

Onderzoekresultaten ICT Barometer over cybercrime

Jaargang 10
24 februari 2010

 **ERNST & YOUNG**
Quality In Everything We Do

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. De ondervraagde groep wordt online geënquêteerd.

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.

Ernst & Young Nederland LLP is een limited liability partnership naar het recht van Engeland en Wales met registratienummer OC335595. Ernst & Young Nederland LLP is statutair gevestigd te Lambeth Palace Road 1, London SE1 7EU, Verenigd Koninkrijk, heeft haar hoofdvestiging aan Boompjes 258, 3011 XZ Rotterdam, Nederland en is geregistreerd bij de Kamer van Koophandel Rotterdam onder nummer 24432942 bijbehorende disclaimer.

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.

Amsterdam, 24 februari 2010

Ernst & Young Nederland LLP

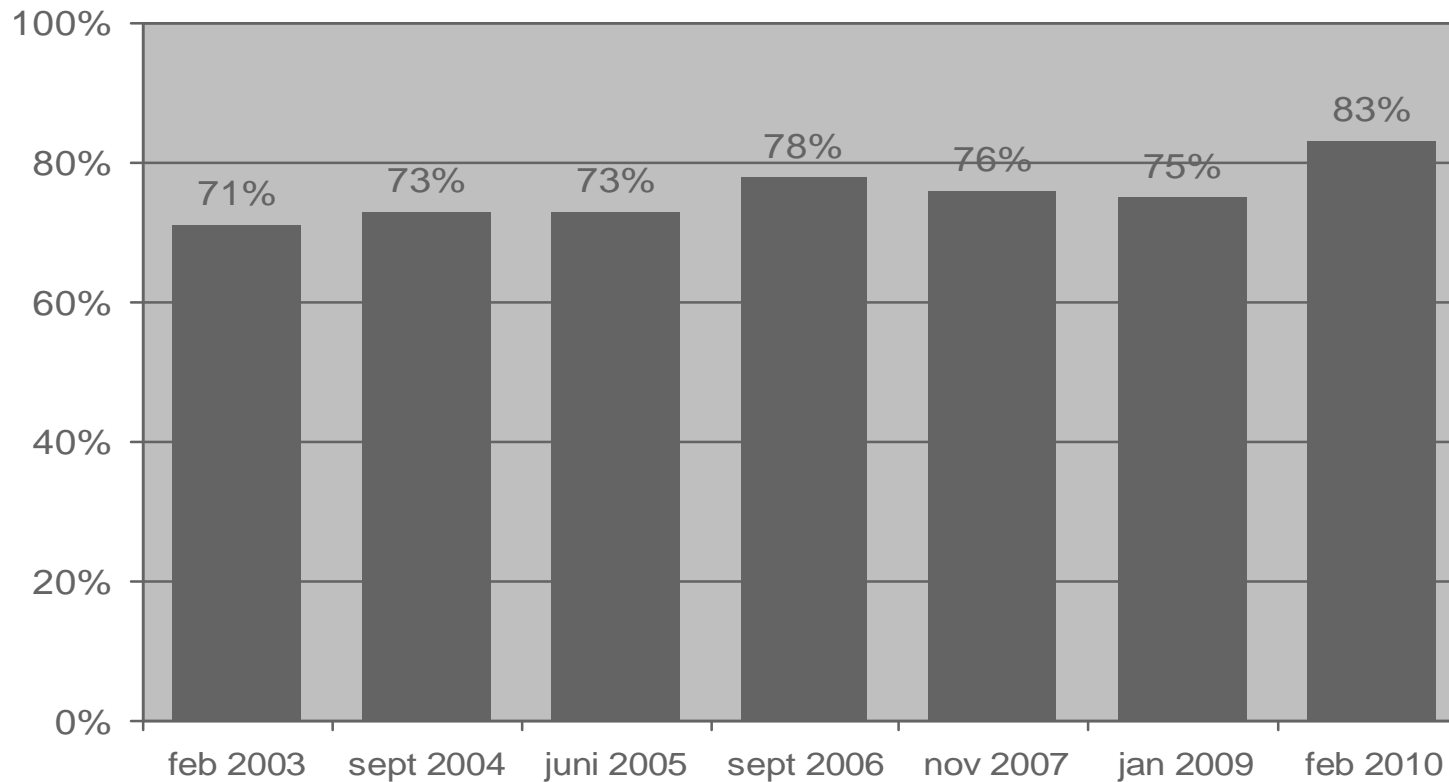
Vraagpunten over cybercrime

- Hoe afhankelijk zijn organisaties van ICT?
- Welke maatregelen neemt de organisatie om ICT te beveiligen?
- Hoe staat het met de bestedingen voor ICT-beveiliging?
- Van welke cybercrime activiteiten hebben organisaties last?
- Welke acties nemen organisaties in het geval van cybercrime?
- Welke nieuwe technieken lijken een veiligheidsrisico met zich mee te brengen?
- Zijn de geënquêteerden voldoende geïnformeerd over de gevaren van cybercrime?
- Welke maatregelen nemen organisaties om schade door cybercrime voorkomen?
- Hebben de ondervraagden vertrouwen in de eigen ICT-beveiliging?

ICT-beveiliging - Afhankelijkheid van ICT

- *De afhankelijkheid van ICT neemt steeds verder toe.*

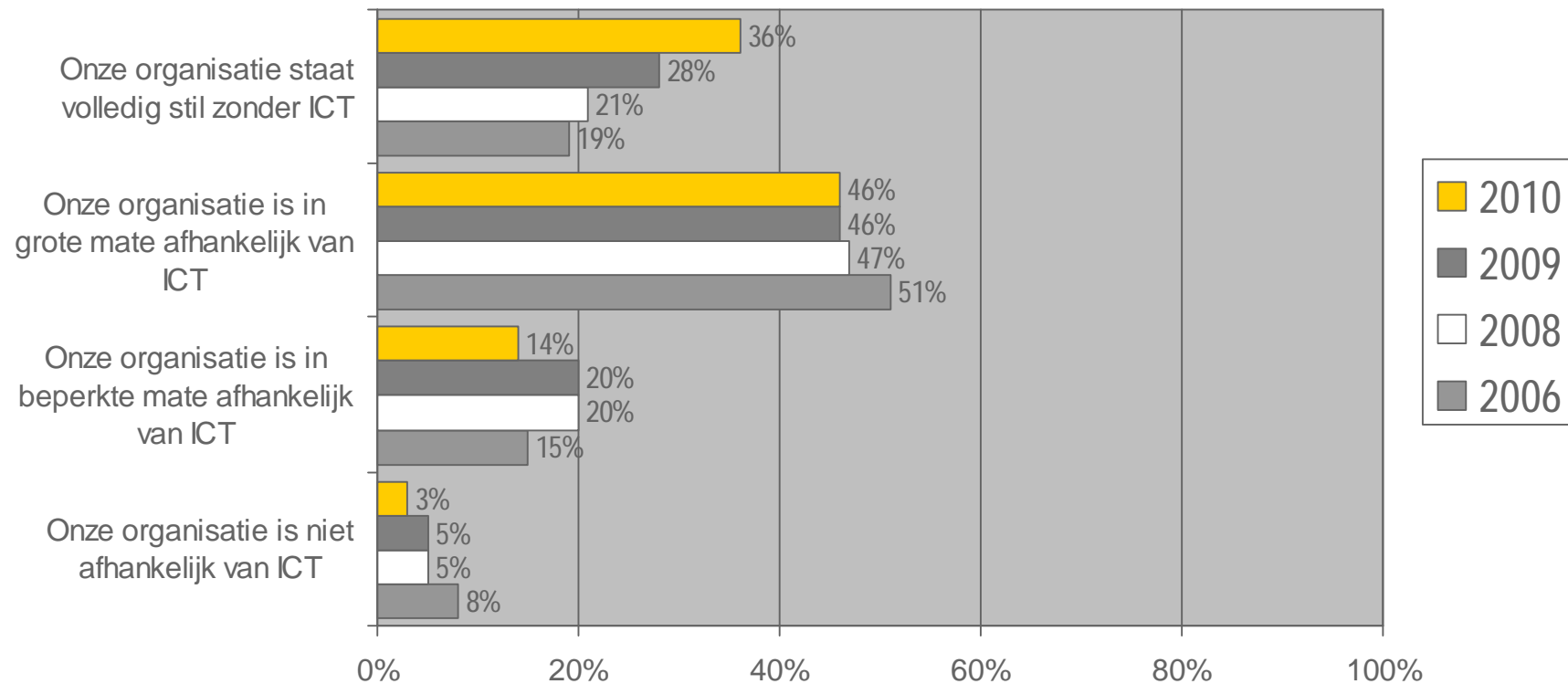
Bedrijfsprocessen in (zeer) grote mate afhankelijk van ICT



Afhankelijkheid van ICT

Ruim eenderde (36%) van alle bedrijven/organisaties staat in 2010 volledig stil zonder ICT. In 2006 was dat nog 19%.

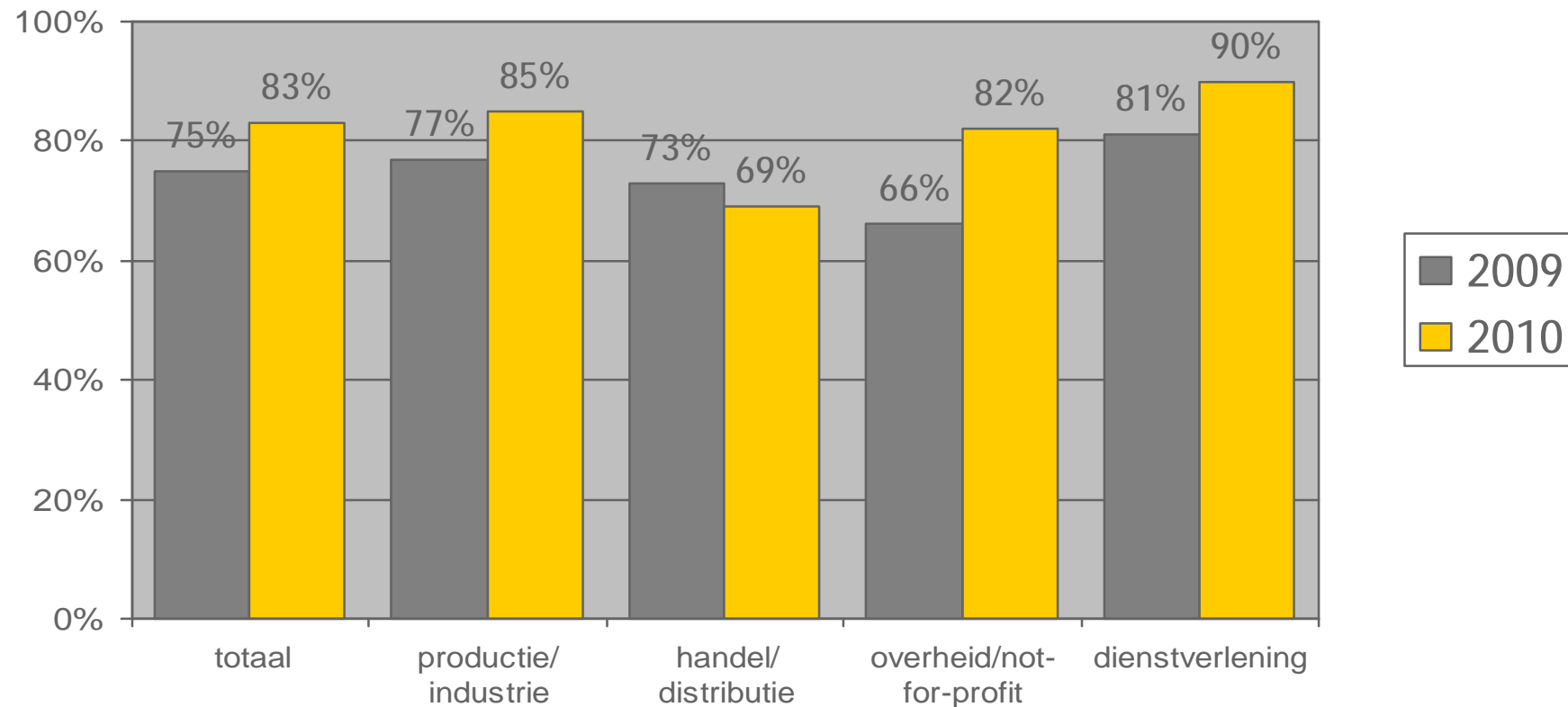
Hoe belangrijk is ICT voor uw organisatie?



Afhankelijkheid van ICT in de sectoren

De afhankelijkheid van ICT is relatief groot onder dienstverlenende bedrijven. In de handel/distributie sectoren is men iets minder sterk afhankelijk van ICT.

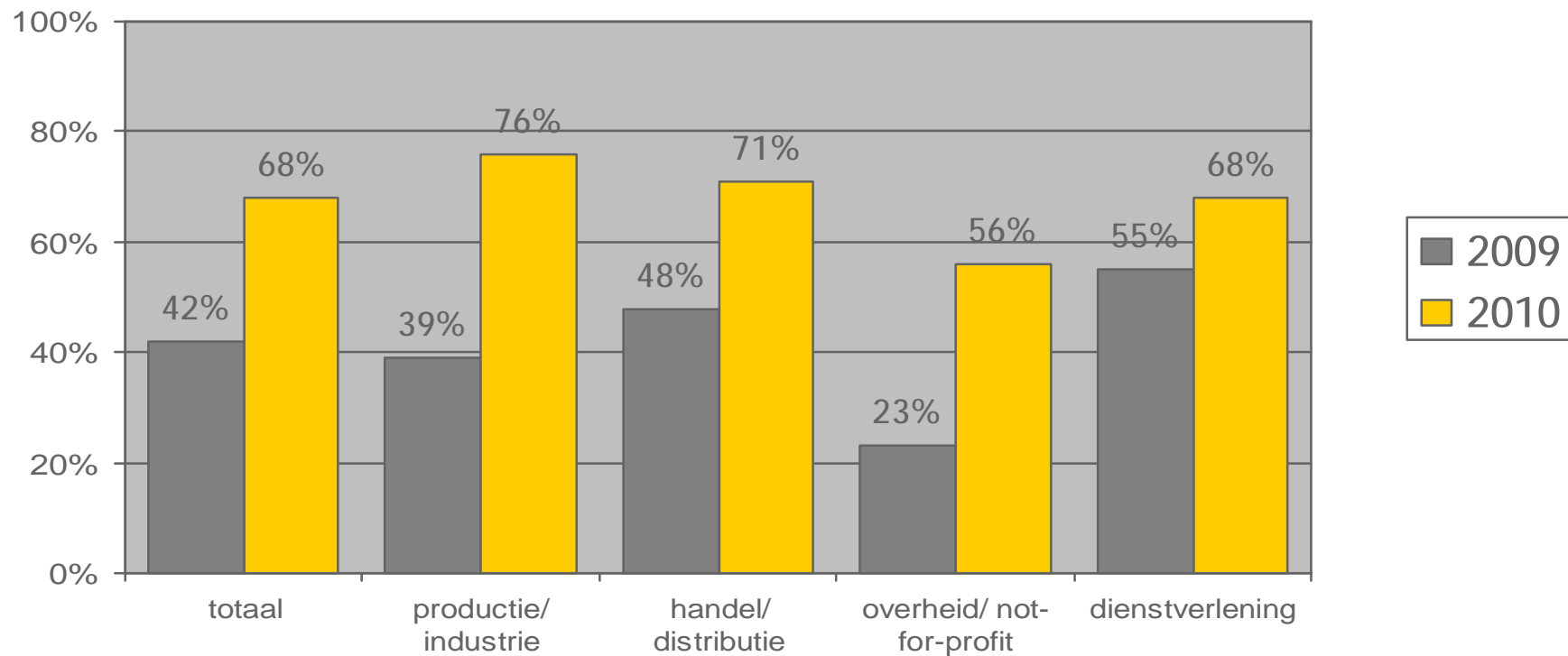
Organisatie in (zeer) grote mate afhankelijk van ICT



Aanwezigheid van noodplan in de sectoren

Twee op de drie organisaties beschikken over een noodplan ingeval de ICT-systemen uitvallen. Binnen de overheid/not-for-profit-sector is dit lager: 44% beschikt niet over een noodplan. In 8 op de 10 gevallen wordt het noodplan periodiek getest.

