



Resultaten ICT Barometer over ICT-beveiliging en cybercrime

Jaargang 9
28 januari 2009

DISCLAIMER. De kleine lettertjes

De ICT Barometer, een onderzoek van Ernst & Young, is de gerenommeerde 'vinger aan de pols' voor managers. Het onderzoek wordt sinds december 2001 gehouden onder gemiddeld zeshonderd Nederlandse directeuren, managers en professionals uit het bedrijfsleven, onderverdeeld naar productie/industrie, handel/distributie en dienstverlening/ financiële instellingen en de (semi)overheid. Het onderzoek is uitgevoerd door het marktonderzoekbureau Synovate en de ondervraagde groep wordt online geënkquêteerd. Het onderzoek is representatief voor directeuren, managers, professionals en/of hoger opgeleide werknemers die beschikken over een internetaansluiting. De ICT Barometer biedt een belangrijk deel 'up to date' informatie door een aantal vaste businessdilemma's te monitoren, aangevuld met actuele vragen.

Met Ernst & Young worden de activiteiten bedoeld van Ernst & Young Accountants LLP, Ernst & Young Belastingadviseurs LLP en andere Ernst & Young deelnemingen in Nederland. Ernst & Young Accountants LLP (KvK 24432944, OC335594) en Ernst & Young Belastingadviseurs LLP (KvK 24432939, OC335596) zijn limited liability partnerships gevestigd in Engeland en Wales, statutair gevestigd te Lambeth Palace Road 1, London SE1 7EU, Verenigd Koninkrijk, met haar hoofdvestiging aan Boompjes 258, 3011 XZ Rotterdam, Nederland.

Hoewel bij het redigeren van dit rapport ICT Barometer de grootst mogelijke zorgvuldigheid is betracht, bestaat de mogelijkheid dat sommige informatie na verloop van tijd verouderd of niet meer juist is. Ernst & Young kan geen aansprakelijkheid aanvaarden voor de gevolgen van activiteiten die worden ondernomen op basis van informatie in dit rapport. Overname van artikelen is toegestaan, mits integraal en met bronvermelding.

Ernst & Young LLP, Rotterdam, 28 januari 2009

ICT Barometer

Ernst & Young ICT Leadership
Jacob Verschuur, director
Antonio Vivaldistraat 150
1083 HP Amsterdam
The Netherlands

Mail to: jacob.verschuur@nl.ey.com
www.ey.nl
www.ictbarometer.nl

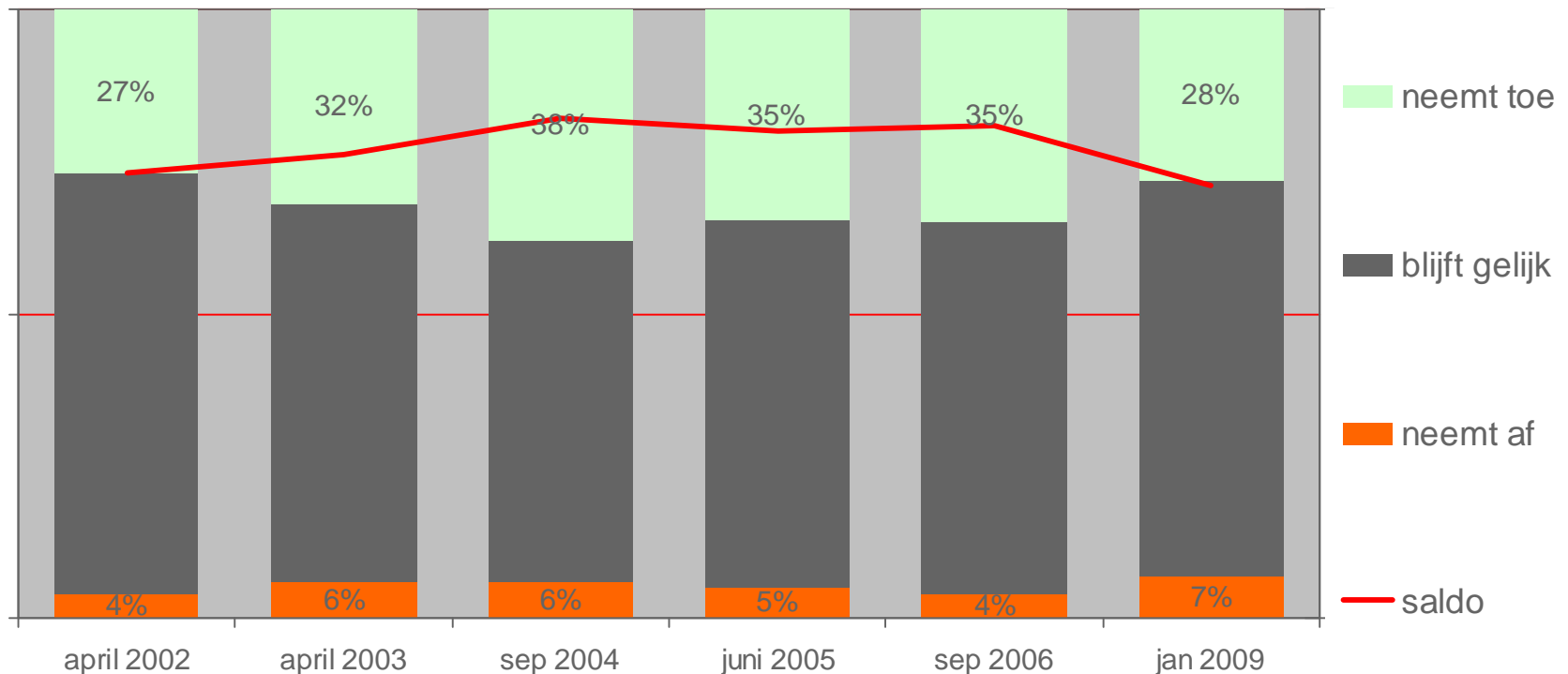
ICT-beveiliging - Vraagpunten

- In welke mate zijn organisaties afhankelijk van ICT?
- Beschikt uw organisatie over een noodplan?
- Welke ontwikkelingen zijn er ten aanzien van de overlast door computervirussen en computerinbraak?

ICT-bestedingen - ICT-beveiliging

De bestedingen aan ICT-beveiliging blijven stijgen, alleen minder hard dan in de jaren hiervoor.

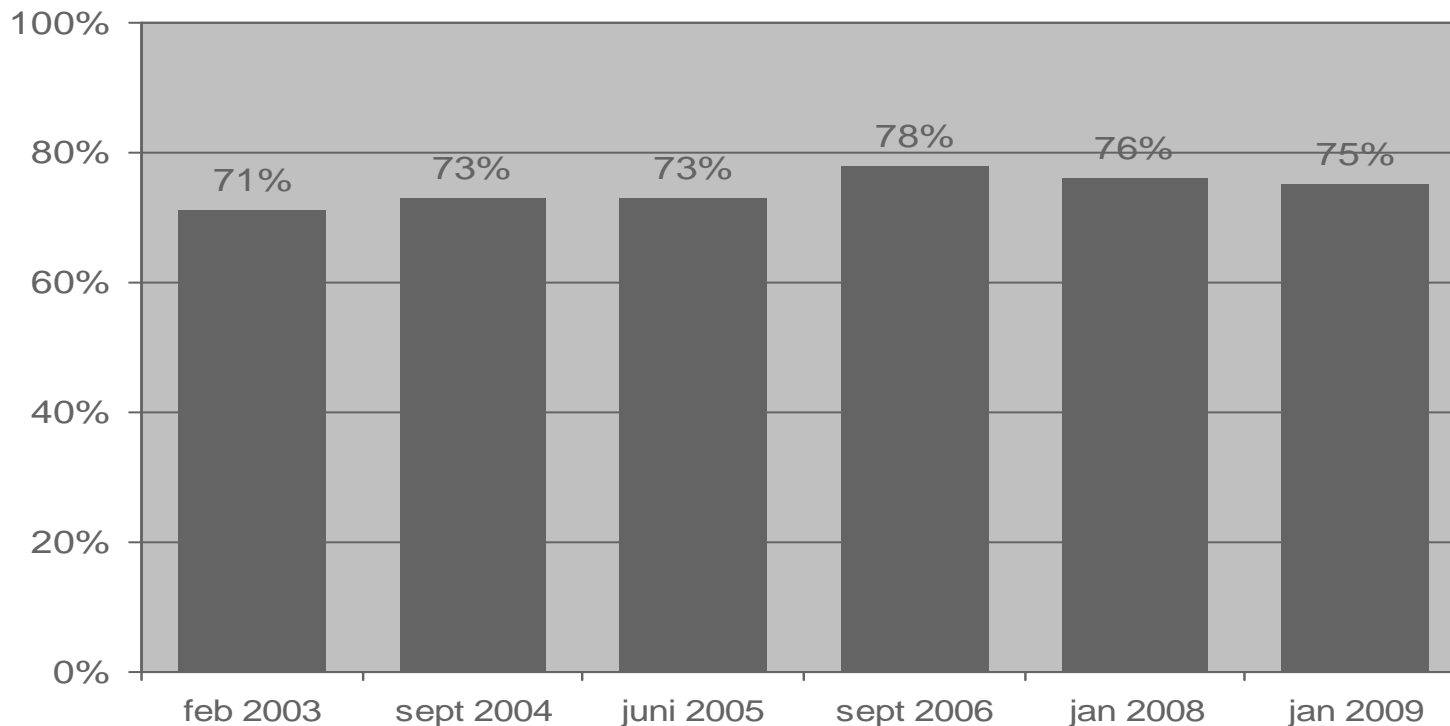
Wat zijn de verwachtingen omtrent de bestedingen van uw organisatie aan ICT-beveiliging voor de komende 12 maanden ten opzichte van de afgelopen 12 maanden?



ICT-beveiliging - Afhankelijkheid van ICT

De afhankelijkheid van ICT wordt al een geruim aantal jaren hoog ingeschat.

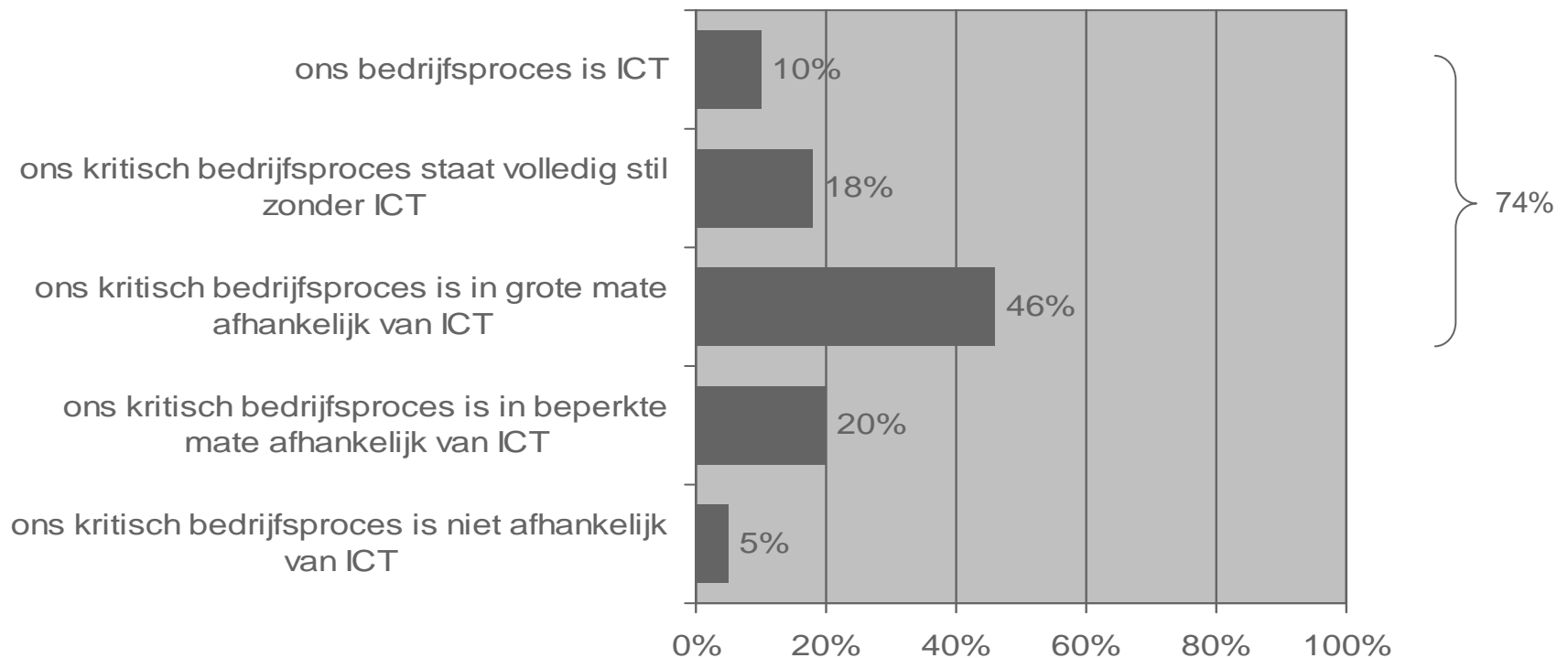
Bedrijfsprocessen in (zeer) grote mate afhankelijk van ICT



ICT-beveiliging - Afhankelijkheid van ICT

Driekwart van de ondervraagden geeft aan dat hun organisatie in sterke mate afhankelijk is van ICT en drie op de tien ondervraagden zijn zelfs volledig afhankelijk hiervan. Dit geeft aan hoe belangrijk een goede beveiliging van ICT toepassingen is.

