# Trendrapport over de ICT Security van de Nederlandse industrie 2016

ICT Industry Insights

# Voorwoord

ICT-dienstverlener Simac en haar partner Cisco hebben de handen ineen geslagen om het ICT-securityniveau van de Nederlandse (maak-)industrie in kaart te brengen. Het onderzoek met de titel “ICT Industry Insights” is uitgevoerd onder een groot aantal ICT-verantwoordelijken van grote en middelgrote, industriële bedrijven in Nederland. Hiermee is een representatief beeld verkregen over de wensen, behoeften en de huidige invulling van het ICT-securitybeleid binnen de Nederlandse (maak-)industrie.

In deze rapportage zijn de resultaten beschreven van het kwantitatieve onderzoek dat is voortgekomen uit eerdere kwalitatieve diepte-interviews met de onderzoeksdoelgroep.

Maart 2016.

# Management Summary

## Uitdagingen, bedreigingen en trends

Security-uitdagingen waar organisaties mee te maken hebben, zijn onder meer de mate van bewustwording bij het management, directie, gebruikers en beheerders. Als het puur gaat om ICT loopt tweederde van de organisaties aan tegen de integratie van verschillende systemen, gevolgd door het gebruik van mobiele devices en toegang tot netwerk en data. Ook het correct naleven van wet- en regelgeving en continuïteitsvraagstukken zijn actuele zaken waar organisaties tegenaan lopen. Ontwikkelingen en ICT-trends die hieraan ten grondslag liggen zijn vooral: de cloud, beveiliging (security), big data, bring your own device, internet of things, mobility en virtualisatie.

## Bekendheid wet- en regelgeving

Ruim driekwart van de respondenten is bekend met de wetgeving datalekken en bijna drievijfde is bekend met security-standaarden zoals ISO27001 en ISO27002. Slechts iets meer dan de helft van hen kan ook daadwerkelijk aanduiden wat de standaarden inhouden. Het gaat volgens hen met name om de manier waarop je met data omgaat en dat je kunt aantonen dat je dit volgens de wet- en regelgeving hebt ingericht. Bij eveneens de helft van de respondenten die bekend zijn met de standaarden wordt er daadwerkelijk gewerkt volgens de standaarden.

# Management Summary

## Prioriteit toekenning en beoordeling organisatie

6,9

omgang met
data-security

6,7

omgang met
security door medewerkers
in organisatie

Gemiddeld geven organisaties zichzelf een 6,9 als het gaat om hoe men omgaat met data-security en een 6,7 hoe medewerkers omgaan met security in de organisatie. Organisaties die aangeven dat het ICT-beleid onvoldoende prioriteit krijgt in de organisatie geven zelfs gemiddeld een 5,4-5,6. Er is met name winst te behalen in de bewustwording bij de gebruiker (wachtwoorden delen, gele post-its op het beeldscherm, etc.) en in het monitoren. Desondanks geeft meer dan viervijfde aan dat de ICT-risico's in de organisatie goed in kaart gebracht zijn, vooral door audits. Slordigheden, onvolledigheden en een gebrek aan belangstelling (onvoldoende prioriteit) zijn de meest genoemde oorzaken bij organisaties die de risico's (nog) niet goed in kaart gebracht hebben. Als het gaat om het toegangs- en wachtwoordenbeleid zien we dat medewerkers in vrijwel alle organisaties hier naar handelen, al dan niet afgedwongen door beleid, management en/of directie. In veel organisaties waar het, naar eigen zeggen goed gaat, wordt dit volgens de respondenten afgedwongen door beleidsregels en/of wordt het personeel bewust gemaakt van de risico's door trainingen/cursussen.

Thuiswerken wordt in de meeste organisaties gefaciliteerd. In bijna tweederde van de organisaties heeft men een gescheiden netwerk tussen kantoor en productie en in de helft van de organisaties werkt men volgens een security architectuur. Verder valt op dat bijna de helft aangeeft dat de netwerken (nog) niet optimaal beveiligd zijn. De helft van hen besteedt momenteel nauwelijks iets uit qua ICT-zaken.

