niet opportuun. Daarom werden bedrijven met een lage adoptiegraad van CS-maatregelen (minstens één en maximum vijf genomen CS-maatregelen) (N = 537) en een hoge adoptiegraad van CS-maatregelen (meer dan vijf genomen CS-maatregelen) (N = 1.823) met elkaar vergeleken. Figuur 12 wijst uit dat bedrijven met een lage adoptiegraad meer obstakels ervaren bij de invoer en het gebruik van CS-maatregelen dan bedrijven met een hoge adoptiegraad. Deze ervaren obstakels zijn daarom wellicht ook de redenen voor de lage adoptiegraad.

Bedrijven met een lage adoptiegraad worstelen vaker met een gebrek aan kennis, vaardigheden en ervaring binnen de organisatie (61,6%) dan bedrijven met een hoge adoptiegraad. Bedrijven met een lage adoptiegraad ervaren ook een sterker gebrek aan kennispartners of begeleiding (41,0%) en meer moeilijkheden om nieuwe werknemers met de juiste kennis, vaardigheden en ervaring aan te werven (38,9%) dan bedrijven met een hoge adoptiegraad. Eveneens observeren we bij bedrijven met een lage adoptiegraad vaker een laag ingeschat nut (40,8%) en gebrek aan prioriteit bij het management (36,4%) in vergelijking met bedrijven met een hoge adoptiegraad.

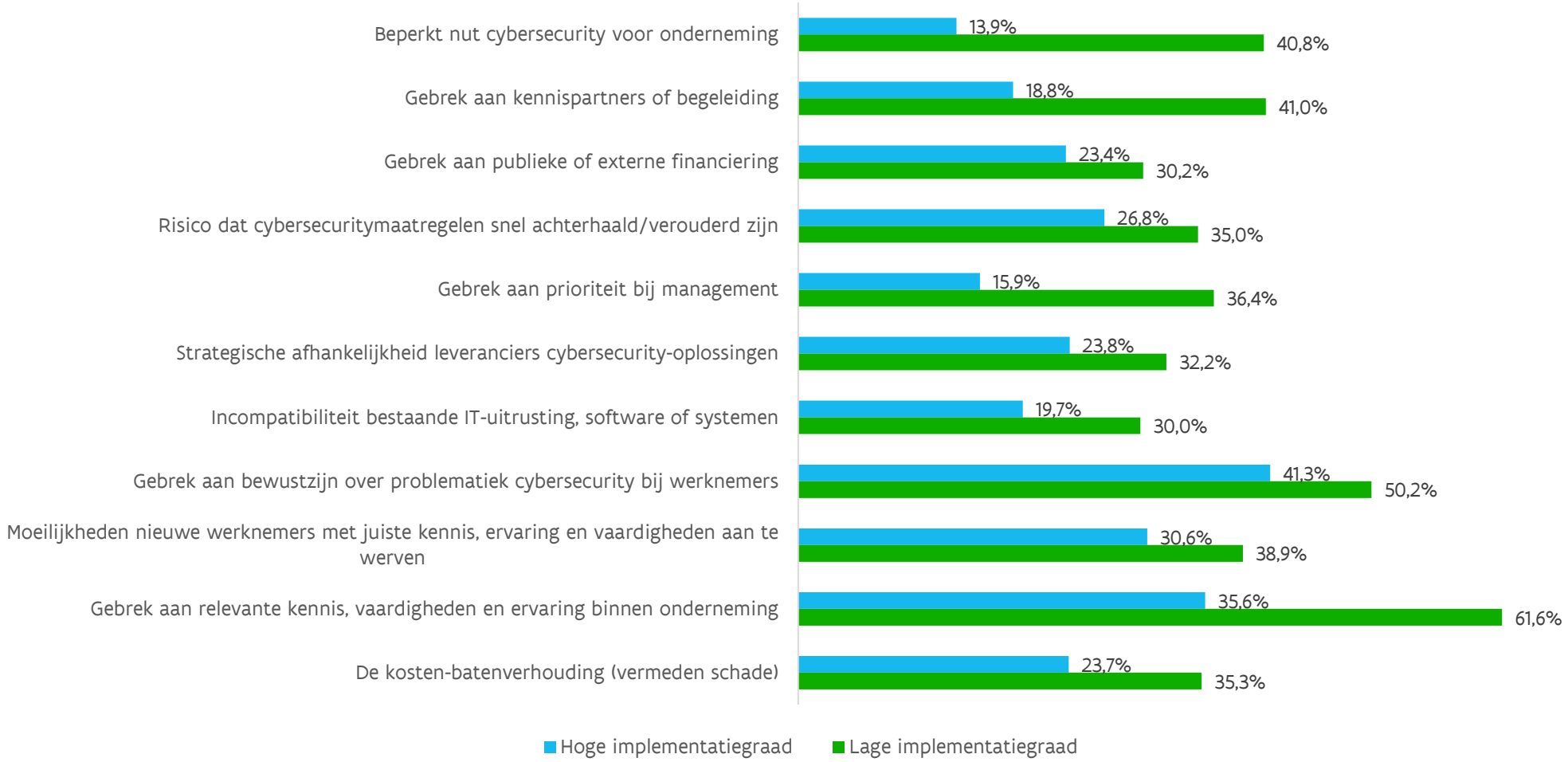
Een aanzienlijk aandeel van de bedrijven met een lage (50,2%) of hoge adoptiegraad (41,3%) vertonen een sterk gebrek aan bewustzijn over de problematiek rond cybersecurity bij werknemers. Dit toont aan dat voor Vlaamse bedrijven het menselijke aspect van cybersecurity een belangrijk obstakel vormt bij de invoer en het gebruik van CS-maatregelen, ongeacht de adoptiegraad van CS-maatregelen.

Figuur 13 geeft weer hoe deze obstakels verschillen naargelang de grootteklasse van de onderneming. Voor meer dan vier op tien bedrijven in alle grootteklassen vormt een gebrek aan bewustzijn bij werknemers een belangrijk obstakel bij de invoer en het gebruik van CS-maatregelen. Grote bedrijven worstelen daarnaast opmerkelijk vaker dan bedrijven in andere grootteklassen met moeilijkheden om nieuwe werknemers met de juiste kennis, ervaring en vaardigheden aan te werven (54,2%).[15] Microbedrijven kampen op hun beurt aanzienlijk vaker dan bedrijven in andere grootteklassen met een gebrek aan relevante kennis, vaardigheden en ervaring binnen de onderneming (48,8%) en een gebrek aan kennispartners of begeleiding (30,7%).