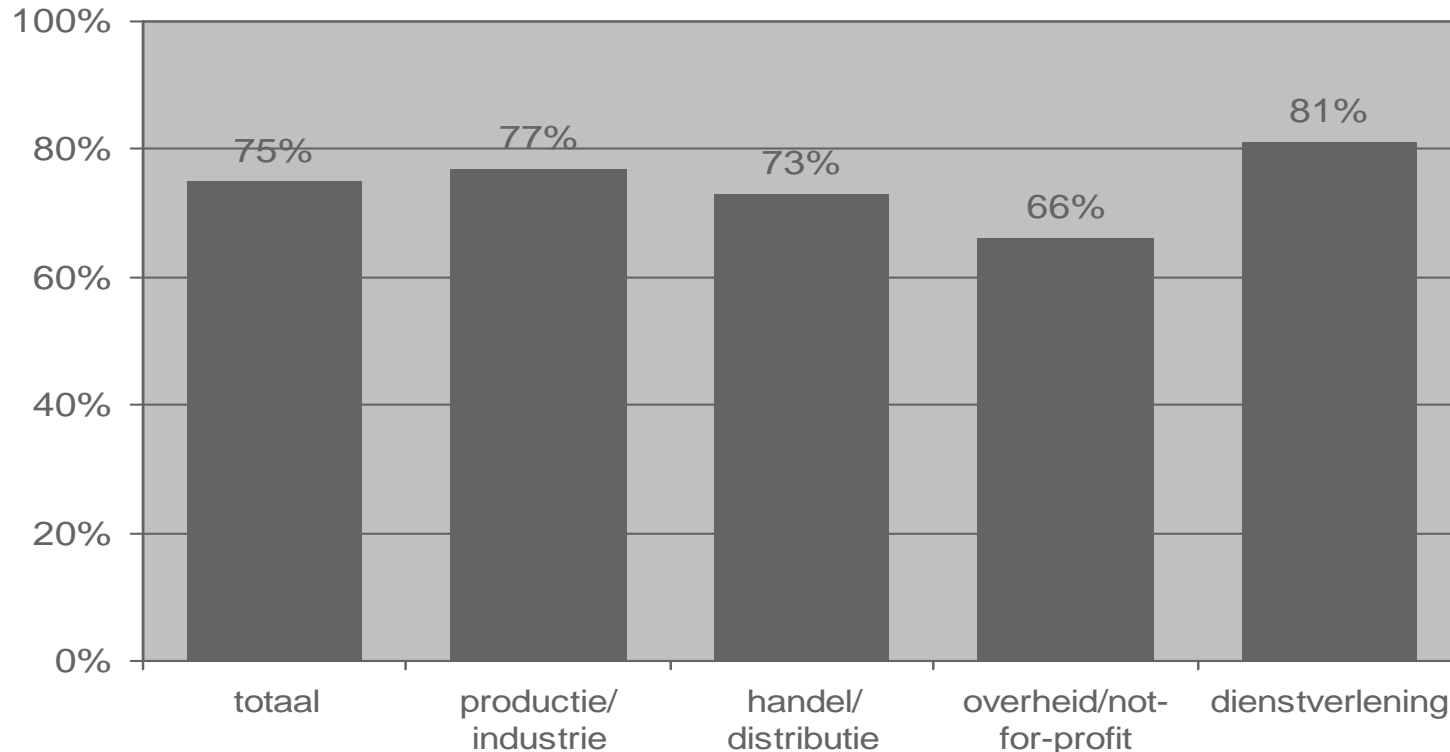
In hoeverre zijn uw bedrijfsprocessen afhankelijk van ICT?



ICT-beveiliging - Afhankelijkheid van ICT

De afhankelijkheid van ICT is relatief groot onder dienstverlenende bedrijven. In de Overheid/not-for-profit sector is men iets minder sterk afhankelijk van ICT.

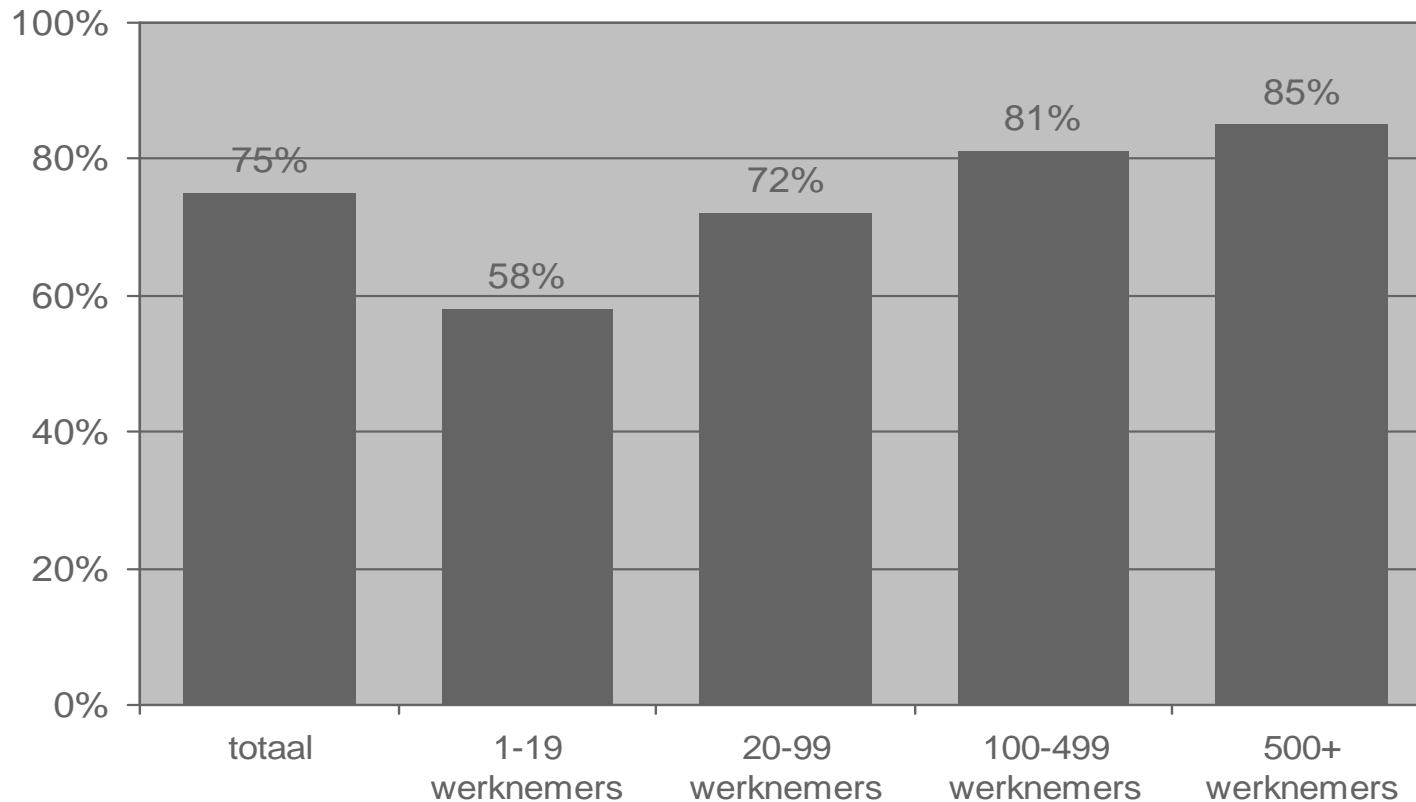
Bedrijfsprocessen in (zeer) grote mate afhankelijk van ICT



ICT-beveiliging - Afhankelijkheid van ICT

Hoe groter het bedrijf, hoe groter de afhankelijkheid van ICT.

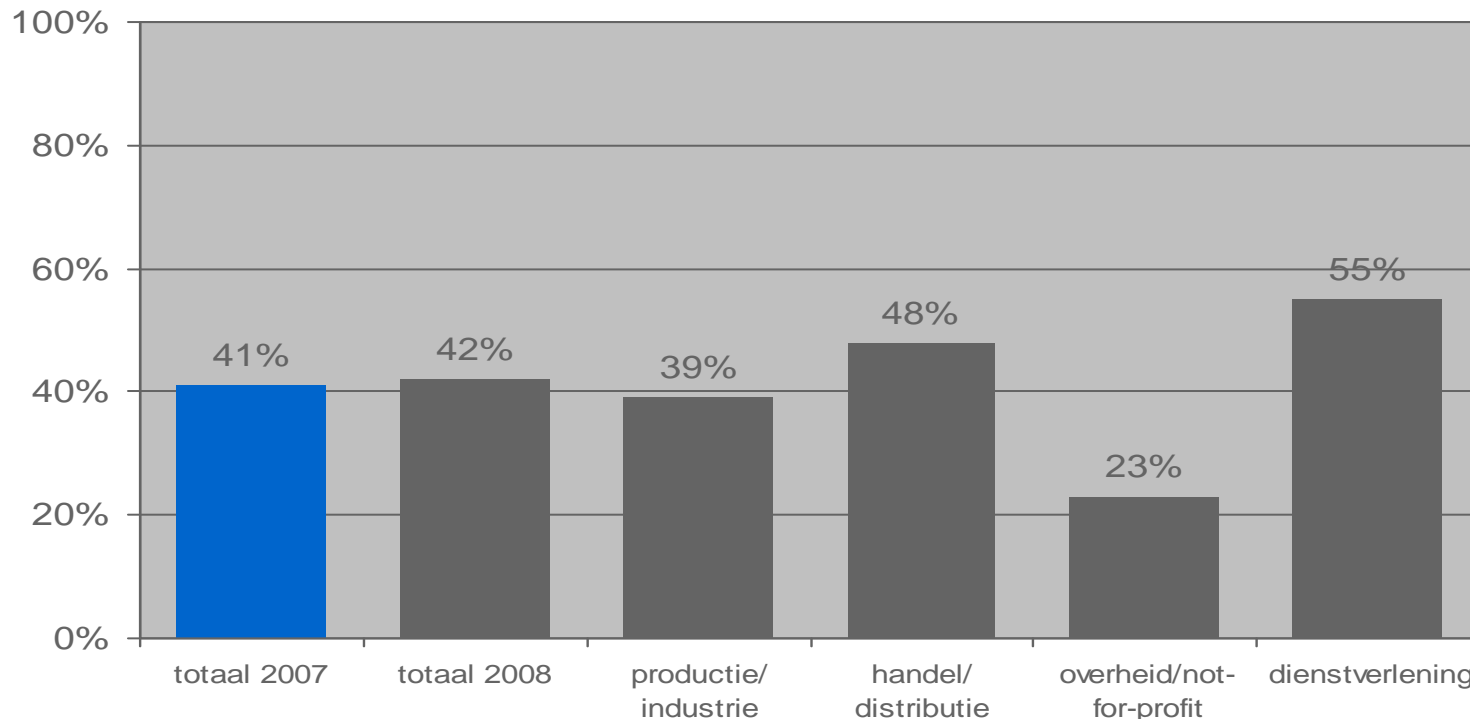
Bedrijfsprocessen in (zeer) grote mate afhankelijk van ICT



ICT-beveiliging - Aanwezigheid van noodplan

Ondanks de sterke afhankelijkheid van ICT beschikken slechts vier op de tien organisaties over een noodplan voor als het bedrijfsproces uitvalt of minder functioneert. Binnen de overheid/not-for-profit sector is dit lager: driekwart beschikt niet over een noodplan.

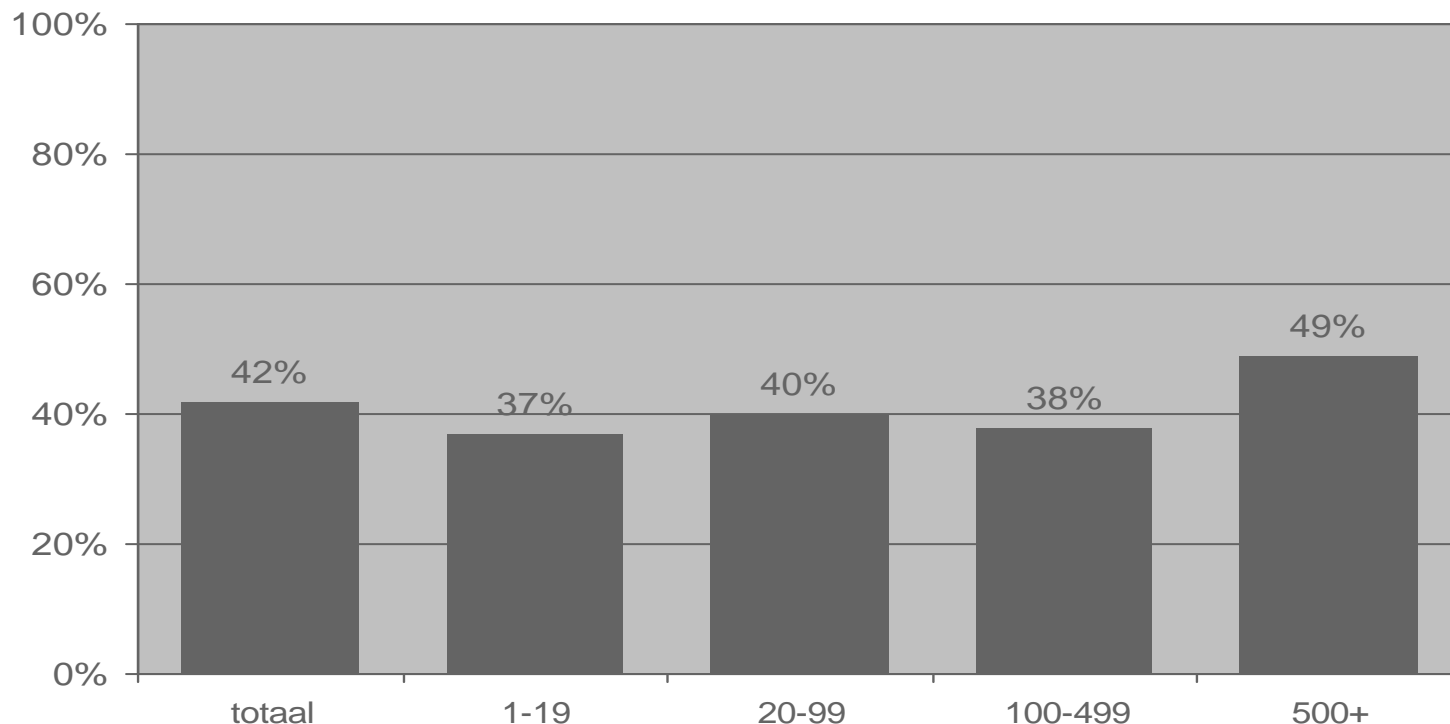
Beschikt uw organisatie over een noodplan voor het geval dat het kritisch bedrijfsproces uitvalt of niet meer goed functioneert?