# Inhoudsopgave

# 1. Inleiding

## 1.1 Onderzoeksopzet

Om inzicht te verkrijgen in de wensen en behoeften van ICT-managers, is onderstaande hoofdonderzoeksvraag geformuleerd:

“ Hoe staan ICT-managers tegenover ICT-compliance, welke wensen en behoeften hebben zij en welke verbeterpunten vloeien hieruit voort? ”

### Onderwerpen

Hierbij komen de volgende onderwerpen aan bod:

- Marktontwikkelingen industriële sector;
- ICT en het belang voor de organisatie;
- ICT in relatie tot compliance;
- ICT in relatie tot security.

### Doelgroep

ICT-managers (of degene die (mede-)verantwoordelijk is voor de ICT binnen de organisatie) van middelgrote en grote industriële bedrijven.

## 1.2 Respons en betrouwbaarheid

Het veldwerk heeft gelopen van 17 december 2015 t/m 24 januari 2016.
Van de 320 bedrijven hebben 88 respondenten deelgenomen aan het onderzoek. Dit komt neer op een responspercentage van 28%.

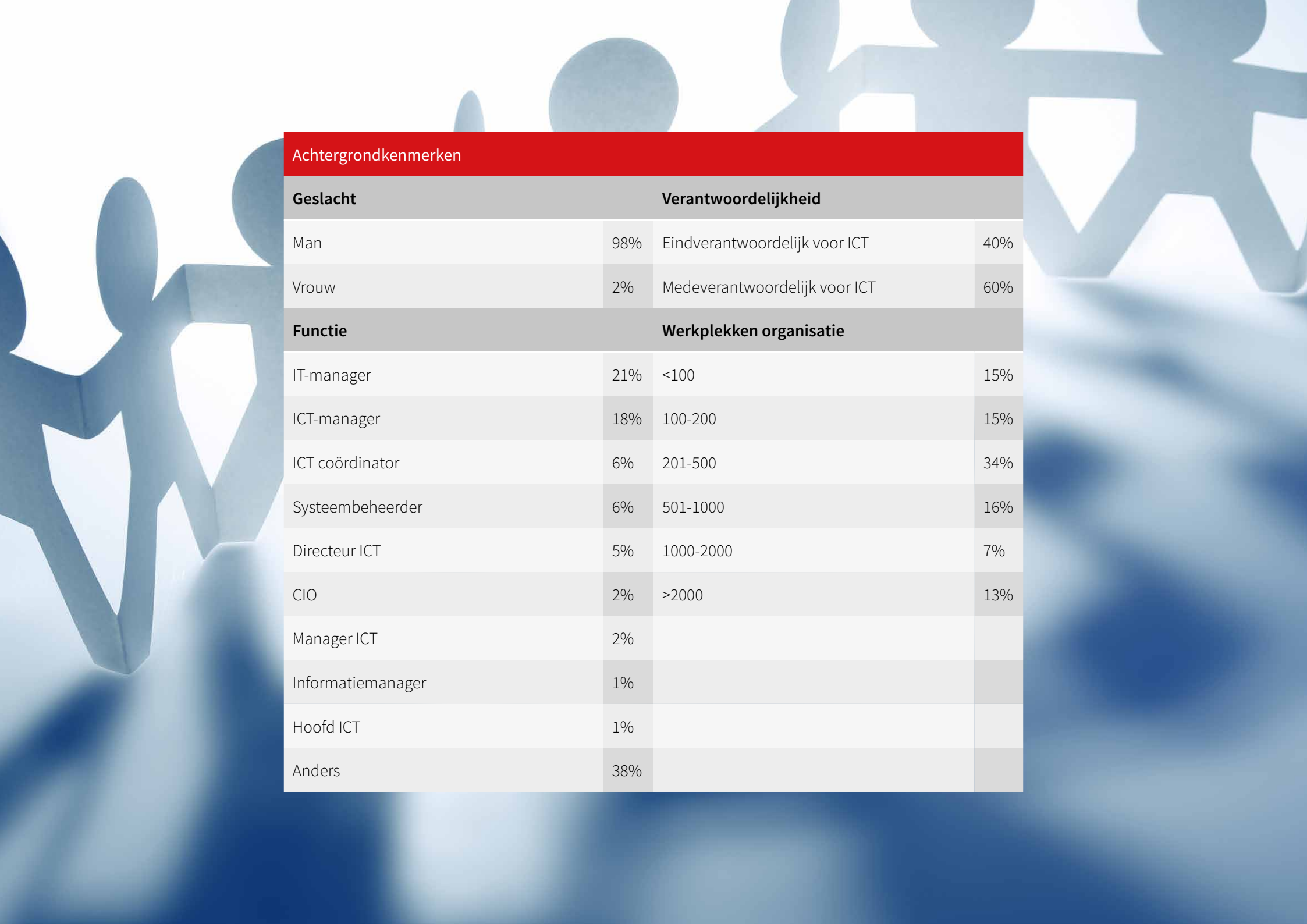
| Respons | | | |
|---|---|---|---|
| | Bruto | Netto | Percentage |
| Respondenten | 320 | 88 | 28% |

