Vlaanderen
verbeelding werkt

CS-Barometer

Maturiteit in cybersecurity bij Vlaamse bedrijven
situatie 2024

DEPARTEMENT
WERK, ECONOMIE
WETENSCHAP, INNOVATIE &
SOCIALE ECONOMIE

ecoom
EXPERTISECENTRUM O&O MONITORING

CS-Barometer

Maturiteit in cybersecurity

bij Vlaamse bedrijven

situatie 2024

Cyber Security Vlaanderen

COLOFON

CS-barometer - Maturiteit in cybersecurity bij Vlaamse bedrijven - situatie 2024 is een publicatie in opdracht van het Departement Werk, Economie, Wetenschap, Innovatie en Sociale Economie (WEWIS) van de Vlaamse overheid uitgevoerd door ECOOM-STORE, UGent.

Verantwoordelijke uitgever

Johan Hanssens, Secretaris-generaal
Departement Werk, Economie, Wetenschap, Innovatie & Sociale Economie
Koning Albert II-laan 15, bus 380
1210 BRUSSEL
02 553 42 56
info.wewis@vlaanderen.be
www.departementwewis.be

Auteurs

Thomas Standaert, Cathy Lecocq en Petra Andries (ECOOM-STORE, UGent)
Tom Evens (Research Group for Media, Innovation & Technology, UGent)

Uitgave

Februari 2025
D/2025/3241/075

Coverfoto © www.shutterstock.com

DEPARTEMENT
WERK, ECONOMIE
WETENSCHAP, INNOVATIE &
SOCIALE ECONOMIE

INHOUD

1 SAMENVATTING

In opdracht van het Departement Werk, Economie, Wetenschap, Innovatie en Sociale Economie (WEWIS) van de Vlaamse Overheid brengt deze CS-Barometer de maturiteit in cybersecurity (CS) bij Vlaamse bedrijven anno 2024 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 10.091 bedrijven, 2.720 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 de twee vorige jaren.[1]

[1] In de editie van vorig jaar werd gebruik gemaakt van een verkorte vragenlijst waardoor bepaalde onderwerpen niet aan bod kwamen. Bijgevolg kan voor deze onderwerpen enkel een vergelijking gemaakt worden met de editie van twee jaar geleden. Daarnaast werd in de huidige editie de vraag rond (kwaadwillige) cyberaanvallen herzien en werd een vraag rond ICT-beveiligingsincidenten geïntroduceerd. Voor deze vragen is geen vergelijking met vorige edities mogelijk.

De belangrijkste bevindingen van de studie zijn de volgende:

- In vergelijking met de metingen in 2022 en 2023 is de **adoptiegraad van minder geavanceerde technische maatregelen** (software-updates, data back-ups, protocol voor toegangsbeheer, paswoordauthenticatie, VPN-netwerk) **vrijwel onveranderd gebleven**. Dit wijst erop dat een niet te verwaarlozen groep bedrijven **ter plaatse trappelt** op het vlak van cyberveiligheid. Bij bedrijven met een zeker basisniveau van cyberveiligheid zit de adoptie van meer geavanceerde technische maatregelen (bijhouden van log files, periodieke ICT-veiligheidsanalyse, ICT-veiligheidstesten, en biometrische authenticatietechnieken) wel in de lift.
- **Slechts een kwart** (25,9%) van de Vlaamse bedrijven die minstens één CS-maatregel namen, heeft **alle vijf procedures van het NIST-kader** in zekere mate geïmplementeerd. Nochtans vallen de **kiemen van enkele positieve trends** te ontwaren. Ten eerste kent het aandeel bedrijven met vijf beheerprocedures een trage maar zekere groei. Ten tweede neemt het aandeel bedrijven zonder enige beheerprocedure af. Ten slotte neemt het aantal beheerprocedures bij de microbedrijven – weliswaar licht – toe.
- **Ongeveer een kwart** (23,4%) van de Vlaamse bedrijven die ten minste één CS-maatregel treffen beschikt over een **beleidsdocument of plan** waarin bedrijven een coherent geheel van acties en procedures inzake CS uitwerken. In vergelijking met de meting in 2022 is het gebruik van een beleidsdocument inzake CS **gestegen voor de micro-, kleine en middelgrote bedrijven**. De achterstand ten opzichte van grote bedrijven blijft echter groot.
- **Bijna driekwart** (71,4%) van de respondenten – een aandeel vergelijkbaar met dat van de meting in 2022 – is **helemaal akkoord of eerder akkoord** met de stelling dat hun onderneming **goed beschermd is tegen cyberaanvallen**. Gezien bij een aanzienlijk aandeel van de Vlaamse bedrijven nog steeds een basis aan beheerprocedures en technische maatregelen ontbreken wijst dit op een al te optimistische perceptie van cyberveiligheid.
- Net als bij de meting in 2022 vormt volgens **bijna de helft** (42,8%) van de respondenten **onvoldoende bewustwording bij medewerkers** het **grootste cyberrisico** voor hun onderneming. Dit aandeel ligt nog een stuk hoger bij de grote en middelgrote bedrijven. **Opleidingen of activiteiten voor medewerkers** kunnen dit risico verlagen, maar de adoptie ervan **ontbreekt nog steeds bij meer dan de helft van de bedrijven**. Daarnaast ziet een niet te verwaarlozen deel van de microbedrijven (14,2%) onvoldoende defensieve maatregelen als het grootste cyberrisico.
- **Minder dan een derde** (28,0%) van de Vlaamse bedrijven stelde het afgelopen jaar **eisen aan bepaalde of alle leveranciers of onderaannemers** inzake CS. **Eén op vier bedrijven** (24,9%) kreeg op zijn beurt **eisen opgelegd van bepaalde of alle klanten**. Deze aandelen liggen beduidend hoger bij grote en middelgrote bedrijven. In vergelijking met de meting in 2022 is vooral het aandeel bedrijven dat eisen opgelegd krijgt van klanten toegenomen. Dit kan deels de verhoogde inspanningen op het vlak van cyberveiligheid die we zien bij een deel van de Vlaamse ondernemingen verklaren.

- **Driekwart** (74,8%) van de bedrijven die minstens één CS-maatregel namen, doet beroep op **externe algemene IT-dienstverleners**, 47,7% doet (daarnaast) beroep op het **eigen personeel** en de minderheid (34,9%) schakelt (daarnaast) **externe gespecialiseerde CS-dienstverleners** in. In vergelijking met de meting in 2022 doet een groter aandeel bedrijven met CS-maatregelen beroep op externe gespecialiseerde CS-dienstverleners. Bij de grote bedrijven, die net zoals bij de meting in 2022 van alle grootteklassen het vaakst beroep doen op het eigen personeel, is de inzet van het eigen personeel voor CS-activiteiten gestegen.
- Bedrijven zien het **gebrek aan kennis, vaardigheden en bewustzijn bij werknemers 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. Grote bedrijven worstelen opmerkelijk vaker dan bedrijven in andere grootteklassen met **moeilijkheden om nieuwe werknemers met de juiste kennis, ervaring en vaardigheden aan te werven**. Deze vaststelling is waarschijnlijk gerelateerd aan het feit dat deze groep bedrijven over het algemeen verder staat op het vlak van CS én hiervoor vaker het eigen personeel inzet. 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**.
- In vergelijking met de meting in 2022 daalde het **aandeel bedrijven waar een CS-beleid weinig nut of prioriteit heeft**. Daartegenover staat **een stijging in de vrees dat CS-maatregelen snel achterhaald/verouderd zijn en bedrijven te afhankelijk worden van leveranciers**. Naarmate het belang van een effectief CS-beleid meer wordt erkend, en de adoptiegraad van meer geavanceerde technische maatregelen en beheerprocedures toeneemt, is het niet geheel onverwacht dat bedrijven met nieuwe obstakels worden geconfronteerd.
- **43,8% van de Vlaamse bedrijven liet een – lichte of sterke – stijging in de uitgaven voor CS noteren in het voorbije jaar**. Voor ongeveer de helft (53,8%) van de bedrijven bleef het budget ongewijzigd. Bij amper 2,4% van de bedrijven daalde het budget. In vergelijking met de metingen in 2022 en 2023 is het **gemiddelde aandeel van het CS-budget in het totale IT-budget (22,0%) gestegen**.
- **3,9% van de Vlaamse bedrijven** geeft aan het afgelopen jaar slachtoffer te zijn geweest van een **geslaagde cyberaanval**, waarbij de werking van computersystemen werd verstoord en/of de toegang tot bedrijfsgegevens werd verhinderd. Daarenboven kreeg **41,9% van de Vlaamse bedrijven** het afgelopen jaar te maken met **één of meerdere pogingen tot cyberaanvallen** waarbij gevolgen voor de werking van computersystemen en/of de toegang tot bedrijfsgegevens uitbleven. Bijna één derde (32,7%) van de Vlaamse bedrijven is verzekerd tegen cyberaanvallen – een stijging ten opzichte van de metingen in 2022 en 2023.
- Naast cyberaanvallen kunnen ook **ICT-beveiligingsincidenten** optreden waarbij **geen sprake is van kwaad opzet**. **Ongeveer één op vijf bedrijven** (19,6%) kreeg het afgelopen jaar te maken met *onbruikbaarheid van ICT-systemen als gevolg van defecten aan hardware of software*. Minder voorkomende veiligheidsincidenten zijn de

openbaarmaking van vertrouwelijke gegevens als gevolg van onopzettelijke handelingen van eigen werknemers (4,2%) en de *vernietiging of corruptie van gegevens als gevolg van defecten aan hardware of software* (2,9%). Grote bedrijven worden meer dan andere ondernemingen geconfronteerd met ICT-beveiligingsincidenten.

- **28,4% van de ondervraagden** zegt weet te hebben van het **Vlaams Actieplan Cybersecurity**, een verdubbeling ten opzichte van de meting in 2022.

2 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 Werk, Economie, Wetenschap, Innovatie en Sociale Economie (WEWIS) 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 vierde meting die sinds 2021 werd uitgevoerd. Toekomstige meetmomenten, waarvan de eerstvolgende gepland staat voor 2026, 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 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.

[2] Zie https://www.vlaio.be/nl/begeleiding-advies/digitalisering/cybersecurity/waarom-inzetten-op-cybersecurity/vlaams-beleidsplan-cybersecurity#:~:text=Met%20het%20Vlaams%20Beleidsplan%20Cybersecurity%20dat%20goedgekeurd%20werd,het%20een%20jaarlijkse%20investering%20van%20%E2%82%AC%2020%20miljoen

3 METHODOLOGIE

3.1 Meetinstrument

Bij de keuze van het meetinstrument werd, net als in de drie vorige edities, 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.

3.2 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 Tabel 3 in Appendix voor een overzicht van de geselecteerde sectoren). Ten opzichte van de vorige editie van de CS-Barometer (situatie 2023) 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- 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

[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).

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 vorige edities van de CS-Barometer 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 10.091 bedrijven, waarvan er initieel 9.401 per e-mail en 690 per brief gecontacteerd werden. De dataverzamelingsperiode liep van juni tot september 2024.

3.3 Respons en weging

Van de 9.401 bedrijven die we via e-mail contacteerden, konden we er 8.793 bereiken. 608 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 402 bedrijven werden bereikt. 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 3.371 bedrijven. Dit impliceert een responsgraad van 33,4% (3.371/10.091). Van deze antwoorden waren uiteindelijk 2.720 antwoorden bruikbaar (zie Tabel 2). 651 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) de verplichte

[8] Contactinformatie voor relevante contactpersonen tewerkgesteld in middelgrote of grote bedrijven is minder frequent beschikbaar in onze databronnen dan bij micro- of kleine 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.

vraag betreffende CS-maatregelen niet werd beantwoord. Bij de bruikbare antwoorden waren ontbrekende gegevens beperkt en werden deze 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	1.545	83	2.586	4.372	993	1.660	671	768	2.102	948	557	16.285
(5-9 werknemers)	*249*	*15*	*414*	*700*	*159*	*266*	*107*	*123*	*336*	*152*	*89*	*2.610*
Klein	2.458	168	2.372	4.605	1.469	946	870	472	1.775	1.052	783	16.970
(10-49 werknemers)	*396*	*30*	*383*	*736*	*236*	*151*	*139*	*75*	*282*	*168*	*125*	*2.721*
Middelgroot	825	48	337	721	332	66	199	84	325	417	606	3.960
(50-249 werknemers)	*806*	*46*	*330*	*661*	*325*	*61*	*191*	*79*	*308*	*388*	*550*	*3.745*
Groot	228	22	48	153	70	15	36	33	79	148	225	1.057
(>= 250 werknemers)	*222*	*22*	*47*	*140*	*66*	*14*	*34*	*33*	*76*	*142*	*219*	*1.015*
Totaal	**5.056**	**321**	**5.343**	**9.851**	**2.864**	**2.687**	**1.776**	**1.357**	**4.281**	**2.565**	**2.171**	**38.272**
	1.673	***113***	***1.174***	***2.237***	***786***	***492***	***471***	***310***	***1.002***	***850***	***983***	***10.091***

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)	50	6	83	132	29	37	39	23	87	26	21	533
Klein (10-49 werknemers)	102	9	80	187	58	22	49	21	82	40	40	690
Middelgroot (50-249 werknemers)	248	15	100	149	79	11	56	25	97	91	239	1.110
Groot (>= 250 werknemers)	69	6	17	39	16	5	10	11	30	54	130	387
Totaal	**469**	**36**	**280**	**507**	**182**	**75**	**154**	**80**	**296**	**211**	**430**	**2.720**

4 RESULTATEN

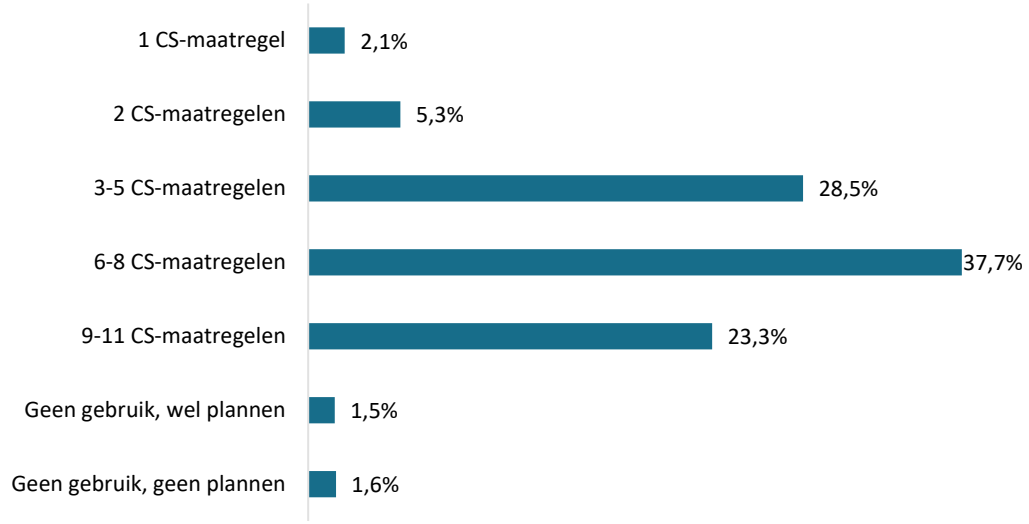
Cybersecurity (CS) verwijst naar het beschermen van computers, servers, netwerken, mobiele toestellen, software, elektronische systemen en data tegen schadelijke cyberaanvallen. Een cyberaanval is een kwaadwillige inbreuk op de veiligheidssystemen van een onderneming met als motief operationele of computersystemen 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.

4.1 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 7,4% van de bedrijven één of twee maatregelen te gebruiken. 28,5% van de bedrijven geeft aan drie tot vijf CS-maatregelen toe te passen. 37,7% past zes tot acht CS-maatregelen toe, terwijl bijna één op vier (23,3%) bedrijven negen of meer van de bevraagde CS-maatregelen toepast. In totaliteit past dus 96,9% van de Vlaamse bedrijven ten minste één CS-maatregel toe. Dit wijst erop dat slechts een kleine minderheid (3,1%) geen enkele CS-maatregel toepast in de dagelijkse werking. 1,6% van de bedrijven zegt geen plannen te hebben om één of meerdere CS-maatregelen te implementeren in het komende jaar; 1,5% heeft daartoe wel plannen.