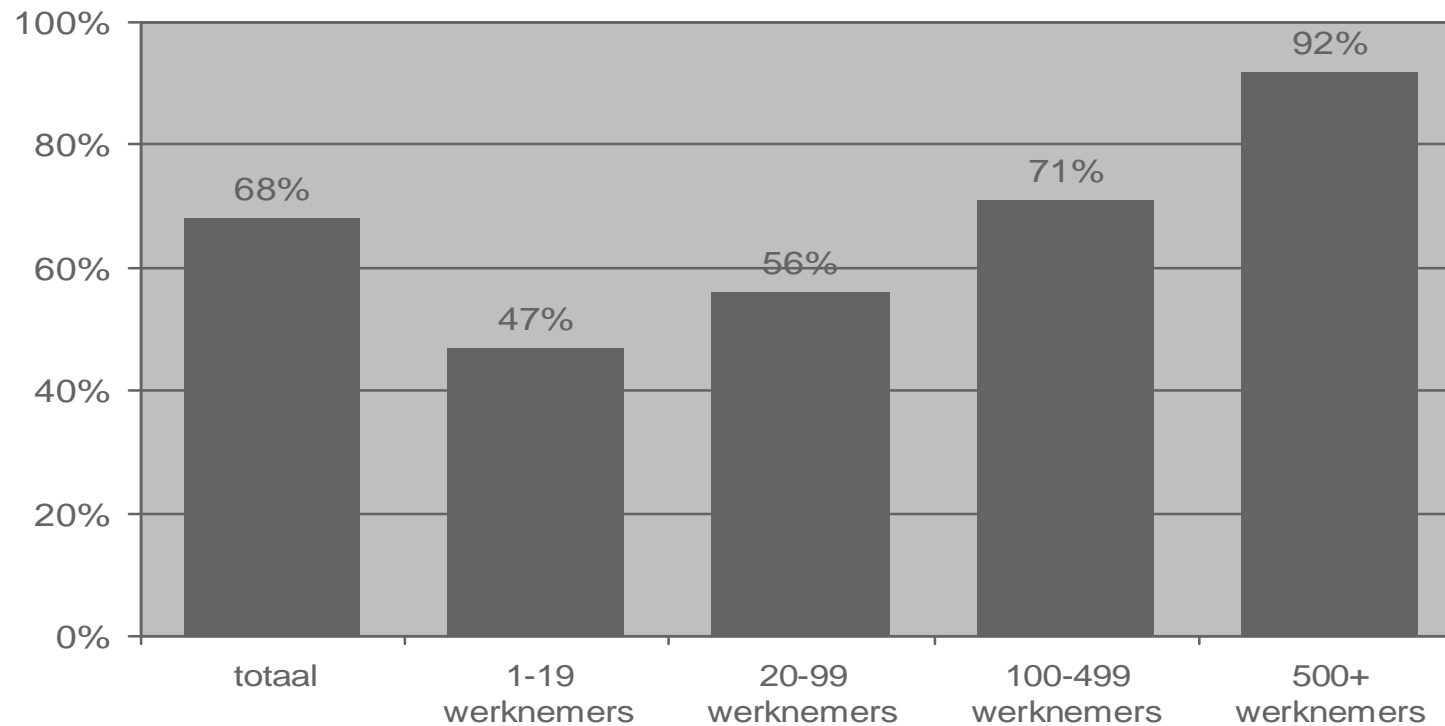
Beschikt uw organisatie over een noodplan voor het geval dat ICT systemen in uw organisatie uitvallen of niet meer goed functioneren?



Aanwezigheid van noodplan naar bedrijfsomvang

Grotere organisaties beschikken relatief vaak over een noodplan. De relatief sterke afhankelijkheid van ICT en de relatief grote gevolgen/schade bij uitval spelen hierbij waarschijnlijk een rol.

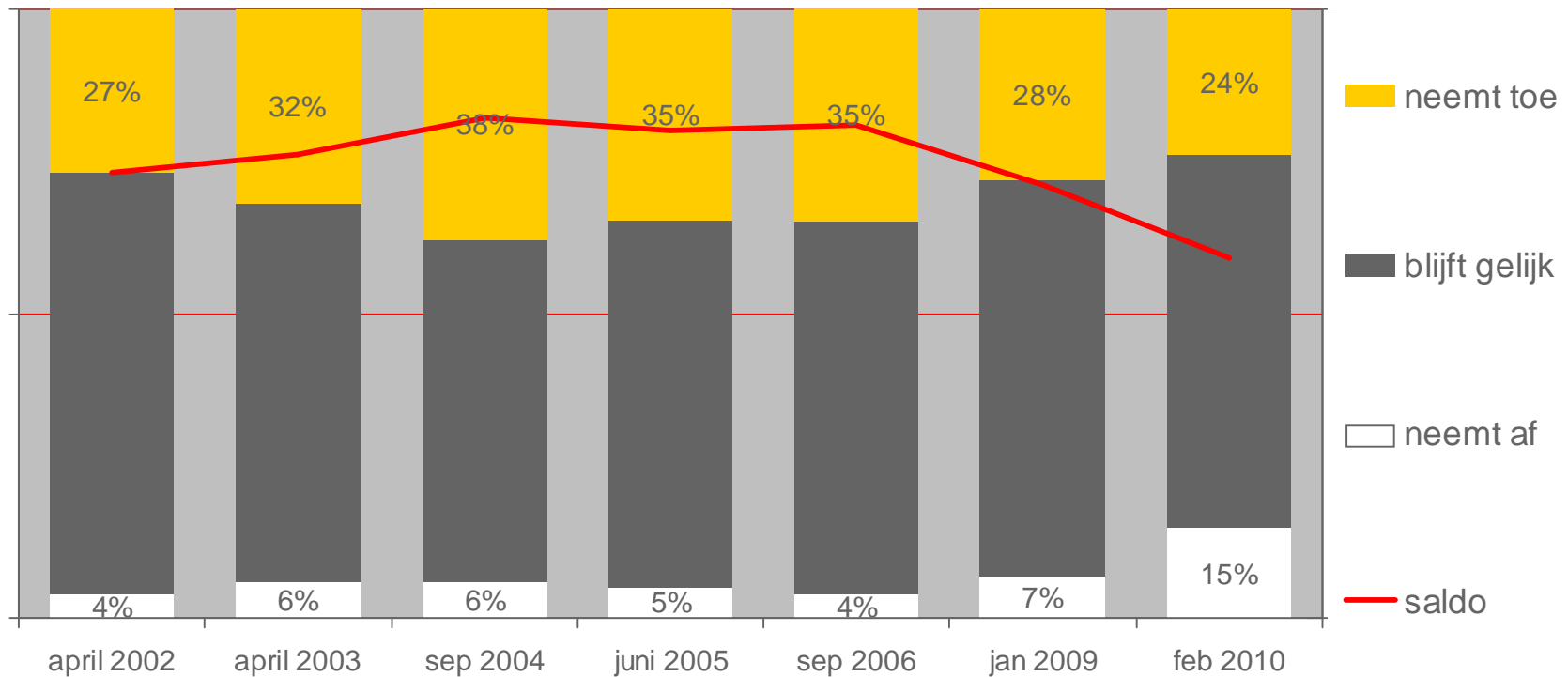
Beschikt uw organisatie over een noodplan voor het geval dat ICT systemen in uw organisatie uitvallen of niet meer goed functioneren?



Bestedingen ICT-beveiliging

De bestedingen aan ICT-beveiliging nemen per saldo nog licht toe, maar veel minder sterk dan in de periode 2004-2006.

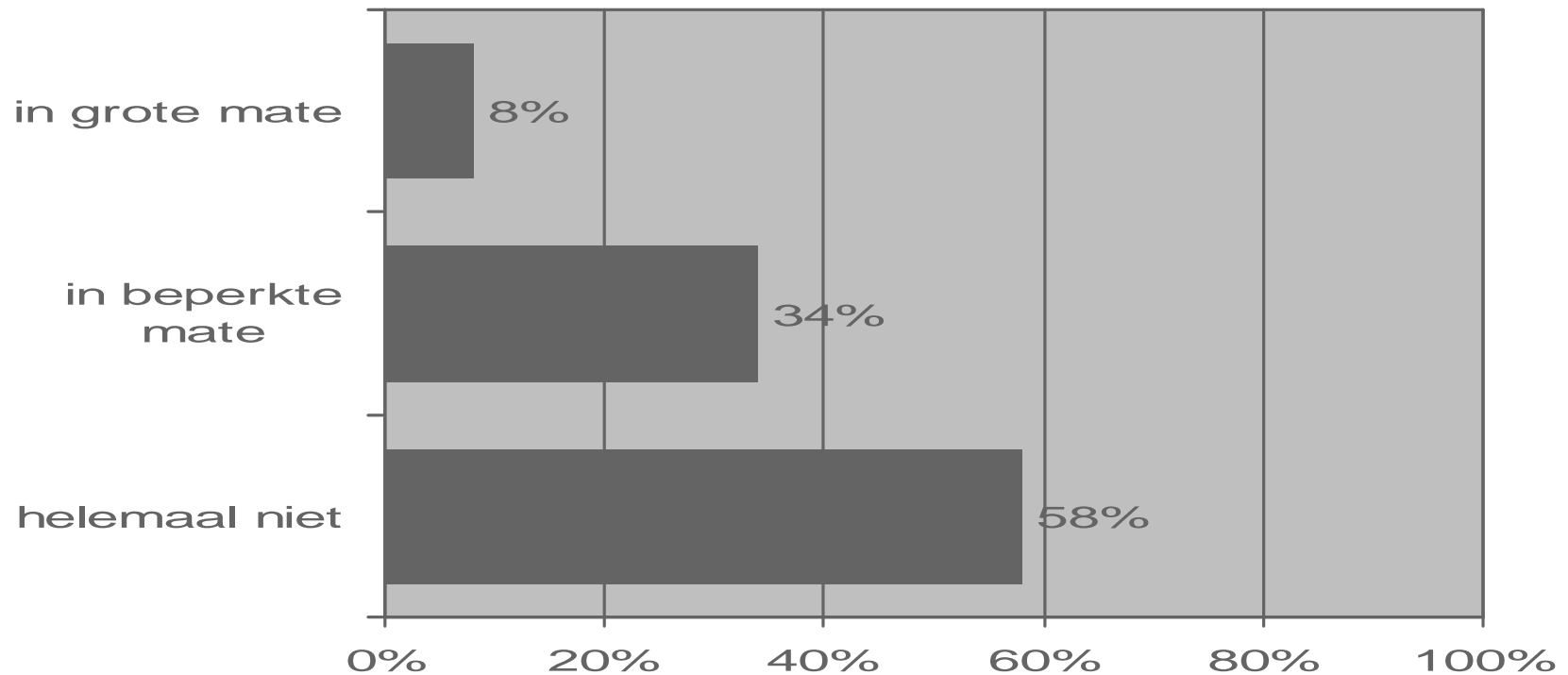
Wat zijn de verwachtingen omtrent de bestedingen van uw organisatie aan ICT-beveiliging voor de komende 12 maanden ten opzichte van de afgelopen 12 maanden?



Bestedingen ICT-beveiliging in economische crisis

De bestedingen aan ICT-beveiliging worden geremd door de economische crisis, hoewel minder sterk dan de totale ICT-bestedingen.

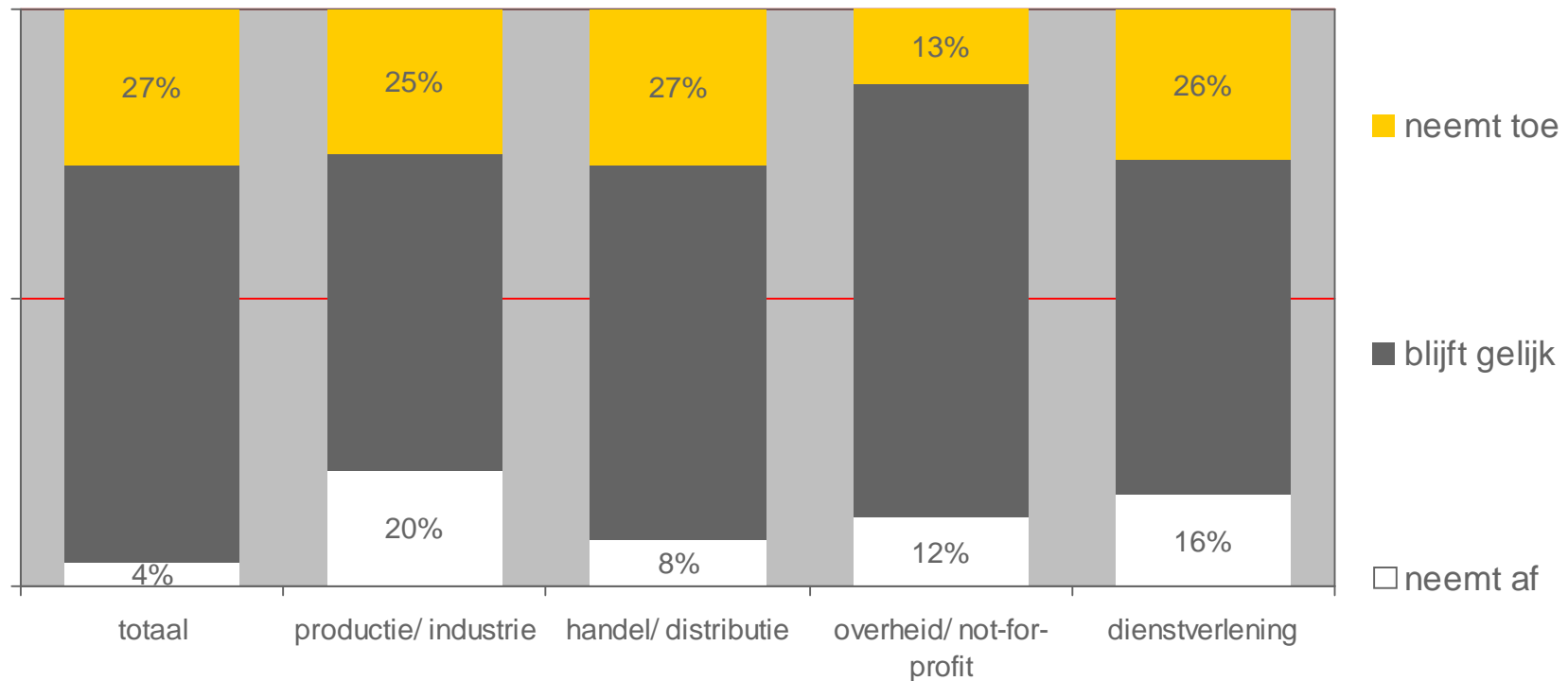
In welke mate heeft de recessie een negatieve invloed op het budget voor ICT-beveiliging?