Met een netto steekproef van 88 respondenten kan een betrouwbaarheid van 95% met een interval van maximaal 8,9% rondom de gevonden antwoorden worden gerealiseerd. In praktijk betekent dit dat wanneer een uitkomst uit het onderzoek 50% is, dit in werkelijkheid tussen de 41,1% en 58,9% ligt.

# 2. Steekproefsamenstelling

## Achtergrondkenmerken

In de tabel op de pagina hiernaast worden de steekproefspecificaties weergegeven van de respondenten die hebben deelgenomen aan het onderzoek. Door afronding kan het voorkomen dat percentages optellen tot boven of onder de 100%.



| Achtergrondkenmerken | | | |
|---|---|---|---|
| **Geslacht** | | **Verantwoordelijkheid** | |
| Man | 98% | Eindverantwoordelijk voor ICT | 40% |
| Vrouw | 2% | Medeverantwoordelijk voor ICT | 60% |
| **Functie** | | **Werkplekken organisatie** | |
| IT-manager | 21% | <100 | 15% |
| ICT-manager | 18% | 100-200 | 15% |
| ICT coördinator | 6% | 201-500 | 34% |
| Systeembeheerder | 6% | 501-1000 | 16% |
| Directeur ICT | 5% | 1000-2000 | 7% |
| CIO | 2% | >2000 | 13% |
| Manager ICT | 2% | | |
| Informatiemanager | 1% | | |
| Hoofd ICT | 1% | | |
| Anders | 38% | | |

# 3. Onderwerpen

## ICT-trends in de industriële sector

Meest genoemde ICT-trend in de industriële sector is volgens de respondenten “de cloud”. Andere trends die meermaals genoemd worden zijn:

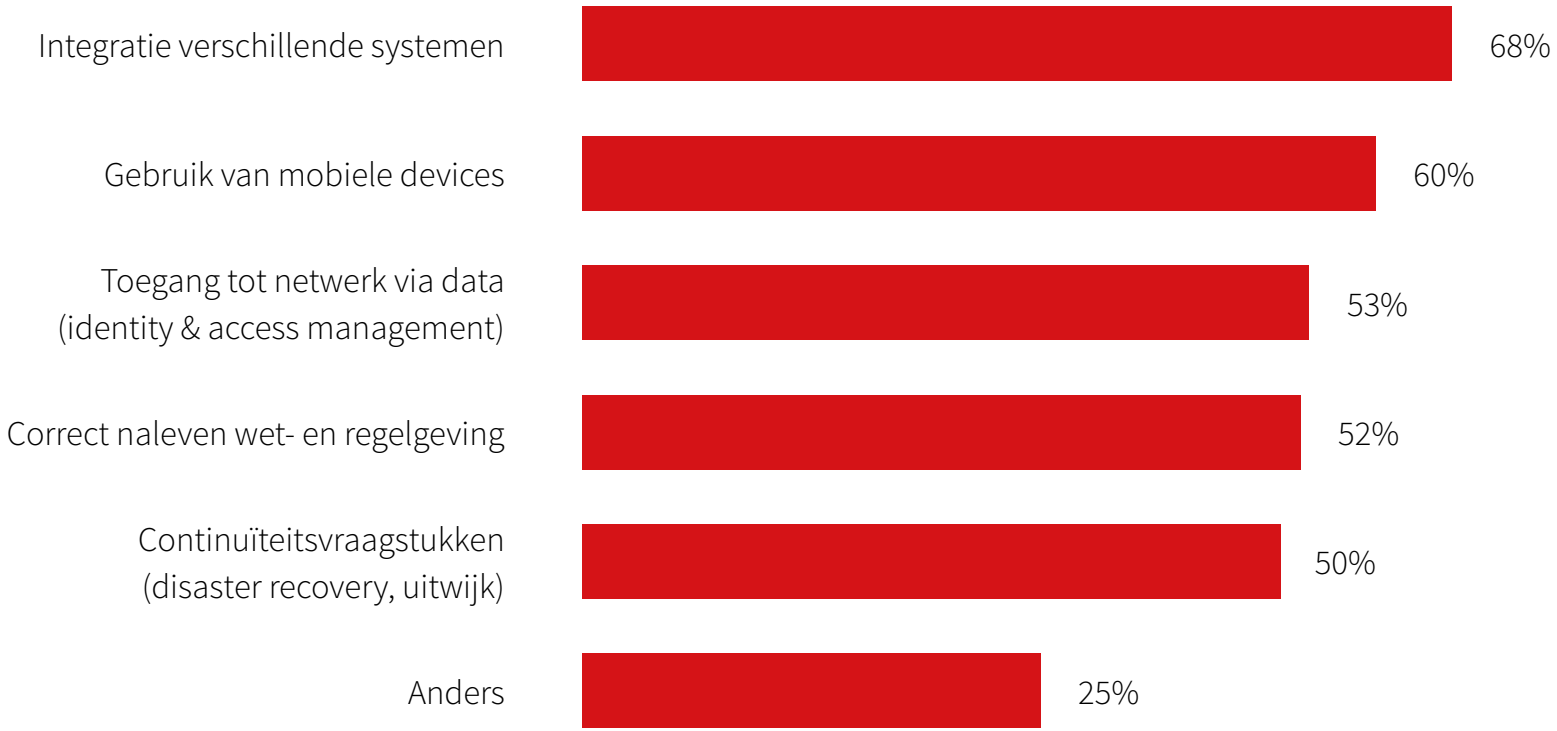
- Beveiliging/security
- Big data
- Bring your own device
- Internet of things
- Mobiel werken
- Mobiliteit
- Mobile devices
- Virtualisatie

## Waar loopt men weleens tegenaan?

Respondenten geven aan met name tegen de integratie van verschillende systemen aan te lopen (68%). Over het algemeen zien we dat hoe meer werkplekken een organisatie heeft (tot 2000), hoe vaker men aangeeft tegen bepaalde problemen aan te lopen.

## Waar loopt men tegen aan

in de organisatie als het gaat om ICT



## 3.1 Marktontwikkelingen industriële sector

### Security-uitdagingen binnen de organisatie

De meest uiteenlopende security-uitdagingen worden genoemd, waar men binnen de organisatie mee te maken heeft. Enkelen hiervan zijn:

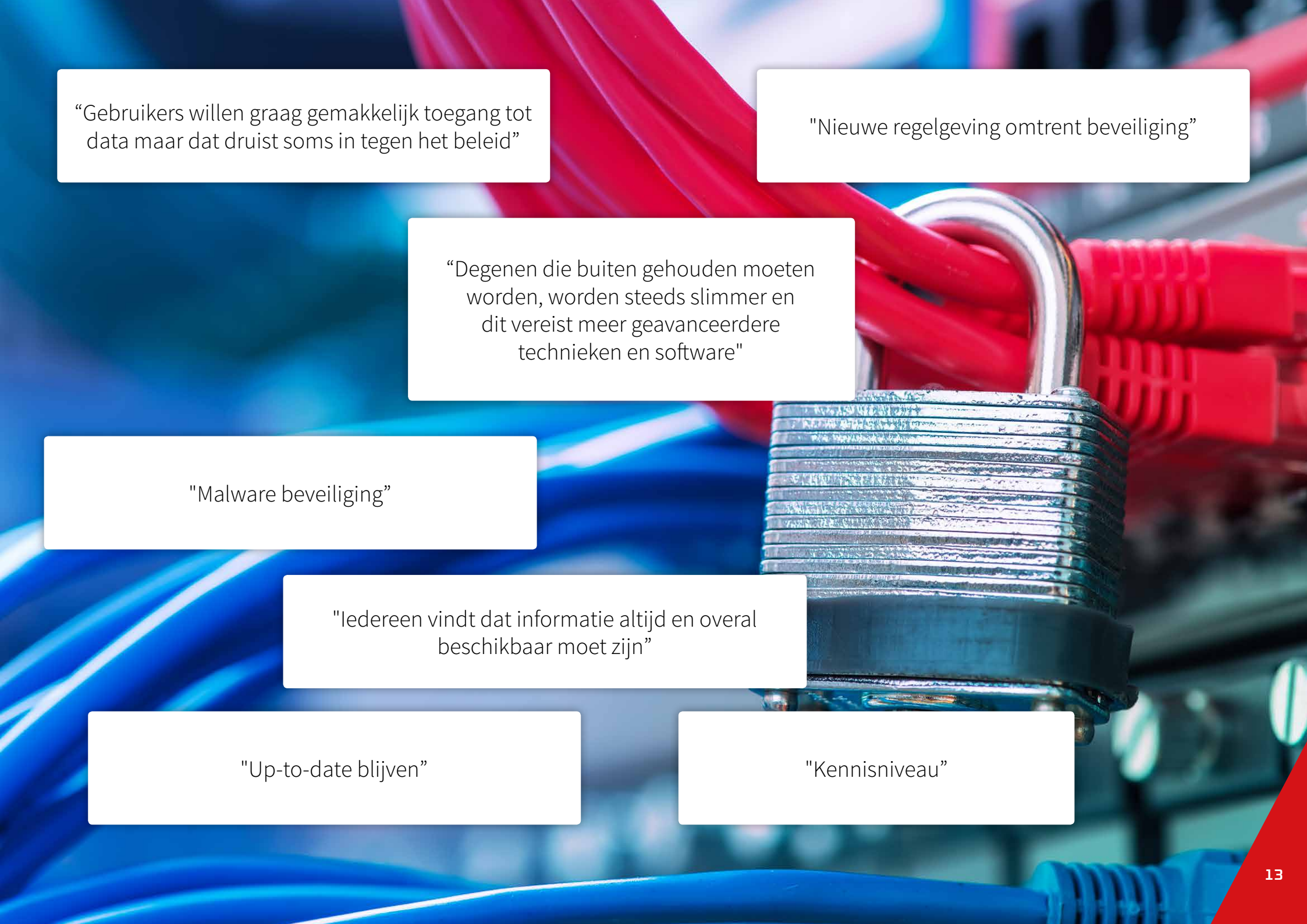
"Awareness bij gebruikers én beheerders"

"Data-beveiliging versus gebruikersgemak"

"Bewustwording bij management en directie"

"De hoge eisen van beveiligingen"

"Wachtwoorden van gebruikers"


“Gebruikers willen graag gemakkelijk toegang tot data maar dat druist soms in tegen het beleid”
"Nieuwe regelgeving omtrent beveiliging”
“Degenen die buiten gehouden moeten worden, worden steeds slimmer en dit vereist meer geavanceerdere technieken en software"
"Malware beveiliging”
"Iedereen vindt dat informatie altijd en overal beschikbaar moet zijn”
"Up-to-date blijven”
"Kennisniveau”

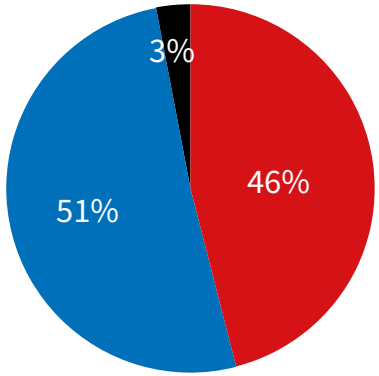
# Helft industriële bedrijven heeft netwerken niet optimaal beveiligd!