Figuur 1 Adoptiegraad aantal CS-maatregelen (N=2.720)

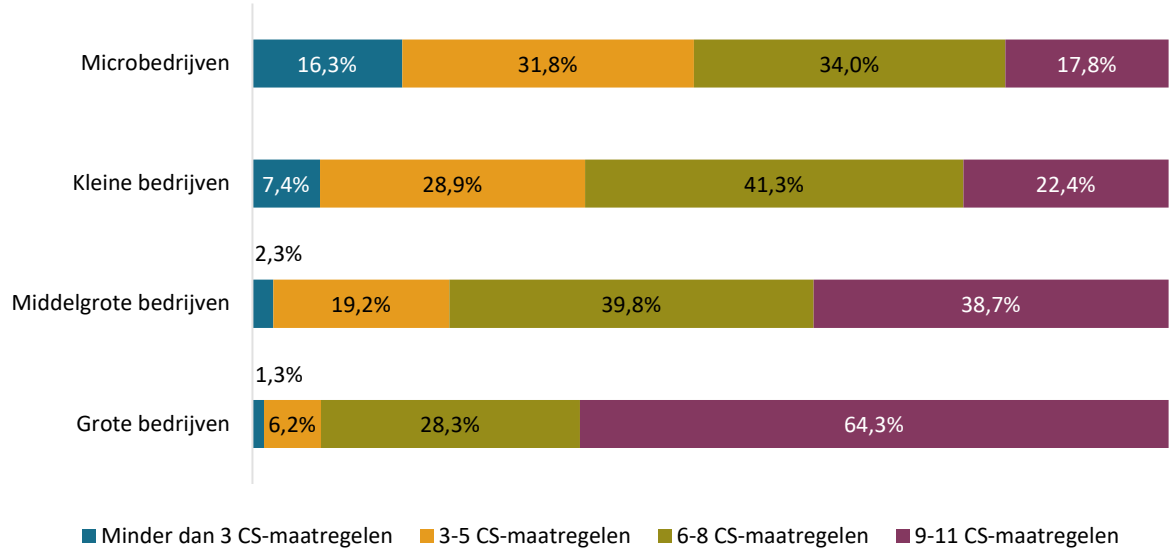


Figuur 25 in Appendix toont aan dat het aantal bedrijven met minstens één maatregel in vergelijking met de meting in 2022 vrijwel gelijk is gebleven. Binnen deze groep is het aandeel bedrijven met drie tot vijf maatregelen gedaald ten voordele van het aandeel bedrijven met 9 of meer maatregelen. Dit resultaat bevestigt de in de vorige editie vastgestelde trend van een toename in het aantal geïmplementeerde CS-maatregelen.[10]

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). 64,3% van de grote bedrijven past minstens negen van de vooropgestelde CS-maatregelen toe, een bijkomende 28,3% neemt zes tot acht CS-maatregelen. Bij de middelgrote bedrijven bedraagt het aandeel organisaties met negen of meer CS-maatregelen slechts 38,7%. Dit aandeel ligt nog lager bij kleine bedrijven (22,4%) en microbedrijven (17,8%). Van deze laatste geeft 16,3% 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.

[10] In vergelijking met de meting in 2023 (30,6%) ligt het aandeel bedrijven met 9 of meer maatregelen dit jaar lager. Een mogelijke verklaring hiervoor is *non-responsbias*, waarop ook bij de meting in 2023 werd gewezen. Vanaf de nulmeting in 2021 tot en met de meting in 2023 werden de bevragingen rond CS en AI gebundeld. In de oneven jaren kwamen de vragen rond AI vóór die rond CS in de vragenlijst, in de even jaren andersom. Dit kan bedrijven zonder interesse in AI hebben afgeschrikt om deel te nemen in de oneven jaren. 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. Indien 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 de editie van 2023 positief kunnen beïnvloed hebben. We kunnen bijgevolg verwachten dat een vergelijking van de resultaten van de huidige editie met de meting in 2022 meer betrouwbaar is. Vanaf de huidige editie werden de bevragingen rond CS en AI ontkoppeld. De bevraging rond CS zal in de even jaren uitgevoerd worden, de bevraging rond AI in de oneven jaren. Hierdoor zal het tijdsinterval tussen twee metingen toenemen, maar de betrouwbaarheid van de resultaten zal verbeteren.

Figuur 2 Adoptiegraad aantal CS-maatregelen volgens bedrijfsgrootte (N=2.720)

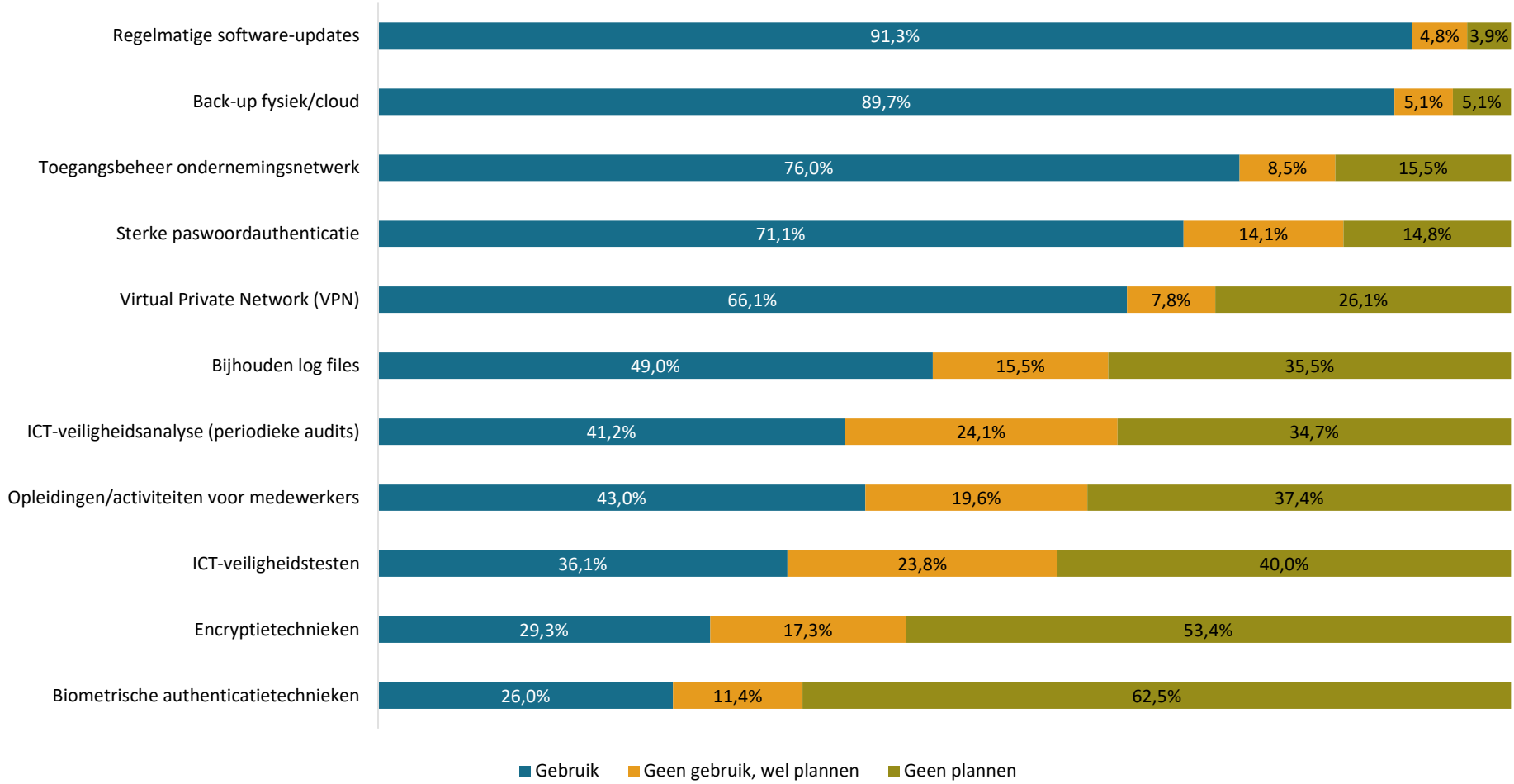


Bedrijven kunnen een breed spectrum aan technische maatregelen nemen om een hogere cyberveiligheid te bewerkstelligen. Deze maatregelen gaan van eerder basis (zoals paswoordauthenticatie of software-updates) tot vrij geavanceerd (bijvoorbeeld biometrische authenticatie of encryptietechnieken).[11] Al 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 (91,3%). Een bijna even vaak toegepaste maatregel is het maken van een data back-up naar een aparte locatie of in de cloud: 89,7% van de bedrijven geeft aan dit te doen. 76,0% heeft een protocol voor toegangsbeheer tot het ondernemingsnetwerk voor toestellen of gebruikers. Ook een sterke paswoordauthenticatie is met 71,1% stevig verankerd in de bedrijfswerking. Daarnaast beschikt ongeveer twee derde (66,1%) 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 (49,0%), periodieke ICT-veiligheidsanalyse (41,2%) of ICT-veiligheidstesten (36,1%). Een minderheid van 29,3% past encryptietechnieken toe op data, documenten en/of e-mails; 26,0% gebruikt biometrische technieken ter identificatie en authenticatie van gebruikers (vingerafdrukken, stem- en/of gezichtsherkenning). Daarnaast stellen we vast dat iets minder dan de helft (43,0%) van de Vlaamse bedrijven zijn werknemers opleidingen of activiteiten aanbiedt om hen bewust te maken van het belang van cybersecurity.[12]

[11] 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.

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

Figuur 3 Adoptiegraad type CS-maatregelen (N=2.720)



In vergelijking met de metingen in 2022 en 2023 is de adoptiegraad van minder geavanceerde technische maatregelen (software-updates, data back-ups, protocol voor toegangsbeheer, paswoordauthenticatie, VPN-netwerk) vrijwel onveranderd gebleven (zie Figuur 26 in Appendix). Voor meer geavanceerde technische maatregelen zoals het bijhouden van log files, periodieke ICT-veiligheidsanalyse, ICT-veiligheidstesten, en biometrische authenticatietechnieken ligt de adoptiegraad weliswaar lager dan bij de meting in 2023, maar hoger dan bij de meting in 2022. Dezelfde vaststelling wordt gemaakt voor opleidingen of activiteiten voor werknemers.[13] Deze resultaten suggereren dat de adoptiegraad van geavanceerde technische maatregelen in de lift zit bij een groep bedrijven met een zeker basisniveau van cyberveiligheid. Daartegenover trappelt een niet te verwaarlozen groep bedrijven ter plaatse op het vlak van cyberveiligheid.

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 groot aantal 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.

4.2 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.

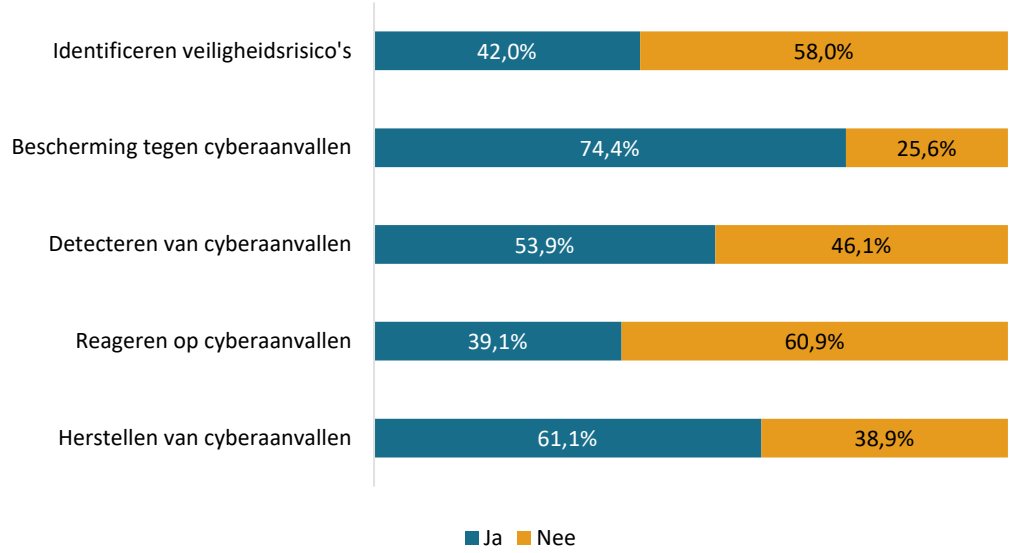
Het NIST-kader, dat onder meer aan de basis ligt van het CyberFundamentals Framework ontwikkeld door het Centrum voor Cybersecurity België (CCB), biedt een reeks van standaarden, richtlijnen en procedures voor bedrijven om cyberveiligheid te beheren en mogelijke risico's te beperken[14]. NIST bestaat 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

[13] De hogere adoptiegraad voor meer geavanceerde technische maatregelen en opleidingen of activiteiten voor werknemers in 2023 is naar alle waarschijnlijkheid gelinkt aan de mogelijke *non-responsbias* besproken in voetnoot 10.
[14] Voor meer informatie, zie https://www.nist.gov/cyberframework

vijf elementen: doorgaans geldt dat de CS-maturiteit van een bedrijf toeneemt naarmate er meer procedures worden geïmplementeerd. Echter, het aantal beheerprocedures op zich is geen garantie voor cyberveiligheid. De effectiviteit van een specifieke procedure is immers afhankelijk van de manier waarop deze geïmplementeerd wordt.

Ten eerste claimt 42,0% van de bedrijven die ten minste één CS-maatregel treffen (i.e. 96,9% 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 74,4% procedures te hebben om zich effectief te beschermen tegen cyberaanvallen, bijvoorbeeld via toegangsbeheer, identificatiemanagement, back-ups, encryptie of regelmatige software-updates. Ten derde heeft 53,9% 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 39,1% van deze bedrijven procedures te hebben om adequaat op cyberaanvallen te reageren, bijvoorbeeld aan de hand van incidentanalyses, dreigingseliminatie en/of crisiscommunicatie. Tot slot heeft 61,1% 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 27 in Appendix).

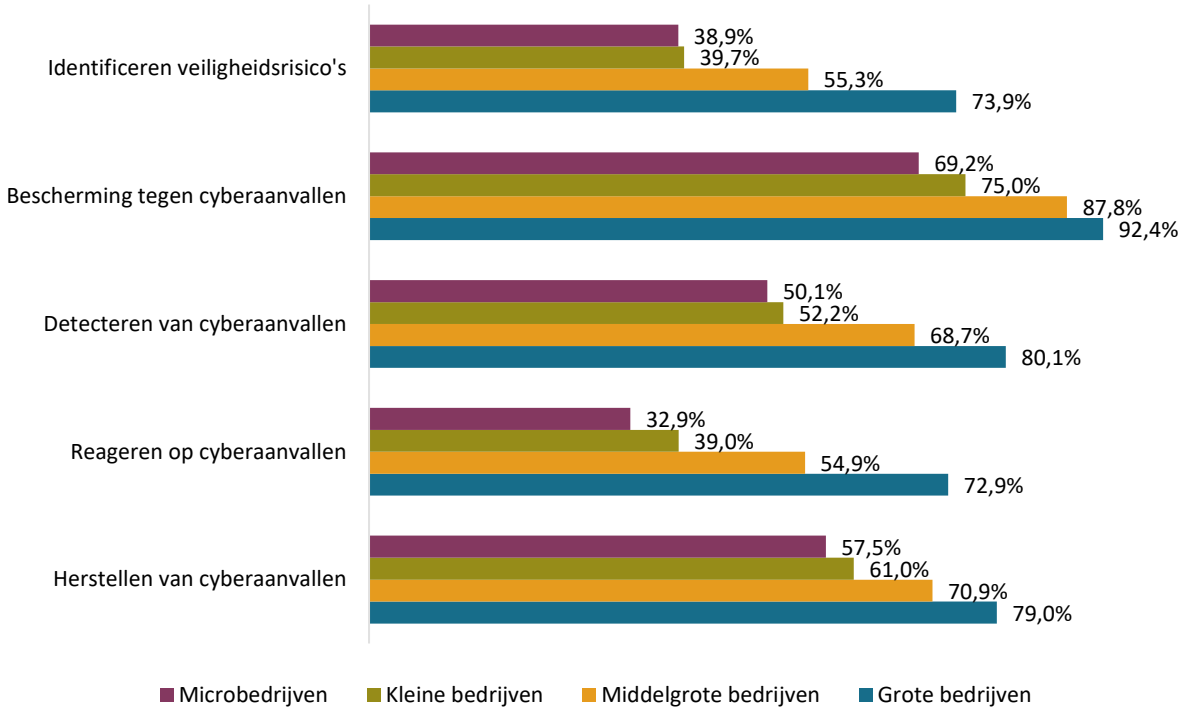
Figuur 4 Type beheerprocedures (N=2.675) – Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen



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 73,9% van de grote bedrijven die minstens één CS-maatregel namen ook effectief procedures om

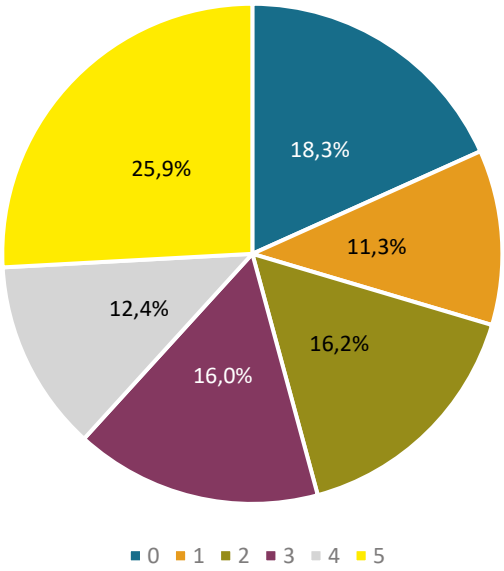
veiligheidsrisico's te identificeren terwijl dit bij kleine en microbedrijven respectievelijk 39,7% en 38,9% is. 92,4% van de grote bedrijven die minstens één CS-maatregel namen heeft procedures om zich te beschermen tegen cyberaanvallen, wat significant hoger is dan bij microbedrijven (69,2%). Procedures om cyberaanvallen te detecteren zijn sterker ingeburgerd bij grote bedrijven (80,1%) dan bij kleine (52,2%) en microbedrijven (50,1%). Deze trend is eveneens waarneembaar inzake procedures om te reageren op cyberaanvallen: 72,9% van de grote bedrijven die minstens één CS-maatregel namen heeft dergelijke procedures; dit is significant hoger dan bij middelgrote bedrijven (54,9%), kleine bedrijven (39,0%) en microbedrijven (32,9%). Tot slot kent 79,0% van de grote bedrijven die minstens één CS-maatregel namen procedures om van cyberaanvallen te herstellen terwijl dit bij microbedrijven beperkt blijft tot 57,5%.