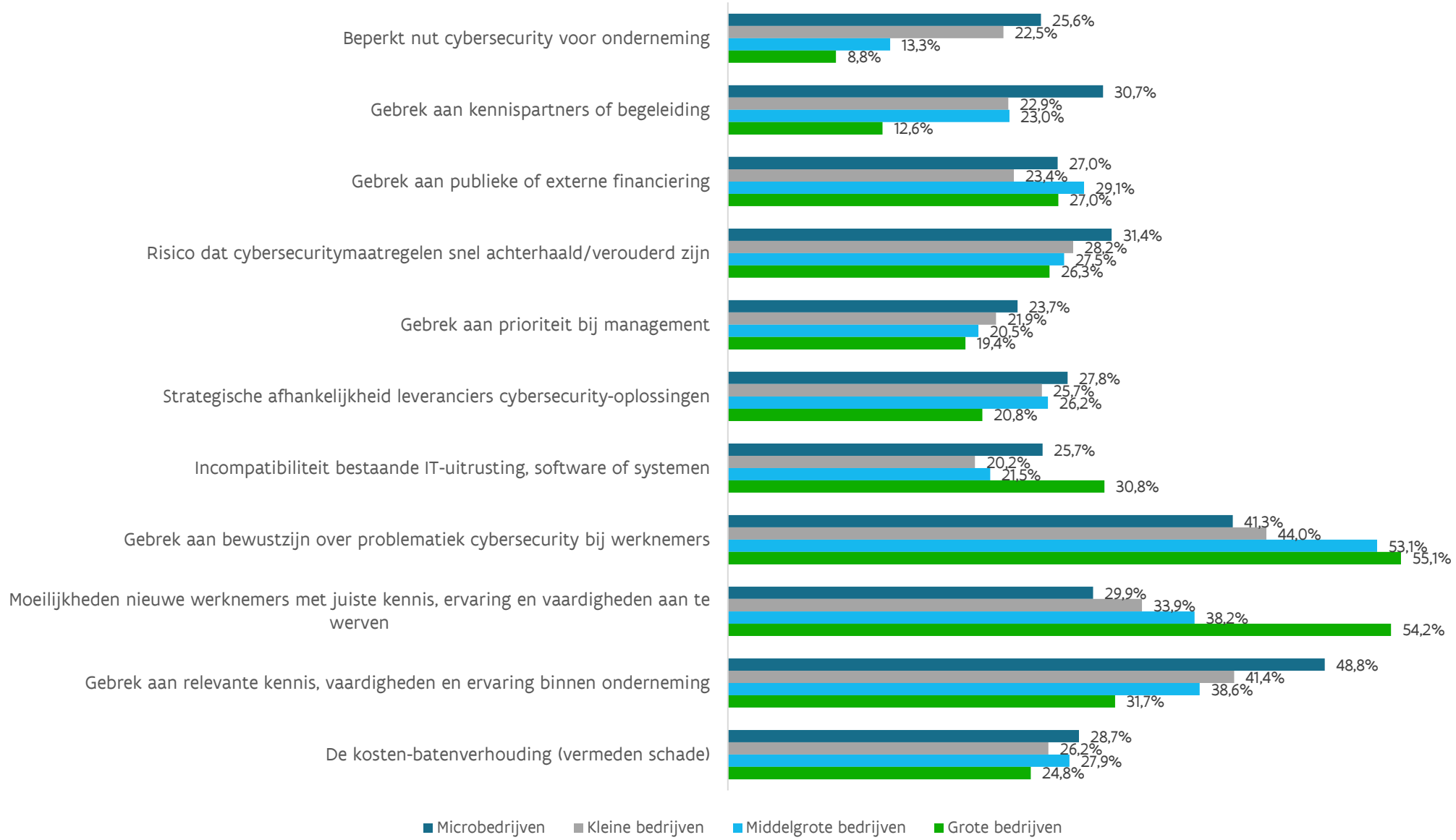
[15] Uit de vorige editie van de CS-barometer bleek dat, in vergelijking met andere grootteklassen, een groter aandeel van de grote bedrijven beroep doet op het eigen personeel voor de uitvoering van ICT-beveiligingsgerelateerde activiteiten. Gezien het aantal CS-experts beperkt is en grote bedrijven meer inzetten op het vlak van cybersecurity, hoeft het niet te verbazen dat grote bedrijven meer moeilijkheden ondervinden om geschikte profielen te vinden (zie ook https://www.vrt.be/vrtnws/nl/2023/01/21/cybersecurity-knelpuntberoep/).

Voor bedrijven uit om het even welke sector zijn een gebrek aan bewustzijn bij werknemers en een gebrek aan relevante kennis, vaardigheden en ervaring binnen de onderneming twee grote obstakels bij de invoer en het gebruik van CS-maatregelen. Daarbuiten ervaren bedrijven actief in financiële activiteiten en verzekeringen (NACE 64-66) en informatie en communicatie (NACE 58-63) over het algemeen minder vaak obstakels vergeleken met bedrijven uit andere sectoren. Bedrijven actief in menselijke gezondheidszorg en maatschappelijke dienstverlening (NACE 86-88) en accommodatie en maaltijden (NACE 55-56) ervaren dan weer vaker obstakels vergeleken met bedrijven uit andere sectoren; bedrijven uit deze twee sectoren wijzen voornamelijk vaker op een gebrek aan kennispartners of begeleiding, een gebrek aan publieke of externe financiering, en een ongunstige kosten-batenverhouding van het CS-beleid.

Figuur 12: Obstakels bij de invoer en het gebruik van CS-maatregelen volgens adoptiegraad voor bedrijven die minstens één CS-maatregel toepassen (N=2.360)



Figuur 13: Obstakels bij de invoer en het gebruik van CS-maatregelen volgens bedrijfsgrootte voor bedrijven die minstens één CS-maatregel toepassen (N=2.360)



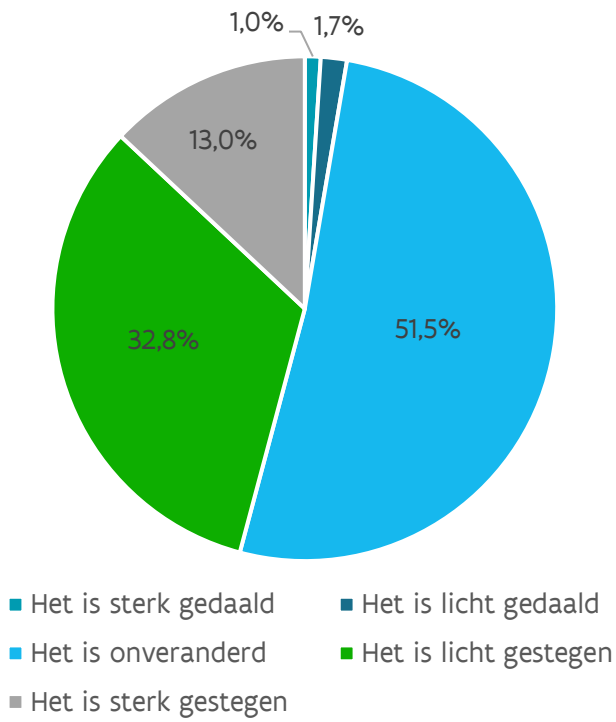
Budget

Bij de meerderheid van de Vlaamse bedrijven die minstens één CS-maatregel namen is het budget voor de implementatie van CS-maatregelen en beheerprocedures het voorbije jaar onveranderd gebleven dan wel gestegen (zie Figuur 14). 45,8% van de bedrijven liet een – lichte of sterke – stijging in de uitgaven voor CS noteren. Voor ongeveer de helft (51,5%) van de bedrijven bleef het budget ongewijzigd. Bij amper 2,7% van de bedrijven daalde het budget het afgelopen jaar. Bijgevolg kunnen we globaal gezien spreken over een stijging in de uitgaven voor CS door Vlaamse bedrijven. De stijging is het sterkst merkbaar bij grote bedrijven; in die groep geeft 46,3% aan dat het budget licht gestegen is terwijl nog eens 29,5% van een sterke toename spreekt. Ook bij middelgrote bedrijven is een stijging meer voorkomend dan bij kleinere ondernemingen: 44,8% voerde een lichte stijging in het CS-budget door, 18,5% spreekt zelfs van een sterke stijging. Bedrijven actief in informatie en communicatie (NACE 58-63) en financiële activiteiten en verzekeringen (NACE 64-66) zien hun budgetten het vaakst stijgen; bedrijven actief in accommodatie en maaltijden (NACE 55-56) en de bouwnijverheid (NACE 41-43) het minst.