## 3.2 ICT en het belang voor de organisatie

### De manier waarop de ICT is ingericht/geregeld in de organisatie

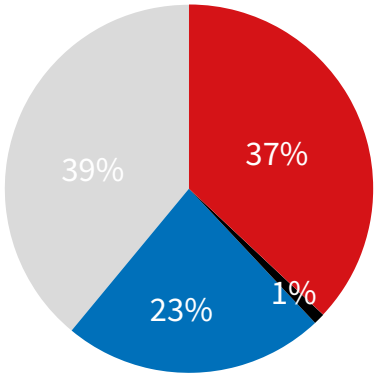
In de meeste organisaties wordt thuiswerken gefaciliteerd, ook kent bijna twee derde een gescheiden netwerk tussen kantoor en productie en de helft werkt volgens een security architectuur.
Bijna de helft van de organisaties geeft aan dat netwerken (nog) niet optimaal beveiligd zijn.
De meeste organisaties werken hybride of op eigen servers. 40% geeft aan veel ICT-zaken uit te besteden en een kwart besteedt nauwelijks iets uit.

## Beveiliging netwerken



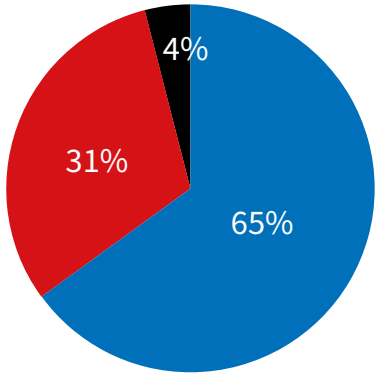

- Optimaal beveiligd
- Nog niet optimaal beveiligd
- Weet niet

## Waar werkt men in?



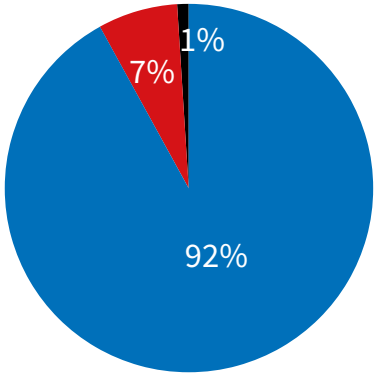

- Hybride
- Private cloud
- Eigen servers
- Public cloud

## Heeft u een gescheiden netwerk tussen kantoor en productie?



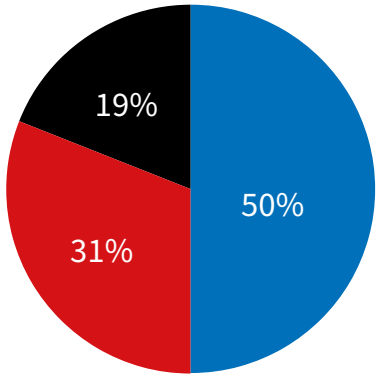

- Ja
- Nee
- Weet niet

## Wordt thuiswerken gefaciliteerd?



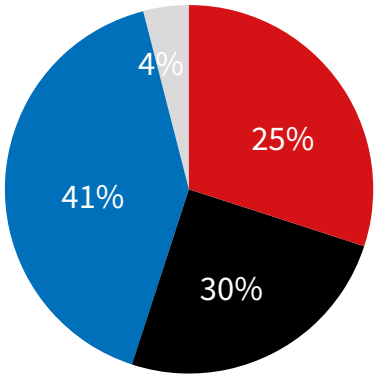

- Ja
- Nee
- Weet niet

## Werkt u volgens een security architectuur?




- Ja
- Nee
- Weet niet

## Besteedt men ICT-zaken uit?




- Alles
- Veel
- Enigszins
- Nauwelijks

Van degenen die aangeven dat het netwerk (nog) niet optimaal beveiligd is, besteedt de helft nauwelijks iets uit qua ICT-zaken.

# Bij bijna 1 op de 5 krijgt het ICT-beleid niet voldoende prioriteit

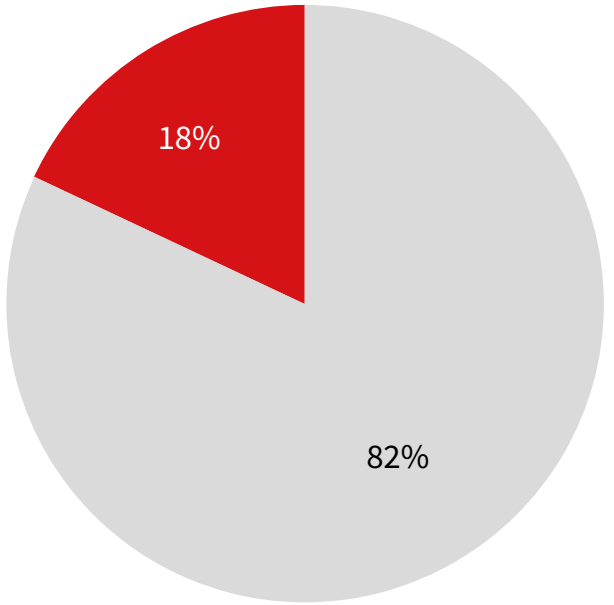
## Krijgt het ICT-beleid voldoende prioriteit?