Bestedingen ICT-beveiliging naar de sectoren

Met name binnen de overheid is het saldo van de groei/afname van de bestedingen voor ICT-beveiliging bijna op nul uitgekomen.

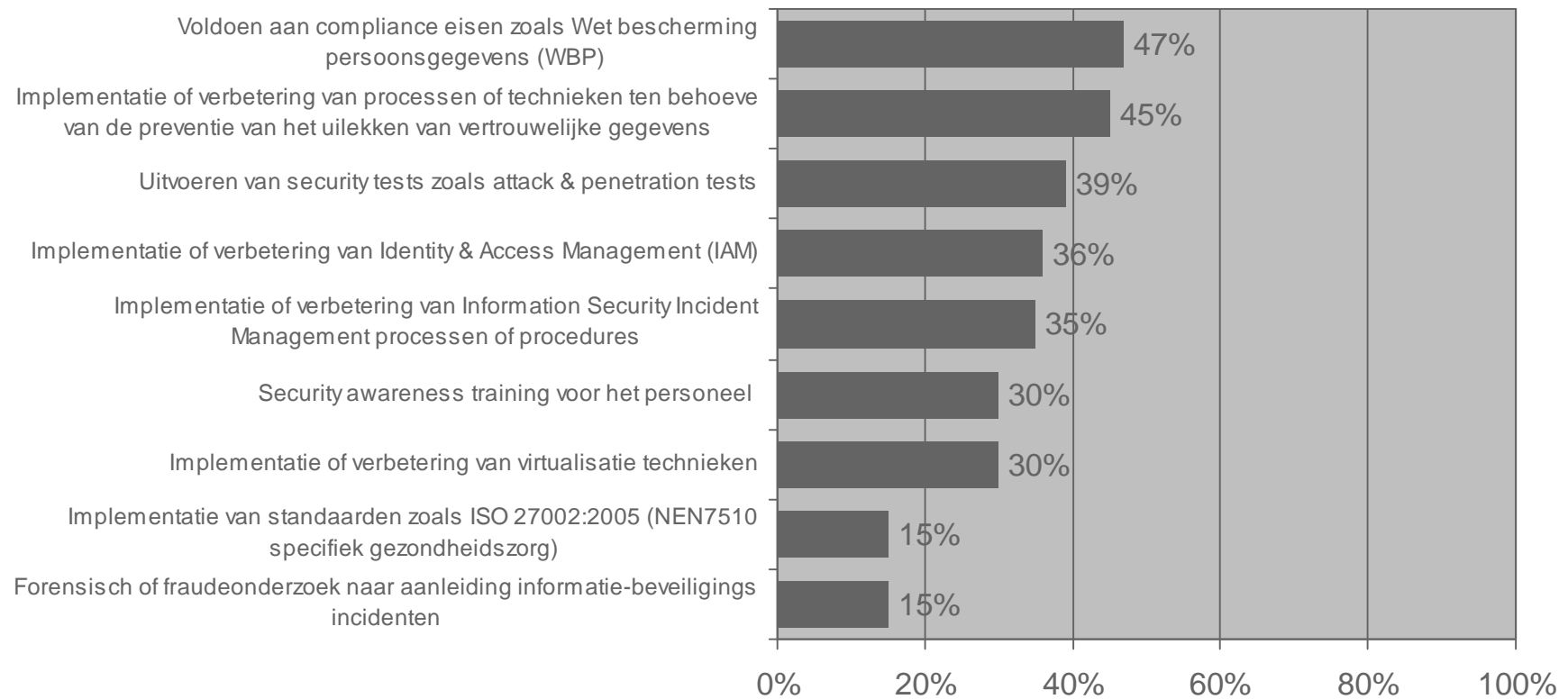
Wat zijn de verwachtingen omtrent de bestedingen van uw organisatie aan ICT-beveiliging voor de komende 12 maanden ten opzichte van de afgelopen 12 maanden?



Bestedingen ICT-beveiliging

Organisaties investeren in een breed spectrum aan maatregelen voor ICT-beveiliging, zoals compliance-eisen en preventie van uitlekken vertrouwelijke gegevens.

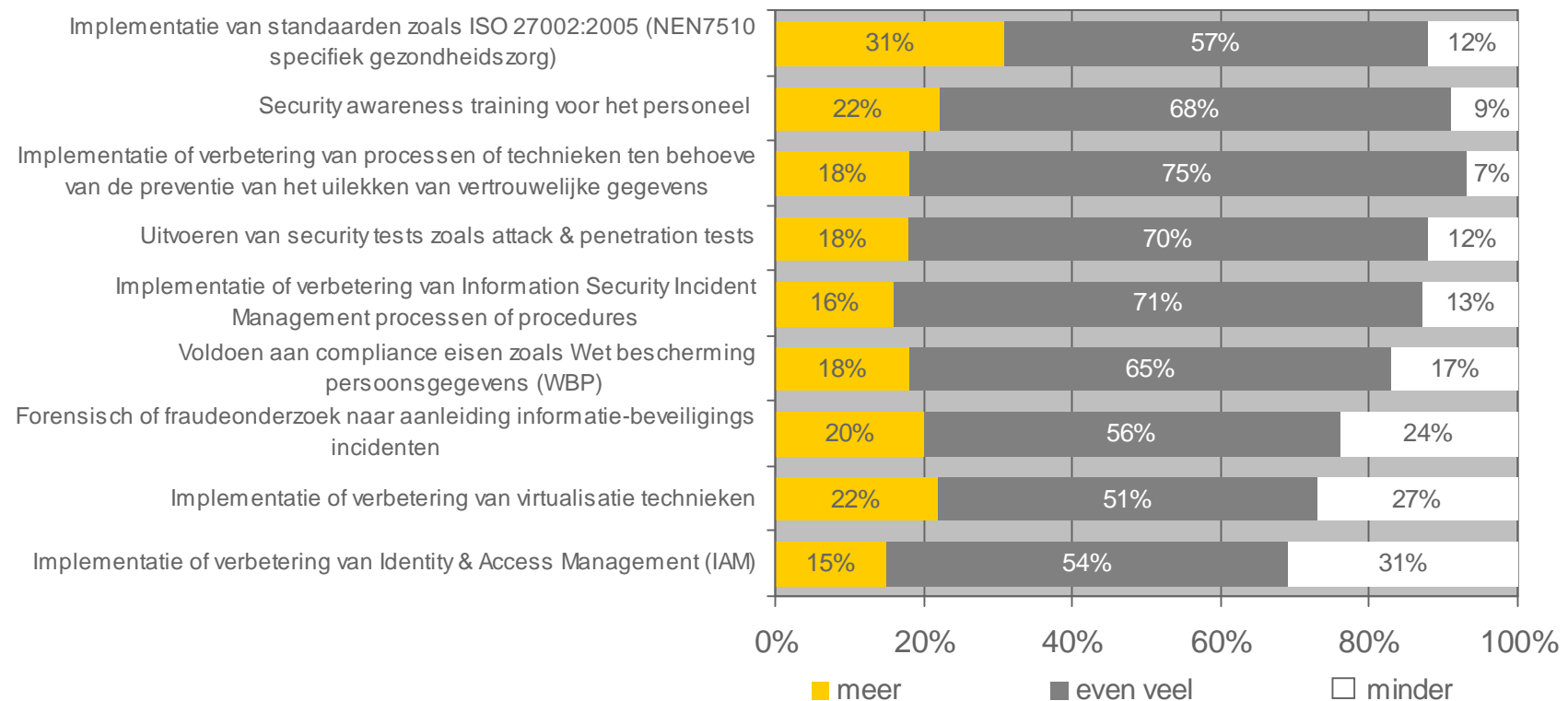
Heeft uw organisatie de afgelopen 12 maanden geïnvesteerd in de volgende maatregelen op het gebied van ICT beveiliging?



Bestedingen ICT-beveiliging

Respondenten verwachten komend jaar meer te investeren in standaarden, security awareness training en preventie van uitlekken vertrouwelijke gegevens. Investeringen in Identity & Access Management nemen per saldo het meest af.

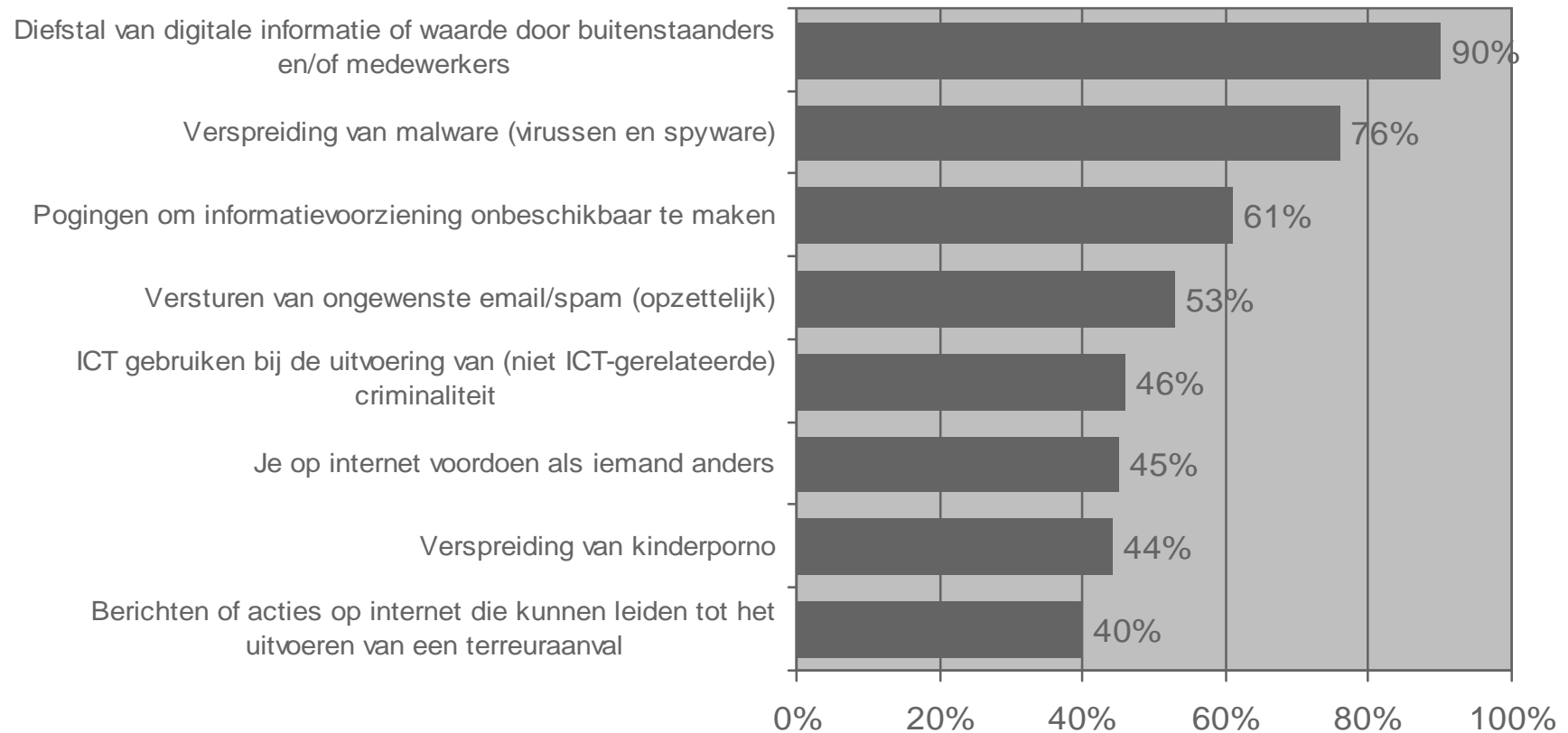
En verwacht uw organisatie de komende 12 maanden minder, even veel of meer te investeren hierin?



Wat is cybercrime?

De meest gedeelde definitie betreft diefstal van digitale informatie of waarde door buitenstaanders en/of medewerkers.

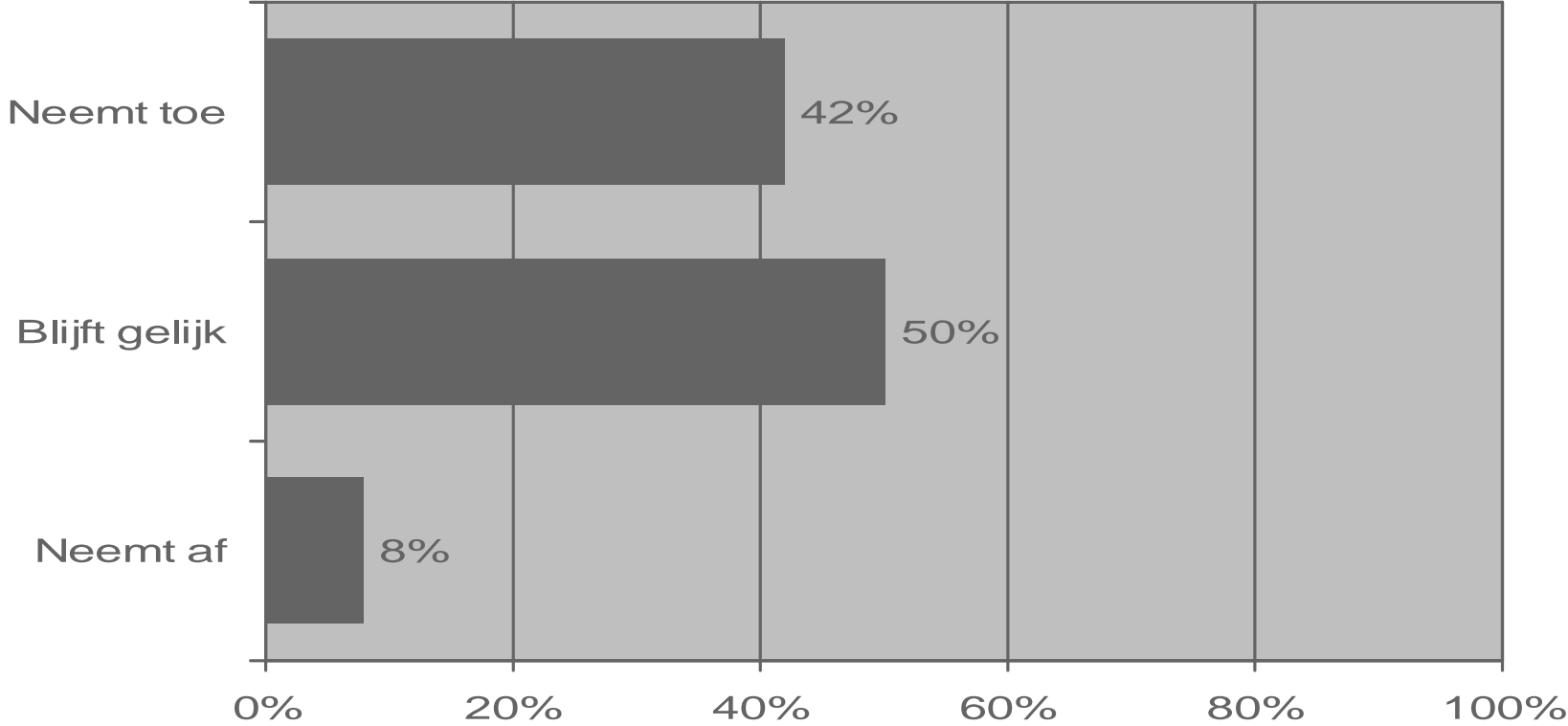
Wat verstaat u onder cybercrime?