Gemiddeld spenderen Vlaamse bedrijven naar schatting 19,7% van hun totale IT-budget aan cybersecurity. Bij de grote bedrijven ligt dit gemiddelde lager op 13,1%, bij microbedrijven bedraagt dit gemiddeld 21,4%. 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 vertegenwoordigt dan de uitgaven van microbedrijven voor CS-maatregelen.

Het aandeel van het CS-budget in het totale IT-budget is onveranderd ten opzichte van de meting in 2022 (zie Figuur 26 in Appendix). Dit suggereert dat de stijging in de uitgaven voor CS evenredig was met de stijging in het totale IT-budget.

Figuur 14: Evolutie CS-budget (N=2.360) – Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen



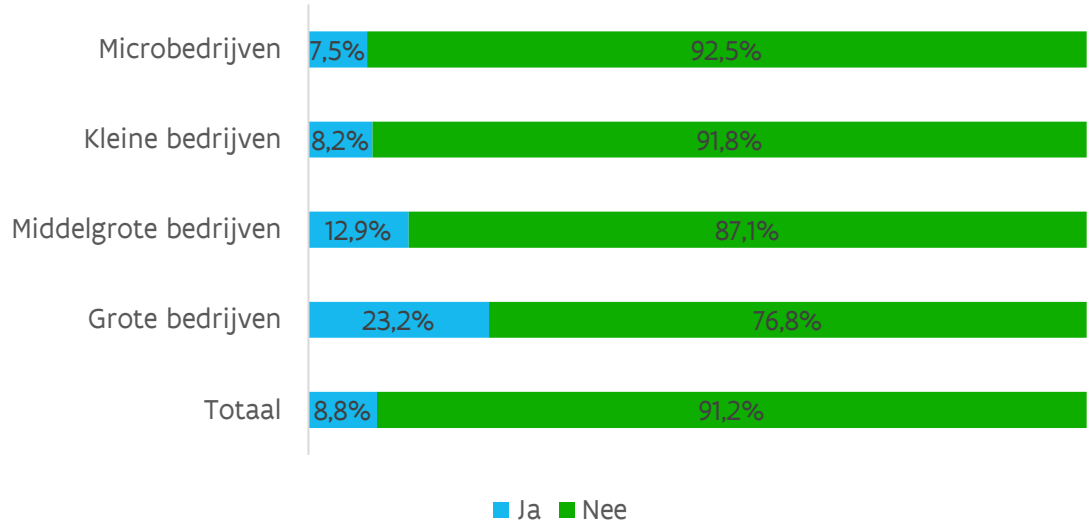
Cyberaanval

Bijna één op tien bedrijven (8,8%) geeft aan het afgelopen jaar het slachtoffer te zijn geweest van een cyberaanval, waarbij cybercriminelen al dan niet met succes trachtten computersystemen onklaar te maken of persoonlijke of confidentiële gegevens te verkrijgen (zie Figuur 15). Dit aandeel is naar alle waarschijnlijkheid een onderschatting van het werkelijke aandeel aangezien (i) een cyberaanval onopgemerkt kan blijven, (ii) respondenten eerder geneigd zijn om zich een cyberaanval te herinneren en deze te rapporteren wanneer de cyberaanval uiteindelijk schade berokkende aan het bedrijf en/of (ii) bedrijven uit vrees voor reputatieschade terughoudend zijn om hierover te communiceren. Grote bedrijven (23,2%) zijn het vaakst slachtoffer van een cyberaanval, ook middelgrote bedrijven (12,9%) worden vaak getroffen. Dit in tegenstelling tot kleine (8,2%) en microbedrijven (7,5%) die in iets mindere mate worden geviseerd door cybercriminelen.[16] Bedrijven actief in de maakindustrie (NACE 10-33) worden opmerkelijk vaker (12,4%) getroffen dan bedrijven uit andere sectoren. Hoewel in vergelijking met de meting in 2022 een kleiner aandeel bedrijven slachtoffer werd van een cyberaanval dient deze statistiek zoals

[16] De resultaten met betrekking tot de frequentie van cyberaanvallen volgens grootteklasse dienen met de nodige voorzichtigheid geïnterpreteerd te worden. Omwille van hun lagere mate van bescherming in vergelijking met grotere bedrijven blijven cyberaanvallen bij kleinere bedrijven vaker onopgemerkt.

eerder werd benadrukt met de nodige voorzichtigheid geïnterpreteerd te worden (zie Figuur 27 in Appendix).

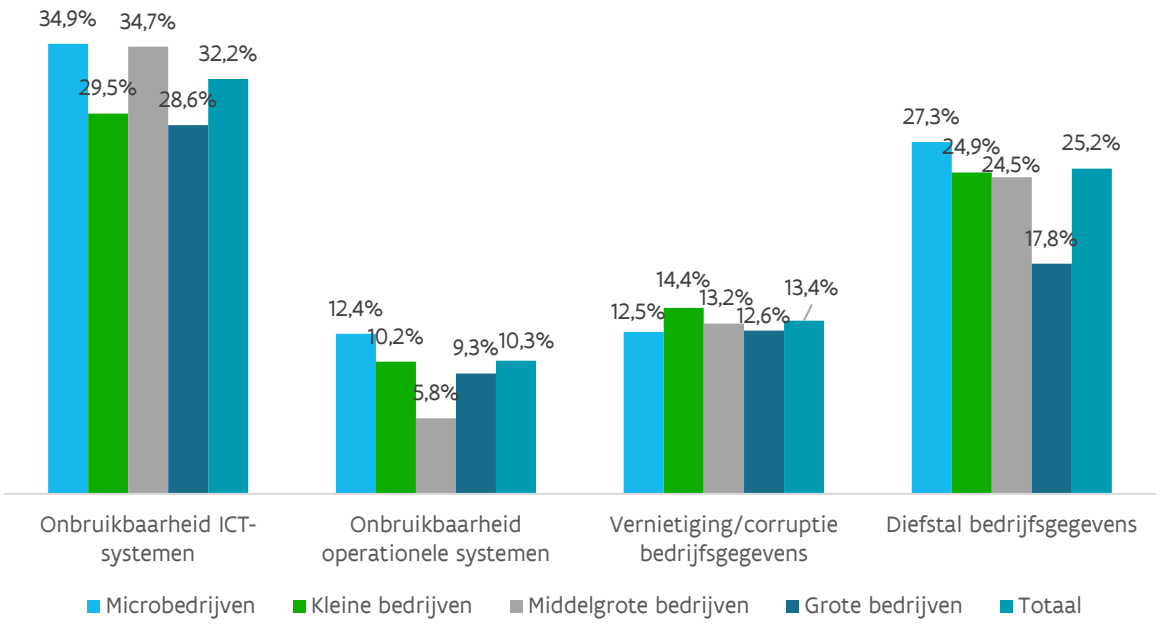
Figuur 15: Slachtoffer van cyberaanval volgens bedrijfsgrootte (N=2.442)



Een dergelijke cyberaanval kan verstrekkende gevolgen hebben voor het getroffen bedrijf. Uit Figuur 16 blijkt dat de *onbruikbaarheid van ICT-systemen* met voorsprong het meest voorkomende operationele gevolg is van een cyberaanval. Bij 32,2% van de geviseerde bedrijven werden ICT-systemen onbruikbaar als gevolg van een cyberaanval, bijvoorbeeld door hacking, kwaadwillige vergrendeling of DDoS-aanval. Dit is in bijzondere mate het geval voor microbedrijven (34,9%) en middelgrote bedrijven (34,7%), bedrijven actief in informatie en communicatie (48,1%), menselijke gezondheidszorg en maatschappelijke dienstverlening (40,7%), en de bouwnijverheid (40,5%).