Figuur 5 Type beheerprocedures volgens bedrijfsgrootte (N=2.675) – Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen



Slechts een kwart (25,9%) 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 58,7% van de grote bedrijven met CS-maatregelen en 37,7% van de middelgrote bedrijven met CS-maatregelen alle vijf procedures van het NIST-kader toepast, is dit slechts voor 23,5% van de kleine bedrijven en 23,1% van de microbedrijven met CS-maatregelen het geval. Net zoals bij de metingen in 2022 en 2023 noteren de sectoren informatie en communicatie en financiële activiteiten en verzekeringen de hoogste scores op dit gebied, met aandelen van respectievelijk 45,1% en 37,7%. 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.

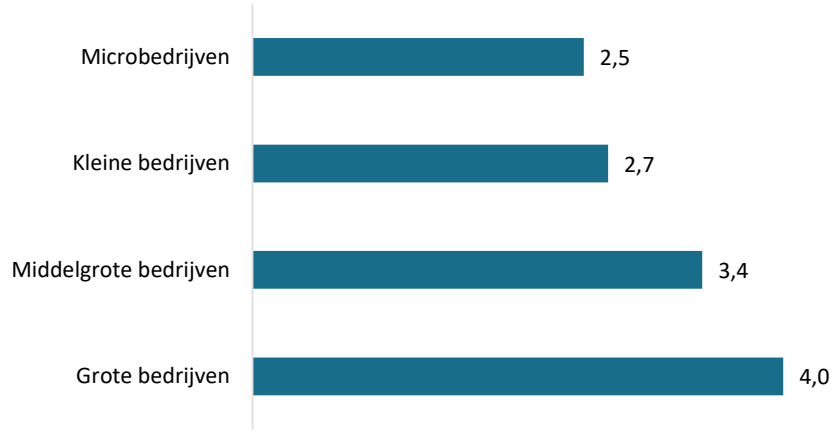
Figuur 6 Aantal beheerprocedures (N=2.675) – Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen



Omgekeerd heeft maar liefst 18,3% 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 gebrek aan bescherming geldt vooral voor microbedrijven en kleine bedrijven (respectievelijk 21,7% en 18,5% zonder enige maatregel). Slechts 7,3% van de middelgrote en 5,7% van de grote bedrijven valt hieronder. Consistent met de metingen in 2022 en 2023 vertonen bedrijven actief in accommodatie en maaltijden en de bouwnijverheid minimale CS-maturiteit; respectievelijk 41,4% en 23,6% van de bedrijven actief in die sector en met minstens één CS-maatregel heeft geen enkele beheerprocedure. In vergelijking met de metingen in 2022 en 2023 is bij de bedrijven die minstens één CS-maatregel namen het aandeel bedrijven zonder enige beheerprocedure afgenomen (zie Figuur 28 in Appendix). Zoals ook bij de meting in 2023 werd vastgesteld vertoont het aandeel bedrijven met vijf beheerprocedures de sterkste groei. Dit wijst op een aanhoudende uitbreiding van het aantal ingevoerde beheerprocedures.

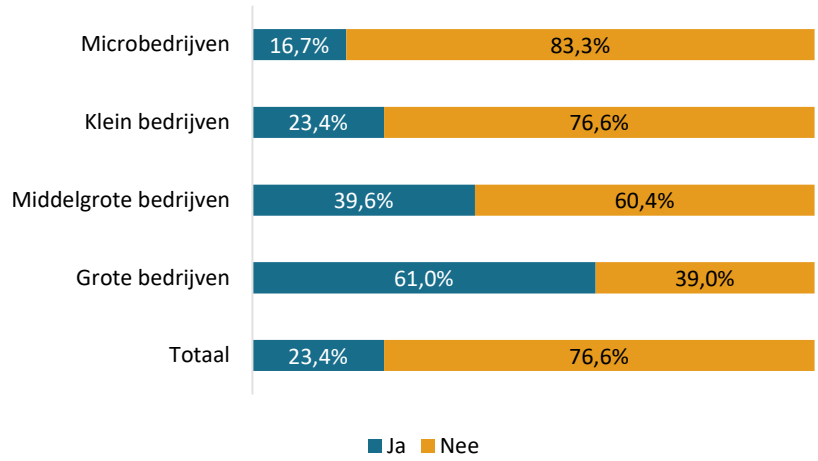
Het belang van bedrijfsgrootte met betrekking tot CS-maturiteit blijkt opnieuw duidelijk uit het gemiddeld aantal beheerprocedures dat bedrijven met CS-maatregelen uit verschillende grootteklassen installeren: microbedrijven hebben gemiddeld 2,5 procedures, kleine bedrijven 2,7, middelgrote bedrijven 3,4 en grote bedrijven 4,0 (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 enkel voor de microbedrijven het aantal beheerprocedures licht gestegen (zie Figuur 29 in Appendix).

Figuur 7 Aantal beheerprocedures volgens bedrijfsgrootte (N=2.675) – 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 (23,4%) van de bedrijven die ten minste één CS-maatregel treffen beschikt over een beleidsdocument inzake cybersecurity (zie Figuur 8). Dit aandeel ligt opnieuw significant hoger bij grote bedrijven (61,0%) dan bij bedrijven in andere grootteklassen. 48,1% van de bedrijven actief in informatie en communicatie en 39,3% van de bedrijven actief in financiële activiteiten en verzekeringen die minstens één CS-maatregel namen heeft effectief een beleidsplan, in tegenstelling tot 14,8% van de bedrijven met CS-maatregelen in accommodatie en maaltijden en 12,5% van de bedrijven met CS-maatregelen in de bouwnijverheid. In vergelijking met de meting in 2022 is het gebruik van een beleidsdocument inzake cybersecurity gestegen voor de micro-, kleine en middelgrote bedrijven (zie Figuur 30 in Appendix). De achterstand ten opzichte van grote bedrijven blijft echter groot.

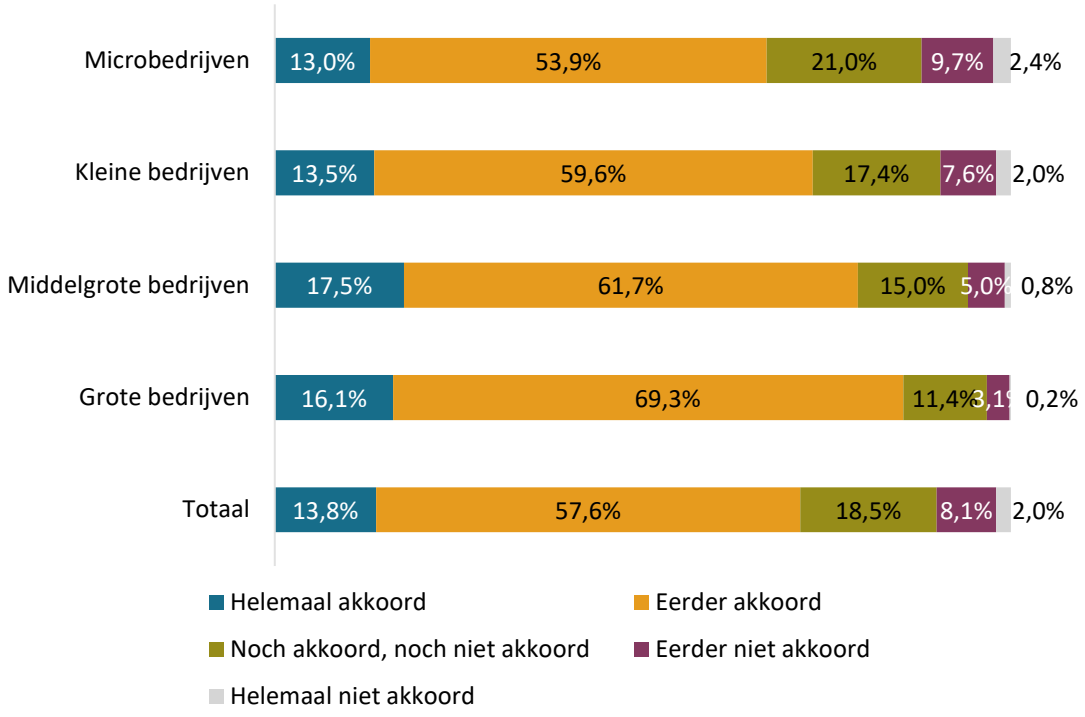
Figuur 8 Plan/beleidsdocument inzake cybersecurity volgens bedrijfsgrootte (N=2.675) – Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen



4.3 Perceptie bescherming en risico's

Technische maatregelen en beheerprocedures zijn objectieve indicatoren aan de hand waarvan de maturiteit van bedrijven inzake cybersecurity kan gemeten worden. Bij wijze van alternatief kunnen percepties van respondenten over de mate van bescherming van hun onderneming tegen cyberaanvallen gebruikt worden om een subjectieve maatstaf van maturiteit te kwantificeren. Wanneer objectieve en subjectieve maatstaven niet met elkaar overeenkomen, duidt dit op de aanwezigheid van mispercepties. Bijna driekwart (71,4%) van de respondenten is helemaal akkoord of eerder akkoord met de stelling dat hun onderneming goed beschermd is tegen cyberaanvallen (zie Figuur 9). Dit aandeel is vergelijkbaar met dat van de meting in 2022 (71,8%) en geeft aan dat Vlaamse ondernemingen nog steeds te optimistisch zijn over hun cyberveiligheid.

Figuur 9 Mate waarin respondent akkoord gaat met de stelling "Onze onderneming is goed beschermd tegen cyberaanvallen" volgens bedrijfsgrootte (N=2.720)



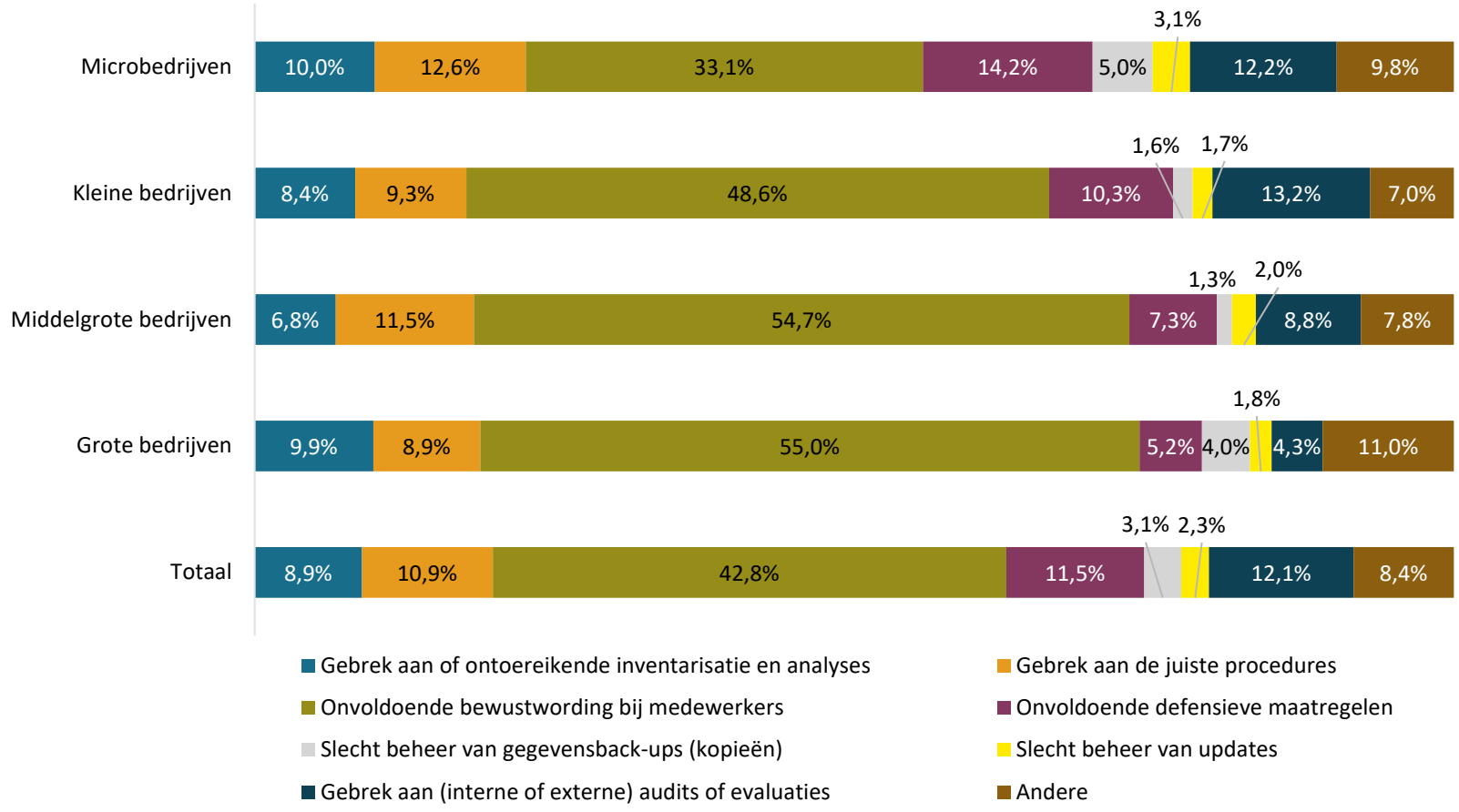
Het aandeel bedrijven waarvoor de respondent helemaal akkoord of eerder akkoord is met de stelling is hoger bij grote (85,4%) en middelgrote (79,2%) bedrijven dan bij kleine (73,1%) en microbedrijven (66,8%). Meer dan 90% van de bedrijven actief in financiële activiteiten en verzekeringen is helemaal of eerder akkoord met de stelling, in tegenstelling tot minder dan de helft (43,2%) van de bedrijven in accommodatie en maaltijden.

Ook werd respondenten gevraagd naar wat volgens hen het grootste cyberrisico voor hun onderneming vormt. Volgens bijna de helft (42,8%) van de respondenten vormt onvoldoende bewustwording bij medewerkers het grootste cyberrisico voor hun onderneming (zie Figuur 10). Een gelijkaardig aandeel (44,1%) werd vastgesteld bij de meting in 2022. Op geruime afstand volgen andere mogelijke cyberrisico's: gebrek aan (interne of externe) audits of evaluaties (12,1%), onvoldoende defensieve maatregelen (11,5%), gebrek aan de juiste procedures (10,9%), gebrek aan of ontoereikende inventarisatie en analyses (8,9%), slecht beheer van gegevensback-ups (3,1%), en slecht beheer van updates (2,3%).[15]

Onvoldoende bewustwording bij medewerkers wordt bij een groter aandeel van de grote (55,0%) en middelgrote (54,7%) bedrijven en bedrijven actief in administratieve en ondersteunende diensten (54,6%) beschouwd als het grootste risico, in vergelijking met microbedrijven (33,1%) en bedrijven actief in de nutssector (22,9%). Microbedrijven (14,2%) en bedrijven actief in de nutssector (25,7%) en accommodatie en maaltijden (25,2%) zien in grotere getale onvoldoende defensieve maatregelen als het grootste cyberrisico. Gebrek aan (interne of externe) audits wordt dan weer bij een groter aandeel van de kleine bedrijven (13,2%) en bedrijven actief in informatie en communicatie (19,6%) en onroerend goed, vrije beroepen en wetenschappelijke en technische activiteiten (17,7%) als grootste cyberrisico beschouwd.

[15] Zoals eerder aangegeven, varieert de effectiviteit van de geïmplementeerde maatregelen en procedures. Slecht beheer van gegevensback-ups en updates vormt een (bijna) even groot cyberrisico als het volledig ontbreken van deze basismaatregelen.

Figuur 10 Grootste cyberrisico volgens bedrijfsgrootte (N=2.420)

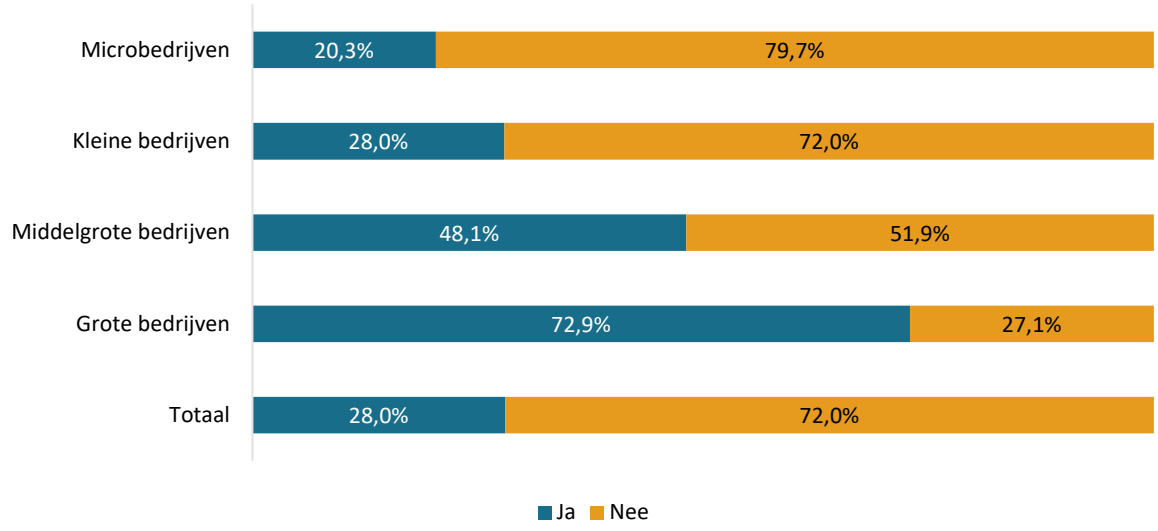


4.4 Druk op en vanuit de waardeketen

Als gevolg van de toenemende automatisering en de 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. Toch zien we dat minder dan een derde (28,0%) van de bedrijven in Vlaanderen het afgelopen jaar eisen stelde aan bepaalde of alle leveranciers of onderaannemers inzake cybersecurity (zie Figuur 11).