ICT-beveiliging - Aanwezigheid van noodplan

Grote organisaties (meer dan 500 werknemers) beschikken vaker over een noodplan. De relatief sterke afhankelijkheid van ICT en de relatief grote gevolgen/schade bij uitval spelen hierbij waarschijnlijk een rol.

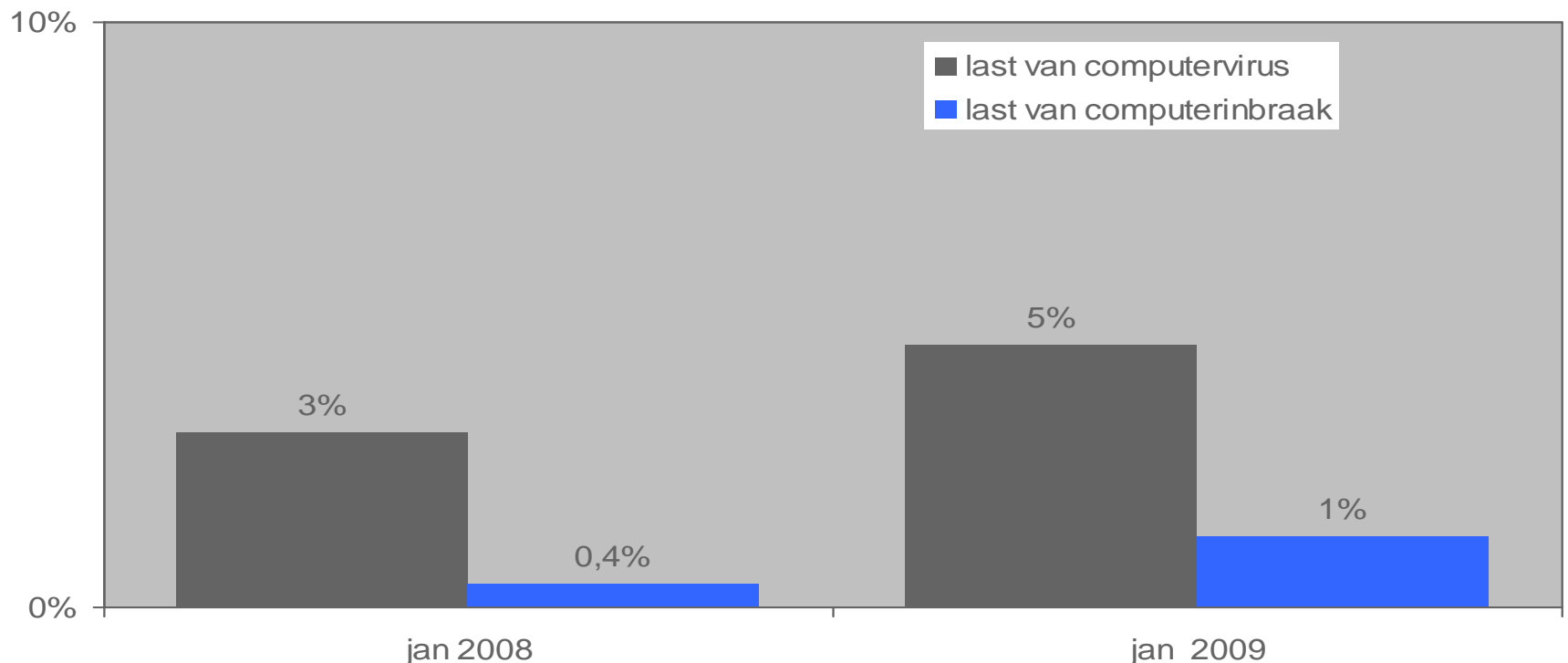
Beschikt uw organisatie over een noodplan voor het geval dat het kritisch bedrijfsproces uitvalt of niet meer goed functioneert?



ICT-beveiliging - Last van computervirussen of computerinbraak?

5% van de ondervraagde bedrijven heeft de afgelopen maand last gehad van een computervirus en 1% heeft last gehad van computerinbraak. In beide gevallen gaat het om een grote stijging ten opzichte van vorig jaar.

Heeft uw organisatie de afgelopen maand last gehad van een computervirus of computerinbraak (hackers)?



ICT-beveiliging - Samenvatting

- **Het belang van ICT-beveiliging blijkt uit het gegeven dat driekwart van de Nederlandse organisaties sterk afhankelijk is van ICT. Drie op de tien organisaties zijn zelfs volledig afhankelijk van ICT. Dit onderstreept het belang van een goede beveiliging van ICT toepassingen. Ondanks de sterke ICT-afhankelijkheid hebben slechts vier van de tien organisaties een noodplan voor als het bedrijfsproces uitvalt of slecht functioneert. Deze situatie is al jaren vrijwel ongewijzigd**

- **5% van de ondervraagde bedrijven heeft de afgelopen maand (december 2008) last gehad van een computervirus (in 2007 was dit nog 3%) en 1% heeft last gehad van computerinbraak (in 2007 was dit 0,4%). In beide gevallen gaat het om een grote stijging ten opzichte van vorig jaar.**

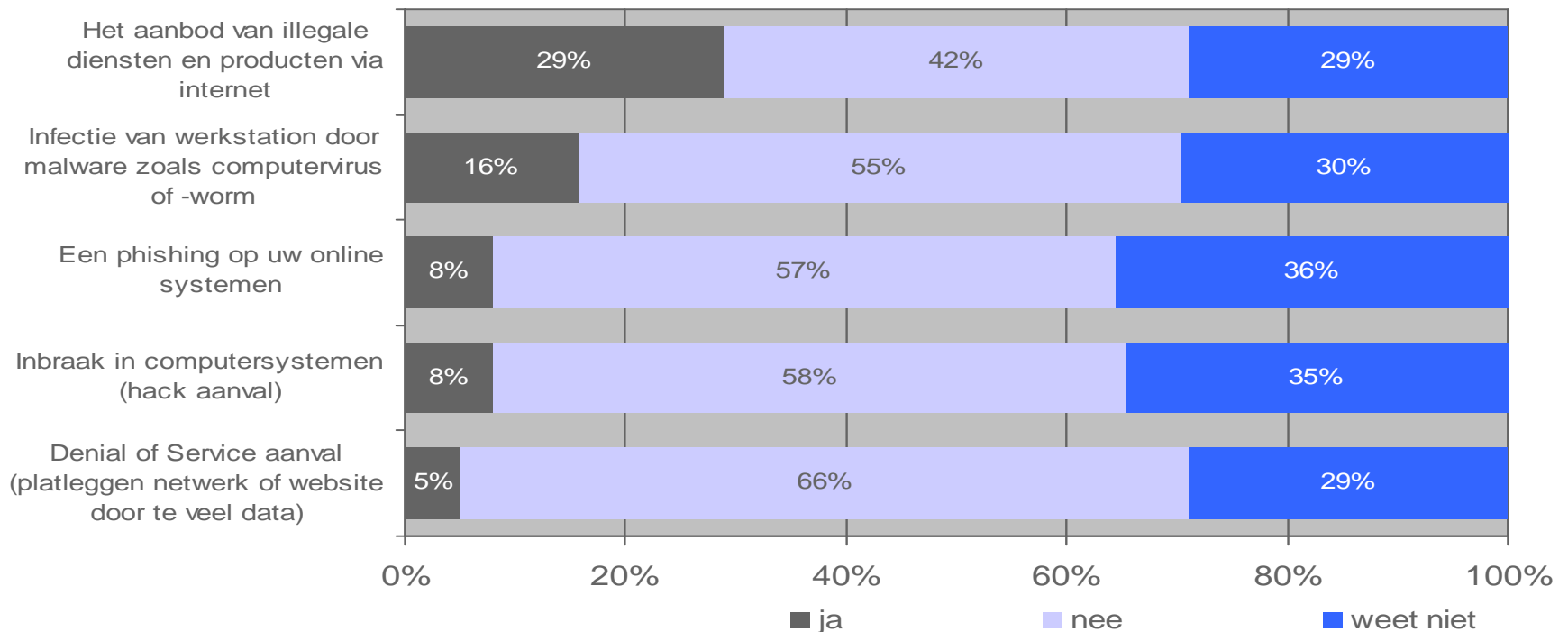
Cybercrime - Vraagpunten

- **Van welke cybercrime activiteiten hebben organisaties last?**
- **Welke nieuwe technieken lijken een veiligheidsrisico met zich mee te brengen?**
- **Welke acties nemen organisaties in het geval van cybercrime? Doet men aangifte of niet?**
- **Is cybercrime met name een interne of externe bedreiging?**
- **Hoeveel vertrouwen heeft men in de beveiliging van de organisatie tegen schade door cybercrime activiteiten?**
- **Welke technische of procedurele maatregelen nemen organisaties om schade door cybercrime te voorkomen of te detecteren ?**
- **Op welke manier zorgen organisaties ervoor dat medewerkers 'beveiligingsbewust' zijn?**
- **Hebben de ondervraagden zelf thuis meer of minder last van cybercrime ten opzichte van een jaar geleden?**

Cybercrime - Afgelopen 12 maanden last van cybercrime

De meest voorkomende cybercrime activiteit is het aanbod van illegale diensten en producten via internet.

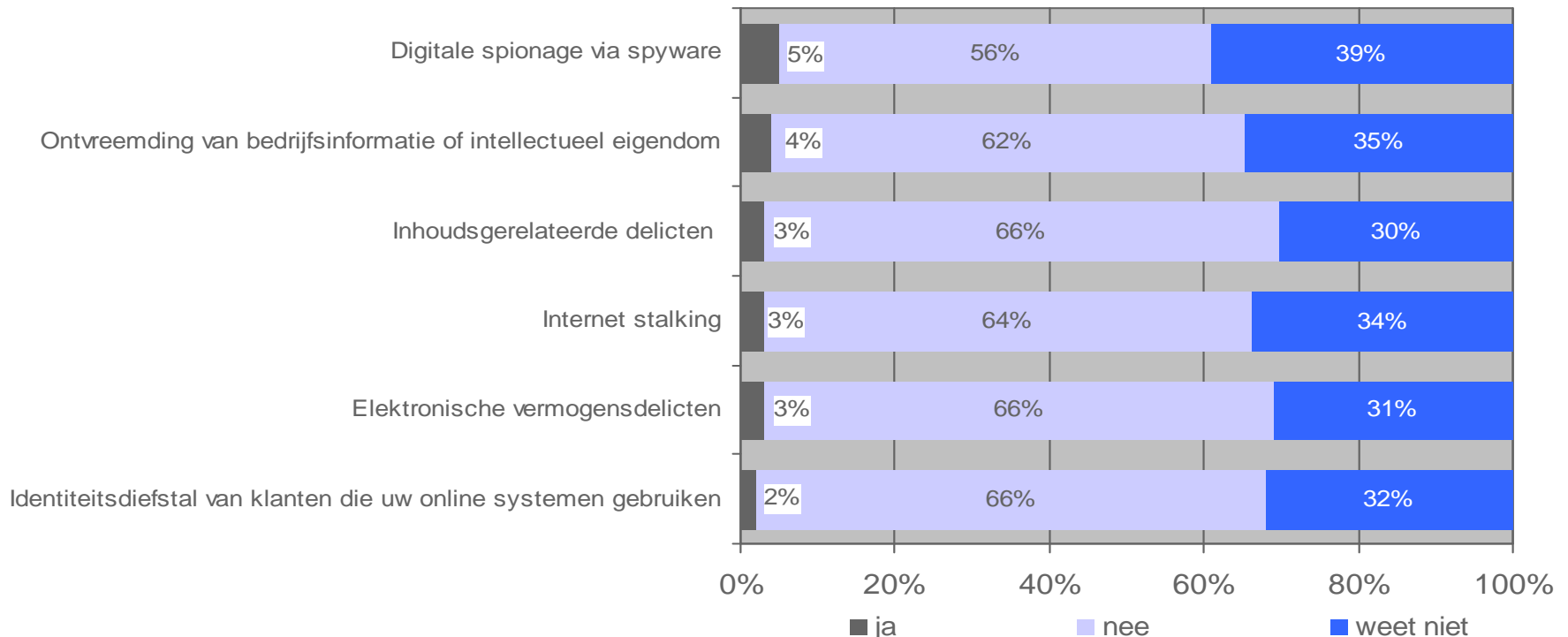
Van welke van de volgende cybercrime activiteiten (of de gevolgen daarvan) heeft uw organisatie in de afgelopen 12 maanden last gehad? (externe dreigingen)



Cybercrime - Afgelopen 12 maanden last van cybercrime

Onderstaande cybercrime activiteiten komen slechts zelden voor. Identiteitsdiefstal van klanten (die online systemen van bedrijven gebruiken), komt vaker voor binnen de handel/distributie sector (9%) dan binnen andere sectoren.