Minder voorkomend is de *onbruikbaarheid van operationele systemen*, zoals machines, gebouwen of andere infrastructuur (10,3%). Ook hier blijken microbedrijven (12,4%) kwetsbaar, net zoals bedrijven actief in menselijke gezondheidszorg en maatschappelijke dienstverlening (17,3%) en informatie en communicatie (14,1%).

Figuur 16: Operationele gevolgen cyberaanval volgens bedrijfsgrootte (N=291) – Deze vraag werd enkel gesteld aan bedrijven die het slachtoffer werden van een cyberaanval



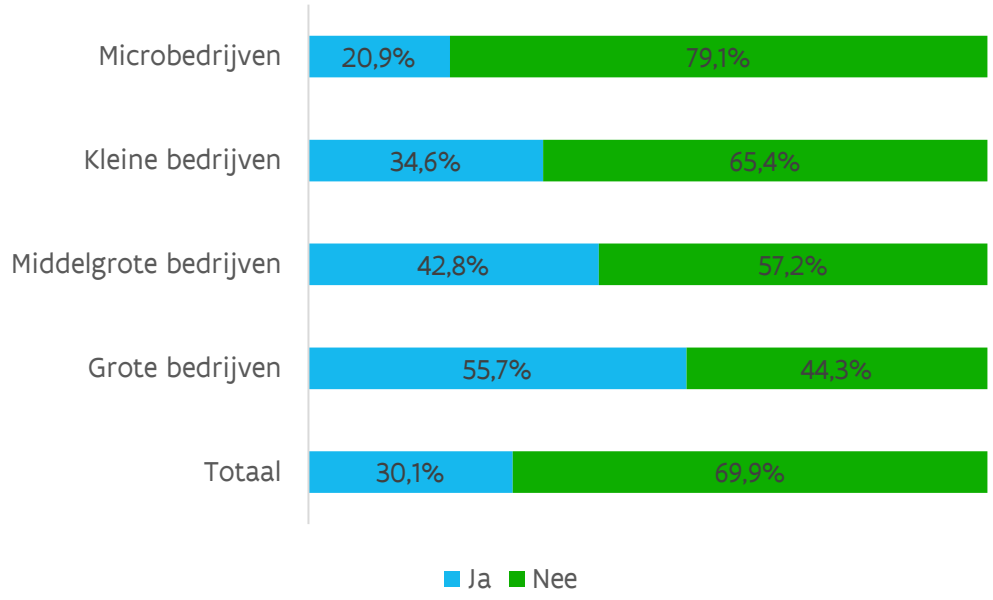
13,4% van de bedrijven die een cyberaanval meemaakten werd geconfronteerd met de *vernietiging of het onbruikbaar maken van bedrijfsgegevens*, bijvoorbeeld door infectie van kwaadaardige software of ongeoorloofde toegang. Slachtoffers uit alle grootteklassen krijgen hier ongeveer in dezelfde mate mee te maken. In verhouding tot bedrijven in andere sectoren krijgen bedrijven actief in vervoer en opslag (30,6%) en de bouwnijverheid (30,4%) opmerkelijk vaker met vernietiging van bedrijfsgegevens te maken.

Tot slot kreeg 25,2% van de bedrijven die aangevallen werden te kampen met *diefstal van (confidentiële) bedrijfsgegevens*, bijvoorbeeld door infectie van kwaadaardige software of phishingberichten. Opnieuw worden vooral microbedrijven (27,3%) hierdoor getroffen, evenals bedrijven actief in financiële activiteiten en verzekeringen (56,3%) en vervoer en opslag (52,2%).

Ondanks het lager aantal slachtoffers, suggereert Figuur 28 in Appendix dat cyberaanvallen vaker gevolgen hebben voor bedrijven. Het aandeel slachtoffers van een cyberaanval dat te maken krijgt met diefstal van bedrijfsgegevens kent een opmerkelijke stijging. Gezien het beperkt aantal bedrijven gebruikt in de analyse (namelijk enkel de 291 bedrijven die aangaven het slachtoffer te zijn geweest van een cyberaanval), moeten deze cijfers echter met voorzichtigheid geïnterpreteerd worden.

Bijna een derde van de Vlaamse bedrijven (30,1%) is verzekerd tegen cyberaanvallen (zie Figuur 17). Een dergelijke verzekering dekt (gedeeltelijk) de financiële schade van een geslaagde cyberaanval (zoals bijvoorbeeld losgeld of schade bij derden) maar verlaagt het risico op een cyberaanval uiteraard niet. Bedrijven blijven ondanks een verzekering tegen cyberaanvallen even kwetsbaar bij gebrek aan technische maatregelen en beheerprocedures. Van de grote bedrijven claimt meer dan de helft (55,7%) een verzekering afgesloten te hebben tegen cyberaanvallen. Dit aandeel ligt een pak lager bij de middelgrote bedrijven (42,8%), de kleine bedrijven (34,6%), en de microbedrijven (20,9%). Terwijl een opmerkelijk hoger aandeel bedrijven actief in financiële activiteiten en verzekeringen (49,7%), onroerend goed, vrije beroepen en wetenschappelijke en technische activiteiten (46,9%), en informatie en communicatie (45,2%) verzekerd is, geldt het omgekeerde voor accommodatie en maaltijden (11,9%). In vergelijking met de meting in 2022 is het aandeel tegen cyberaanvallen verzekerde bedrijven licht gestegen (zie Figuur 29 in Appendix).

Figuur 17: Verzekering tegen cyberaanvallen volgens bedrijfsgrootte (N=2.442)



Conclusies

De resultaten van deze studie wijzen in de richting van een gestage toename in de cybersecurity maturiteit van ondernemingen in Vlaanderen. De adoptie van meer geavanceerde technische maatregelen, beheerprocedures en opleidingen of activiteiten voor werknemers zit in de lift. In vergelijking met de vorige meting kampen minder bedrijven met een gebrek aan bewustzijn omtrent cybersecurity bij de werknemers en met een gebrek aan relevante kennis, vaardigheden en ervaring binnen de onderneming.

Hoewel de algemene tendens – op basis van een beperkt tijdskader – positief is dienen er enkele kanttekeningen gemaakt te geworden. De grootste vooruitgang is immers vast te stellen bij grote ondernemingen. Een omvangrijke groep bedrijven, gaande van middelgrote tot microbedrijven, hinkt nog steeds achterop op het vlak van de investeringen in technische maatregelen en beheerprocedures. Bij een aanzienlijk aandeel van deze groep bedrijven heerst onderliggend een gebrek aan relevante kennis, vaardigheden en ervaring binnen de onderneming, wat in vele gevallen niet kan worden opgevangen als gevolg van een gebrek aan kennispartners of begeleiding. Bovendien bestaat er nog steeds een aanzienlijke groep bedrijven, bestaande uit voornamelijk micro- en kleine bedrijven, die meent dat cybersecurity slechts een beperkt nut heeft. Daarnaast besteedt het management, niet alleen in micro- en kleine bedrijven maar ook in middelgrote bedrijven, nog te vaak onvoldoende prioriteit aan cybersecurity. De implementatie van meer geavanceerde technische maatregelen en een kader van beheerprocedures blijft als gevolg hiervan vaak uit, wat deze groep bedrijven kwetsbaar maakt voor cyberaanvallen, met mogelijk verstrekkende gevolgen. Om deze groep bedrijven te ondersteunen dient het overheidsbeleid in te blijven zetten op het verhogen van het bewustzijn omtrent cybersecurity bij bedrijfsleiders en het faciliteren van de toegang tot externe gespecialiseerde CS-dienstverleners.