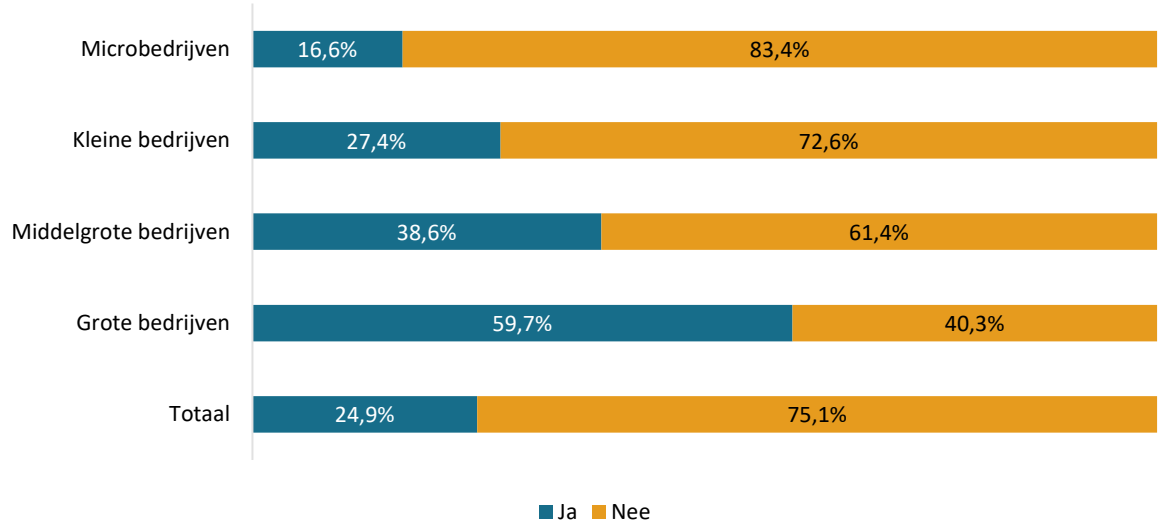
Dit aandeel ligt wel een pak hoger bij grote (72,9%) en middelgrote (48,1%) bedrijven dan bij kleinere ondernemingen. Terwijl bijna de helft van de bedrijven actief in informatie en communicatie en financiële activiteiten en verzekeringen eisen oplegt aan leveranciers of onderaannemers, is dit slechts het geval voor 17,5% van de bedrijven actief in de bouwnijverheid en 9,7% van de bedrijven actief in accommodatie en maaltijden.

Figuur 11 Eisen aan leveranciers/onderaannemers inzake cybersecurity volgens bedrijfsgrootte (N=2.720)



Eén op vier bedrijven (24,9%) kreeg op zijn beurt eisen opgelegd van bepaalde of alle klanten (zie Figuur 12). Opnieuw ligt dit aandeel beduidend hoger bij grote (59,7%) en middelgrote (38,6%) bedrijven. Maar liefst 76,4% van de bedrijven in informatie en communicatie kreeg eisen opgelegd van klanten.

Figuur 12 Eisen van klanten inzake cybersecurity volgens bedrijfsgrootte (N=2.720)



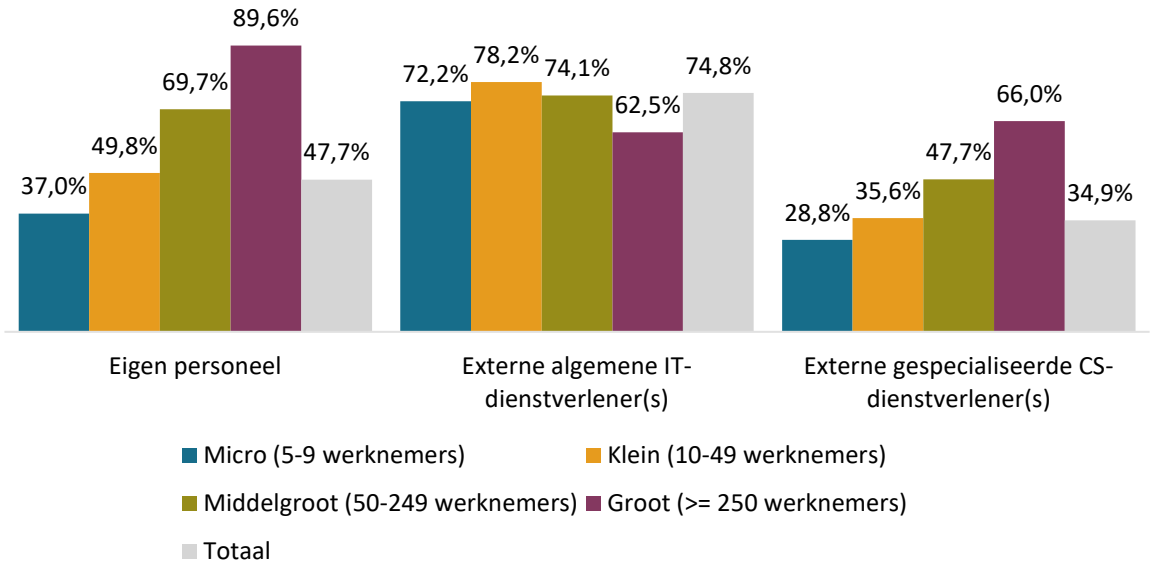
In vergelijking met de meting in 2022 is het aandeel bedrijven dat druk uitoefent op zijn leveranciers licht gestegen (zie Figuur 31 in Appendix). De stijging in het aandeel bedrijven dat eisen opgelegd krijgt van klanten is meer uitgesproken. Dit resultaat wijst op een toename in het bewustzijn omtrent het belang van cybersecurity bij klanten.

4.5 Uitvoering

Zowel het eigen personeel als externe dienstverleners kunnen instaan voor de cybersecurityactiviteiten van bedrijven. Driekwart (74,8%) van de bedrijven die minstens één CS-maatregel namen, doet beroep op externe algemene IT-dienstverleners, 47,7% doet (daarnaast) beroep op het eigen personeel en de minderheid (34,9%) schakelt (daarnaast) externe gespecialiseerde CS-dienstverleners in (zie Figuur 13). Grote bedrijven en middelgrote bedrijven met CS-maatregelen maken vaker gebruik van het eigen personeel (respectievelijk 89,6% en 69,7%) dan bedrijven in andere grootteklassen, terwijl ongeveer twee derde (66,0%) van de grote bedrijven met minstens één CS-maatregel aanklopt bij externe gespecialiseerde CS-dienstverleners. Een hoger aandeel (57,1%) bedrijven actief in financiële activiteiten en verzekeringen doet voor hun CS-activiteiten beroep op externe gespecialiseerde CS-dienstverleners, in tegenstelling tot bedrijven actief in menselijke gezondheidszorg en maatschappelijke dienstverlening en accommodatie en maaltijden (respectievelijk 23,4% en 20,1%). De overgrote meerderheid (89,6%) van de bedrijven actief in informatie en communicatie schakelt het eigen personeel in, terwijl slechts 35,8% gebruikt maakt van algemene IT-dienstverleners.

In vergelijking met de meting in 2022 doet een groter aandeel bedrijven met CS-maatregelen beroep op externe gespecialiseerde CS-dienstverleners (zie Figuur 32 in Appendix).

Figuur 13 Uitvoering ICT-beveiligingsgerelateerde activiteiten volgens bedrijfsgrootte (N=2.675) – Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen



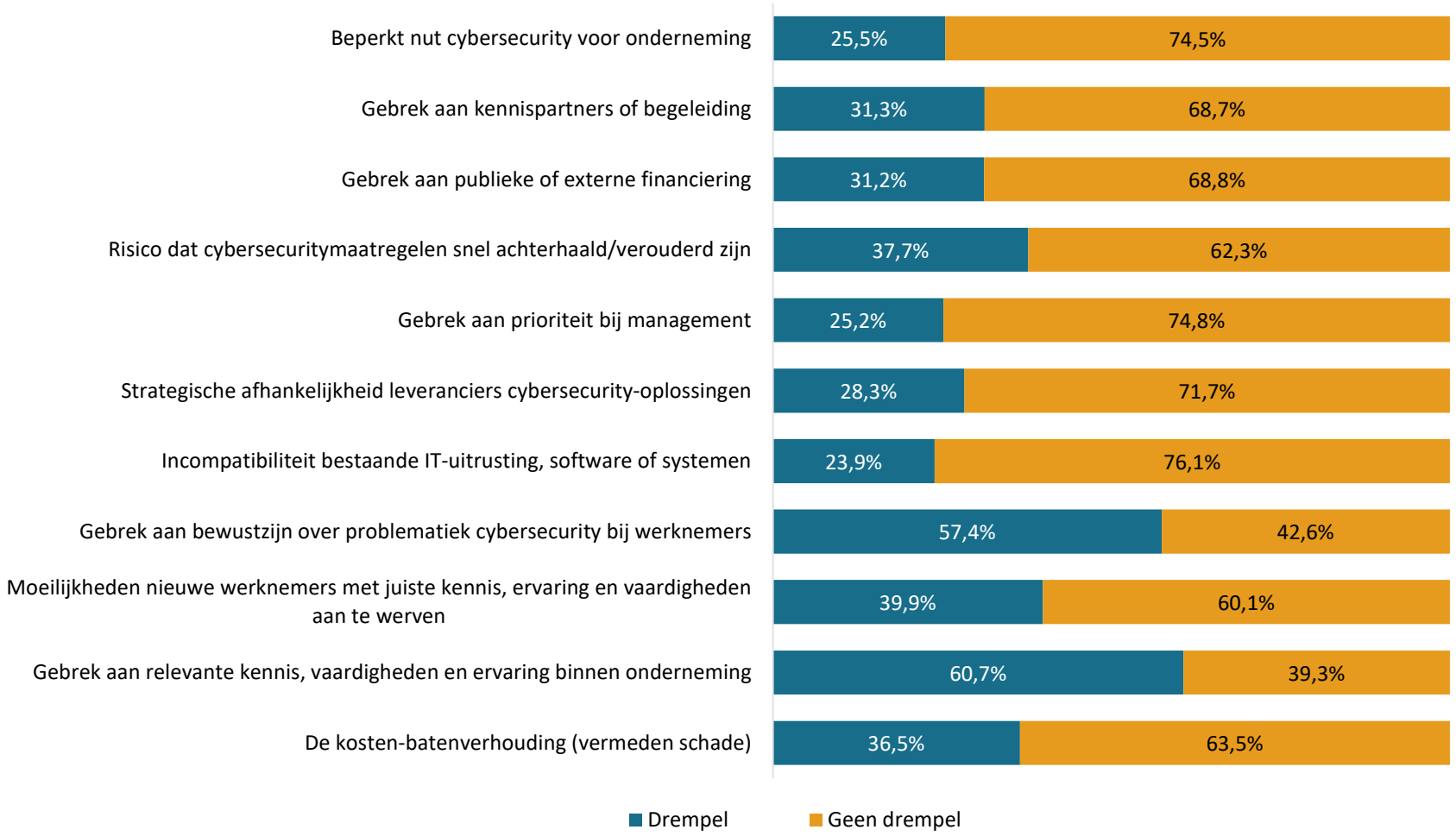
4.6 Obstakels

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 14 toont welke obstakels bedrijven voornamelijk ondervinden. 60,7% 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; 39,9% ondervindt bovendien moeilijkheden om nieuwe werknemers met deze kennis, vaardigheden en ervaring aan te werven. Behalve kennis en vaardigheden erkent 57,4% van de bedrijven die CS-maatregelen namen ook een gebrek aan bewustzijn omtrent cybersecurity bij de werknemers. Daarnaast ziet 31,3% 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 vier op tien (37,7%) 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 een gelijkaardig aandeel (36,5%) wegen de kosten van een adequaat CS-beleid zwaarder dan de baten (i.e., vermeden schade). 31,2% van de bedrijven 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 25,5% en 25,2% van de ondernemingen die minstens één CS-maatregel toepassen.

Figuur 14 Obstakels bij de invoer en het gebruik van CS-maatregelen voor bedrijven die minstens één CS-maatregel toepassen (N=2.675)



Op basis van de vergelijking met de meting in 2022 zijn enkele trends waar te nemen in de mate waarin Vlaamse bedrijven obstakels ondervinden bij de invoer en het gebruik van CS-maatregelen (zie Figuur 33 in Appendix). Zo is het aandeel bedrijven waarvoor een CS-beleid weinig nut of prioriteit toegekend krijgt gedaald. Daartegenover staat een stijging in de vrees dat CS-maatregelen snel achterhaald/verouderd zijn en bedrijven te afhankelijk worden van leveranciers. Naarmate het belang van een effectief CS-beleid meer wordt erkend, en de adoptiegraad van meer geavanceerde technische maatregelen en beheerprocedures toeneemt, is het niet geheel onverwacht dat bedrijven met nieuwe obstakels worden geconfronteerd.

Omdat slechts 45 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 = 726) en een hoge adoptiegraad van CS-maatregelen (meer dan vijf genomen CS-maatregelen) (N = 1.949) met elkaar vergeleken. Figuur 15 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.

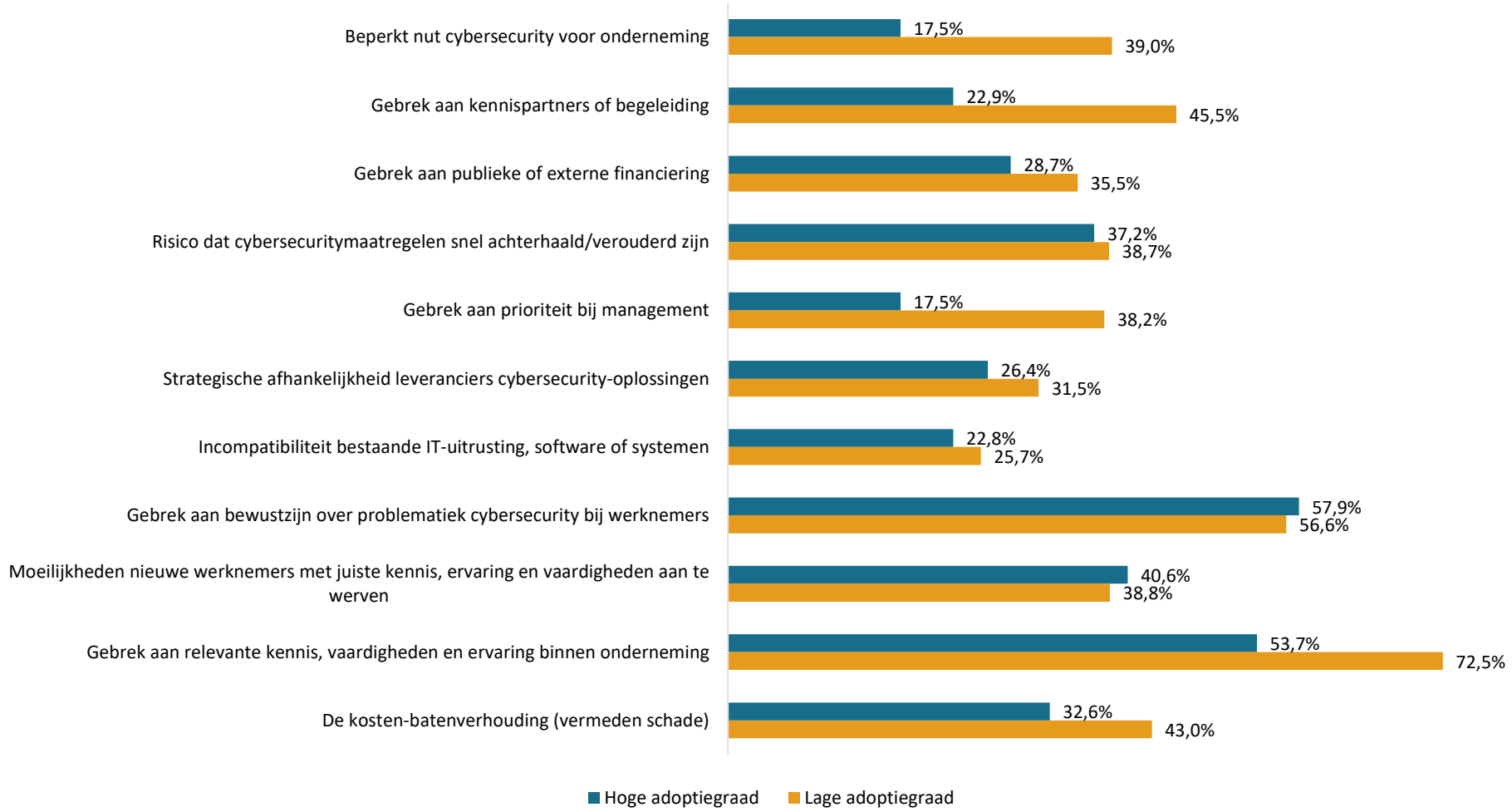
Bedrijven met een lage adoptiegraad worstelen vaker met een gebrek aan kennis, vaardigheden en ervaring binnen de organisatie (72,5%) dan bedrijven met een hoge adoptiegraad. Bedrijven met een lage adoptiegraad ervaren ook een sterker gebrek aan kennispartners of begeleiding (45,5%) en publieke of externe financiering (35,5%) dan bedrijven met een hoge adoptiegraad. Eveneens observeren we bij bedrijven met een lage adoptiegraad vaker een laag ingeschat nut (39,0%) en gebrek aan prioriteit bij het management (38,2%) in vergelijking met bedrijven met een hoge adoptiegraad.