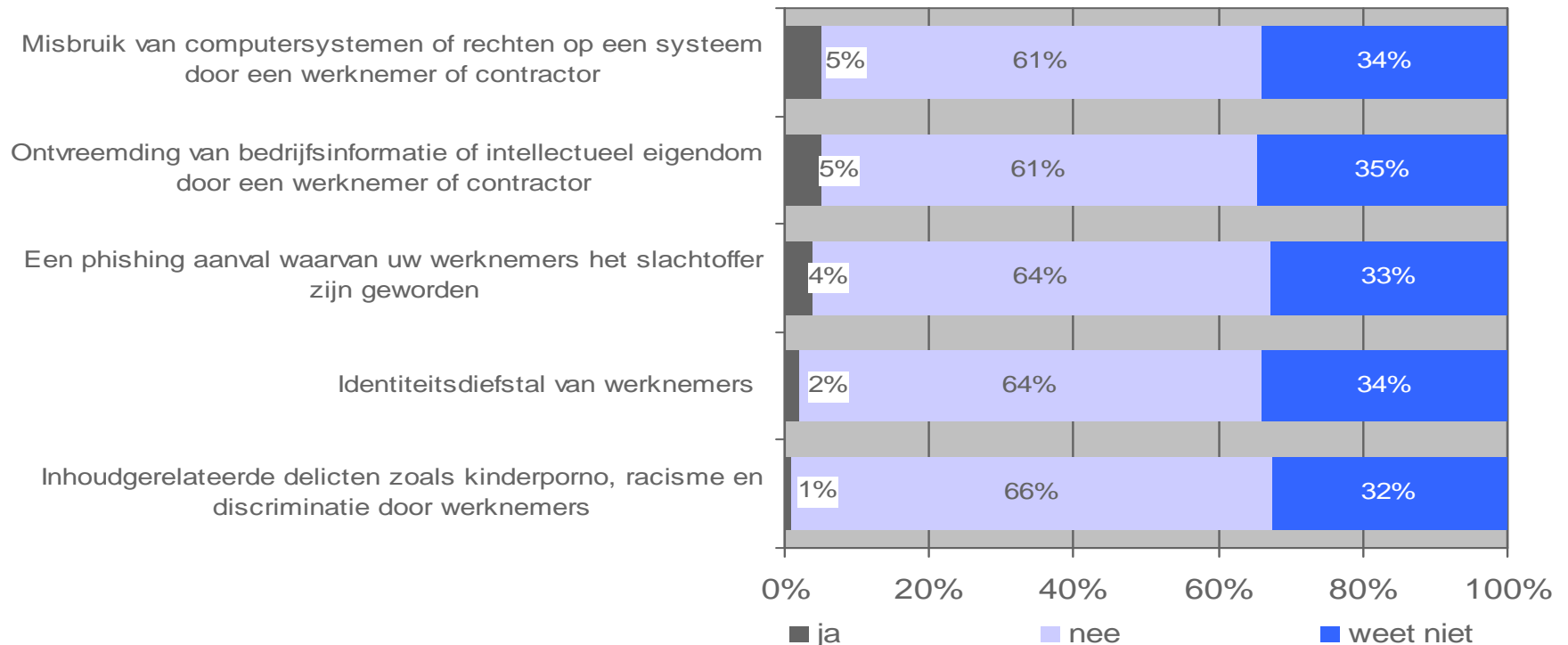
Van welke van de volgende cybercrime activiteiten (of de gevolgen daarvan) heeft uw organisatie in de afgelopen 12 maanden last gehad? (externe dreigingen)



Cybercrime - Afgelopen 12 maanden last van cybercrime

Onderstaande activiteiten hebben betrekking op interne cybercrime (door werknemers) en komen maar weinig voor.

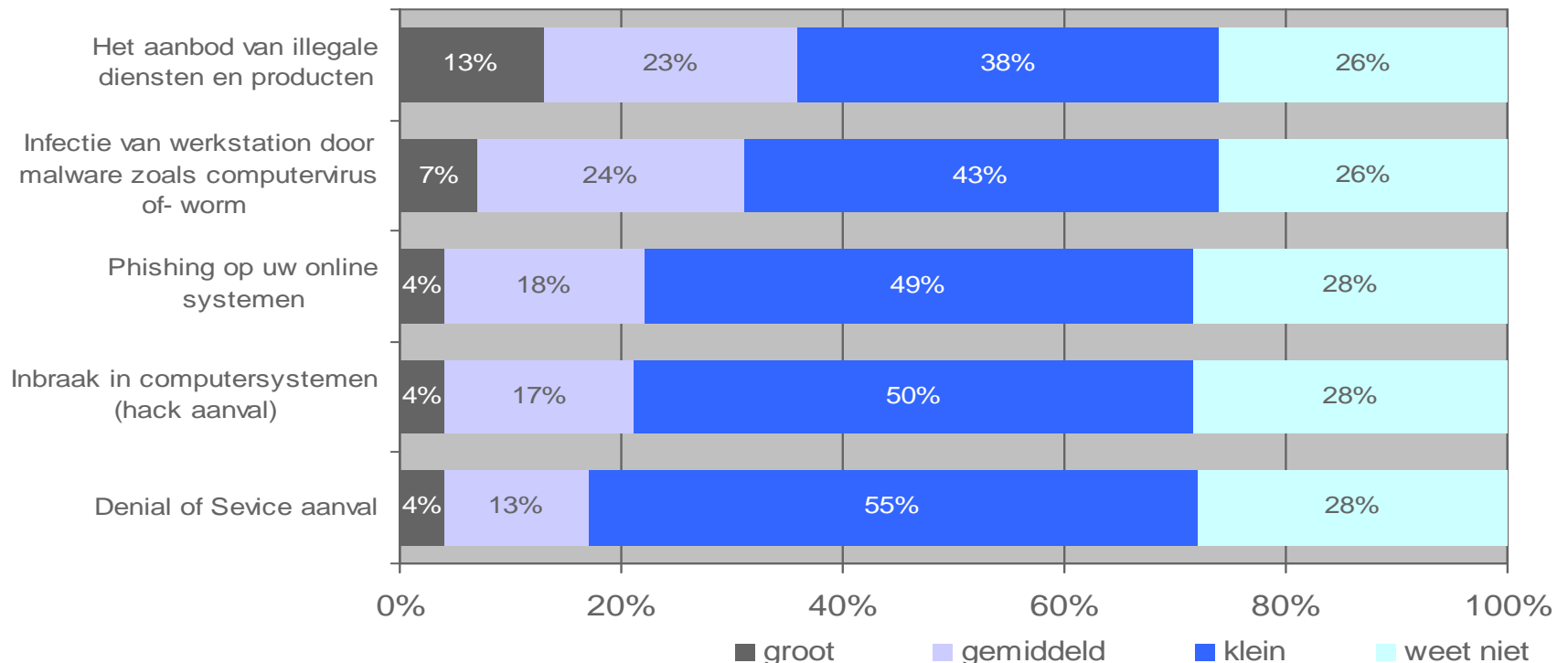
Van welke van de volgende cybercrime activiteiten (of de gevolgen daarvan) heeft uw organisatie in de afgelopen 12 maanden last gehad? (interne dreigingen)



Cybercrime - Kans cybercrime komende 12 maanden

Voor de toekomst verwacht men het meest last te ondervinden van het aanbod van illegale diensten en producten.

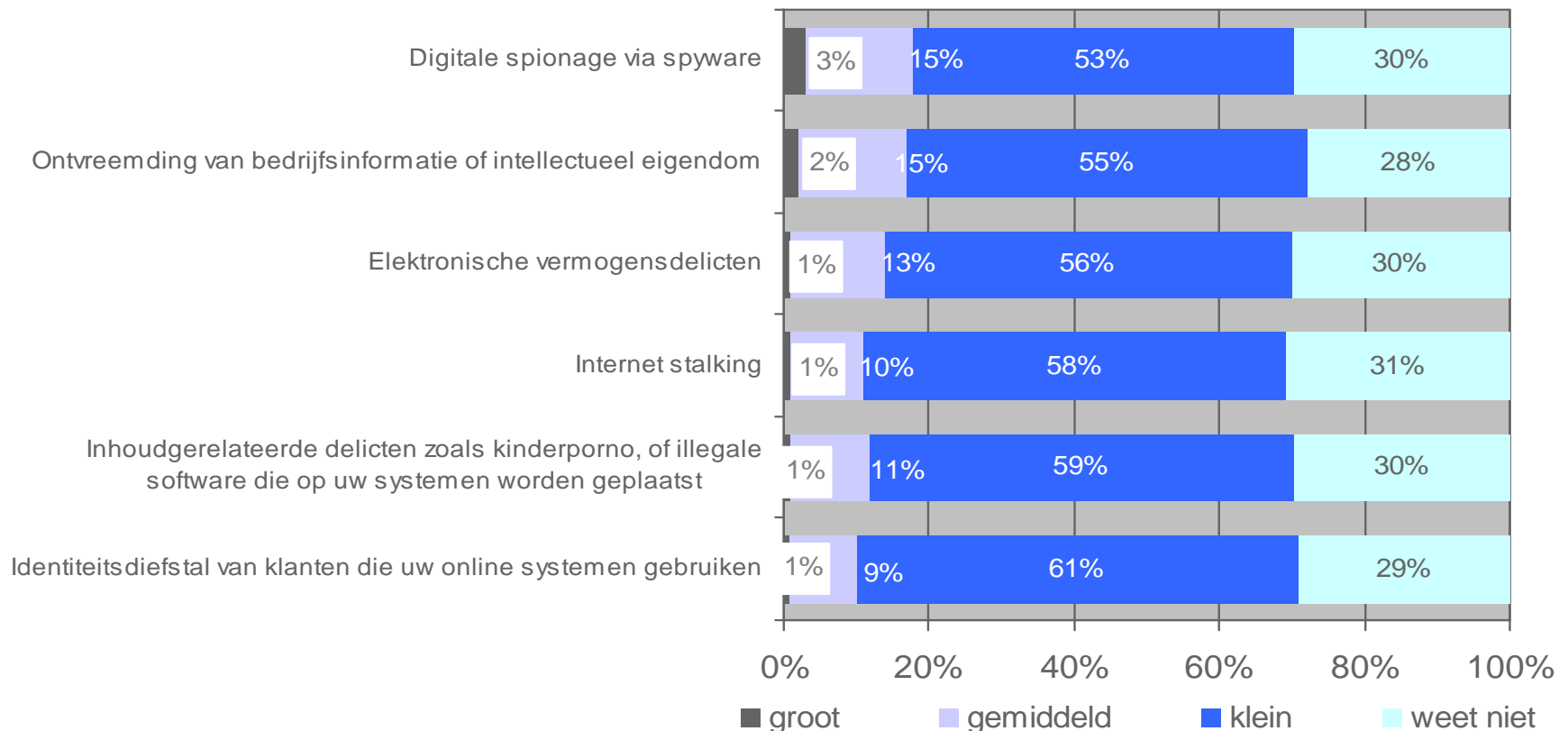
Hoe groot schat u de kans in dat uw organisatie in de komende 12 maanden te maken krijgt met een van de volgende cybercrime activiteiten (of de gevolgen daarvan)? (externe dreigingen)



Cybercrime - Kans cybercrime komende 12 maanden

Onderstaande cybercrime activiteiten komen slechts zelden voor.