Ook bij de grote ondernemingen blijft er ruimte voor verbetering. Cybercriminelen worden almaar inventiever. Als gevolg hiervan blijft een aanzienlijk aandeel van de grote bedrijven, ondanks hun hogere beschermingsgraad (in vergelijking met bedrijven uit andere grootteklassen), ten prooi vallen aan cyberaanvallen. Door verder in te zetten op geavanceerde technische maatregelen en performante beheerprocedures (waarbij ook AI-technologie een belangrijke rol kan spelen), opleidingen en activiteiten voor werknemers, en het inschakelen van externe gespecialiseerde CS-dienstverleners kunnen grote bedrijven het risico op een cyberaanval verkleinen. Voor het invoeren en het aanpassen van technische maatregelen en beheerprocedures doen grote bedrijven in vergelijking met bedrijven uit andere grootteklassen vaker beroep op het eigen personeel. Onze

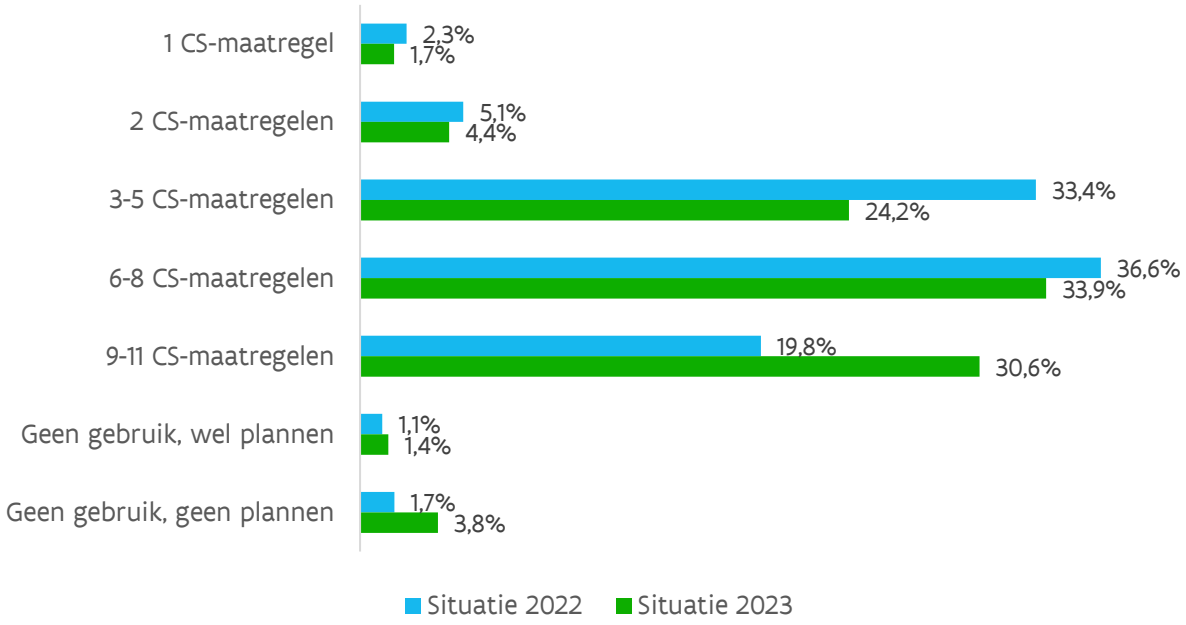
bevraging toont aan dat een aanzienlijk aandeel van de grote bedrijven moeilijkheden ervaart bij het aanwerven van deze profielen. Het overheidsbeleid dienst dus ook voor deze grote ondernemingen in te zetten op maatregelen die het aanbod van geschikte profielen bevorderen én de toegang tot externe kennispartners vergemakkelijken.