Een aanzienlijk aandeel van de bedrijven met een lage (56,6%) of hoge adoptiegraad (57,9%) 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.

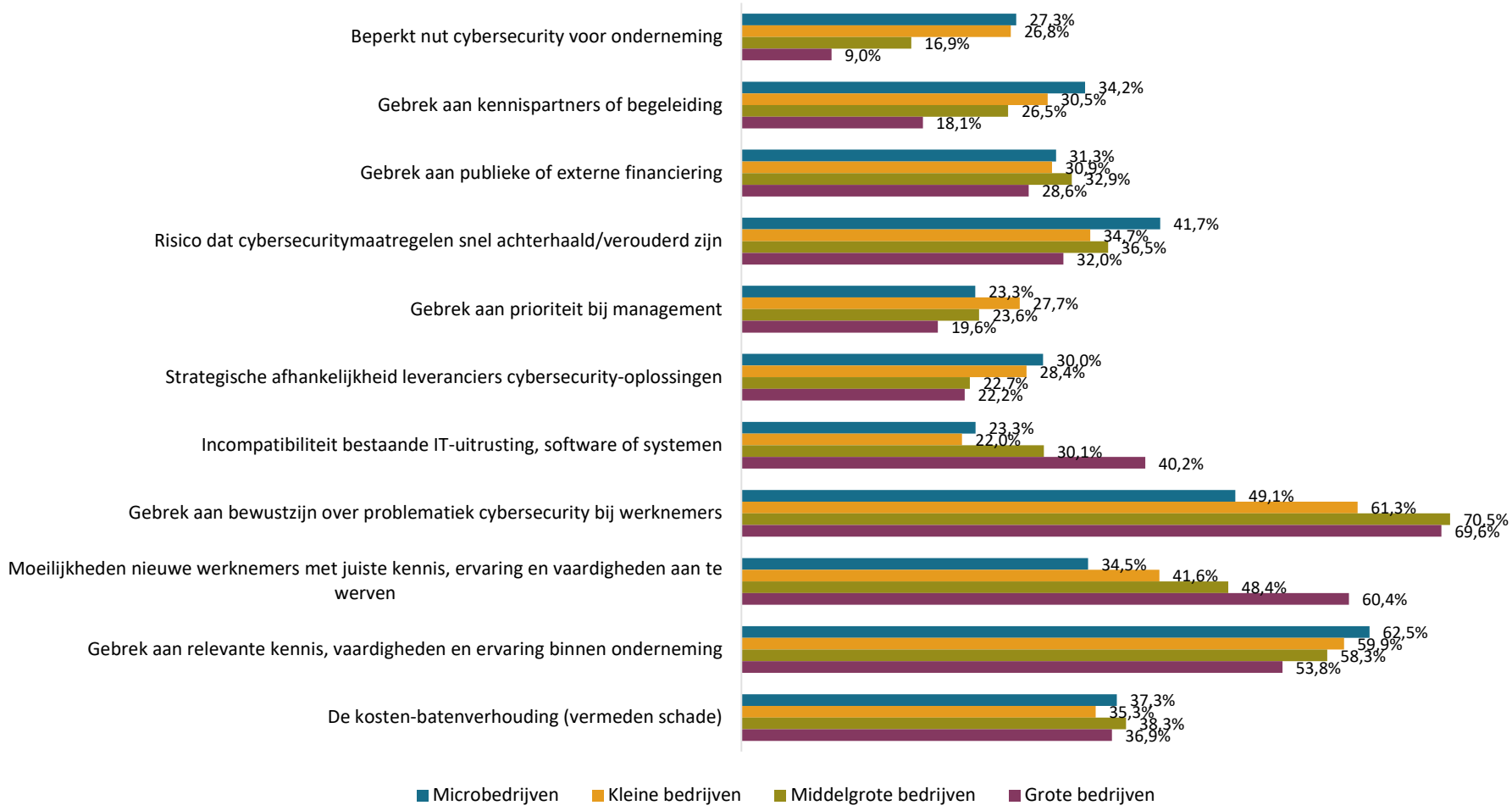
Figuur 16 geeft weer hoe deze obstakels verschillen naargelang de grootteklasse van de onderneming. Voor meer dan de helft van de bedrijven in alle grootteklassen vormt een gebrek aan bewustzijn bij werknemers een belangrijk obstakel bij de invoer en het gebruik van CS-maatregelen. Grote bedrijven worstelen daarnaast opmerkelijk vaker dan bedrijven in andere grootteklassen met moeilijkheden om nieuwe werknemers met de juiste kennis, ervaring en vaardigheden aan te werven (60,4%). Deze vaststelling is waarschijnlijk gerelateerd aan het feit dat deze groep bedrijven over het algemeen verder staat op het vlak van CS én hiervoor vaker het eigen personeel inzet. Microbedrijven kampen op hun beurt aanzienlijk vaker dan bedrijven in andere grootteklassen met een gebrek aan relevante kennis, vaardigheden en ervaring binnen de onderneming (62,5%) en een gebrek aan kennispartners of begeleiding (34,2%).

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 minder vaak obstakels vergeleken met bedrijven uit andere sectoren. Sterke reglementering zorgt er waarschijnlijk voor dat bedrijven actief in deze sector een meer matuur CS-beleid hebben, waardoor obstakels worden vermeden. Bedrijven actief in menselijke gezondheidszorg en maatschappelijke dienstverlening en accommodatie en maaltijden ervaren dan weer vaker obstakels vergeleken met bedrijven uit andere sectoren; bedrijven uit deze twee sectoren wijzen voornamelijk vaker op een gebrek aan kennispartners, een lage prioriteit bij het management en een ongunstige kosten-batenverhouding van het CS-beleid. Bedrijven in administratieve en ondersteunende diensten maken zich op hun beurt in grotere getale zorgen om technisch-strategische aspecten (risico dat CS-maatregelen snel achterhaald/verouderd zijn en strategische afhankelijkheid van leveranciers).

Figuur 15 Obstakels bij de invoer en het gebruik van CS-maatregelen volgens adoptiegraad voor bedrijven die minstens één CS-maatregel toepassen (N=2.675)



Figuur 16 Obstakels bij de invoer en het gebruik van CS-maatregelen volgens bedrijfsgrootte voor bedrijven die minstens één CS-maatregel toepassen (N=2.675)

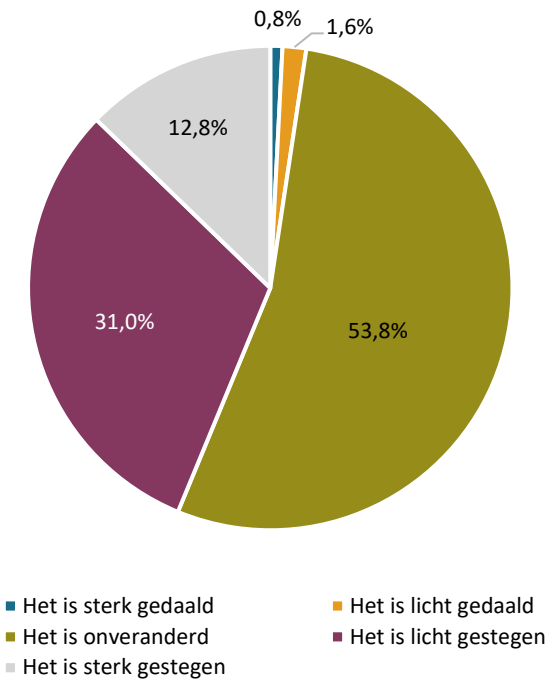


4.7 Budget

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 17). 43,8% van de bedrijven liet een – lichte of sterke – stijging in de uitgaven voor CS noteren. Voor ongeveer de helft (53,8%) van de bedrijven bleef het budget ongewijzigd. Bij amper 2,4% 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 48,1% aan dat het budget licht gestegen is terwijl nog eens 25,8% van een sterke toename spreekt. Ook bij middelgrote bedrijven is een stijging meer voorkomend dan bij kleinere ondernemingen: 44,6% voerde een lichte stijging in het CS-budget door, 20,6% spreekt zelfs van een sterke stijging. Bedrijven actief in informatie en communicatie zien hun budgetten het vaakst stijgen; bedrijven actief in accommodatie en maaltijden het minst.

Gemiddeld spenderen Vlaamse bedrijven naar schatting 22,0% van hun totale IT-budget aan cybersecurity. Bij de grote bedrijven ligt dit gemiddelde op 13,5%, bij microbedrijven bedraagt dit gemiddeld 23,9%. 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 gestegen ten opzichte van de meting in 2022 (zie Figuur 34 in Appendix).

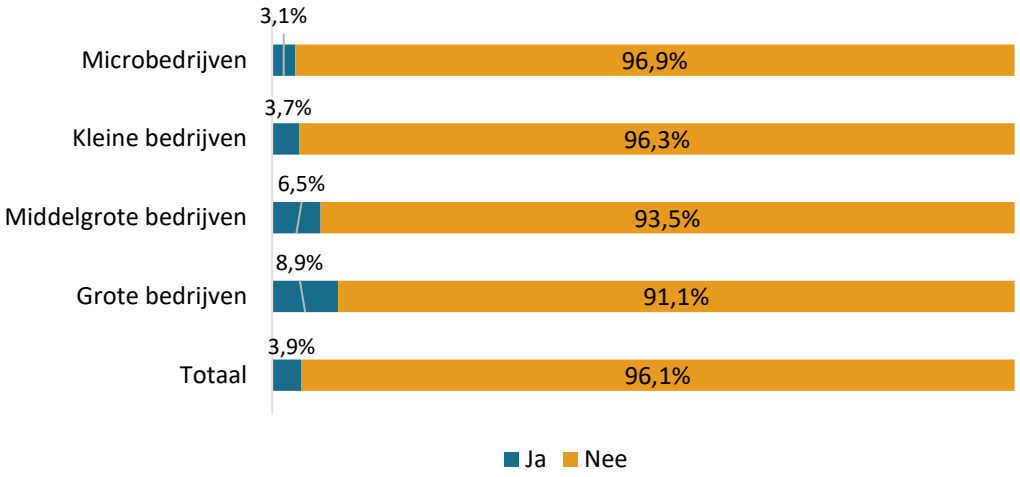
Figuur 17 Evolutie CS-budget (N=2.675) – Deze vraag werd enkel gesteld aan bedrijven die minstens één CS-maatregel toepassen



4.8 Cyberaanvallen en beveiligingsincidenten

Eén op 25 bedrijven (3,9%) geeft aan het afgelopen jaar slachtoffer te zijn geweest van een geslaagde cyberaanval, waarbij de werking van computersystemen werd verstoord en/of de toegang tot bedrijfsgegevens werd verhinderd (zie Figuur 18).[16] Dit aandeel is naar alle waarschijnlijkheid een onderschatting van het werkelijke aandeel aangezien (i) een cyberaanval onopgemerkt kan blijven, en/of (ii) bedrijven uit vrees voor reputatieschade terughoudend zijn om hierover te communiceren. Grote bedrijven (8,9%) zijn het vaakst het slachtoffer van een geslaagde cyberaanval, ook middelgrote bedrijven (6,5%) worden vaker dan gemiddeld getroffen. Dit in tegenstelling tot kleine (3,7%) en microbedrijven (3,1%) die in mindere mate worden getroffen. Het aandeel getroffen bedrijven is het hoogst voor bedrijven actief in financiële activiteiten en verzekeringen (12,5%) en het laagst voor bedrijven actief in accommodatie en maaltijden (1,9%).

Figuur 18 Slachtoffer van geslaagde cyberaanval volgens bedrijfsgrootte (N=2.720)



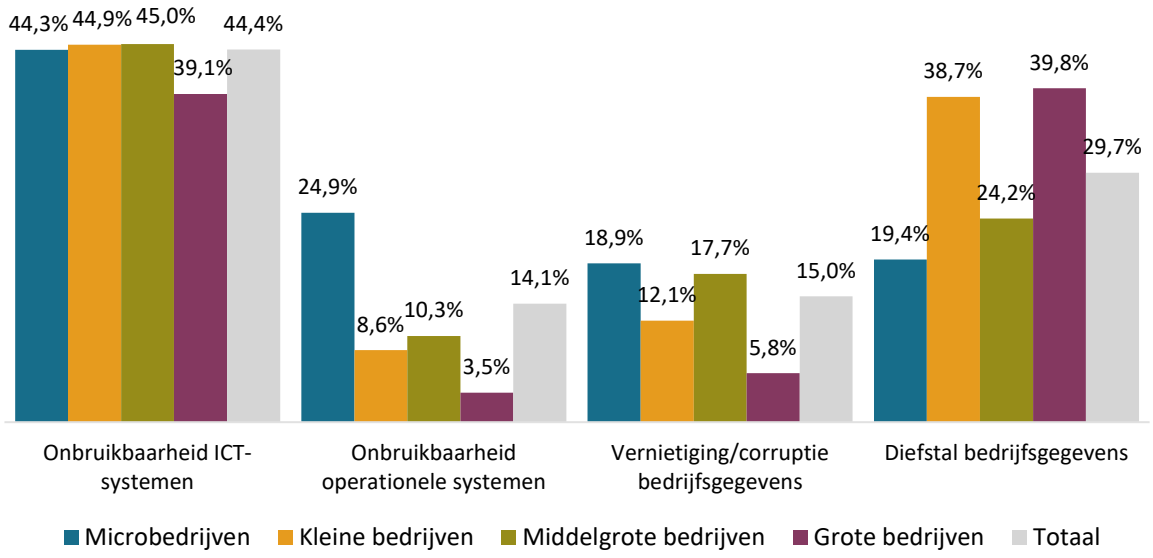
Een geslaagde cyberaanval kan verstrekkende gevolgen hebben voor het getroffen bedrijf. Uit Figuur 19 blijkt dat de *onbruikbaarheid van ICT-systemen* met voorsprong het meest voorkomende operationele gevolg is van een cyberaanval. Bij bijna de helft (44,4%) van de getroffen bedrijven werden ICT-systemen onbruikbaar als gevolg van een geslaagde cyberaanval, bijvoorbeeld door hacking, kwaadwillige vergrendeling of DDoS-aanval. Dit aandeel is hoger bij getroffen bedrijven actief in menselijke gezondheidszorg en maatschappelijke dienstverlening (61,5%) en de bouwnijverheid (59,7%) dan bij getroffen bedrijven in andere sectoren.

[16] De vraag gehanteerd in vorige edities werd aangepast met het doel een onderscheid te maken tussen (i) geslaagde cybervallen *met gevolgen* en (ii) pogingen tot cyberaanvallen *zonder gevolgen*. Bijgevolg kan het merendeel van de statistieken in deze sectie niet vergeleken worden met vorige edities.

Bij ongeveer drie op de tien getroffen bedrijven (29,7%) leidt een cyberaanval tot *diefstal van (confidentiële) bedrijfsgegevens*, bijvoorbeeld door infectie van kwaadaardige software of phishingberichten. Diefstal van bedrijfsgegevens komt vaker voor bij getroffen grote bedrijven (39,8%), kleine bedrijven (38,7%) en bedrijven actief in vervoer en opslag (75,1%) dan bij bedrijven in andere grootteklassen en sectoren.

Minder voorkomende operationele gevolgen zijn de *vernietiging of corruptie van bedrijfsgegevens* (15,0%) en *onbruikbaarheid van operationele systemen* (14,1%). Vernietiging of corruptie van bedrijfsgegevens komt vaker dan gemiddeld voor bij getroffen microbedrijven (18,9%) en bedrijven actief in vervoer en opslag (39,9%) en administratieve en ondersteunende diensten (30,0%). Onbruikbaarheid van operationele systemen komt dan weer vaker voor bij microbedrijven (24,9%) en bedrijven actief in de maakindustrie (44,8%), vervoer en opslag (23,7%) en de nutssector (23,3%) dan bij bedrijven in andere grootteklassen en sectoren.