Ontwikkeling overlast cybercrime

De overlast van cybercrime is het afgelopen jaar toegenomen.

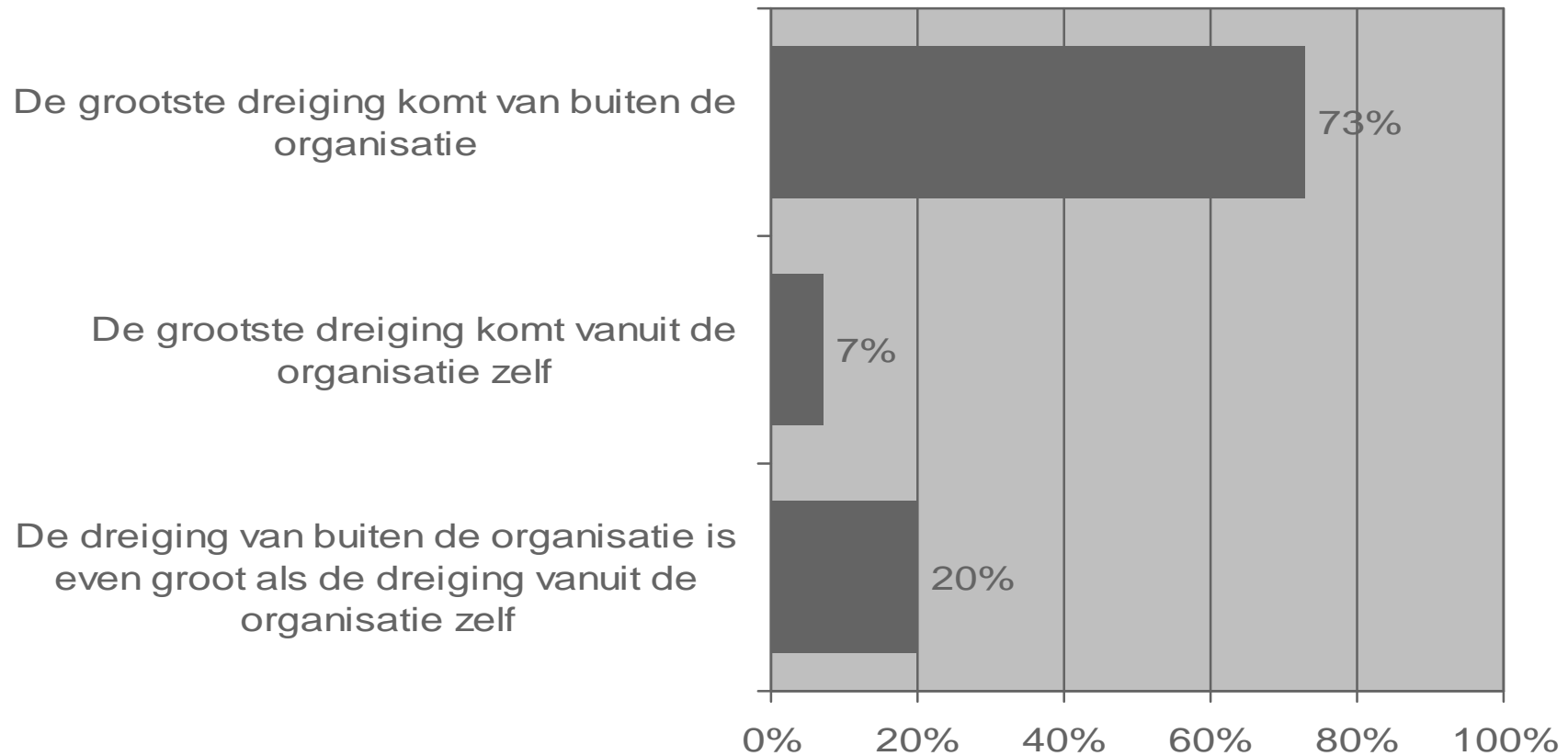
Is de overlast van cybercrime activiteiten naar uw gevoel het afgelopen jaar afgenomen, gelijk gebleven of toegenomen?



Cybercrime: interne of externe bedreiging

Cybercrime wordt meer gezien als externe bedreiging dan als interne bedreiging.

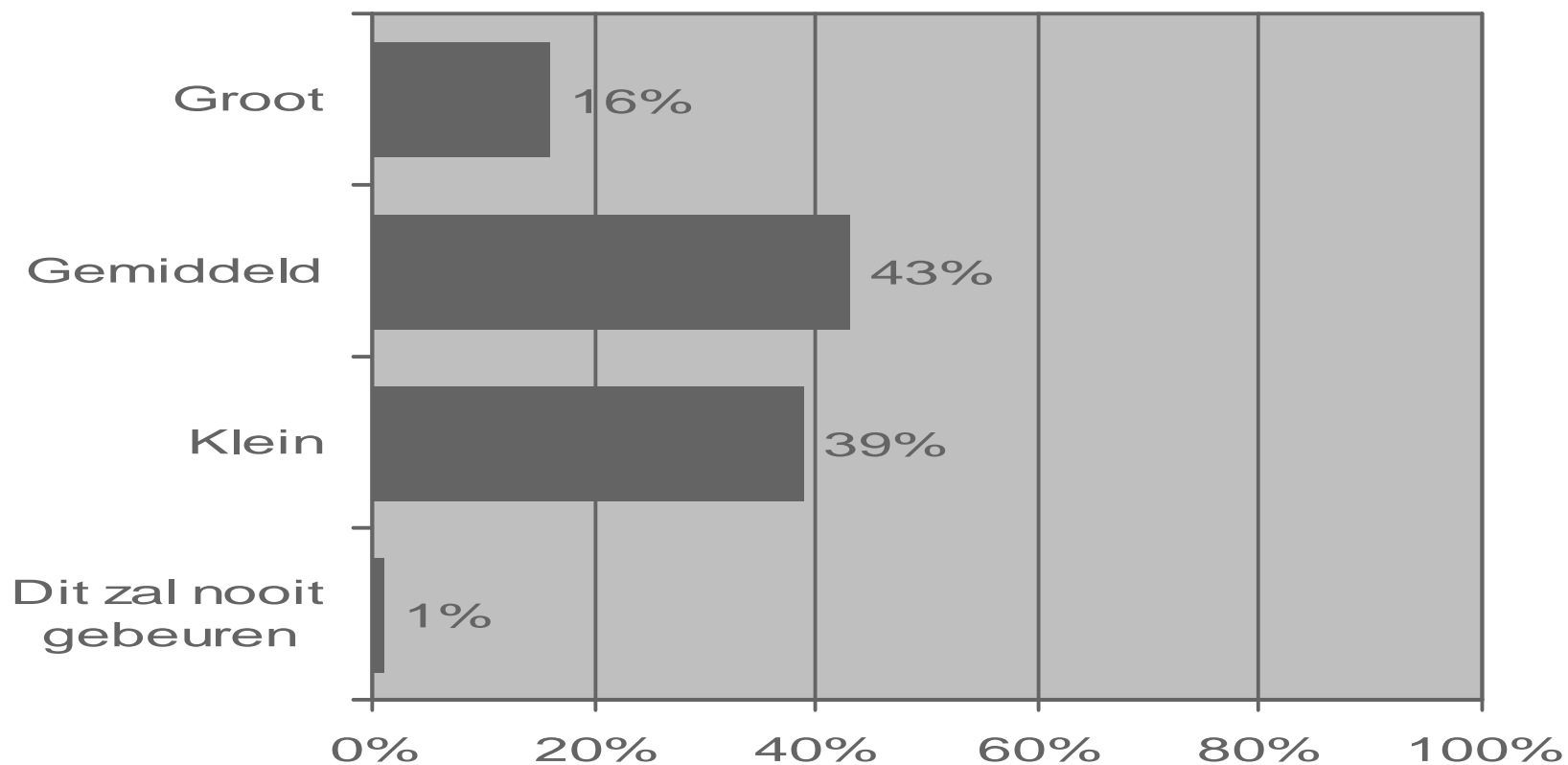
Is cybercrime naar uw mening voornamelijk een interne of externe bedreiging?



Cybercrime: kans op terreuraanval

De meeste ondervraagden vinden het realistisch dat er in de toekomst een terreuraanval gaat plaatsvinden met behulp van cybercrime. Slechts 1% denkt dat dit nooit zal gebeuren.

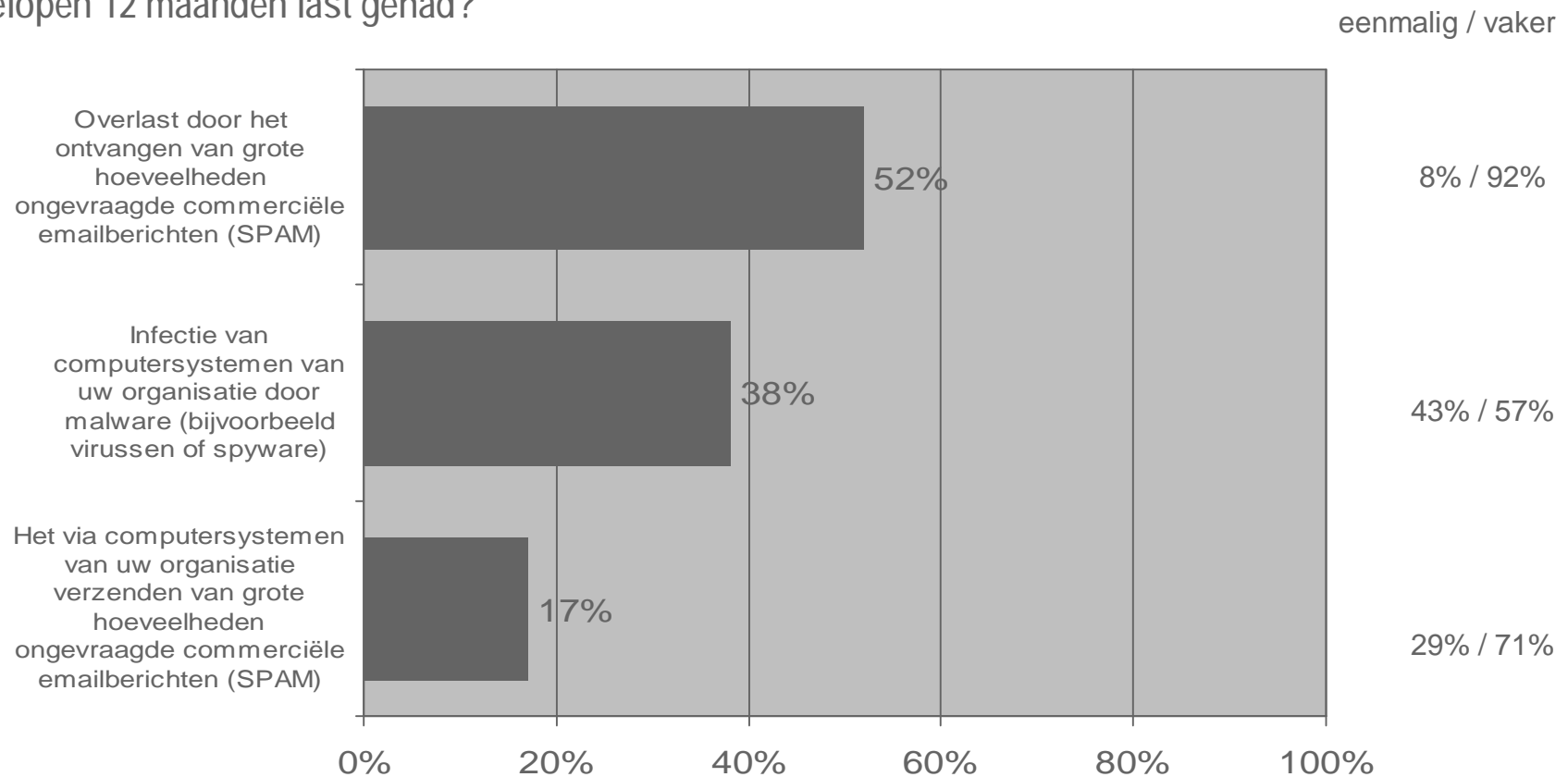
Hoe groot acht u de kans dat in de toekomst een terreuraanval plaatsvindt met behulp van cybercrime?



Afgelopen 12 maanden last van cybercrime

De meest voorkomende cybercrime-activiteiten op dit moment zijn spam en malware (virussen of spyware). Deze activiteiten komen in veel gevallen meerdere keren per jaar voor.