Appendix

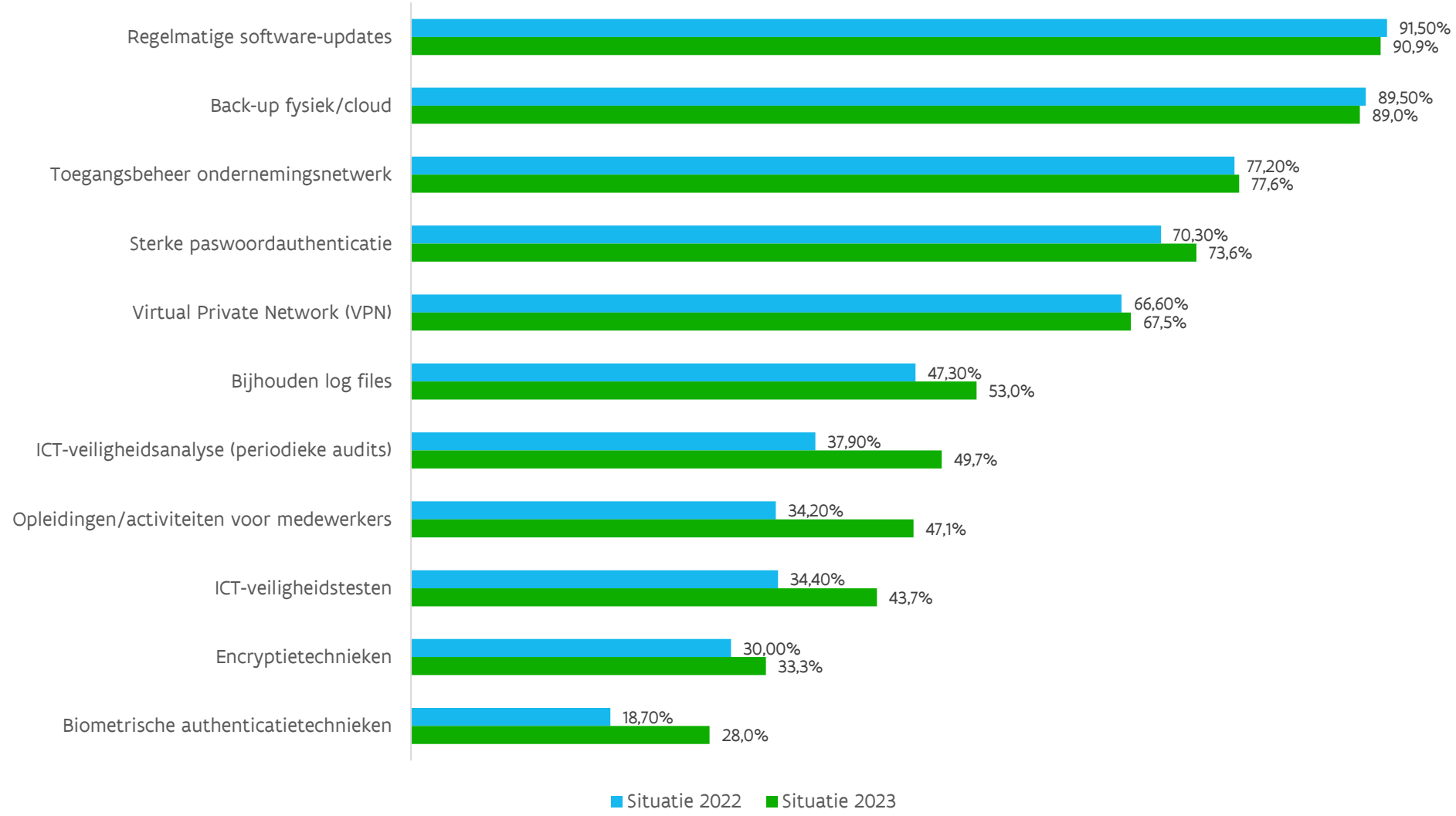
Tabel 3: Geselecteerde sectoren

NACE-codes	Omschrijving
NACE 10-33	Maakindustrie
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	Accommodatie en maaltijden
NACE 58-63	Informatie en communicatie
NACE 64-66	Financiële activiteiten en verzekeringen
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 86-88	Menselijke gezondheidszorg en maatschappelijke dienstverlening
NACE 95.1	Reparatie van computers en communicatieapparatuur

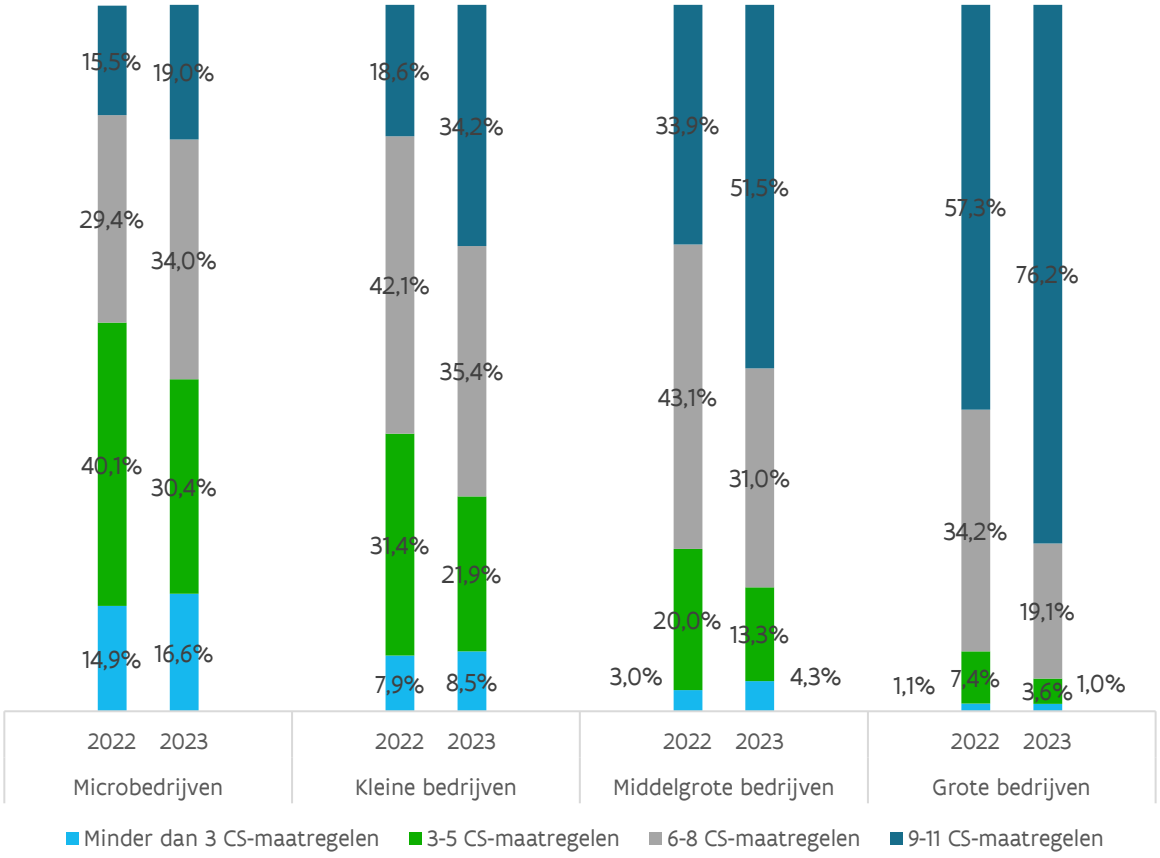
Figuur 18: Evolutie adoptiegraad aantal CS-maatregelen



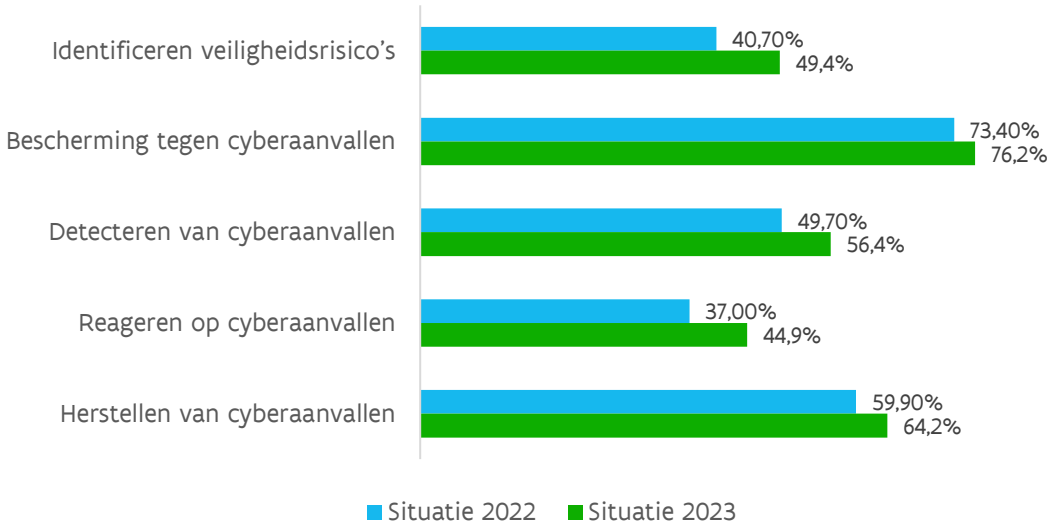
Figuur 19: Evolutie adoptiegraad CS-maatregelen volgens type