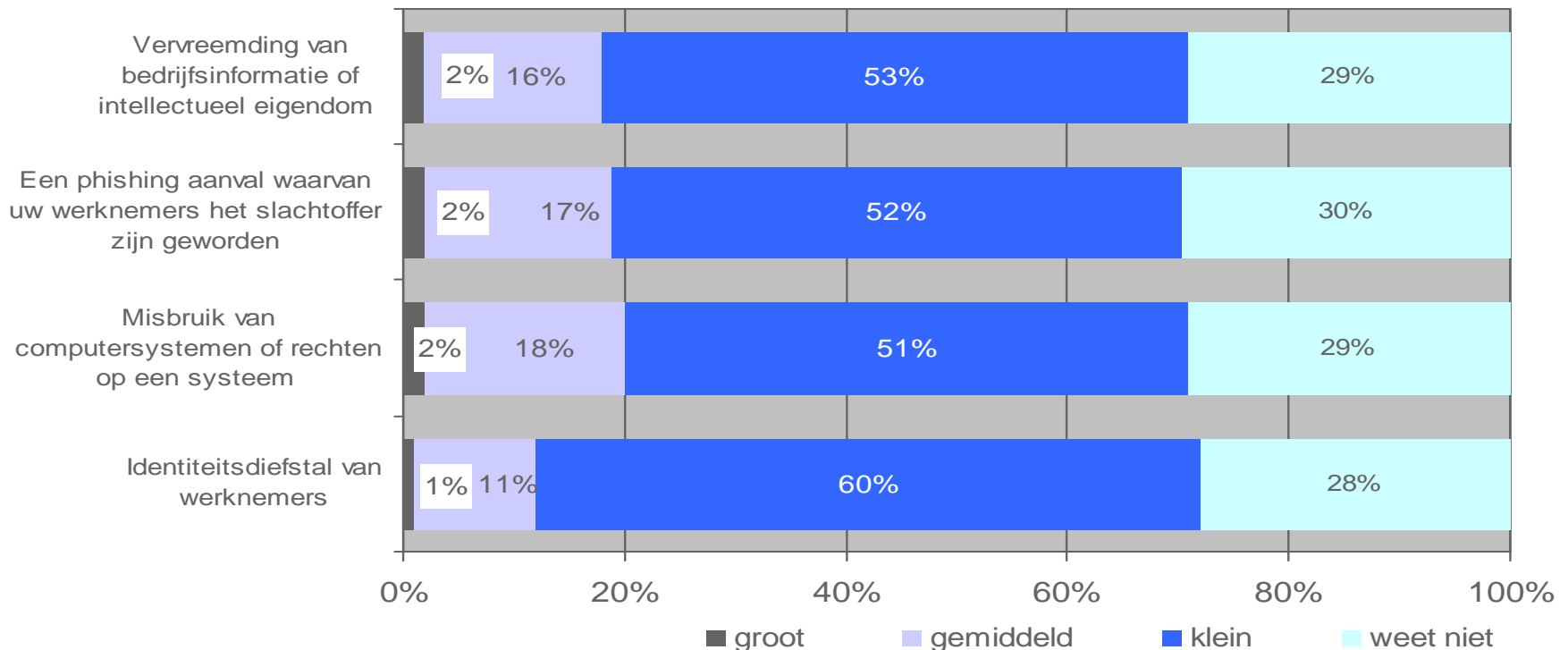
Hoe groot schat u de kans in dat uw organisatie in de komende 12 maanden te maken krijgt met een van de volgende cybercrime activiteiten (of de gevolgen daarvan)? (externe dreigingen)



Cybercrime - Kans cybercrime komende 12 maanden

Organisaties verwachten de komende 12 maanden nauwelijks te maken te krijgen met interne cybercrime (onder werknemers).

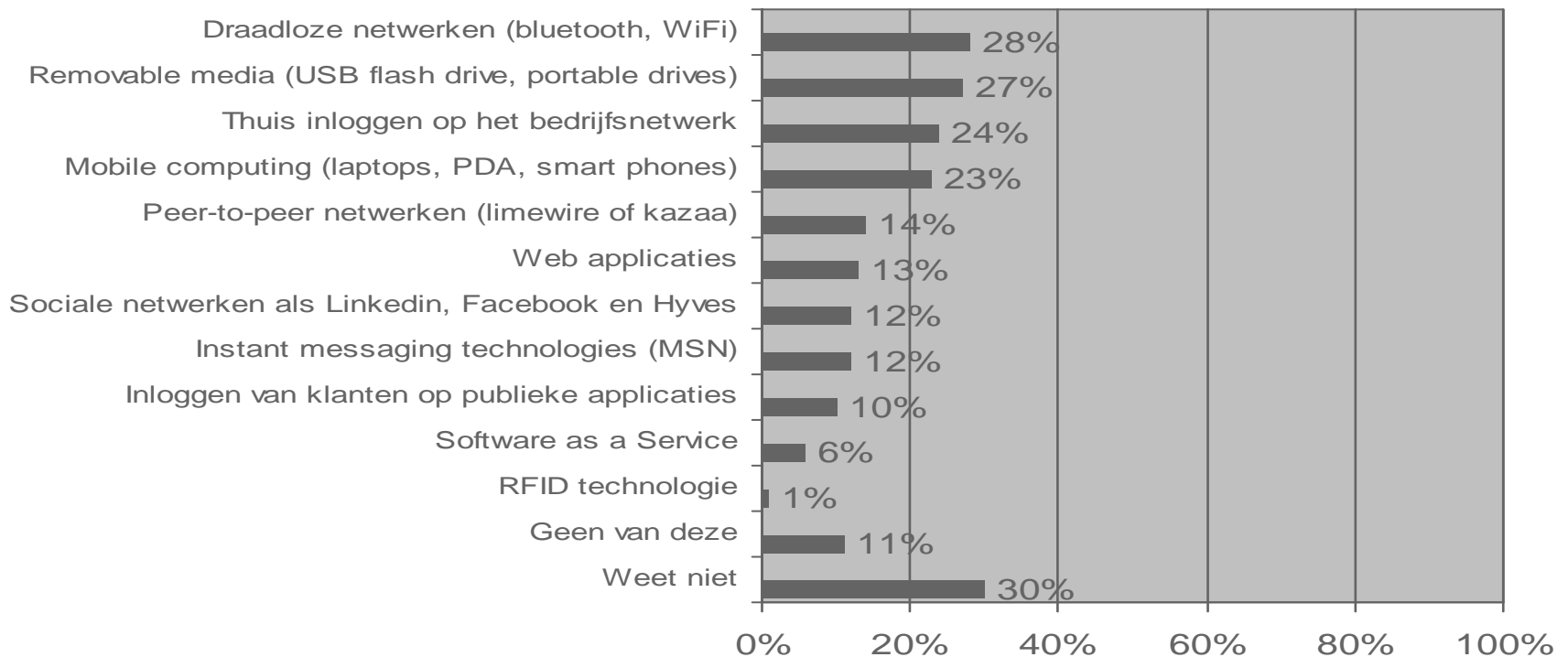
Hoe groot schat u de kans in dat uw organisatie in de komende 12 maanden te maken krijgt met een van de volgende cybercrime activiteiten (of de gevolgen daarvan)? (interne dreigingen)



Cybercrime - Risico nieuwe technologieën

Vanuit beveiligingsoptiek maakt men zich het meeste zorgen over technieken die vooral te maken hebben met het ontsluiten van informatie via nieuwe kanalen.

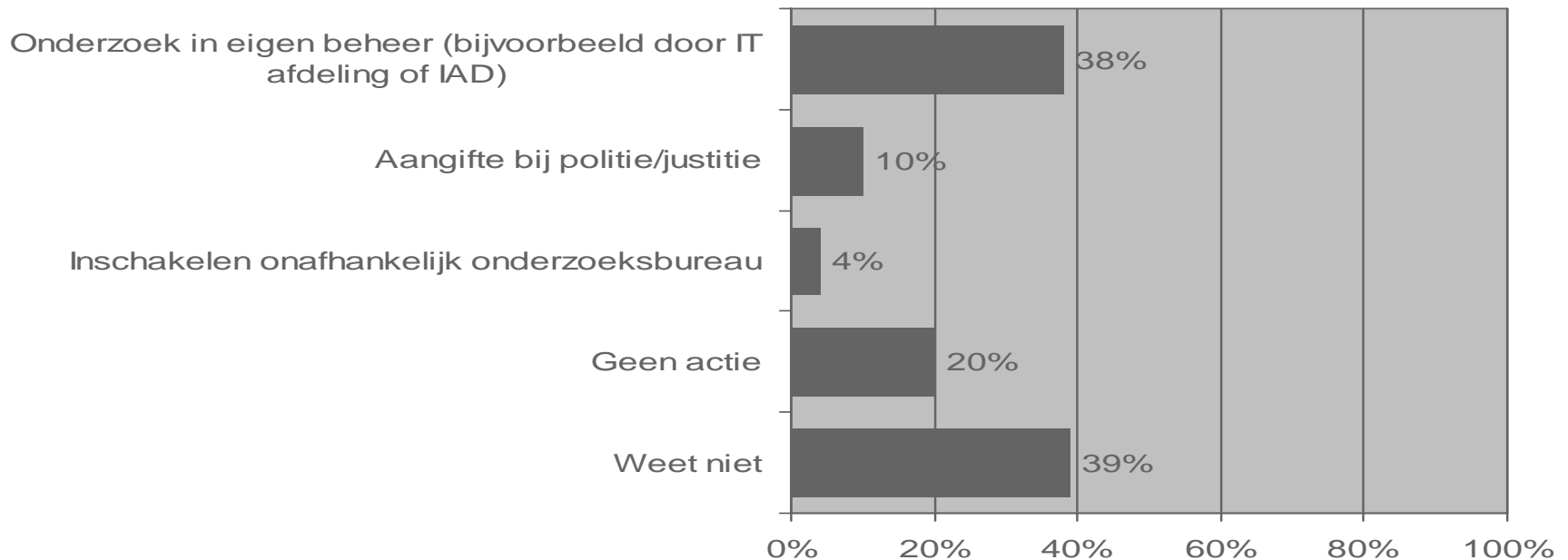
Welke technologieën baren uw organisatie de meeste zorgen vanuit beveiligingsoptiek?



Cybercrime - Actie ondernomen bij cybercrime

Organisaties die het slachtoffer zijn geworden van cybercrime activiteiten beantwoorden dit in de meeste gevallen met een onderzoek in eigen beheer. Slechts een kleine groep doet aangifte bij politie/justitie. Twee op de tien organisaties ondernemen helemaal geen actie. Onder kleine bedrijven (tot 20 werknemers) is dit zelfs vier op de tien.

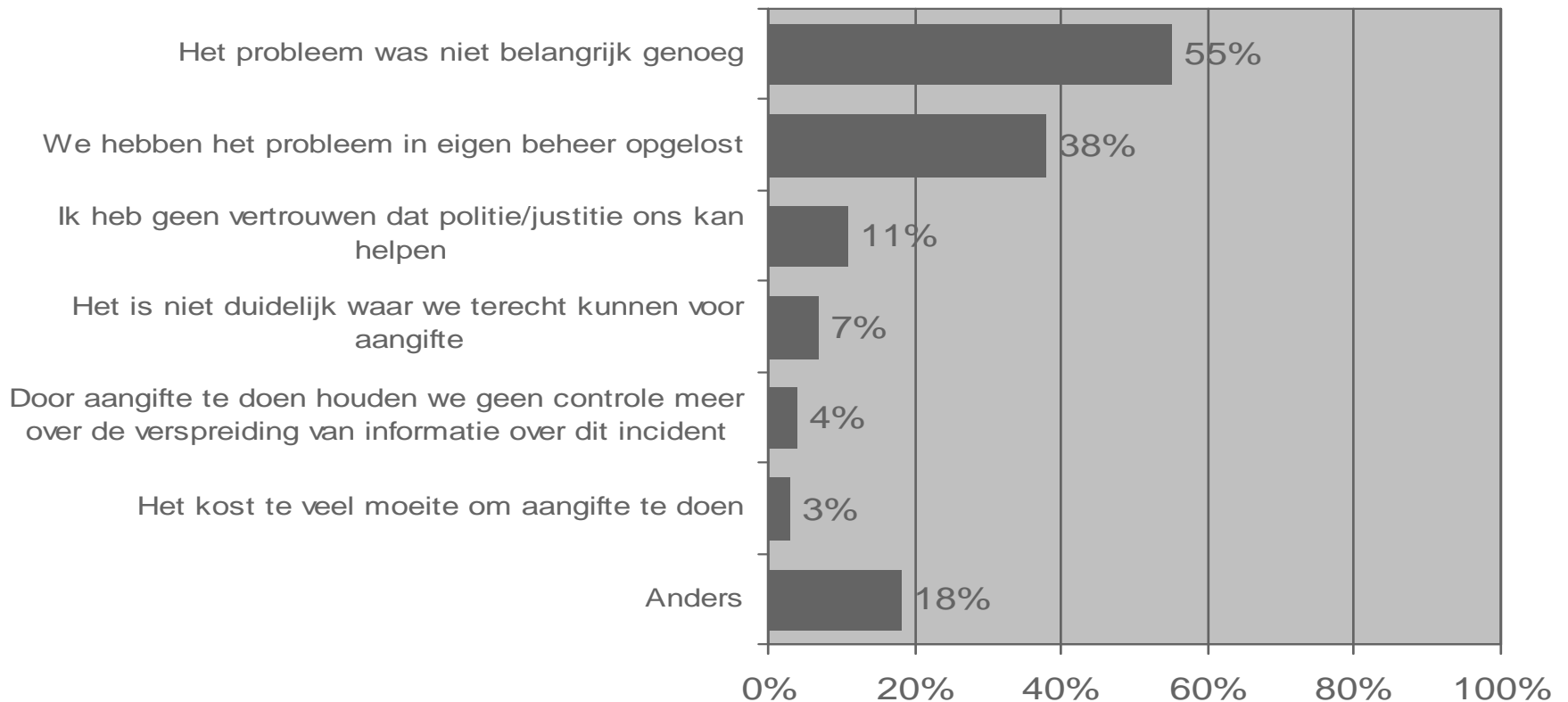
Indien uw organisatie slachtoffer is geworden van cybercrime activiteiten, welke actie heeft uw organisatie daarop ondernomen?