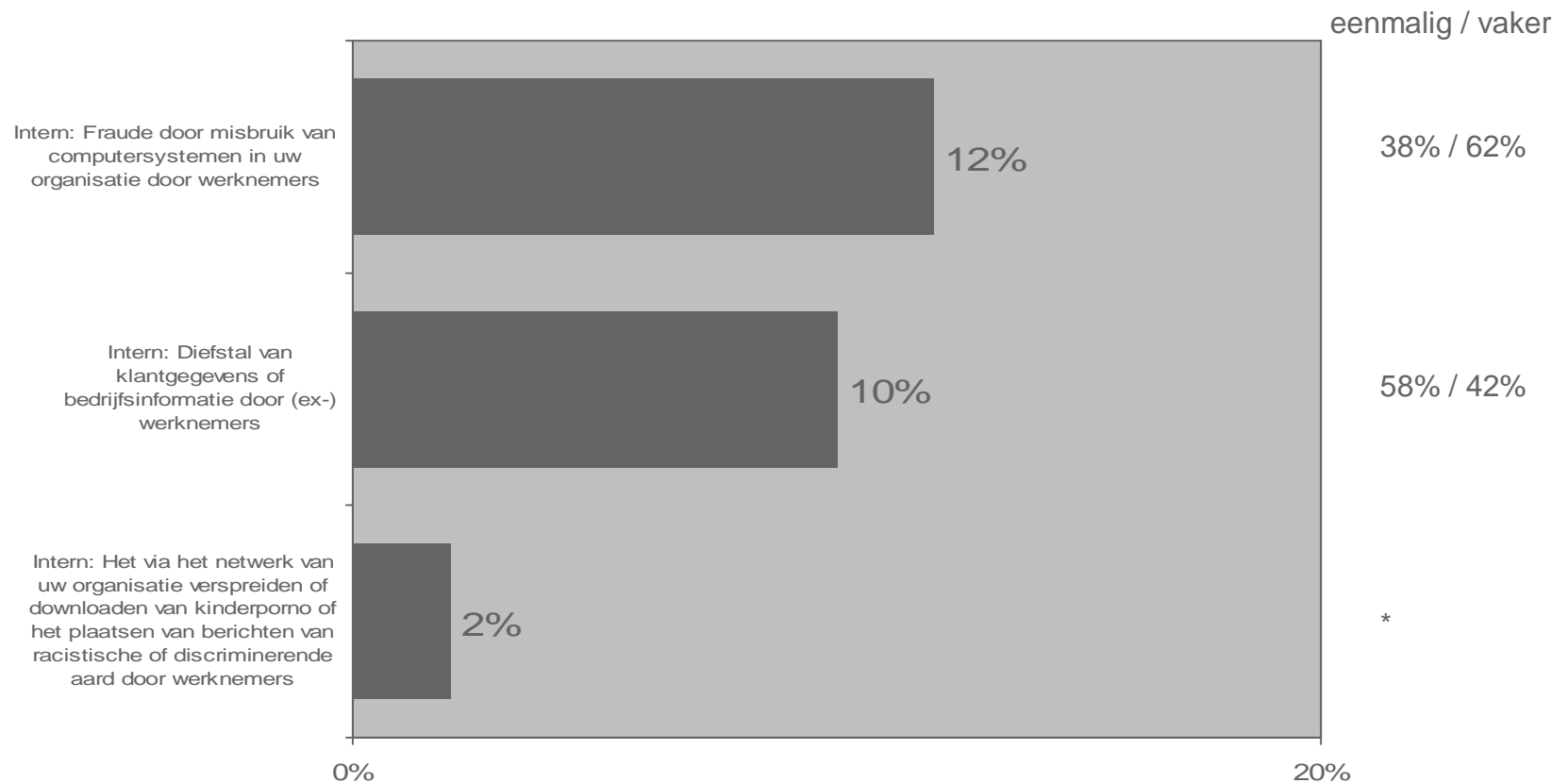
Van welke van de volgende cybercrime activiteiten (of de gevolgen daarvan) heeft uw organisatie in de afgelopen 12 maanden last gehad?



Afgelopen 12 maanden last van cybercrime

Bij 1 op de 8 bedrijven heeft fraude plaatsgevonden door misbruik van computersystemen. Bij tweederde daarvan gebeurde dat zelfs meer dan eens.

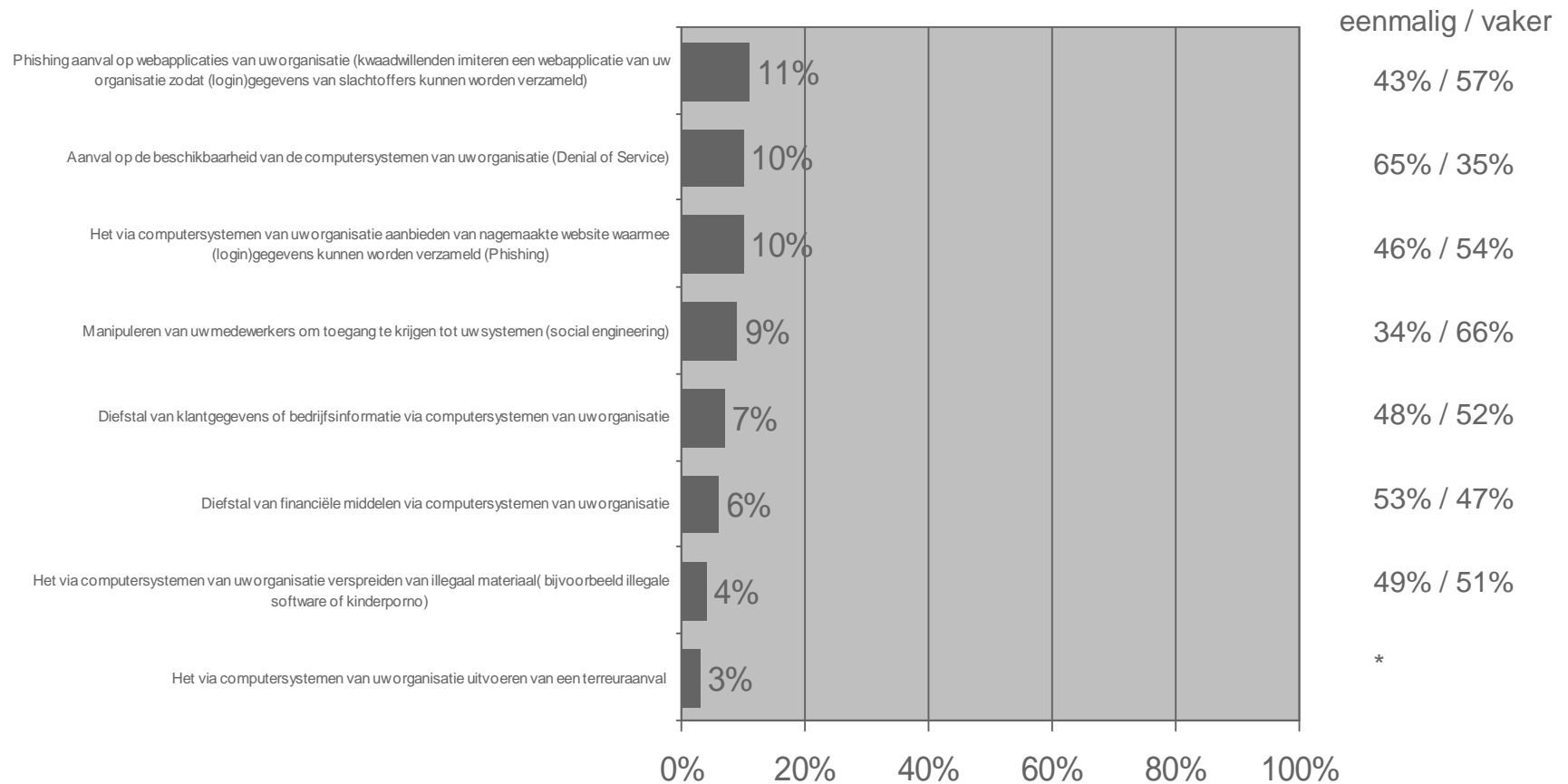
Van welke van de volgende cybercrime activiteiten (of de gevolgen daarvan) heeft uw organisatie in de afgelopen 12 maanden last gehad?



Afgelopen 12 maanden last van cybercrime

Onderstaande externe cybercrime-activiteiten komen maar incidenteel voor, maar impact is heel groot.

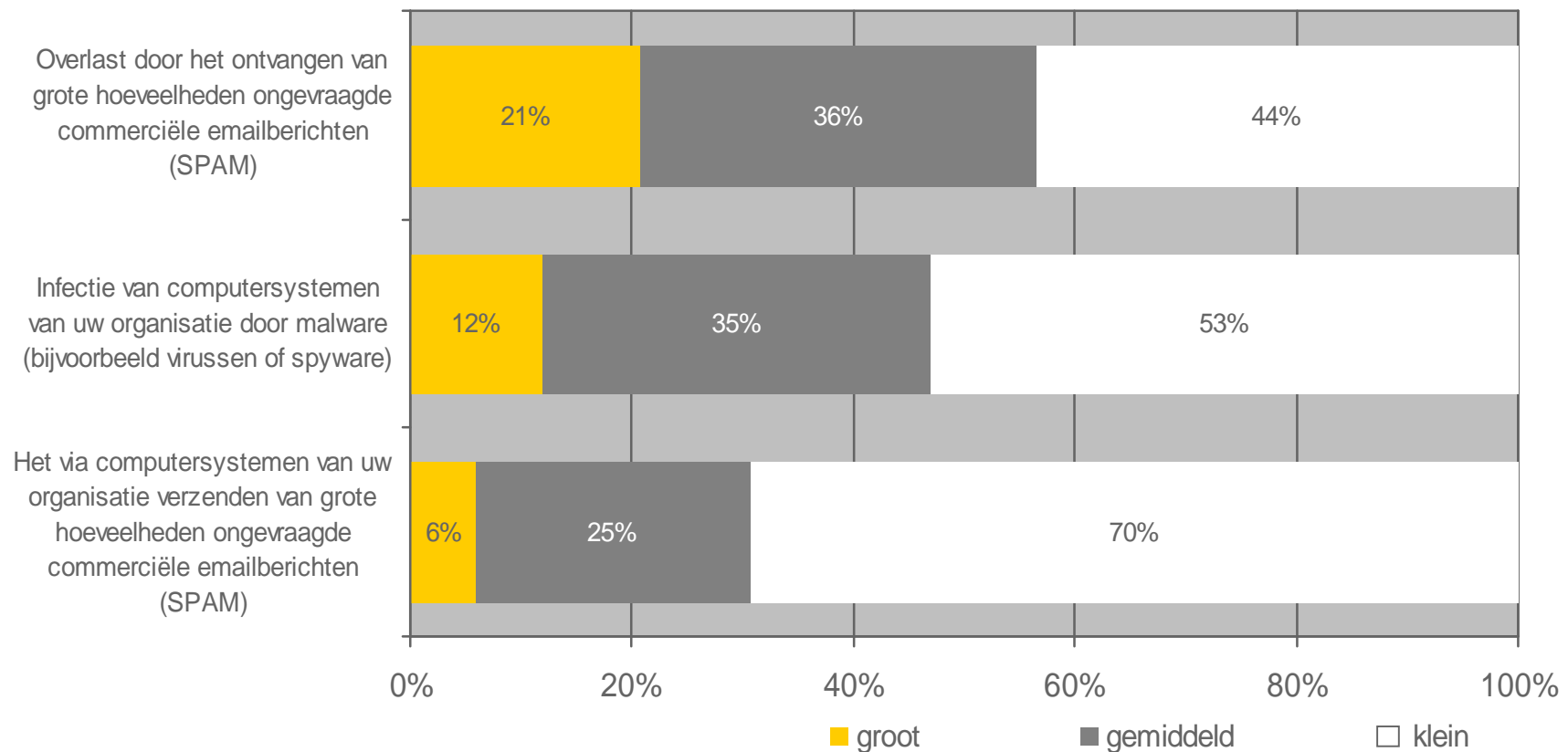
Van welke van de volgende cybercrime activiteiten (of de gevolgen daarvan) heeft uw organisatie in de afgelopen 12 maanden last gehad?



Kans op cybercrime komende 12 maanden

In de toekomst verwacht men het meeste last te hebben van spam en malware.

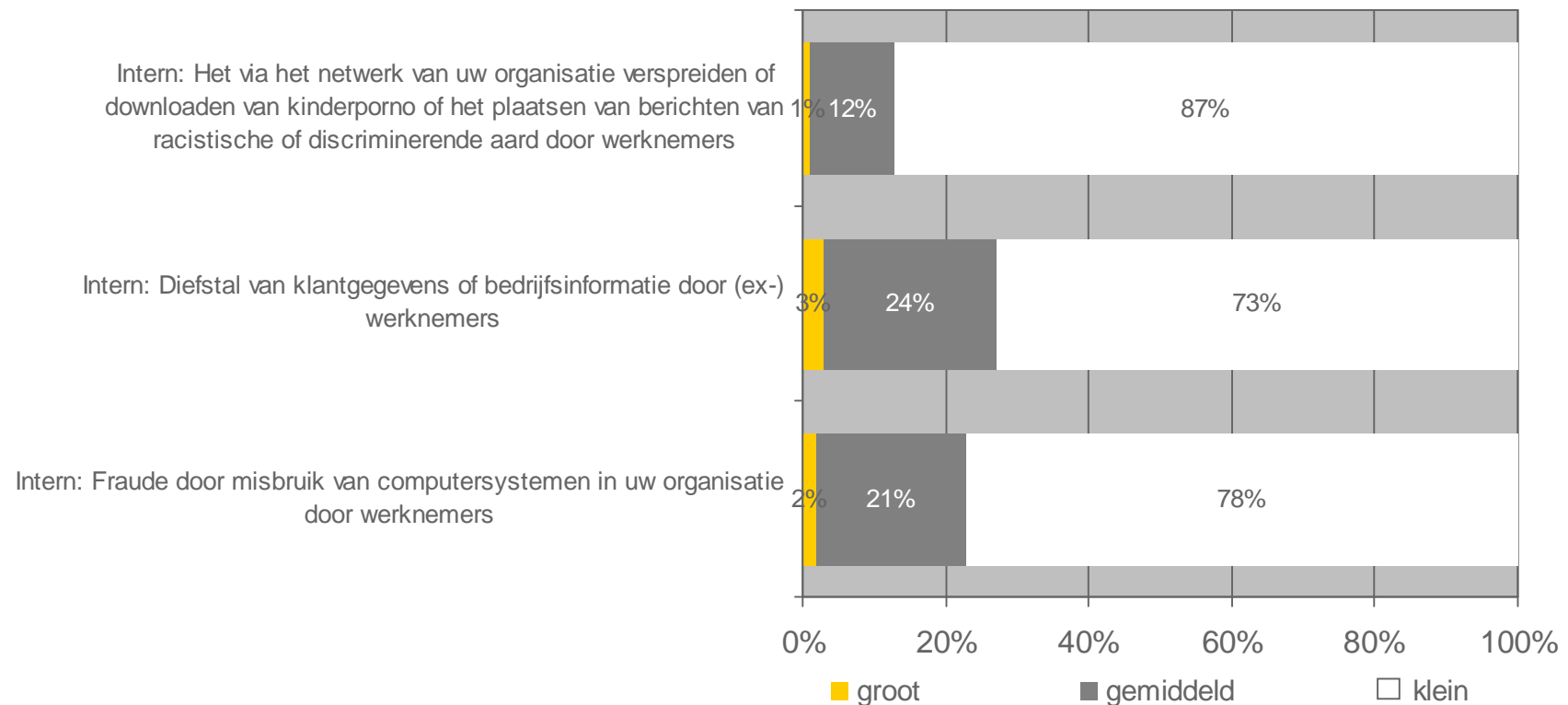
Hoe groot schat u de kans in dat uw organisatie in de komende 12 maanden te maken krijgt met een van de volgende cybercrime activiteiten (of de gevolgen daarvan)?



Kans op cybercrime komende 12 maanden

Onderstaande interne cybercrime-activiteiten komen maar incidenteel voor, maar impact is heel groot.