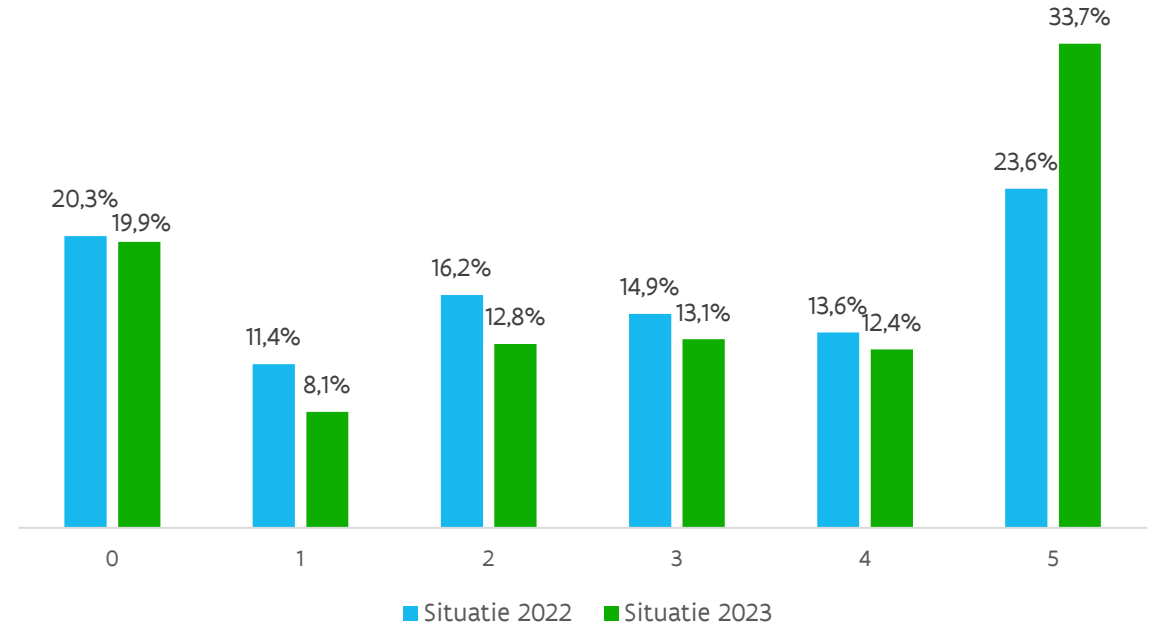
Figuur 20: Evolutie adoptiegraad aantal CS-maatregelen volgens bedrijfsgrootte



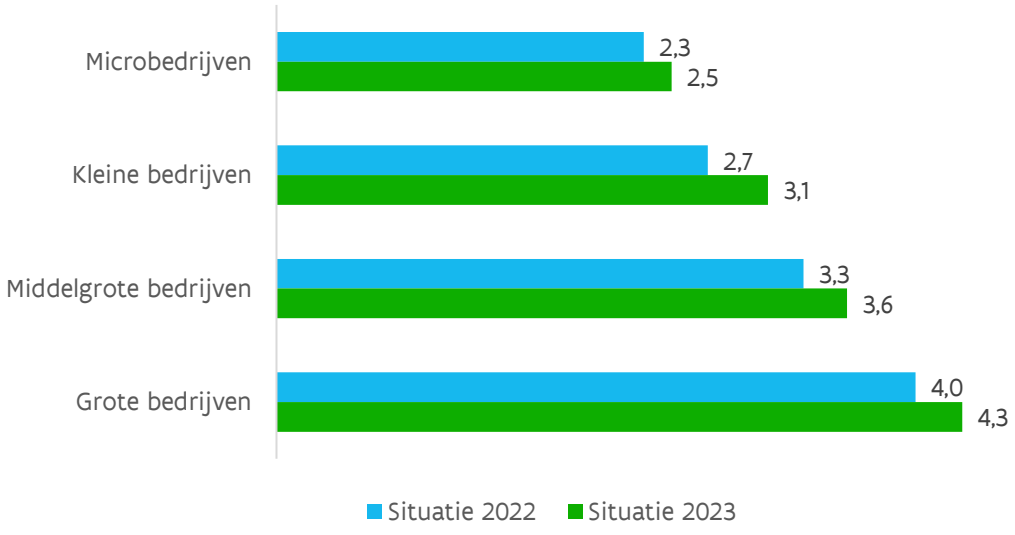
Figuur 21: Evolutie implementatie beheerprocedures volgens type



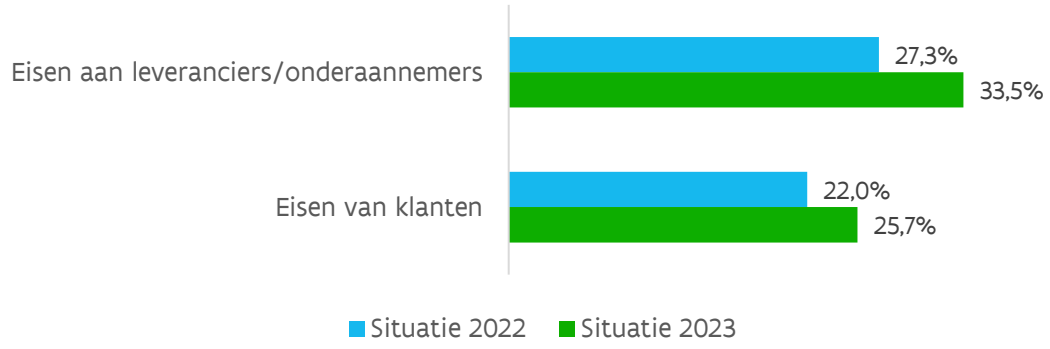
Figuur 22: Evolutie aantal beheerprocedures



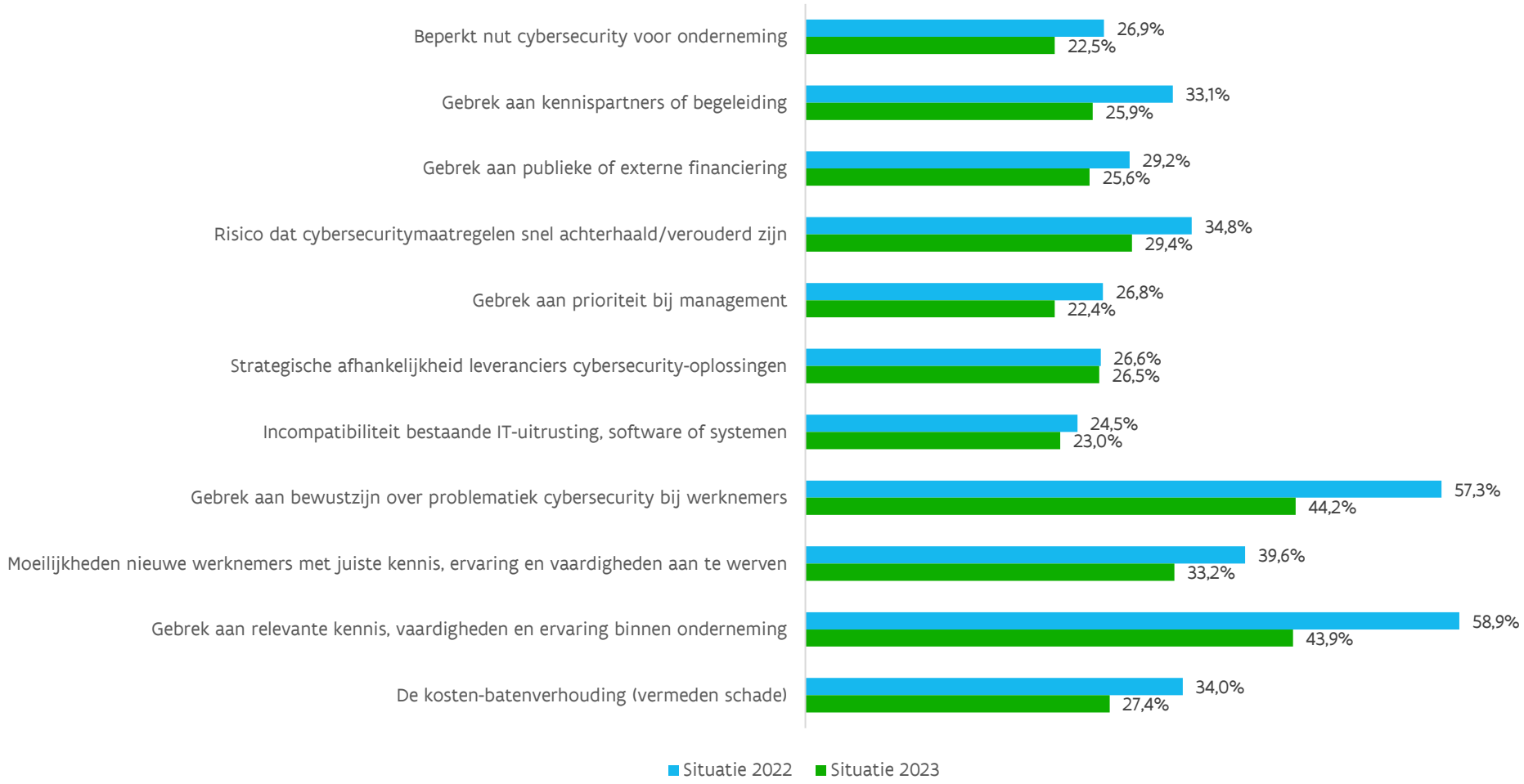
Figuur 23: Evolutie aantal beheerprocedures volgens bedrijfsgrootte