Cybercrime - Redenen voor geen aangifte bij politie/justitie

In de meeste gevallen is er geen aangifte gedaan bij politie/justitie omdat het probleem niet belangrijk genoeg was, of omdat het probleem in eigen beheer is opgelost.

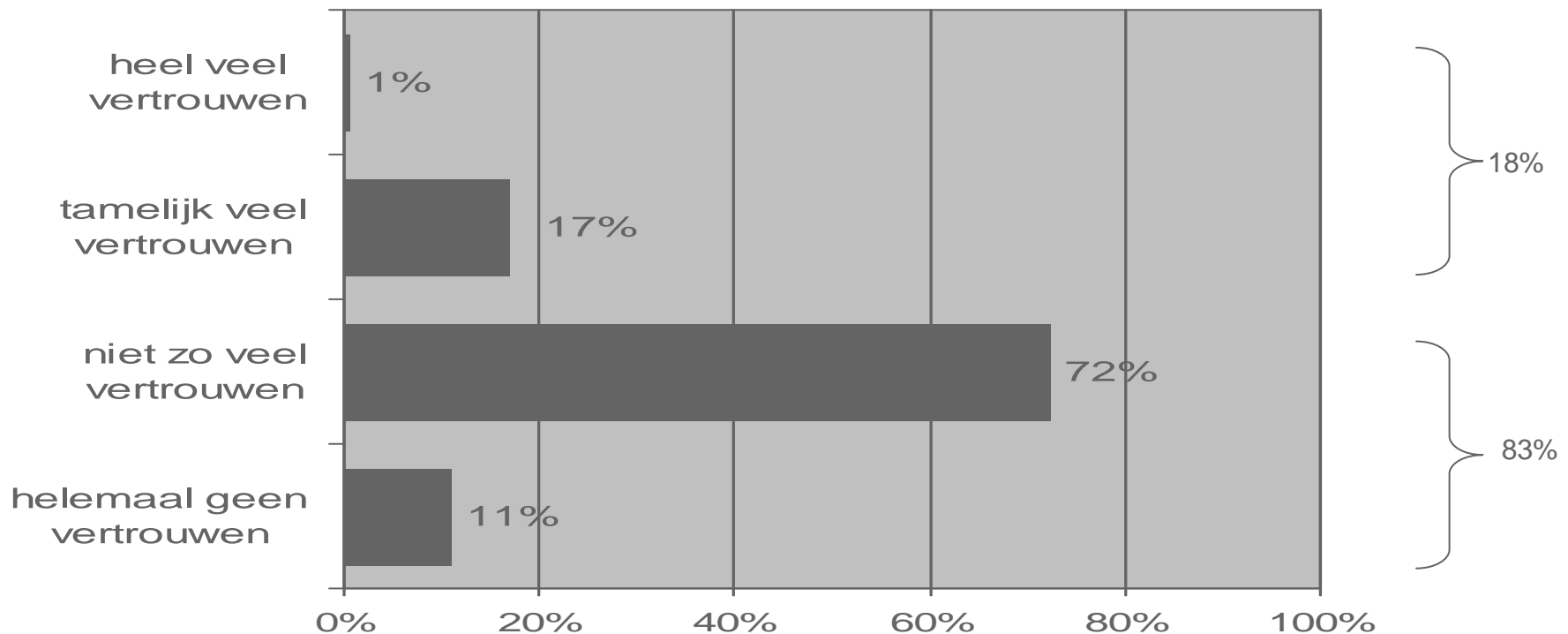
Waarom heeft uw organisatie geen aangifte gedaan van cybercrime bij politie/justitie?



Cybercrime - Vertrouwen in politie/justitie voor wat betreft cybercrime bestrijding

De meeste ondervraagden hebben niet zo veel vertrouwen in de bestrijding van cybercrime door politie/justitie. Dit verklaart mede waarom slechts een beperkt deel aangifte doet.

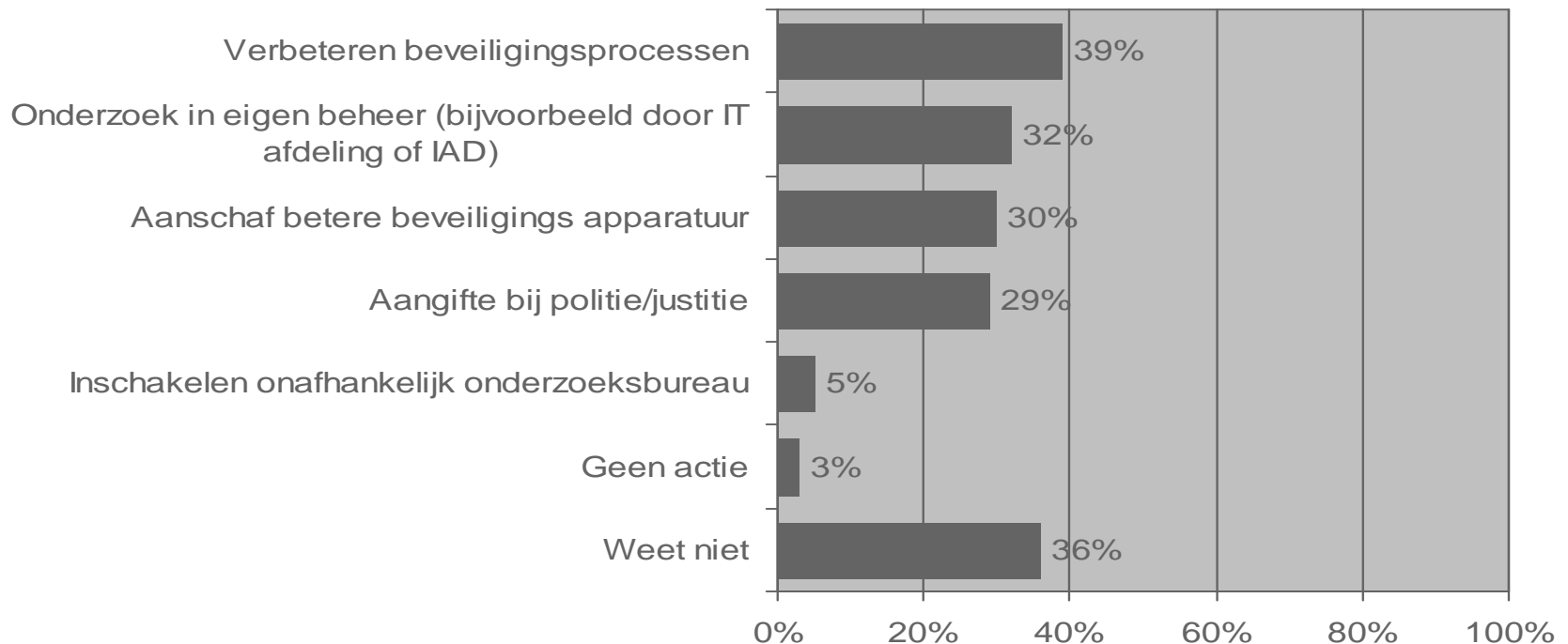
Hoe groot is uw vertrouwen in politie/justitie voor wat betreft cybercrime bestrijding? Heeft u:



Cybercrime - Te ondernemen actie bij cybercrime in toekomst

In het geval van een toekomstige cybercrime activiteit zullen de meeste organisaties hun beveiligingsprocessen verbeteren. Ook een eigen onderzoek starten, betere beveiligingsapparatuur aanschaffen en aangifte bij de politie worden vaak genoemd.

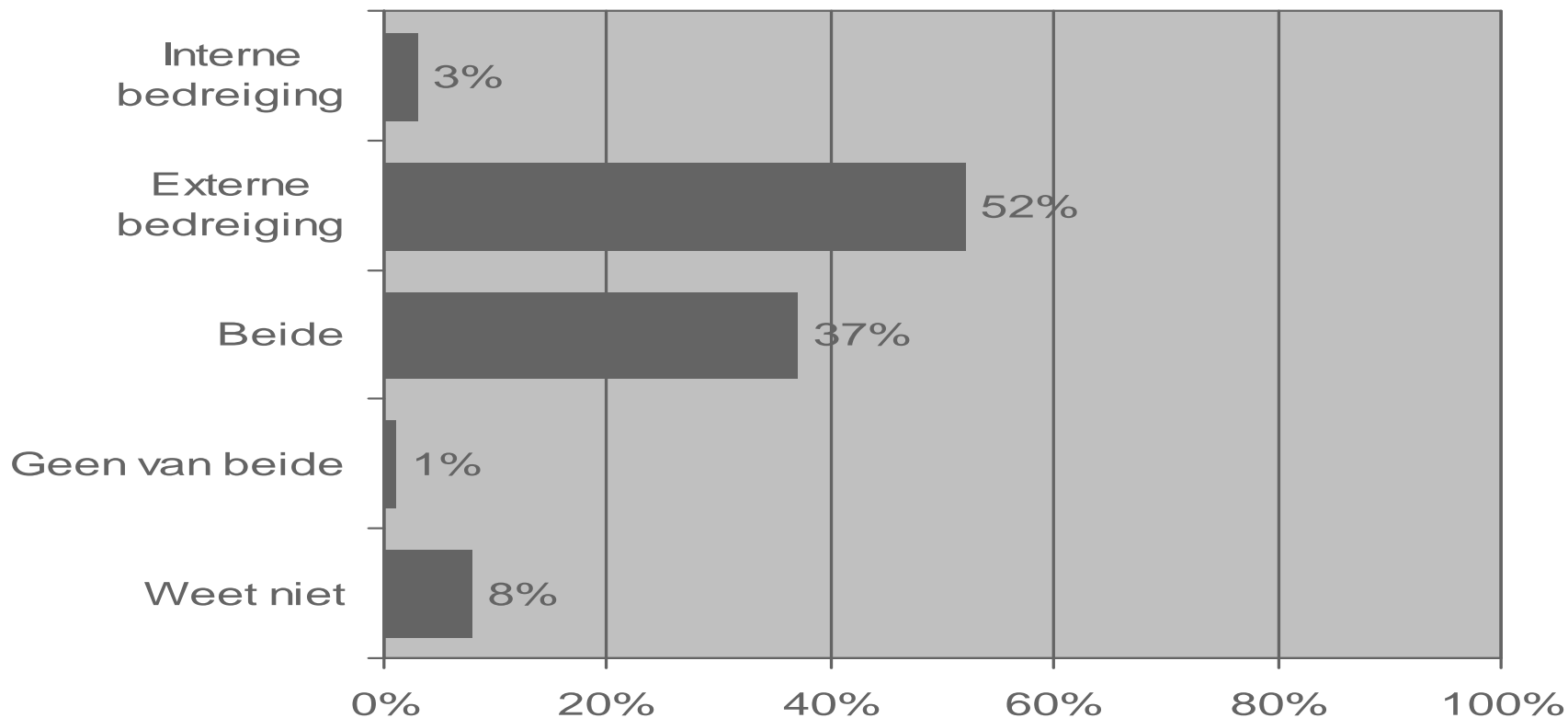
Indien uw organisatie in de toekomst slachtoffer wordt van cybercrime activiteiten, welke actie gaat uw organisatie daarop ondernemen?



Cybercrime - Interne of externe bedreiging

Cybercrime wordt meer gezien als externe bedreiging dan als interne bedreiging. Een deel van de ondervraagden ziet het als een combinatie van beide.

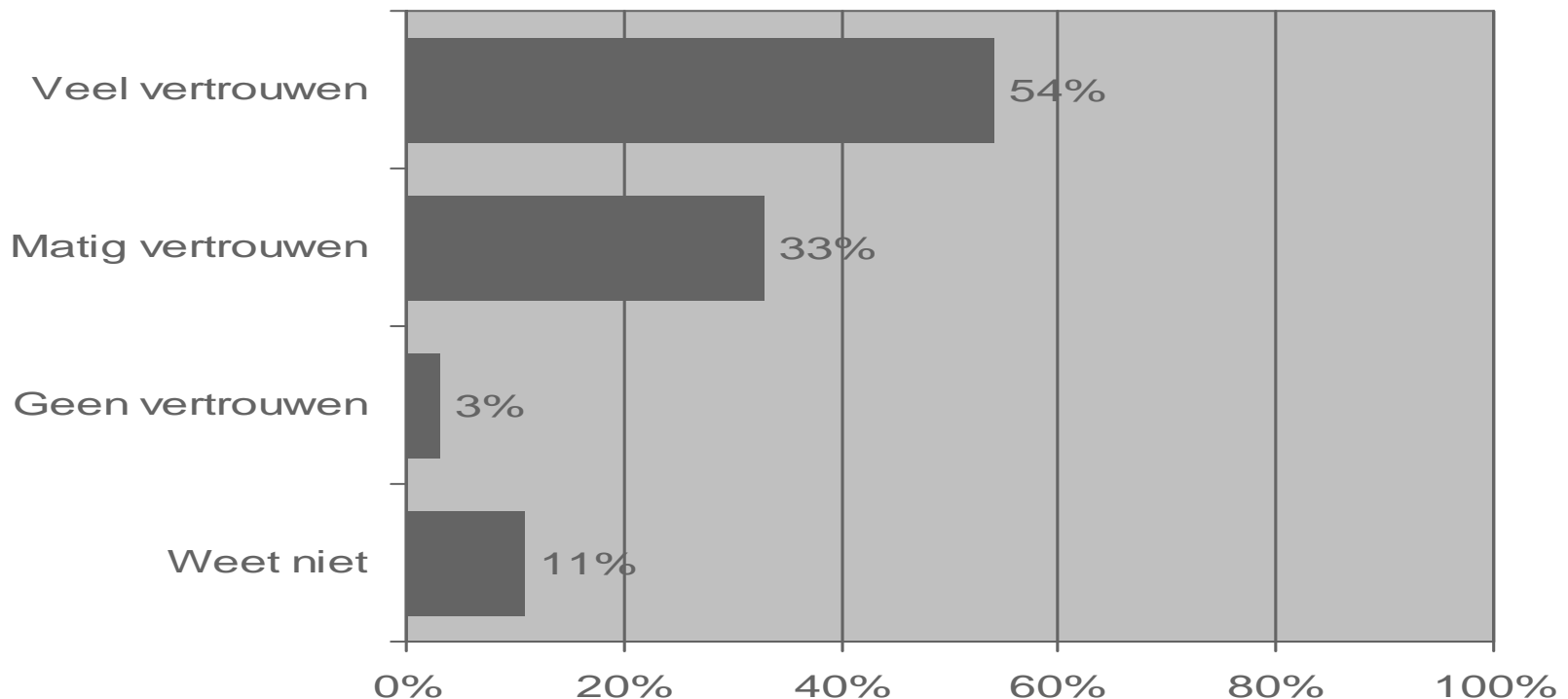
Is cybercrime naar uw mening voornamelijk een interne of externe bedreiging?