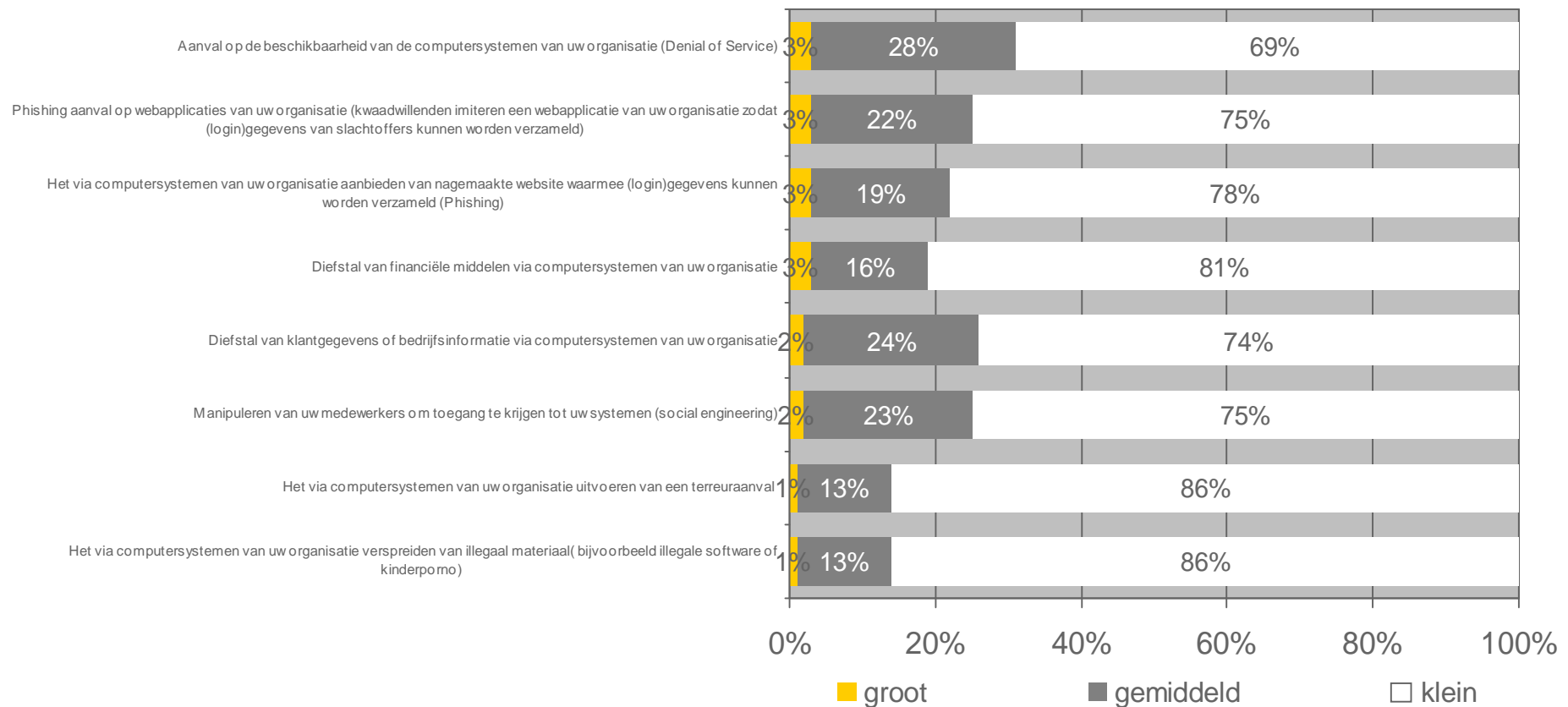
Hoe groot schat u de kans in dat uw organisatie in de komende 12 maanden te maken krijgt met een van de volgende cybercrime activiteiten (of de gevolgen daarvan)?



Kans op cybercrime komende 12 maanden

Onderstaande cybercrime-activiteiten worden niet vaak verwacht, maar impact is heel groot.

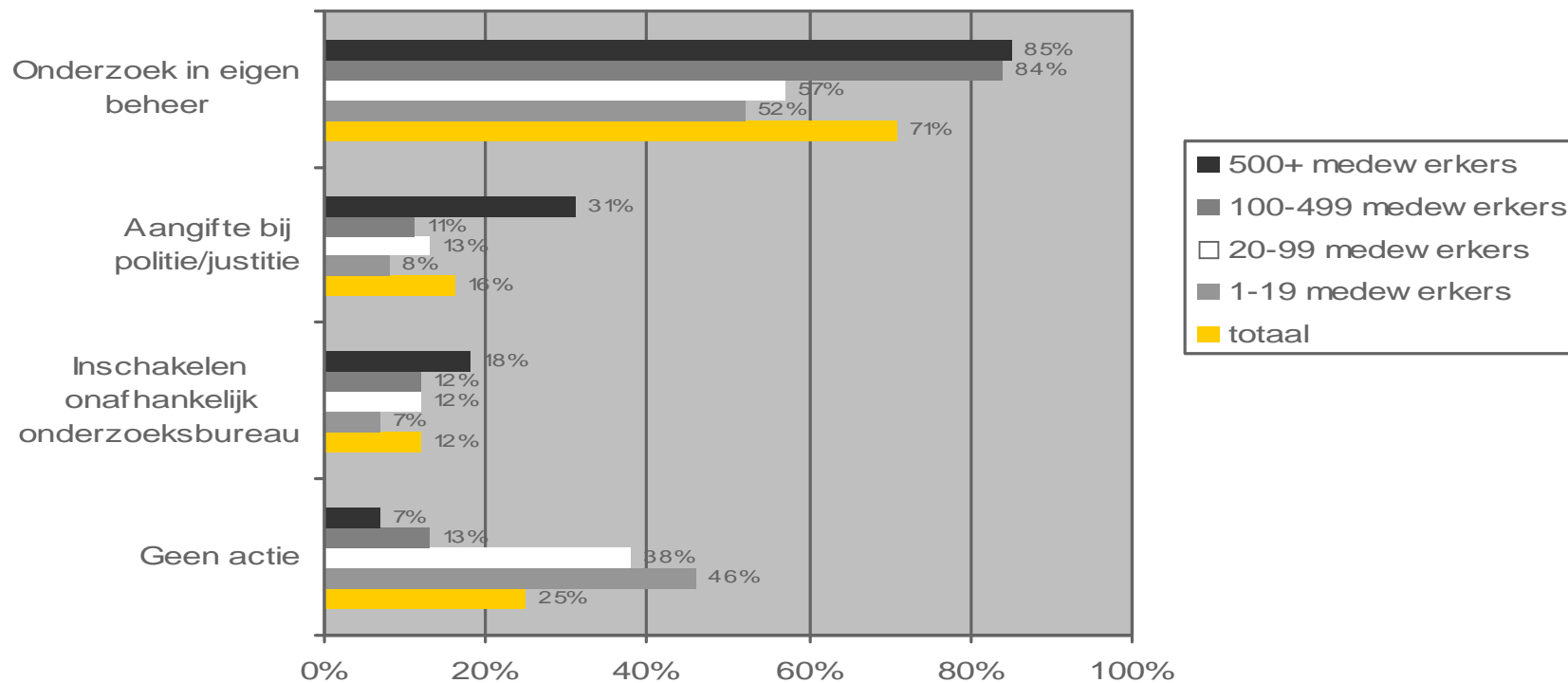
Hoe groot schat u de kans in dat uw organisatie in de komende 12 maanden te maken krijgt met een van de volgende cybercrime activiteiten (of de gevolgen daarvan)?



Actie ondernomen bij cybercrime naar bedrijfsomvang

Organisaties die slachtoffer zijn van cybercrime-activiteiten doen in de meeste gevallen een onderzoek in eigen beheer. Behalve grotere organisaties (31%), doet slechts een klein deel aangifte bij politie/justitie en/of schakelt een extern bureau in. Gemiddeld onderneemt een kwart helemaal geen actie. Dit zijn vooral kleinere organisaties/bedrijven.

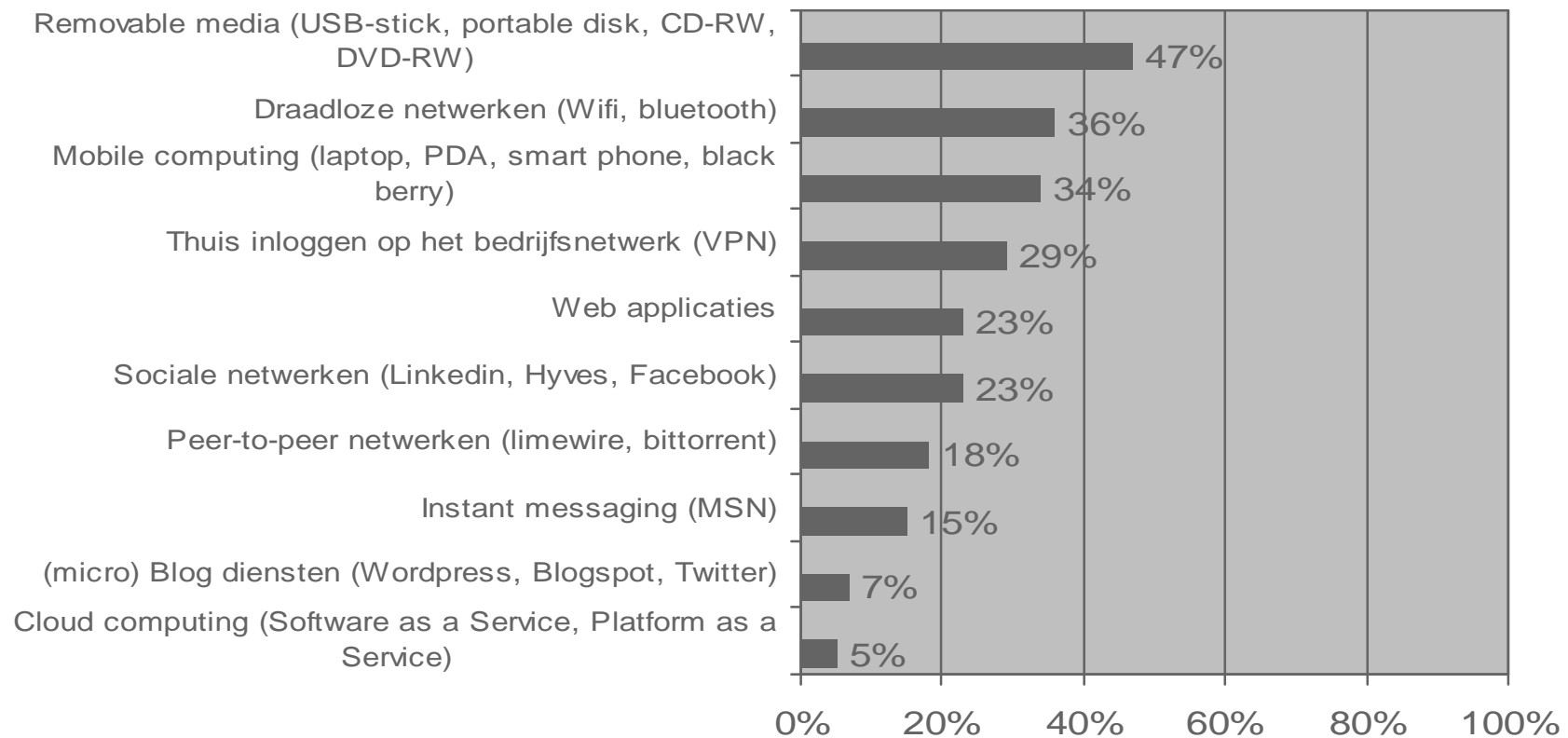
Indien uw organisatie slachtoffer is geworden van cybercrime activiteiten, welk actie heeft uw organisatie daarop ondernomen?



Risico nieuwe technologieën

Vanuit beveiligingsoptiek maakt men zich het meeste zorgen over removable media, draadloze netwerken, mobile computing en thuis inloggen op het bedrijfsnetwerk.

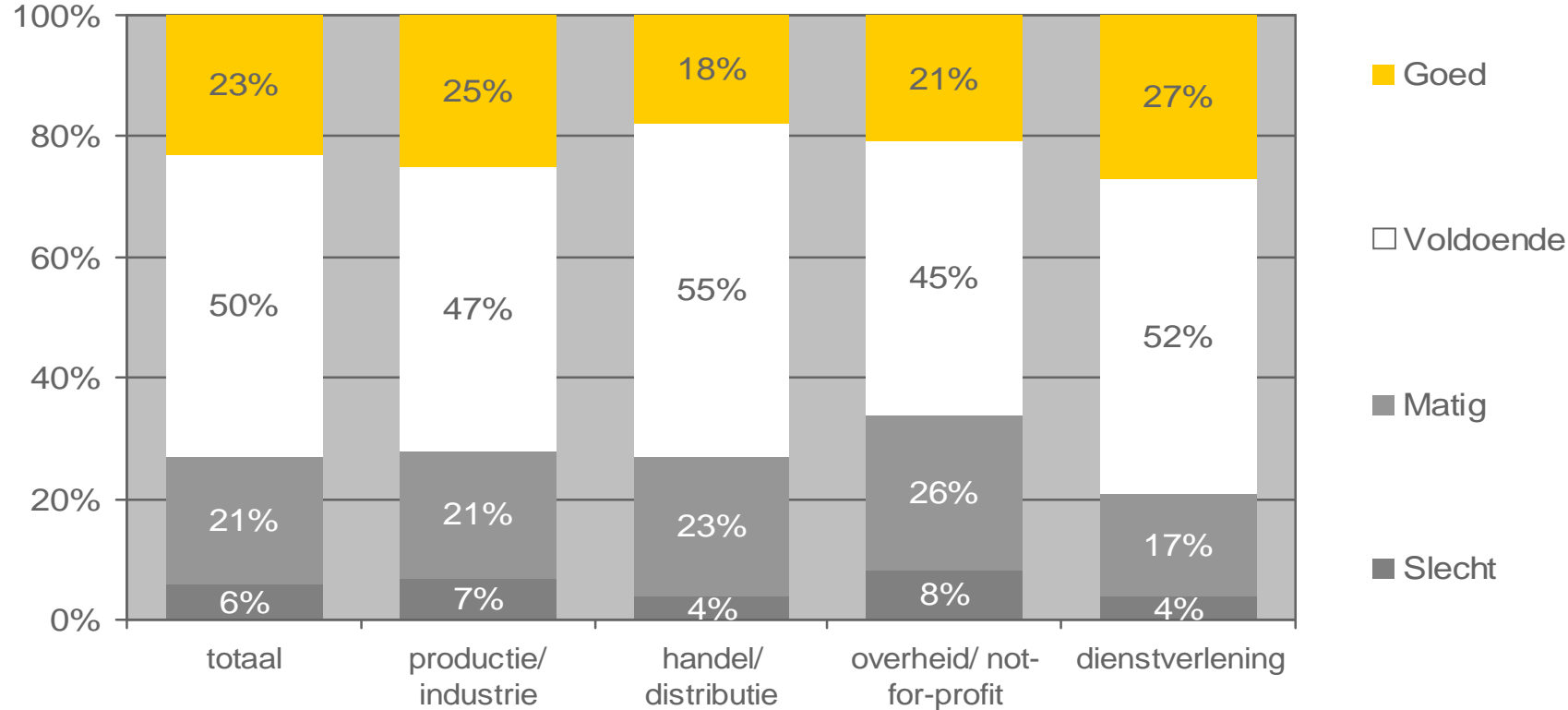
Welke technologieën baren uw organisatie de meeste zorgen vanuit beveiligingsoptiek?