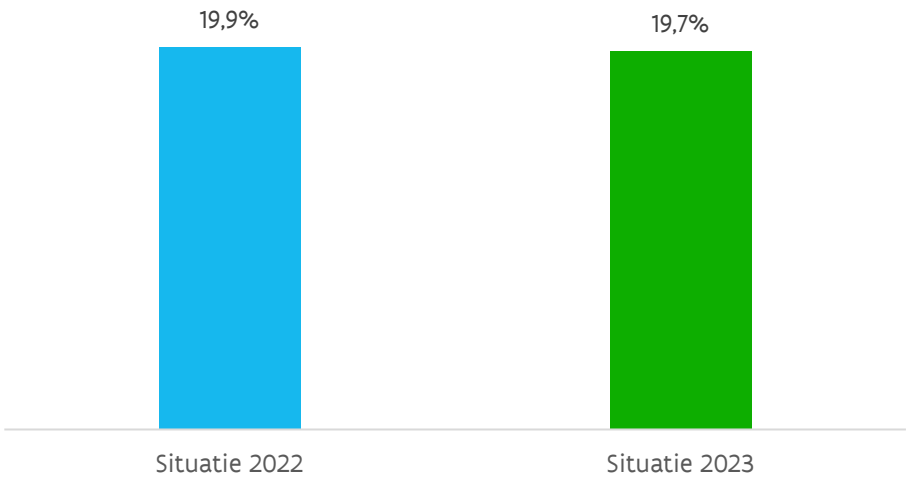
Figuur 24: Evolutie eisen inzake cybersecurity



Figuur 25: Evolutie aandeel bedrijven die minstens één CS-maatregel toepassen dat obstakels ondervond bij de invoer en het gebruik van CS-maatregelen

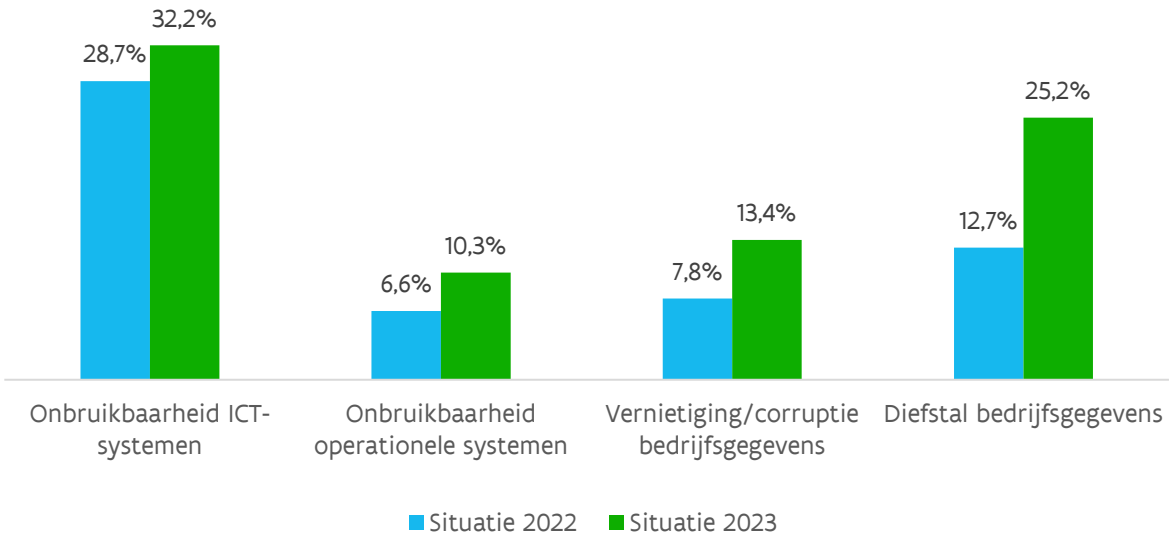


Figuur 26: Evolutie aandeel van het IT-budget gespendeerd aan cybersecurity

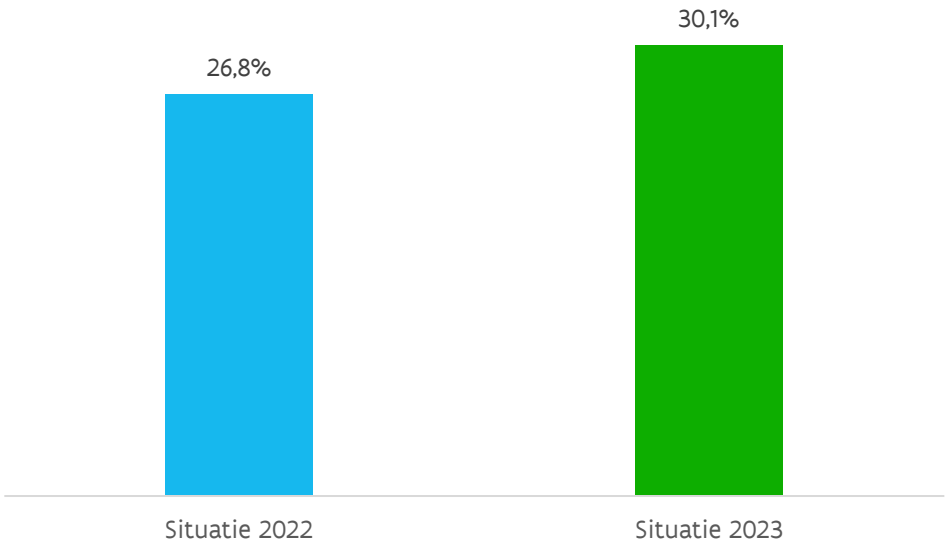


Figuur 27: Evolutie aandeel bedrijven dat het slachtoffer was van een cyberaanval

Figuur 28: Evolutie frequentie operationele gevolgen bij slachtoffers van een cyberaanval



Figuur 29: Evolutie aandeel bedrijven met een verzekering tegen cyberaanvallen



Vlaamse overheid
Departement Economie
Wetenschap en Innovatie
Koning Albert II-laan 35
1030 Brussel
info.ewi@vlaanderen.be

www.ewi-vlaanderen.be

Cyber Security Vlaanderen