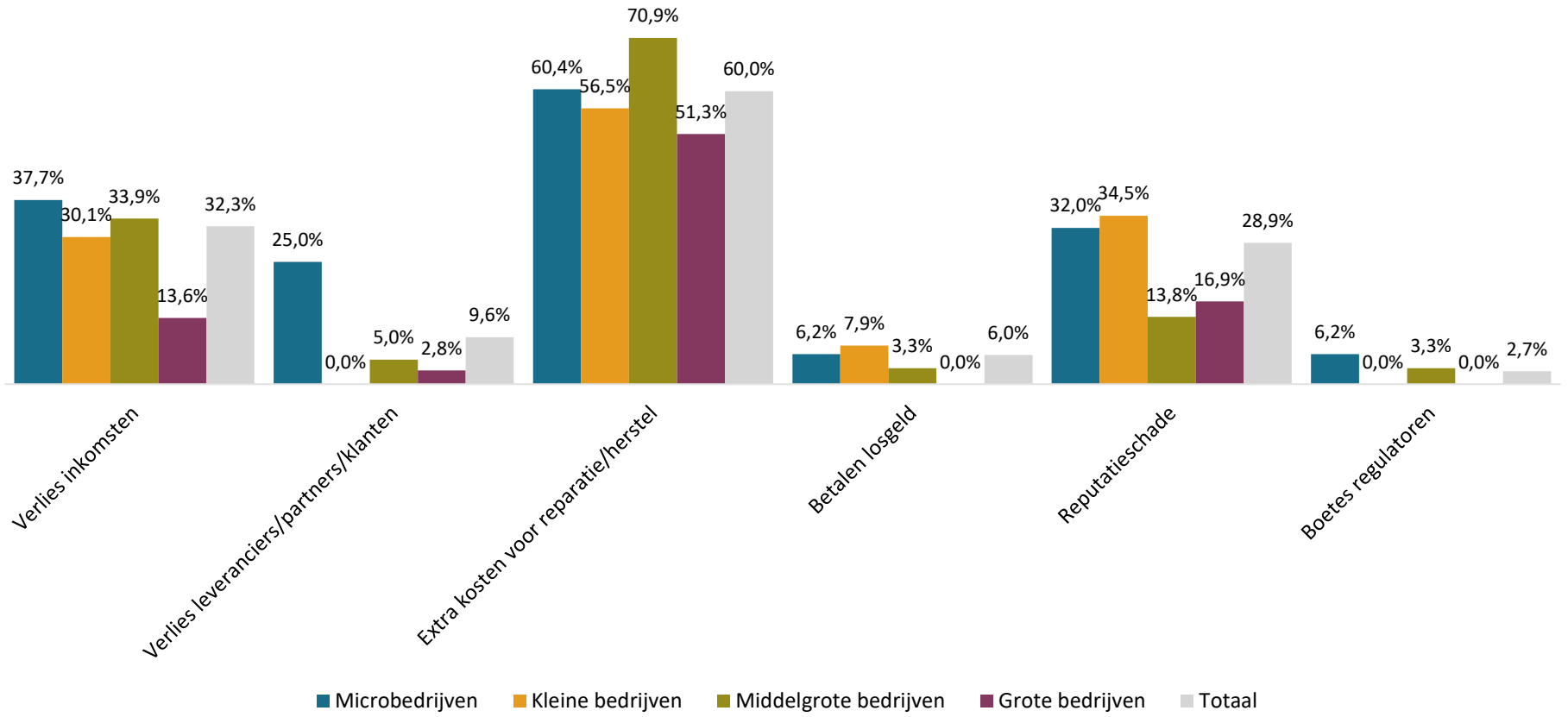
Figuur 19 Operationele gevolgen geslaagde cyberaanval volgens bedrijfsgrootte (N=145) – Deze vraag werd enkel gesteld aan bedrijven die het slachtoffer werden van een geslaagde cyberaanval



Figuur 20 geeft mogelijke andere gevolgen van een geslaagde cyberaanval weer. Zes op de tien (60,0%) getroffen bedrijven geeft aan met extra kosten voor reparatie of herstel ten gevolge van een cyberaanval geconfronteerd te worden; 32,3% lijdt onder een verlies van inkomsten; en 28,9% loopt reputatieschade op. Verlies van leveranciers, partners of klanten (9,6%); betalen van losgeld (6,0%); en boetes van regulatoren (2,7%) komen minder vaak voor. Getroffen microbedrijven (grote bedrijven) ondervinden in grotere (kleinere) mate voorgaande gevolgen. Extra kosten voor reparatie en herstel ten gevolge van een cyberaanval komen vaker dan gemiddeld voor bij bedrijven actief in accommodatie en maaltijden (100%), vervoer en opslag (89,8%), en de bouwnijverheid (85,5%). Verlies van inkomsten doet zich vaker voor bij bedrijven actief in de maakindustrie (52,6%); de nutssector (46,6%); onroerend

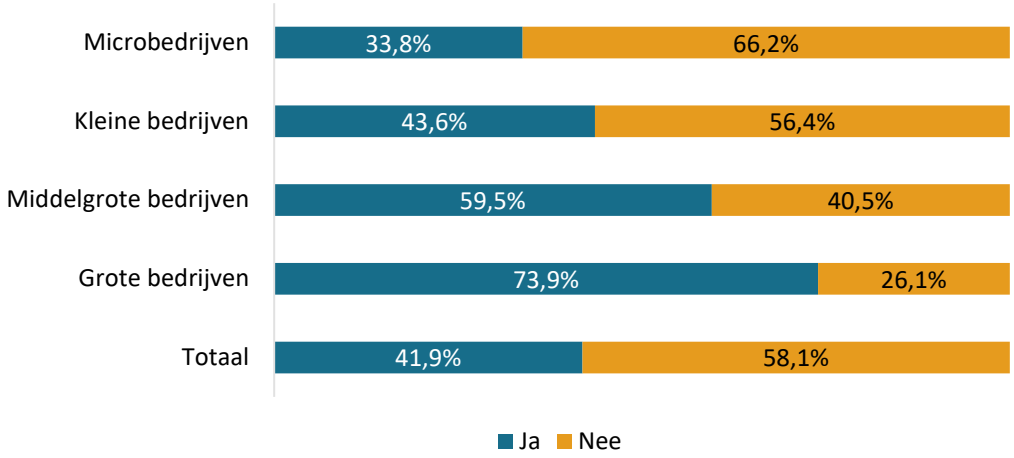
goed, vrije beroepen en wetenschappelijke en technische activiteiten (44,9%); en informatie en communicatie (43,3%) dan in andere sectoren. Reputatieschade komt vaker dan gemiddeld voor bij bedrijven actief in accommodatie en maaltijden (82,7%), vervoer en opslag (69,9%), en financiële activiteiten en verzekeringen (41,4%). Verlies van leveranciers, partners, of klanten plaagt vooral bedrijven actief in de bouwnijverheid (23,0%) en financiële activiteiten en verzekeringen (19,7%).

Figuur 20 Andere gevolgen geslaagde cyberaanval volgens bedrijfsgrootte (N=145) – Deze vraag werd enkel gesteld aan bedrijven die het slachtoffer werden van een geslaagde cyberaanval



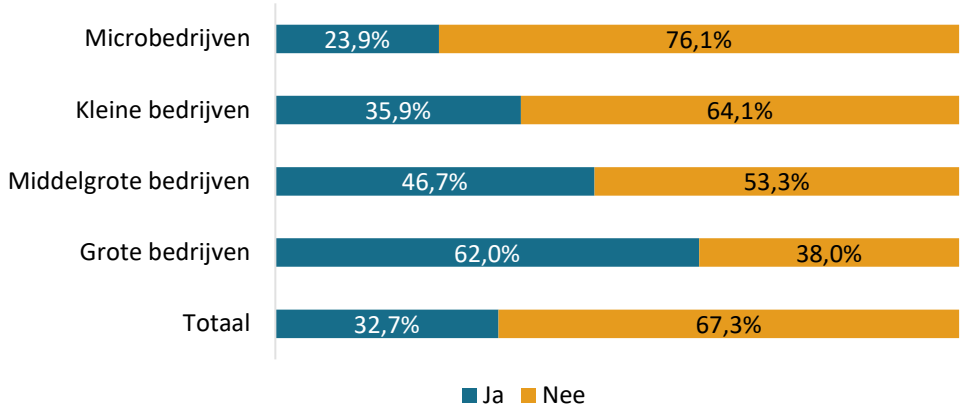
Om een volledig beeld te schetsen van de prevalentie van cyberaanvallen dient eveneens rekening gehouden te worden met het aandeel bedrijven dat te maken kreeg met pogingen tot cyberaanvallen waarbij gevolgen voor de werking van computersystemen en/of de toegang tot bedrijfsgegevens uitbleven. Maar liefst vier op tien bedrijven (41,9%) kreeg het afgelopen jaar te maken met één of meerdere pogingen tot cyberaanvallen die (voorlopig) zonder gevolg bleven (zie Figuur 21). Opnieuw is dit aandeel een pak hoger bij grote (73,9%) en middelgrote (59,5%) bedrijven dan bij kleine (43,6%) en microbedrijven (33,8%). Het aandeel bedrijven dat vaststelling deed van een poging tot cyberaanval is het hoogst in informatie en communicatie (53,7%) en het laagst in accommodatie en maaltijden (21,3%).

Figuur 21 Doelwit van poging tot cyberaanval zonder gevolgen volgens bedrijfsgrootte (N=2.720)



Bijna één derde (32,7%) van de Vlaamse bedrijven is verzekerd tegen cyberaanvallen (zie Figuur 22). 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 ongeveer zes op tien (62,0%) een verzekering tegen cyberaanvallen afgesloten te hebben. Dit aandeel ligt een pak lager bij middelgrote bedrijven (46,7%), kleine bedrijven (35,9%), en microbedrijven (23,9%). Terwijl een opmerkelijk hoger aandeel van de bedrijven actief in financiële activiteiten en verzekeringen (59,5%) en informatie en communicatie (53,7%) verzekerd is, geldt het tegendeel voor accommodatie en maaltijden (12,6%). In vergelijking met de metingen in 2022 en 2023 is het aandeel verzekerde bedrijven gestegen (zie Figuur 35 in Appendix).

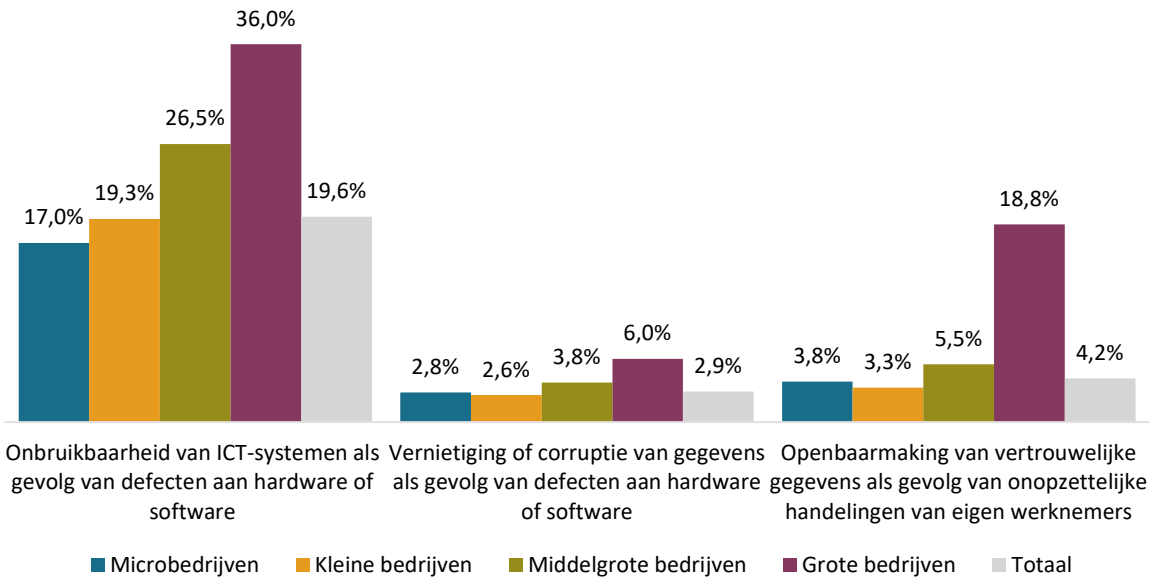
Figuur 22 Verzekering tegen cyberaanvallen volgens bedrijfsgrootte (N=2.720)



Naast cyberaanvallen kunnen ook ICT-beveiligingsincidenten optreden waarbij geen sprake is van kwaad opzet. Ongeveer één op vijf bedrijven (19,6%) kreeg het afgelopen jaar te maken met *onbruikbaarheid van ICT-systemen als gevolg van defecten aan hardware of software* (zie Figuur 23). Dit aandeel ligt hoger bij grote (36,0%) en middelgrote (26,5%) bedrijven en bedrijven actief in financiële activiteiten en verzekeringen (24,6%) en informatie en communicatie (23,4%) dan bij bedrijven in andere grootteklassen en sectoren.

Minder voorkomende veiligheidsincidenten zijn de *openbaarmaking van vertrouwelijke gegevens als gevolg van onopzettelijke handelingen van eigen werknemers* (4,2%) en de *vernietiging of corruptie van gegevens als gevolg van defecten aan hardware of software* (2,9%). Grote bedrijven (18,8%) en bedrijven actief in financiële activiteiten en verzekeringen (13,5%) en administratieve en ondersteunende diensten (8,4%) worden ten opzichte van bedrijven uit andere grootteklassen en sectoren vaker geconfronteerd met de openbaarmaking van vertrouwelijke gegevens.

Figuur 23 ICT-beveiligingsincidenten volgens bedrijfsgrootte (N=2.720)

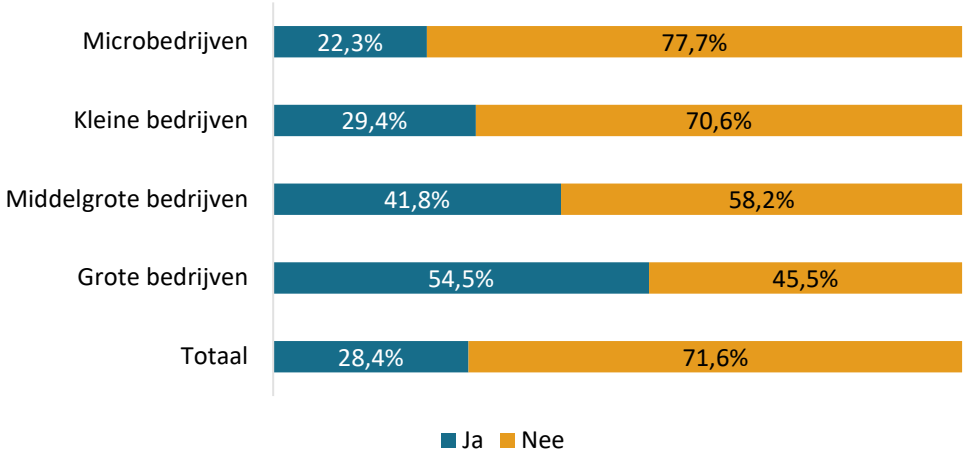


4.9 Overheidsbeleid

In maart 2019 lanceerde de Vlaamse overheid het Vlaams Actieplan Cybersecurity met de ambitie om cyberveiligheid in Vlaamse bedrijven een topprioriteit te maken. Het Actieplan werd in maart 2024 verlengd. Het plan bestaat uit drie luiken: (1) onderzoek, (2) gebruik van CS-oplossingen door bedrijven en (3) bewustmaking en opleiding. Het speelt hiermee duidelijk in op een aantal van de hierboven gedocumenteerde struikelblokken. Gevraagd naar het bestaan van dit actieplan zegt 28,4% van de Vlaamse bedrijven weet te hebben van dit beleidsplan; 71,6% daarentegen stelt niet op de hoogte te zijn (zie Figuur 24). Het aandeel bedrijven dat kennis heeft van het actieplan is hoger voor grote bedrijven (54,5%) en middelgrote bedrijven (41,8%) dan voor kleine bedrijven (29,4%) en microbedrijven (22,3%). Vooral bedrijven actief in financiële activiteiten en verzekeringen (47,8%) en informatie en communicatie (45,8%) zijn op de hoogte van het actieplan, in tegenstelling tot bedrijven actief in accommodatie en maaltijden (19,9%), de bouwnijverheid (19,0%), en de nutssector (18,2%)[17].

In vergelijking met de (eerste) meting in 2022 is de kennis omtrent het actieplan meer dan verdubbeld (zie Figuur 36 in Appendix).

Figuur 24 Kennis specifiek actieplan Vlaamse overheid volgens bedrijfsgrootte (N=2.720)



[17] Gezien het geringe aantal responsen voor de nutssector dient deze statistiek met de nodige voorzichtigheid geïnterpreteerd te worden.