Informatievoorziening over cybercrime

Ruim een kwart (27%) van de ondervraagden is niet tevreden over de informatie over cybercrime binnen de organisatie. Binnen de overheid is zelfs 34% niet tevreden.

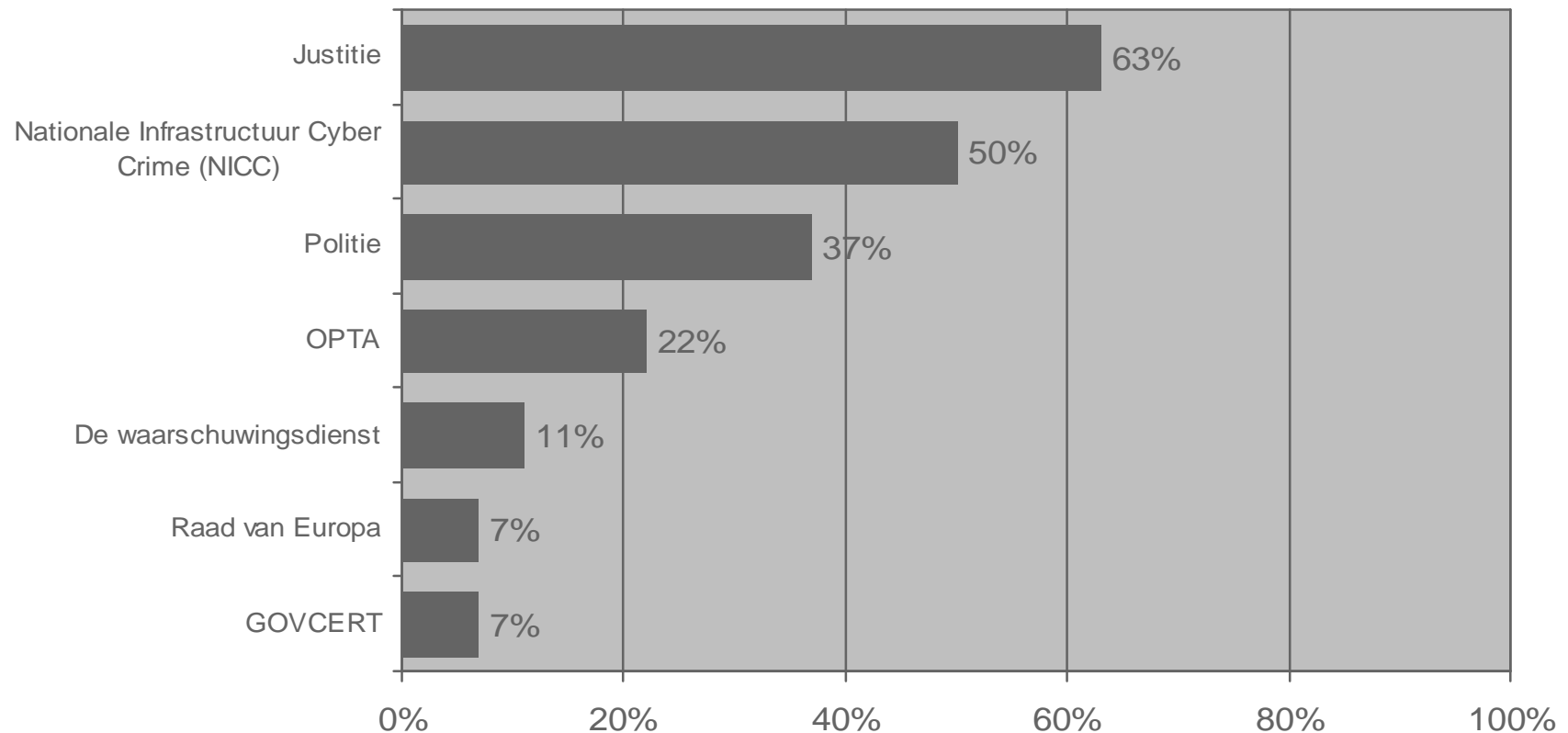
Vindt u dat uw organisatie voldoende is geïnformeerd over de gevaren van cybercrime?



Verantwoordelijkheid informatievoorziening over cybercrime

De verantwoordelijkheid voor de informatievoorziening over cybercrime ligt vooral bij Justitie en bij het NICC. Daarnaast noemt men ook politie en OPTA.

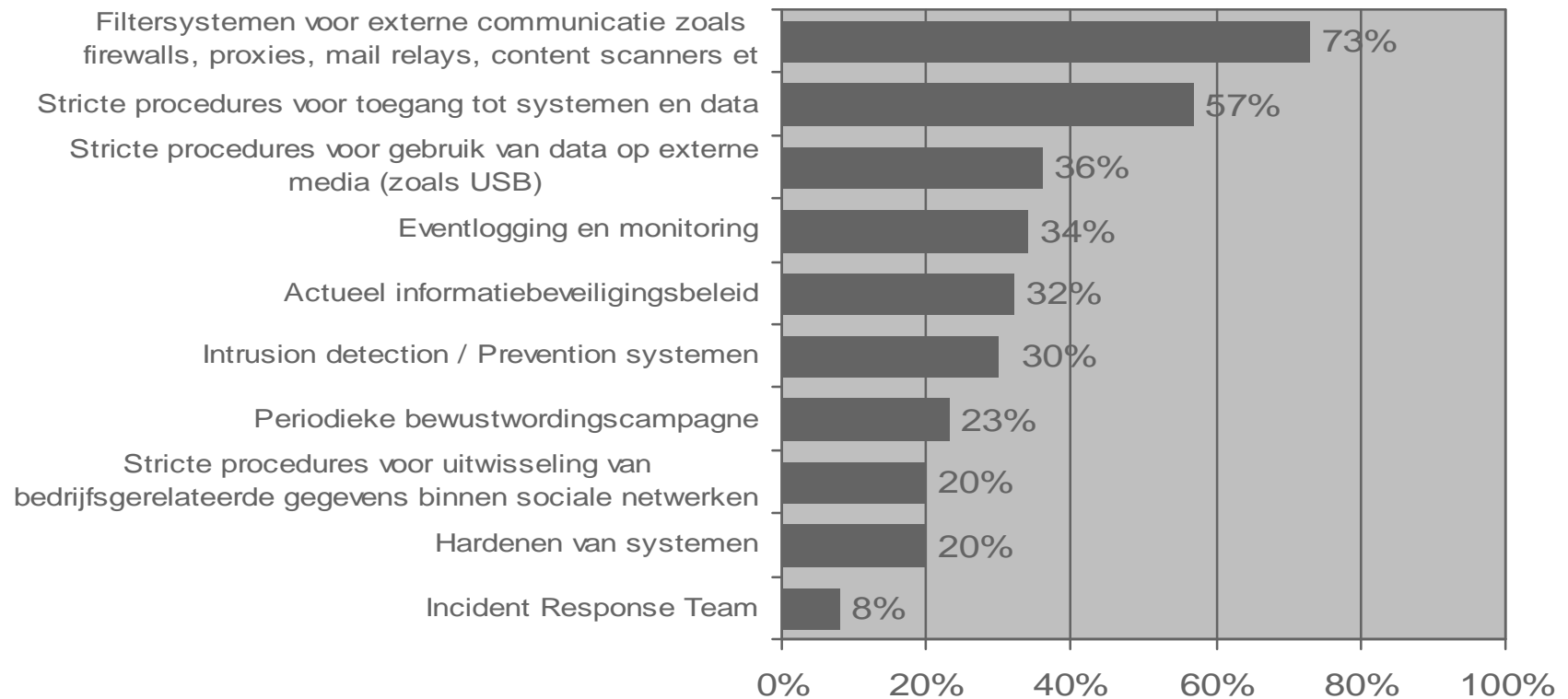
Wie is volgens u verantwoordelijk voor de informatieverstrekking over de gevaren van cybercrime?



Technische maatregelen tegen cybercrime

De meest voorkomende technische maatregelen tegen cybercrime zijn filtersystemen en procedures voor toegang tot systemen en data.

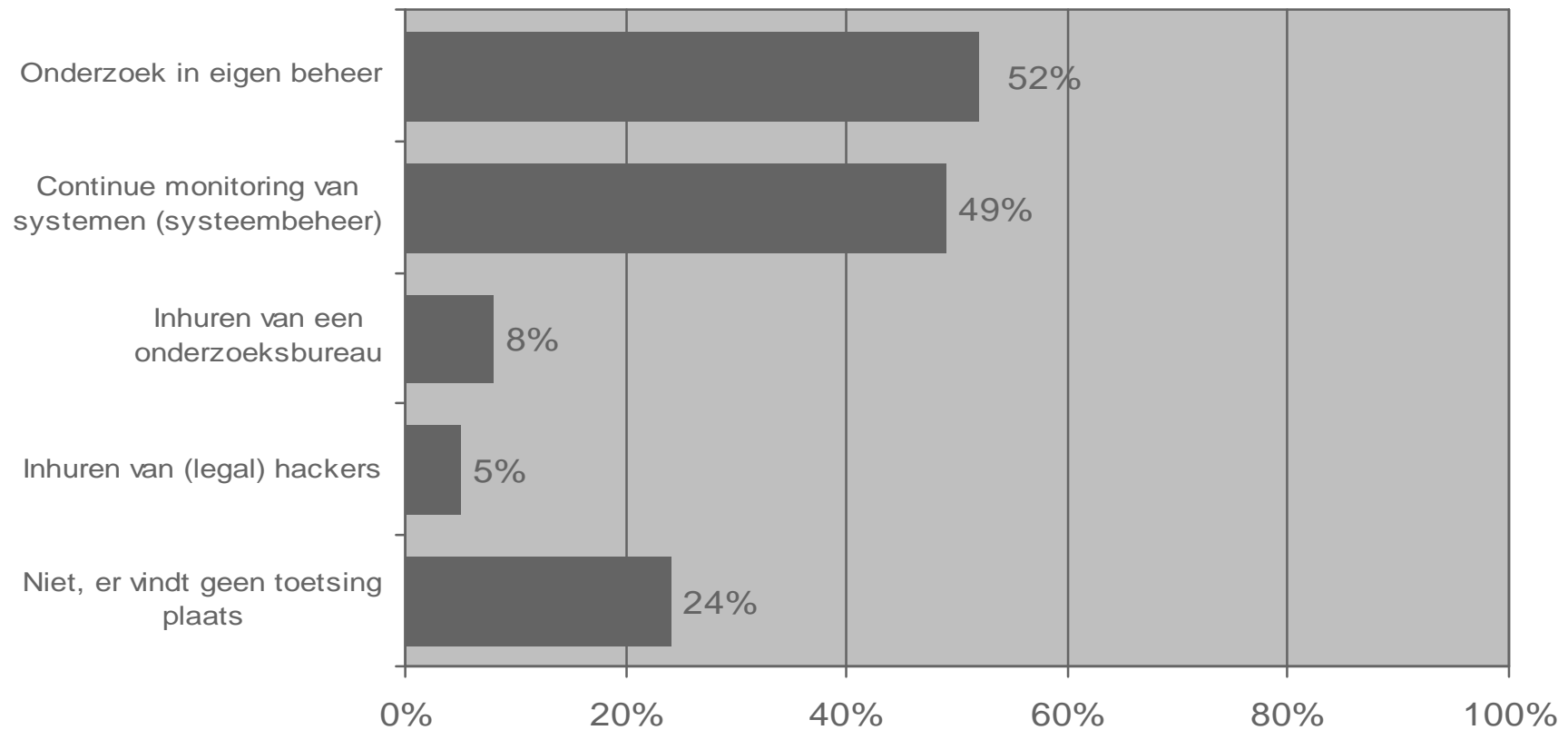
Welke technische of procedurele maatregelen heeft uw organisatie getroffen om schade door cybercrime activiteiten te voorkomen of te detecteren?



Toetsing maatregelen tegen cybercrime

Toetsing van de maatregelen gebeurt vooral in eigen beheer via onderzoek en continue monitoring van systemen. In een kwart van de gevallen vindt er helemaal geen toetsing plaats. Het gaat daarbij vooral om kleinere bedrijven.

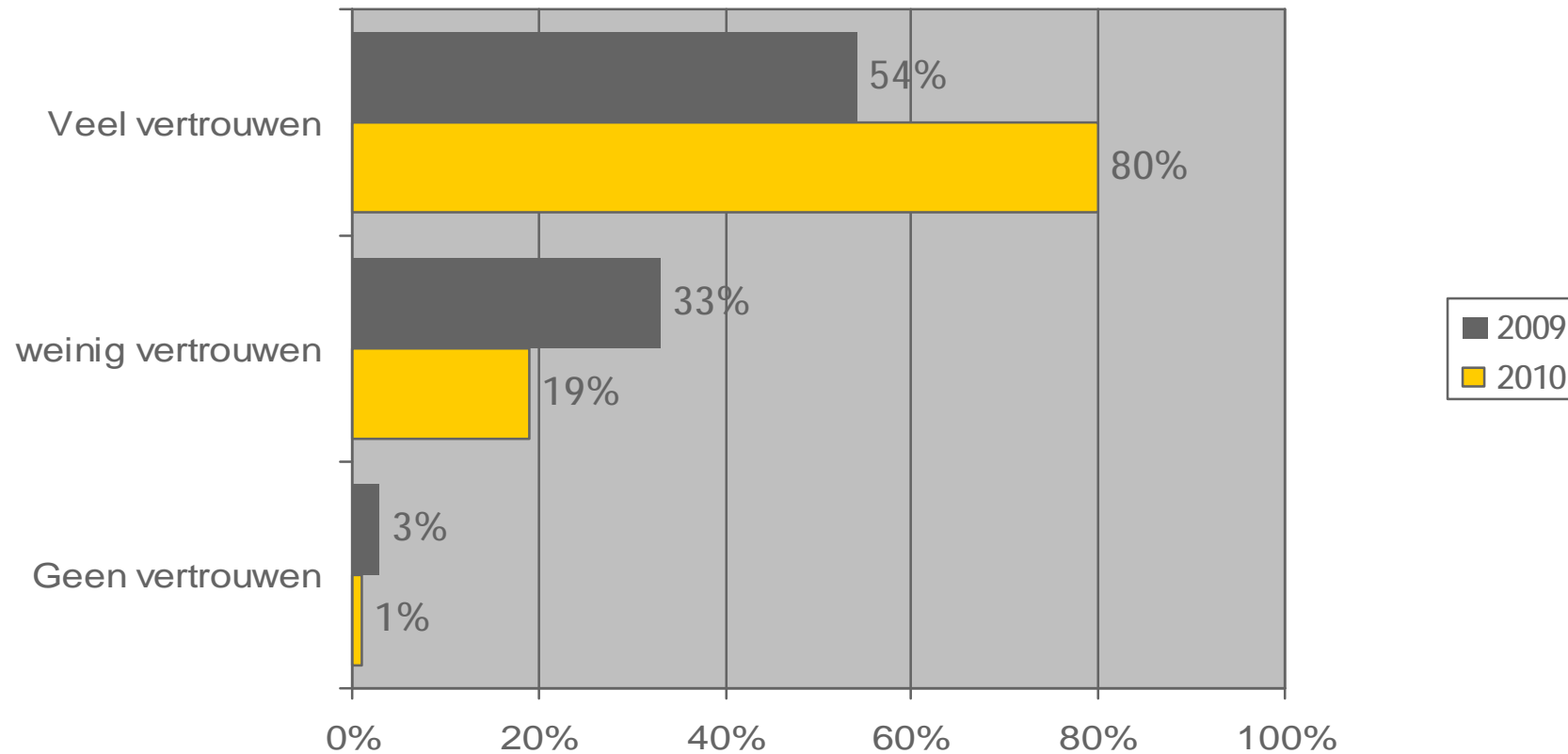
Op welke wijze toetst u de effectiviteit van de maatregelen?