Volgens 82% van de respondenten krijgt het ICT-beleid voldoende prioriteit in de organisatie. Men beargumenteert dit onder meer als volgt:

- “Absoluut, er zijn behoorlijke budgetten en een strategisch plan van waar wij naar toe willen.”;
- “De prioriteit stelling moet gezien worden t.o.v. andere bedrijfsaspecten. Er zou meer aandacht kunnen zijn voor het ICT-beleid maar dat mag niet ten koste gaan van onze core business.”;
- “Er is nooit genoeg budget. Derde partijen worden behoorlijk onder druk gezet om zo goedkoop mogelijk, maar wel volgens alle regels te leveren.”;
- “Het belang van ICT wordt door de directie goed ingezien, voldoende mogelijkheid nieuwe ontwikkelingen te testen en eventueel in te voeren.”;
- “Jaarlijkse audit met daar aangekoppeld een plan van aanpak.”

Respondenten die aangeven dat het niet voldoende prioriteit krijgt, zeggen onder meer:

- “IT is een ondersteunende activiteit maar kan meer betekenen voor een organisatie. Er kan nog meer uitgehaald worden en dus meer mogelijkheden aanbieden.”;
- “Loopt altijd achter de feiten aan.”



# 44% van de ICT-managers uit de industrie weet niet wat ISO-standaarden inhouden

## 3.3 ICT in relatie tot compliance

### Wordt er in de organisatie via security-standaarden gewerkt?

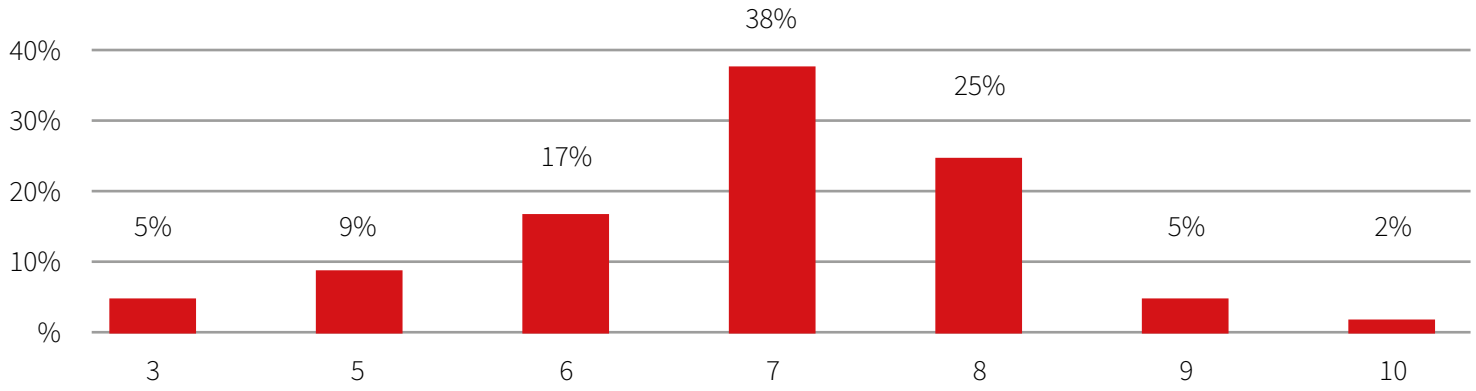
Ruim de helft van de respondenten (54%) die bekend zijn met de security-standaarden geeft aan dat er in de organisatie volgens deze standaarden gewerkt wordt. Minder eindverantwoordelijken voor ICT (41%) geven aan dat er volgens deze standaarden gewerkt wordt dan medeverantwoordelijken (63%).
Wat verder opvalt is dat 44% van de ICT-managers uit de industrie niet weet wat de ISO-standaarden inhouden!