Cybercrime - Vertrouwen in beveiliging organisatie

Lang niet iedereen heeft veel vertrouwen in de beveiliging van de organisatie tegen cybercrime. Eén op de drie ondervraagden heeft slechts matig vertrouwen hierin.

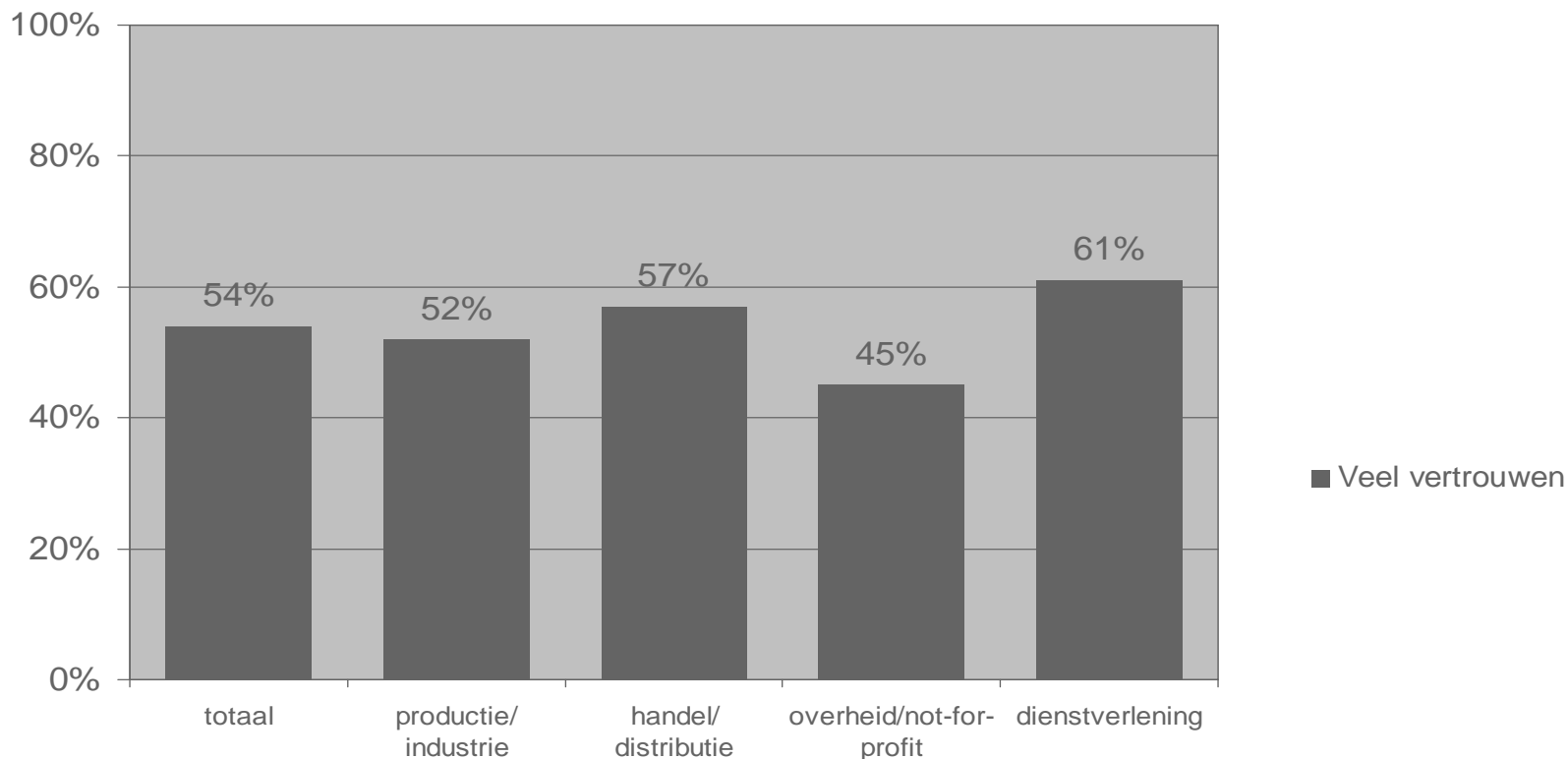
Hoeveel vertrouwen heeft u in de beveiliging van uw organisatie tegen schade door cybercrime activiteiten?



Cybercrime - Vertrouwen in beveiliging organisatie

Binnen de overheid/ not-for-profit sector heeft men minder vertrouwen in de beveiliging van hun organisatie tegen cybercrime dan binnen de overige sectoren.

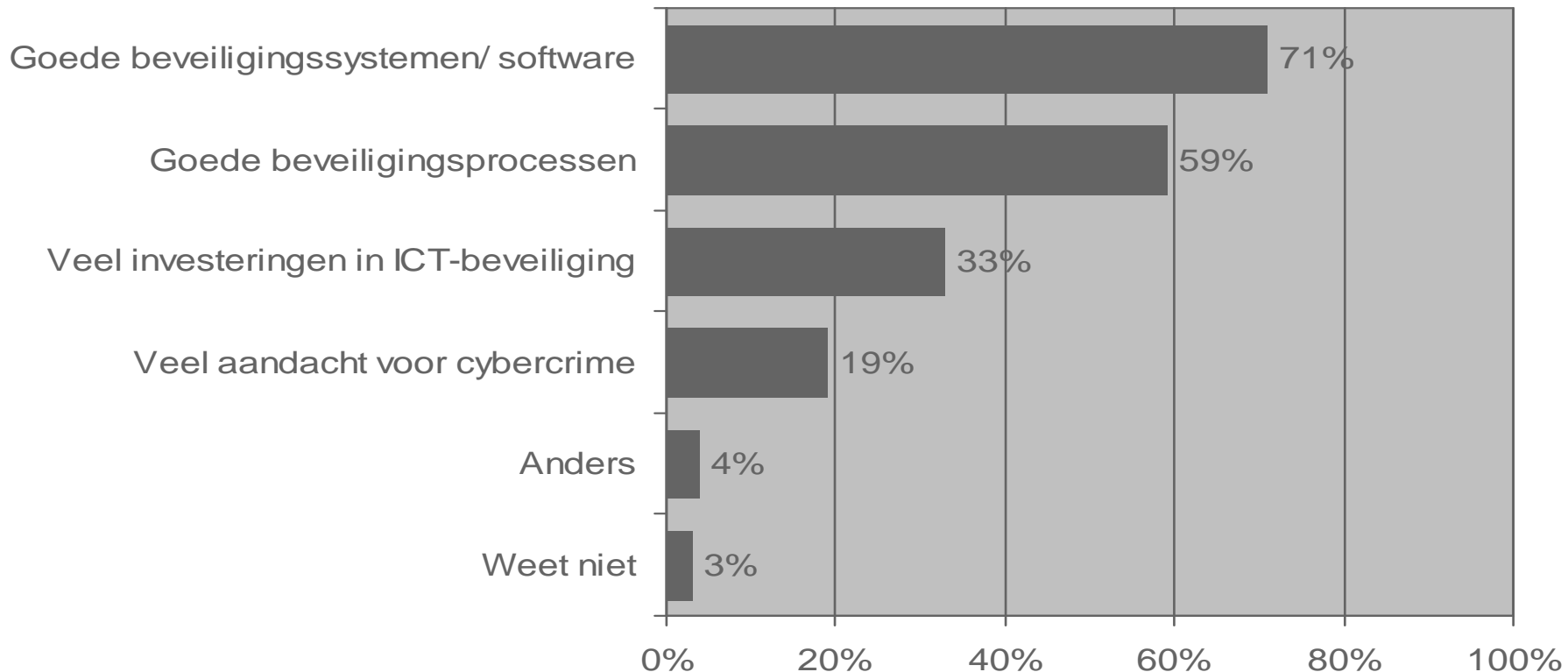
Hoeveel vertrouwen heeft u in de beveiliging van uw organisatie tegen schade door cybercrime activiteiten?



Cybercrime - Redenen voor veel vertrouwen in de beveiliging tegen cybercrime

De voornaamste reden dat men veel vertrouwen heeft in de beveiliging tegen cybercrime, is de aanwezigheid van goede beveiligingssystemen en -processen. Met name ICT'ers (78%) noemen goede beveiligingssystemen als reden.

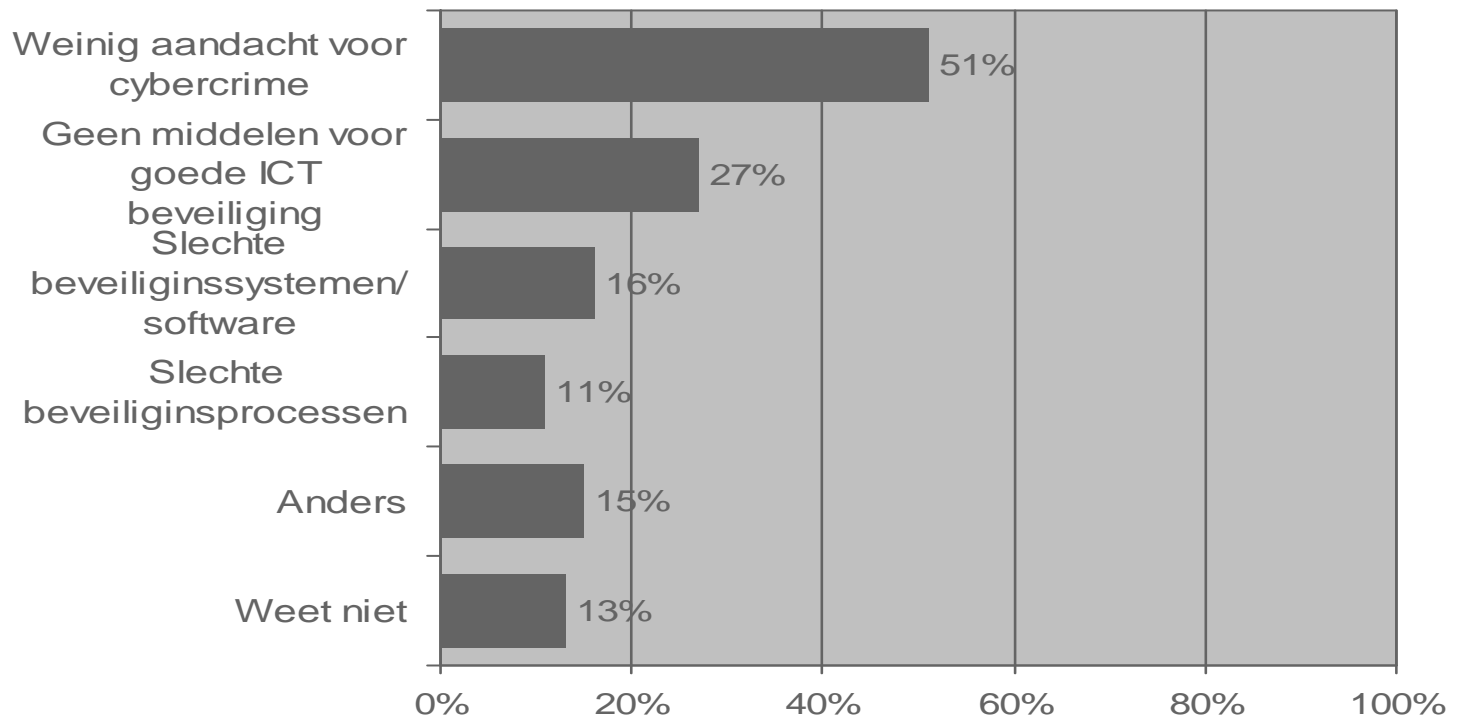
Waarom heeft u veel vertrouwen in de beveiliging van uw organisatie tegen schade door cybercrime activiteiten?



Cybercrime - Redenen geen/ weinig vertrouwen in beveiliging

Degenen die maar matig vertrouwen hebben in de beveiliging geven aan dat de organisatie te weinig aandacht heeft voor cybercrime of onvoldoende middelen heeft voor goede beveiligingssystemen.