Vertrouwen in beveiliging organisatie

80% van de ondervraagden heeft veel vertrouwen in de beveiliging van de organisatie tegen cybercrime.

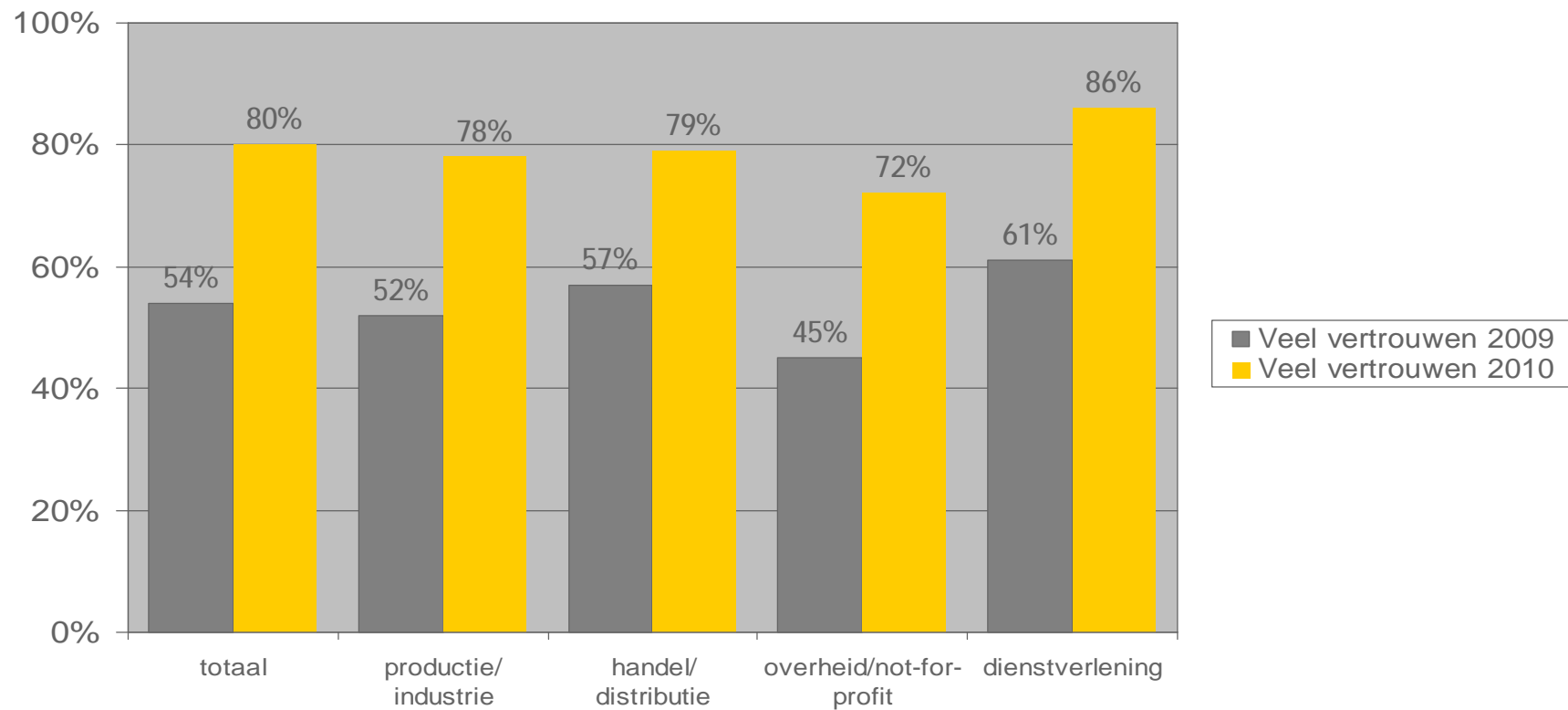
Hoeveel vertrouwen heeft u in de beveiliging van uw organisatie tegen schade door cybercrime activiteiten?



Vertrouwen in beveiliging organisatie in de sectoren

In alle sectoren is het vertrouwen relatief hoog, de overheid blijft wat achter.

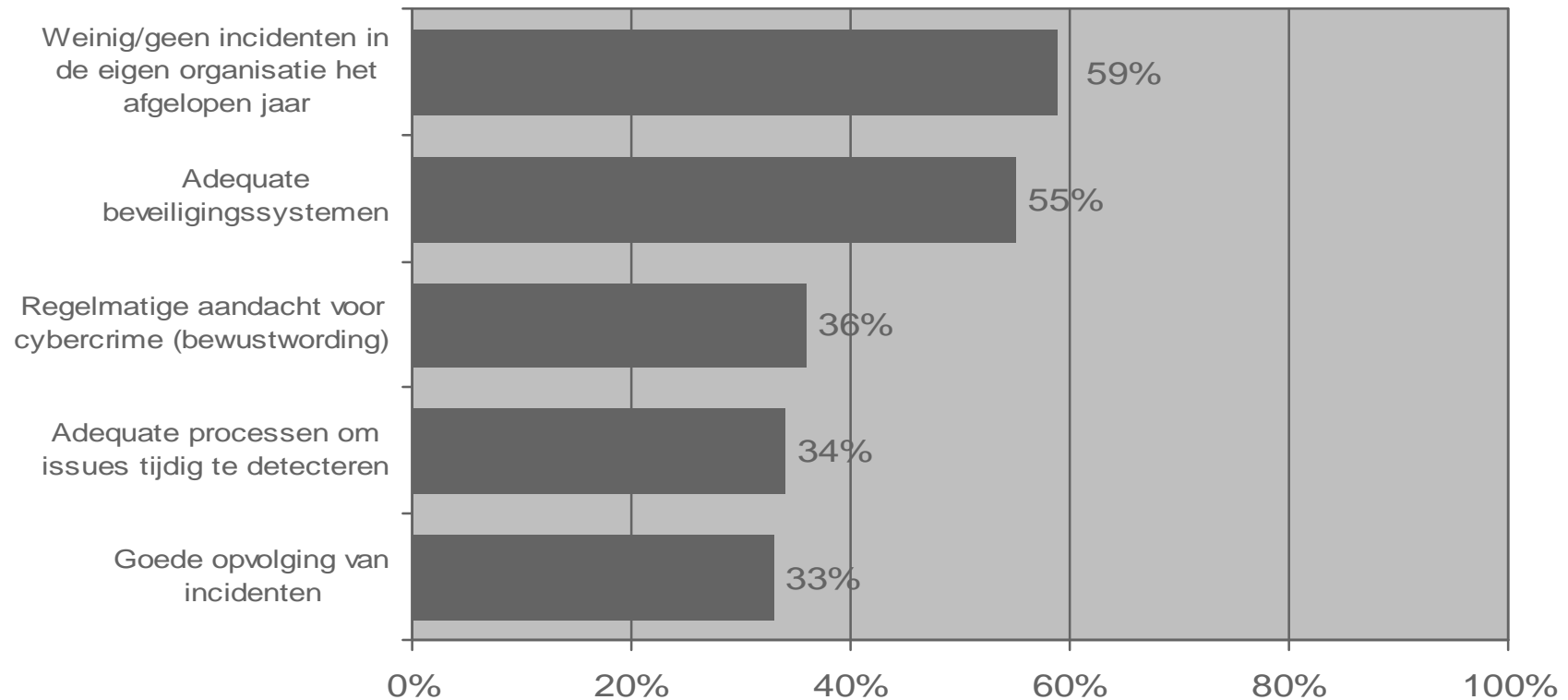
Hoeveel vertrouwen heeft u in de beveiliging van uw organisatie tegen schade door cybercrime activiteiten?



Reden veel vertrouwen in beveiliging

Men heeft vooral veel vertrouwen in de beveiliging vanwege het lage aantal incidenten en goede beveiligingssystemen. Daarnaast is er regelmatig aandacht voor cybercrime en worden issues tijdig gedetecteerd en opgevolgd.

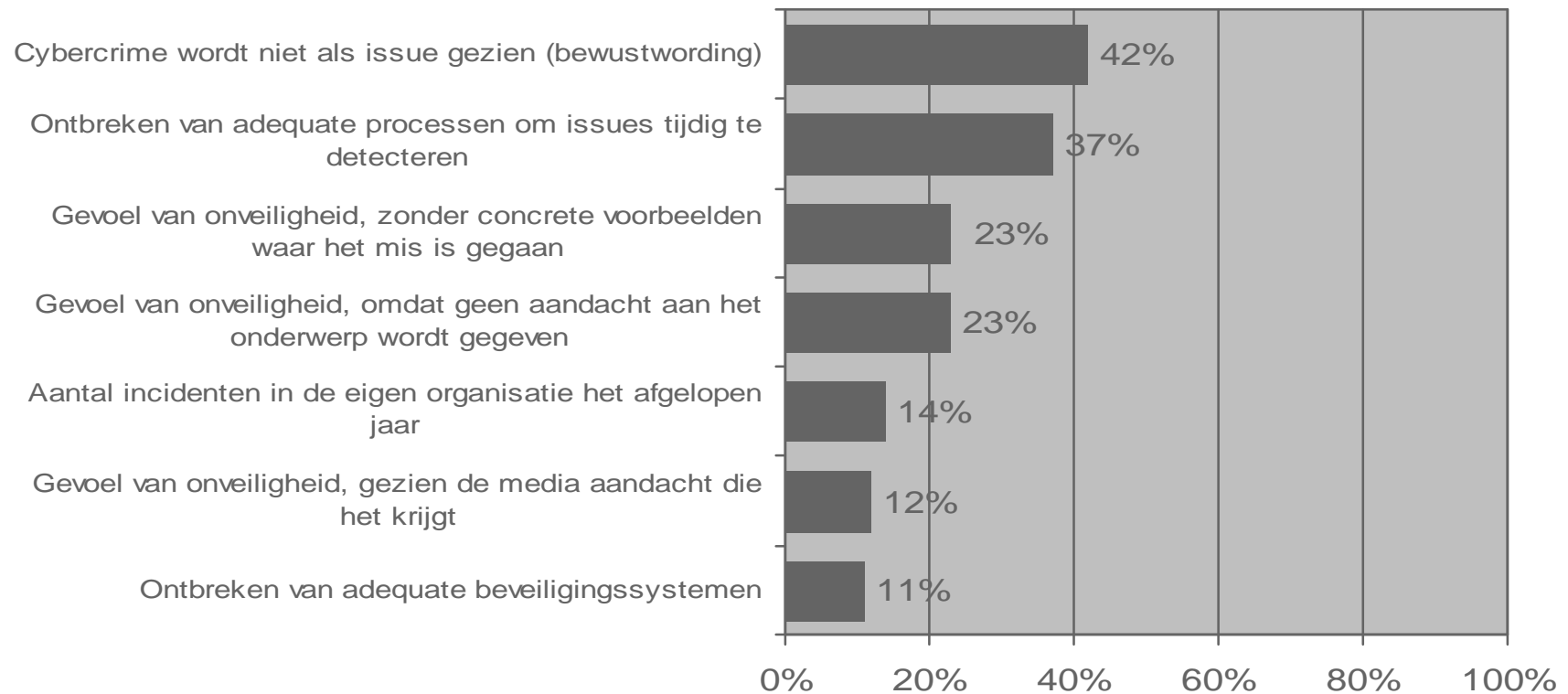
Waarom heeft u veel vertrouwen in de beveiliging van uw organisatie tegen schade door cybercrime activiteiten?



Reden weinig vertrouwen in beveiliging

Men heeft vooral weinig vertrouwen in de beveiliging omdat cybercrime niet als issue wordt gezien en omdat processen voor tijdige detectie ontbreken. Daarnaast heerst er een gevoel van onveiligheid door beperkte aandacht en communicatie.

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



Samenvatting (1/2)

- Acht op de tien organisaties zijn in grote mate afhankelijk van ICT. Dit onderstreept het belang van een goede ICT-beveiliging. Toch beschikt een op de drie organisaties niet over een noodplan voor als de ICT-systemen uitvallen.
- De bestedingen aan ICT-beveiliging nemen per saldo nog licht toe, maar veel minder gestaag dan in periode 2004-2006. De economische crisis speelt hierbij een belangrijke rol. De overheid laat bijna geen groei meer zien. Het komend jaar verwachten de geënquêteerden meer te investeren in (ISO) standaarden, security awareness training en preventie van uitlekken vertrouwelijke gegevens.
- De noodzaak van investeringen in ICT-beveiliging blijkt wel uit de groeiende overlast van cybercrime. De respondenten hebben vooral last van externe bedreigingen, zoals spam en malware. Andere bedreigingen zijn meer incidenteel van aard, maar met grotere gevolgen.
- Voor de toekomst maken de ondervraagden zich de meeste zorgen over opkomende technieken zoals removable media, draadloze netwerken, mobile computing en thuis inloggen op het bedrijfsnetwerk.

Samenvatting (2/2)

- **Bedrijven die het slachtoffer zijn van cybercrime lossen dit meestal zelf op met een onderzoek in eigen beheer. Veel kleinere bedrijven ondernemen helemaal geen actie. Ruim 30% van de grotere organisaties neemt wel degelijk actie.**
- **Een kwart van de organisaties is niet tevreden over de informatievoorziening rondom cybercrime. Justitie en het NICC worden het meest aangewezen als verantwoordelijk voor de informatievoorziening.**
- **De meeste voorkomende maatregelen die worden genomen tegen cybercrime zijn filtersystemen en procedures voor toegang tot systemen en data. Toetsing van deze maatregelen gebeurt vooral in eigen beheer via onderzoek en monitoring.**
- **Acht op de tien organisaties hebben veel vertrouwen in de eigen beveiliging, met name door het lage aantal incidenten, de goede systemen en de regelmatige aandacht. De ondervraagden die weinig vertrouwen hebben (20%) vinden juist dat cybercrime binnen hun organisatie niet als issue wordt gezien en geven aan dat processen voor tijdige detectie ontbreken.**

Informatie



Jacob Verschuur
Director

Telephone: +31 (0)88 40 71521
Fax: +31 (0)88 40 10 05
Mobile: +31 (0)6 21251598
jacob.verschuur@nl.ey.com
www.ey.nl

Ernst & Young Nederland LLP

Ernst & Young ICT Leadership
Cross Towers
Antonio Vivaldistraat 150
1083 HP Amsterdam
P.O. Box 7883
1008 AB Amsterdam
The Netherlands

 **ERNST & YOUNG**

<http://www.ict-barometer.nl>