5 CONCLUSIES

Deze studie, die gebaseerd is op de vierde bevraging op rij van een representatieve steekproef van Vlaamse bedrijven, bevestigt de in eerdere edities vastgestelde toename in de adoptie van meer geavanceerde technische maatregelen en beheerprocedures in het kader van cyberveiligheid. Deze studie identificeert mogelijke oorzaken die aan de basis liggen van de verhoogde inspanningen van een grote groep Vlaamse bedrijven op het vlak van cyberveiligheid. Ten eerste zien we een toename in het nut of prioriteit toegekend aan een effectief CS-beleid. Ten tweede wordt er meer druk uitgeoefend door klanten om cyberveiligheid te garanderen. Ten derde worden er vaker externe gespecialiseerde CS-dienstverleners ingeschakeld, die de nodige expertise hebben om cyberveiligheidsmaatregelen en – procedures te implementeren. Deze tendenzen zijn zeer waarschijnlijk ingegeven door het wettelijke kader. Meer specifiek trad op 18 oktober 2024 de NIS2-wet in werking. Deze wet verplicht bedrijven uit kritieke sectoren (i.e., NIS2-entiteiten) tot de implementatie van maatregelen voor het beheer van cyberrisico's, melding van veiligheidsincidenten, en opleidingen voor het management. NIS2-entiteiten zijn bovendien verplicht om de beveiliging van hun toeleveringsketen te verzekeren.

De verhoogde inspanningen op het vlak van cyberveiligheid brengen nieuwe obstakels met zich mee. Het optrekken van CS-budgetten doet bedrijven in grotere getale twijfelen aan de kosten-batenverhouding van hun CS-beleid. Het hogere kostenplaatje van het CS-beleid vertaalt zich in toenemende mate in een hoger ervaren gebrek aan publieke of externe financiering. Het toegenomen gebruik van externe gespecialiseerde CS-dienstverleners – in combinatie met een stagnering of geringe toename van de relevante kennis, vaardigheden en ervaring binnen de onderneming – doet bij bedrijven de vrees toenemen dat zij te afhankelijk worden van leveranciers.

Ondanks deze positieve evolutie blijft een niet te verwaarlozen groep bedrijven ter plaatse trappelen op het vlak van cyberveiligheid. Bij hen ontbreken één of zelfs meerdere niet-geavanceerde technische maatregelen (software-updates, data back-ups, protocol voor toegangsbeheer, paswoordauthenticatie, VPN-netwerk). In veel van deze bedrijven bestaat het besef van het gebrek aan deze maatregelen, maar ontbreken de relevante kennis, vaardigheden en ervaring binnen de onderneming om deze maatregelen te implementeren. Bovendien vindt deze groep bedrijven vaak niet de weg naar kennispartners of begeleiding. Daarom is het vanuit de overheid belangrijk om blijvend in te zetten op deze groep bedrijven, en dit met een diverse mix van acties.

Menselijke aspecten vormen niet alleen een barrière om cyberveiligheidsmaatregelen en – procedures te introduceren, maar liggen vaak ook aan de basis van cyberrisico's. Onvoldoende bewustwording bij medewerkers blijft volgens bijna de helft van de respondenten het grootste cyberrisico voor hun onderneming. Dit aandeel ligt bovendien een stuk hoger bij de grotere bedrijven. Deze bedrijven kampen dan ook in hogere getale met ICT-beveiligingsincidenten. Opleidingen of activiteiten voor medewerkers kunnen het risico op deze incidenten verlagen, maar de adoptie ervan ontbreekt nog steeds te vaak.

Cyberaanvallen vormen voor Vlaamse bedrijven een reëel risico. Vier op tien bedrijven kreeg het afgelopen jaar te maken met één of meerdere pogingen tot cyberaanvallen die zonder gevolgen bleven. Eén op 25 bedrijven werd daarenboven het slachtoffer van een geslaagde cyberaanval, waarbij de werking van computersystemen werd verstoord en/of de toegang tot bedrijfsgegevens werd verhinderd. Verwacht wordt dat dit aandeel in de toekomst zal toenemen. Cybercriminelen maken in toenemende mate gebruik van AI-technologieën die toelaten om op grote schaal geavanceerde aanvallen te plaatsen[18]. Daartegenover staat dat de toename in de CS-maturiteit van Vlaamse bedrijven traag verloopt.

Het Vlaams Actieplan Cybersecurity, dat in 2019 werd gelanceerd, werd in maart 2024 verlengd voor een periode van vier jaar. De resultaten van deze studie toont de blijvende nood aan van een actieplan dat is gericht op het sensibiliseren, informeren, opleiden en financieel ondersteunen van Vlaamse bedrijven met het oog op het verbeteren van hun cyberveiligheid. Nog steeds zijn niet alle bedrijven overtuigd van het nut en de prioriteit van een CS-beleid. Nog steeds kampt een groot deel van de Vlaamse bedrijven met een gebrek aan kennis, vaardigheden en bewustzijn bij werknemers. Nog steeds vinden niet alle bedrijven de weg naar kennispartners of begeleiding. De verhoogde inspanningen op het vlak van cyberveiligheid gaan bij een deel van de Vlaamse bedrijven bovendien gepaard met obstakels gerelateerd aan financiering en afhankelijkheid van leveranciers. Op deze bestaande en nieuwe fronten kan het Vlaams Actieplan Cybersecurity een rol van betekenis spelen.

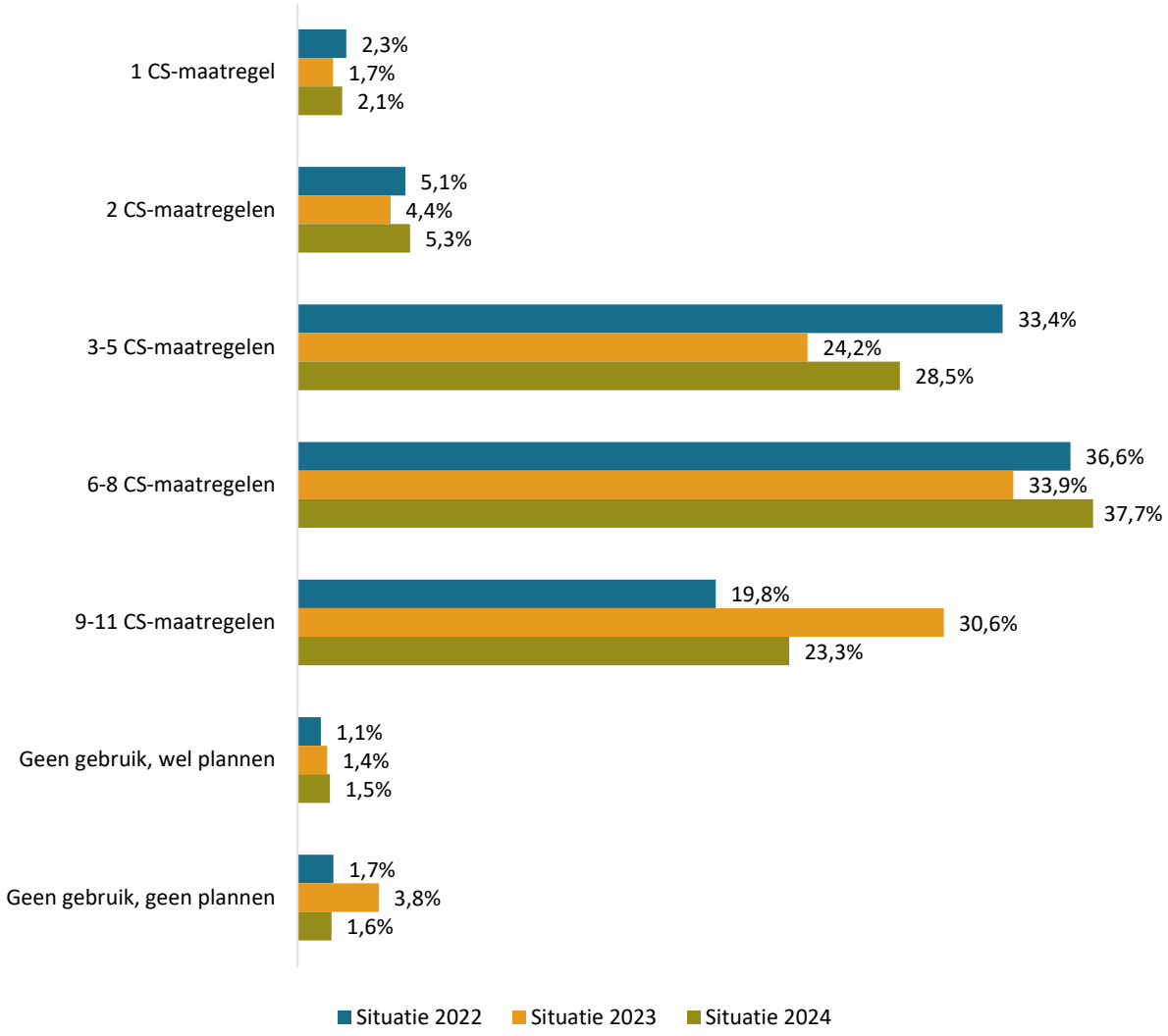
18 Zie https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

6 APPENDIX

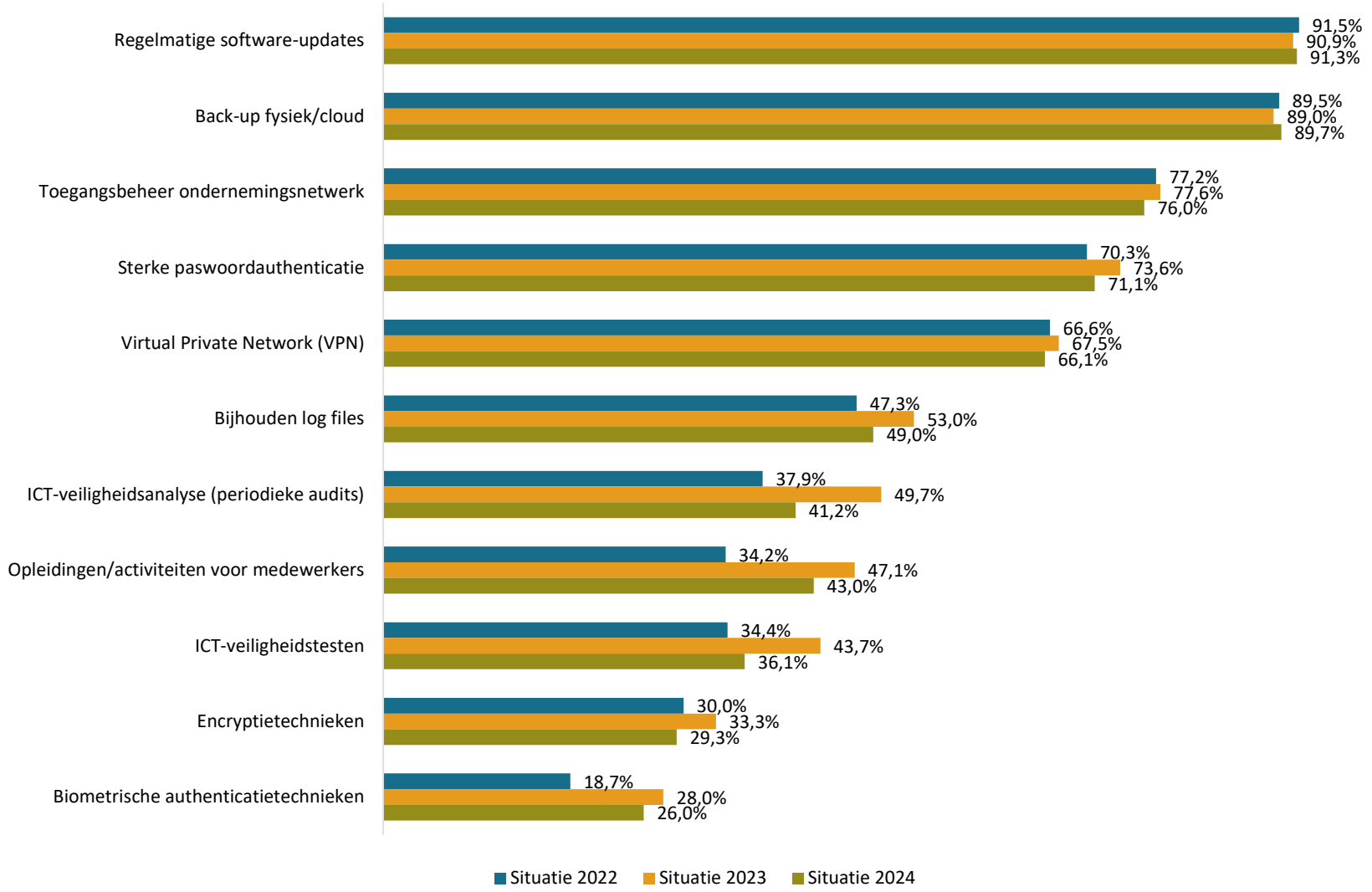
Tabel 3 Geselecteerde sectoren

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

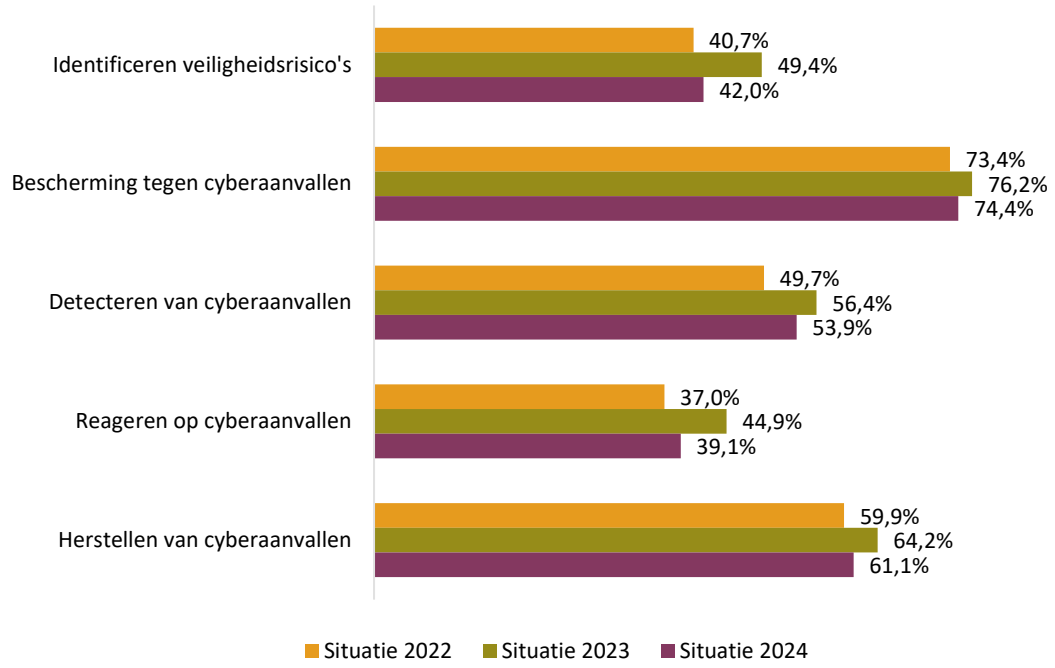
Figuur 25 Evolutie adoptiegraad aantal CS-maatregelen



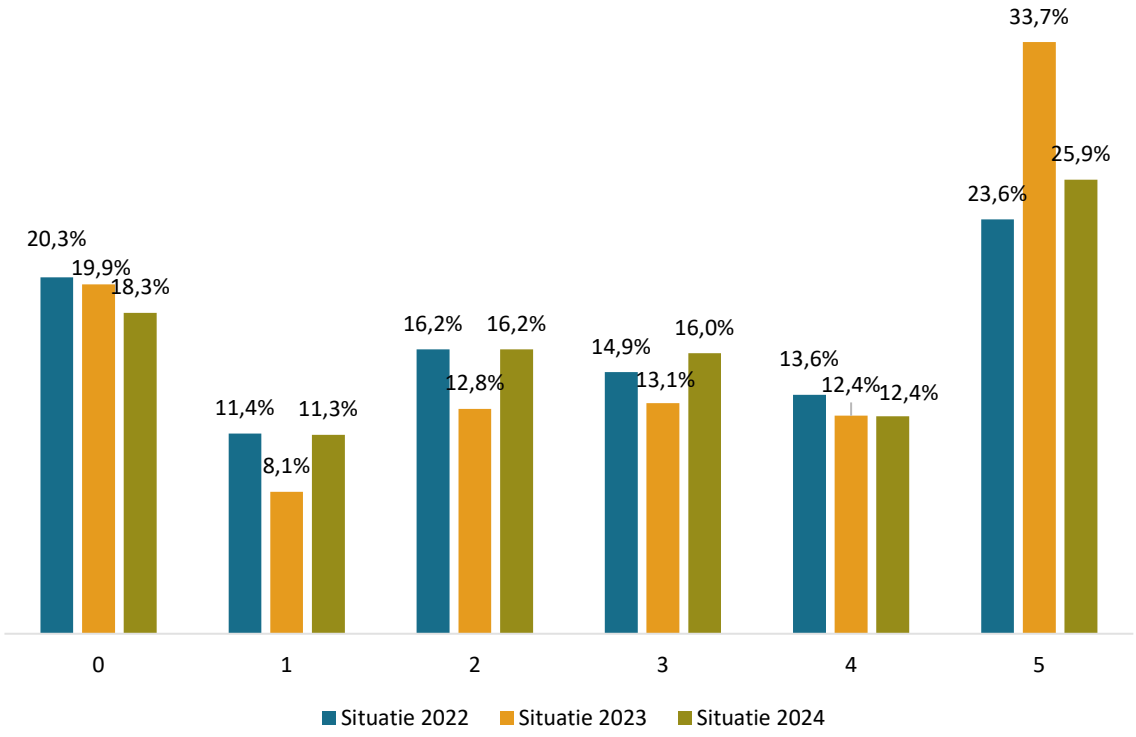
Figuur 26 Evolutie adoptiegraad CS-maatregelen volgens type