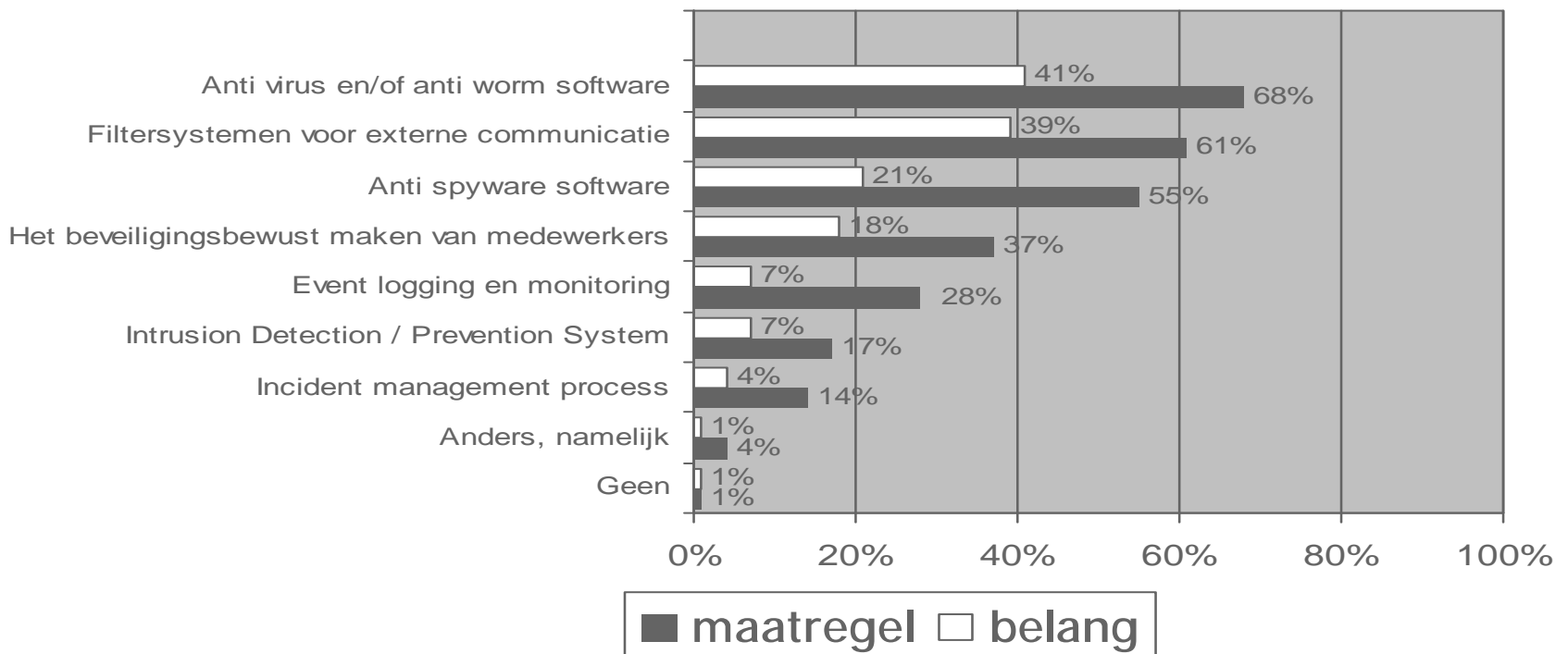
Waarom heeft u geen/weinig vertrouwen in de beveiliging van uw organisatie tegen schade door cybercrime activiteiten?



Cybercrime - Technische maatregelen

De meest voorkomende technische maatregelen tegen cybercrime zijn anti virus en/of anti worm software, de filtersystemen voor externe communicatie (zoals firewalls, proxies, mail relays, content scanners) en anti spyware software.

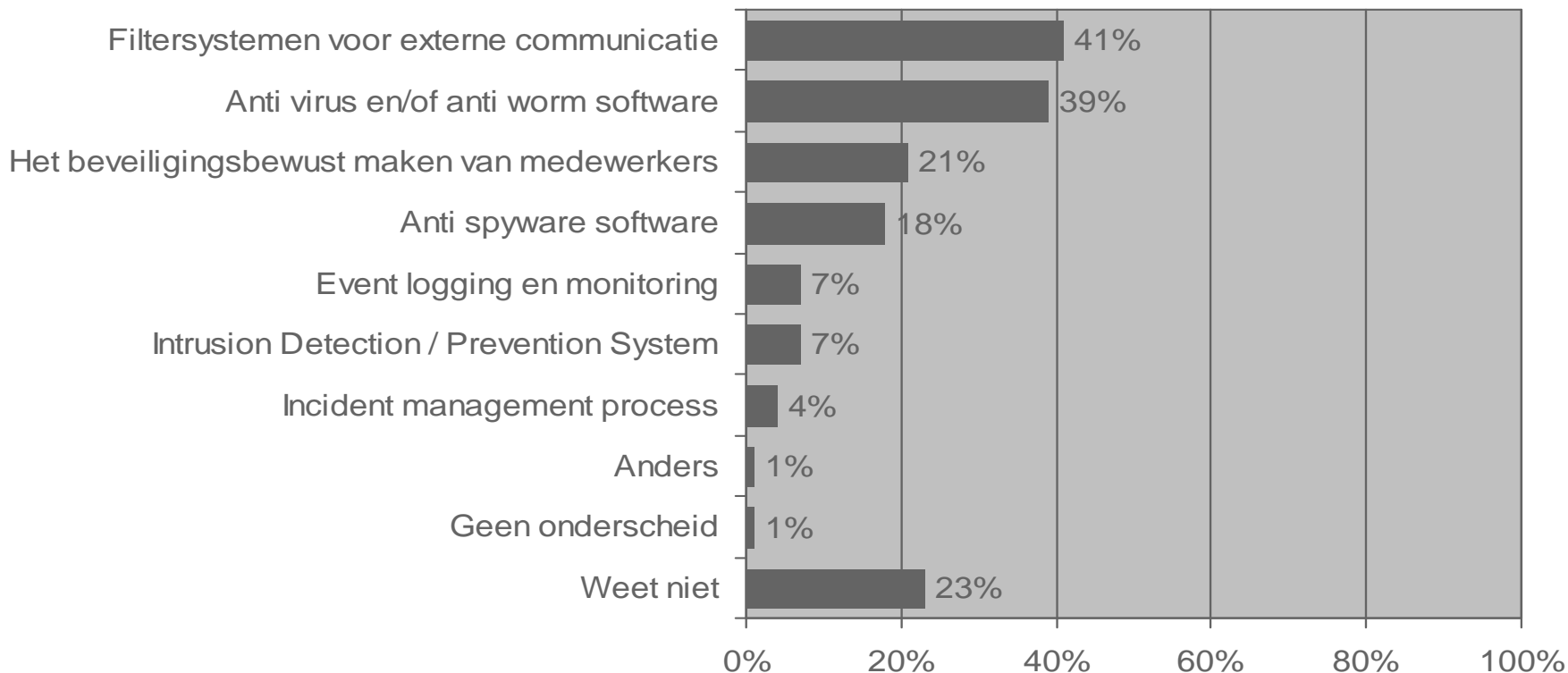
Welke technische of procedurele maatregelen heeft uw organisatie getroffen om schade door cybercrime activiteiten te voorkomen of te detecteren en welke belang hecht u aan deze maatregel.



Cybercrime - Technische maatregelen

De filtersystemen voor externe communicatie (zoals firewalls, proxies, mail relays, content scanners) en anti virus en/of anti worm software worden gezien als de belangrijkste technische maatregelen tegen cybercrime.

Welke van deze technische of procedurele maatregelen vindt u het belangrijkste?



Cybercrime - Medewerkers beveiligingsbewust

Er zijn verschillende manieren waarop organisaties ervoor zorgen dat medewerkers 'beveiligingsbewust' zijn. In de meeste gevallen gaat het daarbij om het informeren van de medewerkers. Dit gebeurt meer binnen grote organisaties dan binnen kleine bedrijven.

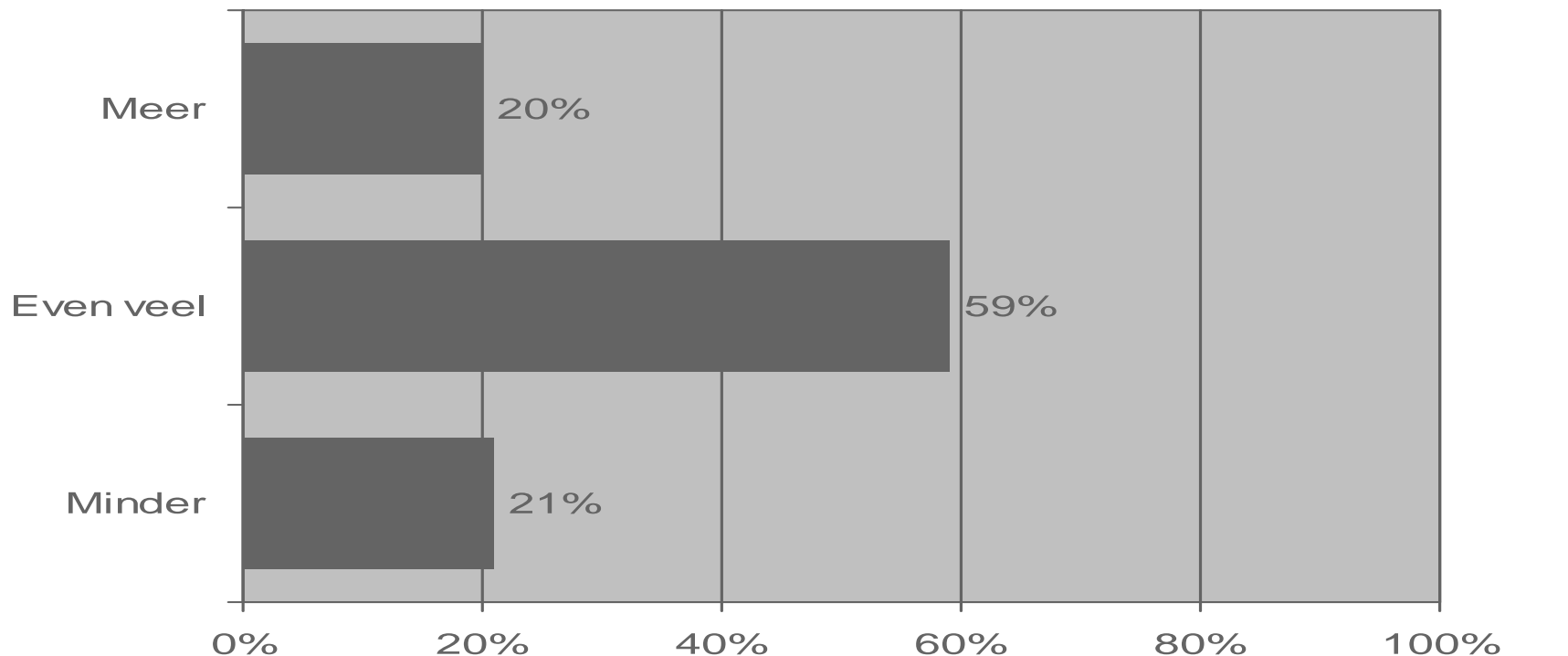
Op welke manier zorgt uw organisatie ervoor dat medewerkers 'beveiligingsbewust' zijn?



Cybercrime - Thuis last van cybercrime

De overlast van cybercrime thuis is per saldo gelijk aan vorig jaar.

Heeft u zelf thuis meer of minder last van cybercrime ten opzichte van een jaar geleden?



Cybercrime - Samenvatting (1/2)

- De meest voorkomende vormen van cybercrime zijn het aanbieden van illegale diensten en producten via internet en (in mindere mate) de verspreiding van virussen/wormen. Ook in de toekomst verwacht men vooral last te krijgen van het aanbod van illegale diensten en producten. Van interne cybercrime activiteiten hebben en verwachten organisaties weinig last.
- Nieuwe technologieën die een risico vormen voor de veiligheid zijn vooral draadloze netwerken (zoals Bluetooth en Wifi), removable media (zoals USB flash drives en portables drives), thuis inloggen op het bedrijfsnetwerk en mobile computing (laptops, PDA, smart phones).
- Bij cybercrime starten de meeste organisaties een onderzoek in eigen beheer. Kleine bedrijven ondernemen in veel gevallen helemaal geen actie. De groep die aangifte doet bij politie/justitie is klein. Ook het vertrouwen in de politie/justitie als bestrijders van cybercrime is niet zo groot.
- Bij cybercrime in de toekomst, zullen organisaties onder andere de beveiligingsprocessen verbeteren of een onderzoek starten in eigen beheer.

Cybercrime - Samenvatting (2/2)

- **Cybercrime wordt met name gezien als een externe bedreiging, maar ook als een combinatie van een interne en een externe dreiging.**
- **Vrijwel alle organisaties hebben technische maatregelen getroffen om schade door cybercrime te voorkomen, zoals anti virus en/of anti worm software en filtersystemen voor externe communicatie.**
- **Ondanks al deze maatregelen hebben vier op de tien ondervraagden niet veel vertrouwen in de beveiliging van de organisatie tegen cybercrime. Deze groep geeft aan dat de organisatie te weinig aandacht heeft voor cybercrime of over onvoldoende middelen beschikt voor goede beveiligingssystemen.**



ICT Barometer over ICT- beveiliging en cybercrime

End slide