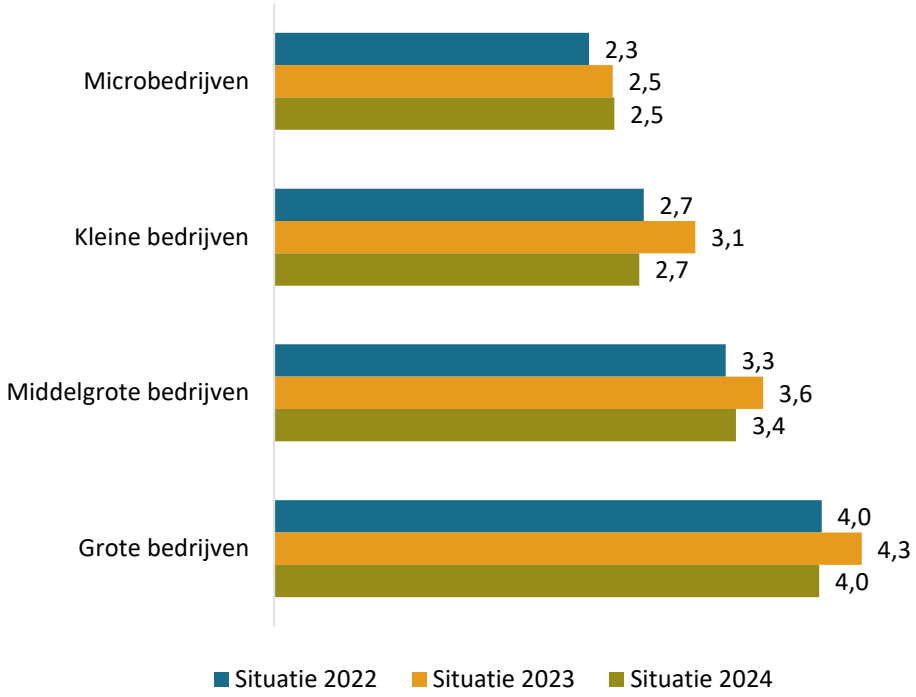
Figuur 27 Evolutie implementatie beheerprocedures volgens type



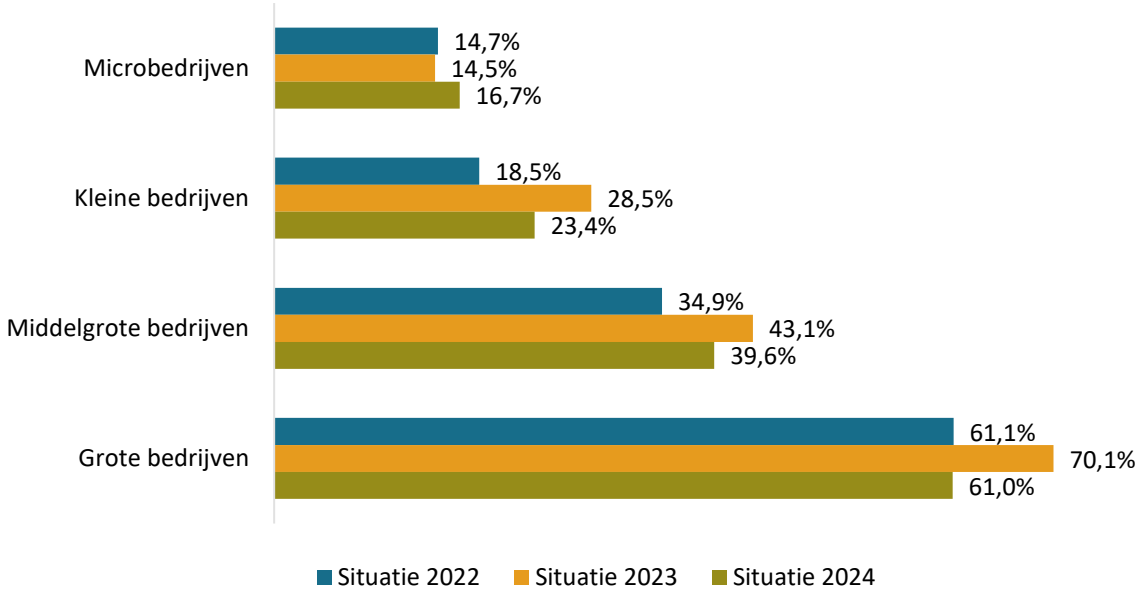
Figuur 28 Evolutie aantal beheerprocedures



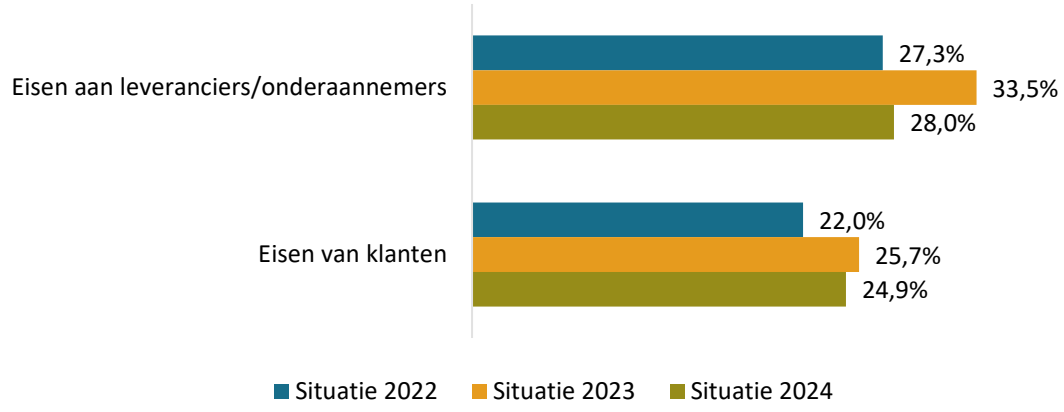
Figuur 29 Evolutie aantal beheerprocedures volgens bedrijfsgrootte



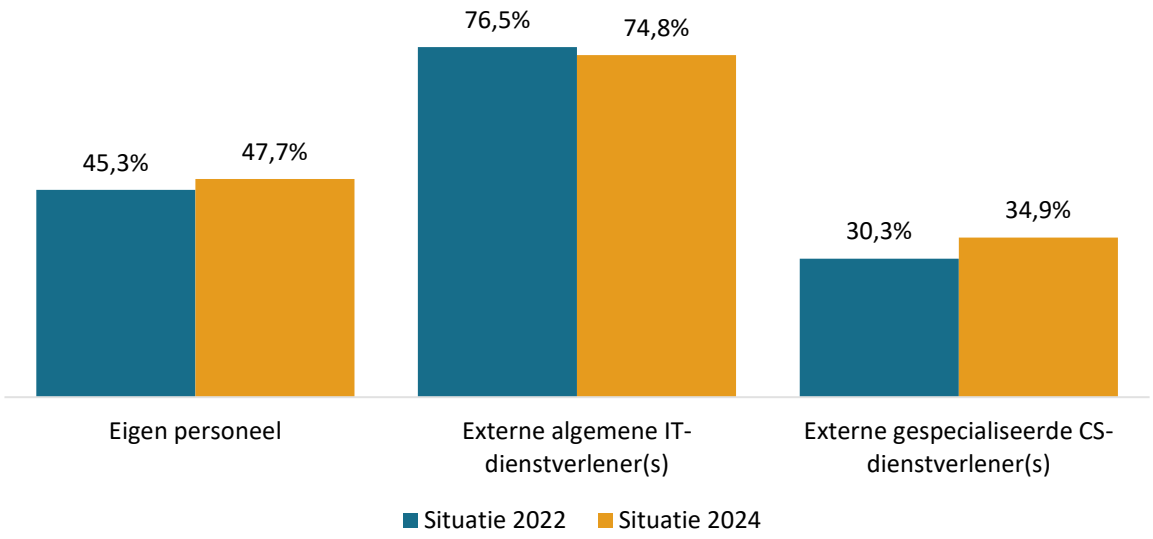
Figuur 30 Evolutie plan/beleidsdocument inzake cybersecurity volgens bedrijfsgrootte



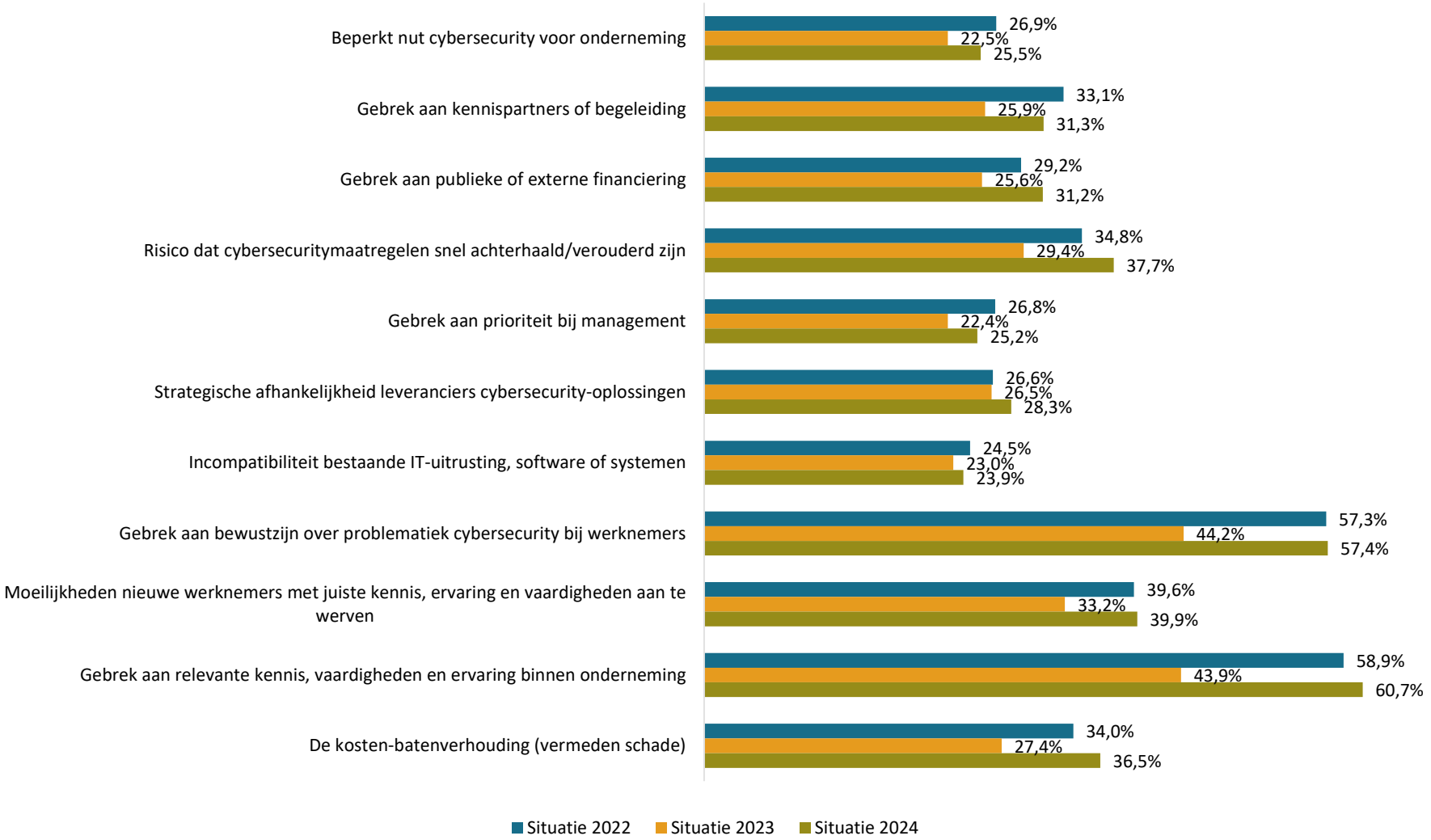
Figuur 31 Evolutie eisen inzake cybersecurity



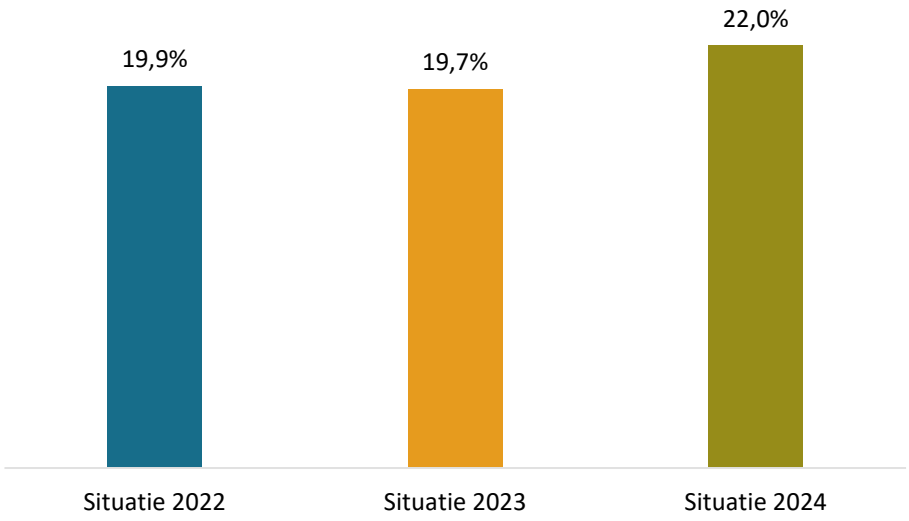
Figuur 32 Evolutie uitvoering ICT-beveiligingsgerelateerde activiteiten



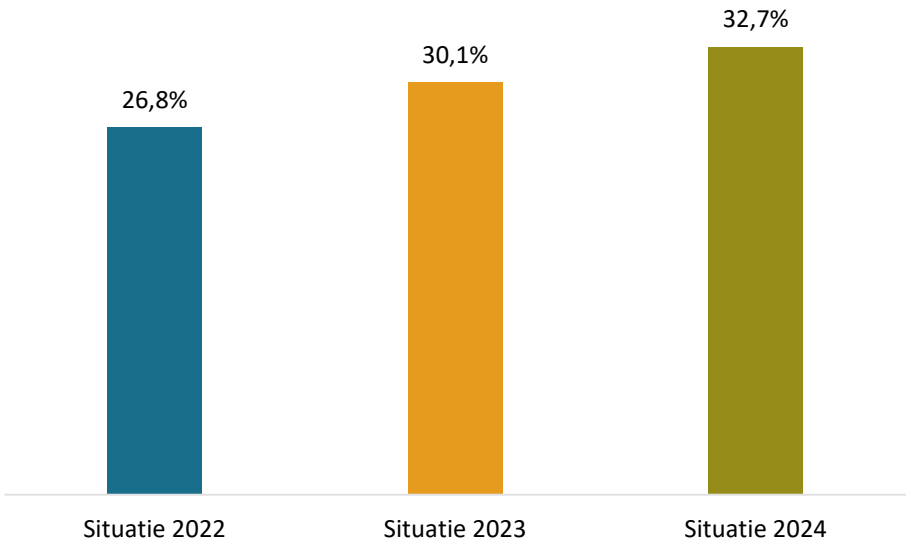
Figuur 33 Evolutie aandeel bedrijven die minstens één CS-maatregel toepassen dat obstakels ondervond bij de invoer en het gebruik van CS-maatregelen



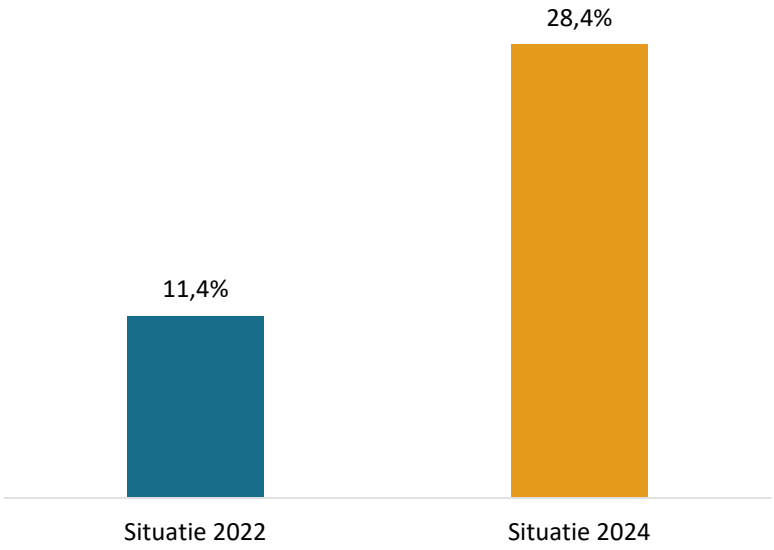
Figuur 34 Evolutie aandeel van het IT-budget gespendeerd aan cybersecurity



Figuur 35 Evolutie aandeel bedrijven met een verzekering tegen cyberaanvallen



Figuur 36 Evolutie kennis specifiek actieplan Vlaamse overheid



DEPARTEMENT
**WERK, ECONOMIE
WETENSCHAP, INNOVATIE &
SOCIALE ECONOMIE**

www.departementwewis.be