## Hoe gaat men om met data-security?

Als respondenten een cijfer moeten geven op een schaal van 1 t/m 10 aan de manier waarop de organisatie omgaat met data-security, zien we een gemiddeld cijfer van 6,9.

Meest gegeven cijfer is een 7 (38%), 14% geeft de eigen organisatie een onvoldoende en 7% geeft een 9 of een 10. Organisaties die aangeven dat het ICT-beleid niet voldoende prioriteit krijgt (18%), zijn een stuk kritischer (5,4) dan organisaties die aangeven dat het ICT-beleid wel voldoende prioriteit krijgt (7,2).

1 staat voor helemaal niet goed, 10 staat voor heel erg goed



## Beargumentering

**0-5**

Cijfer 5 of lager

- “Denk dat we het technisch voor elkaar hebben, maar er zijn voortdurend nieuwe bedreigingen. Het bewustzijn van de gebruikers is het grootste risico. Daar moeten we voortdurend aan werken.”
- “Enkel een simpele basis is geïmplementeerd, maar er wordt niet aan monitoring gedaan.”
- “Er is eigenlijk totaal géén beveiliging.”
- “Het maken van een kopie is zeer eenvoudig. Validatie daarvan ligt bij de gebruiker. MT heeft onvoldoende aandacht hiervoor.”
- “Onvoldoende, de awareness bij de gebruiker.”
- “Vanuit corporate misschien wel een 7, vanuit de medewerkers 4/5.”
- “Veel werkstations nog niet gelocked als men wegloopt, veel geprinte informatie makkelijk bereikbaar door derden etc., makkelijk wachtwoorden delen met collega's i.v.m. vakantie back-up en dergelijke.”

**6-8**

Cijfer 6 t/m 8

- “De beveiliging is goed, werken met encripted mobile devices, packet inspection firewalls, alles is beleidsmatig vastgelegd.”
- “Eindgebruikers zijn nog steeds niet goed op de hoogte van de risico's van IT.”
- “Iedereen bij ons weet hoe belangrijk data-security is. Het besef is aanwezig.”
- “Omdat het een klein bedrijf is en de gebruikers zelf installatierechten hebben, is de security misschien wat minder.”
- “Technisch zijn veel maatregelen genomen er is echter nog niet veel gedaan met het "opvoeden" van de medewerkers.”

**9/10**

Cijfer 9 of 10

- “Gescheiden netwerken voor gasten en medewerkers.”;
- “Ze zijn heel streng in de security. De mensen zijn zich bewust en leven de regels goed na. Er is een trainingsprogramma voor de medewerkers en er is kortgeleden een spam-test gehouden met meting. Slechts 17% heeft de link geopend.”

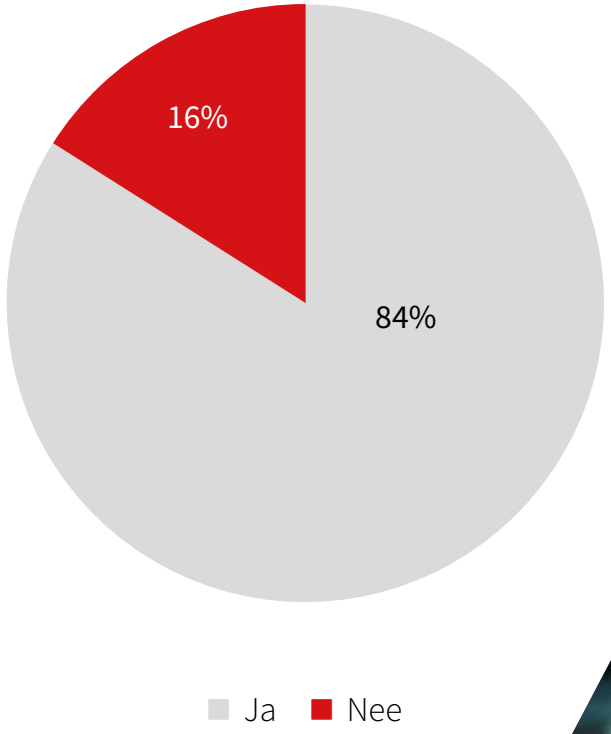
## Risico's goed in kaart gebracht?

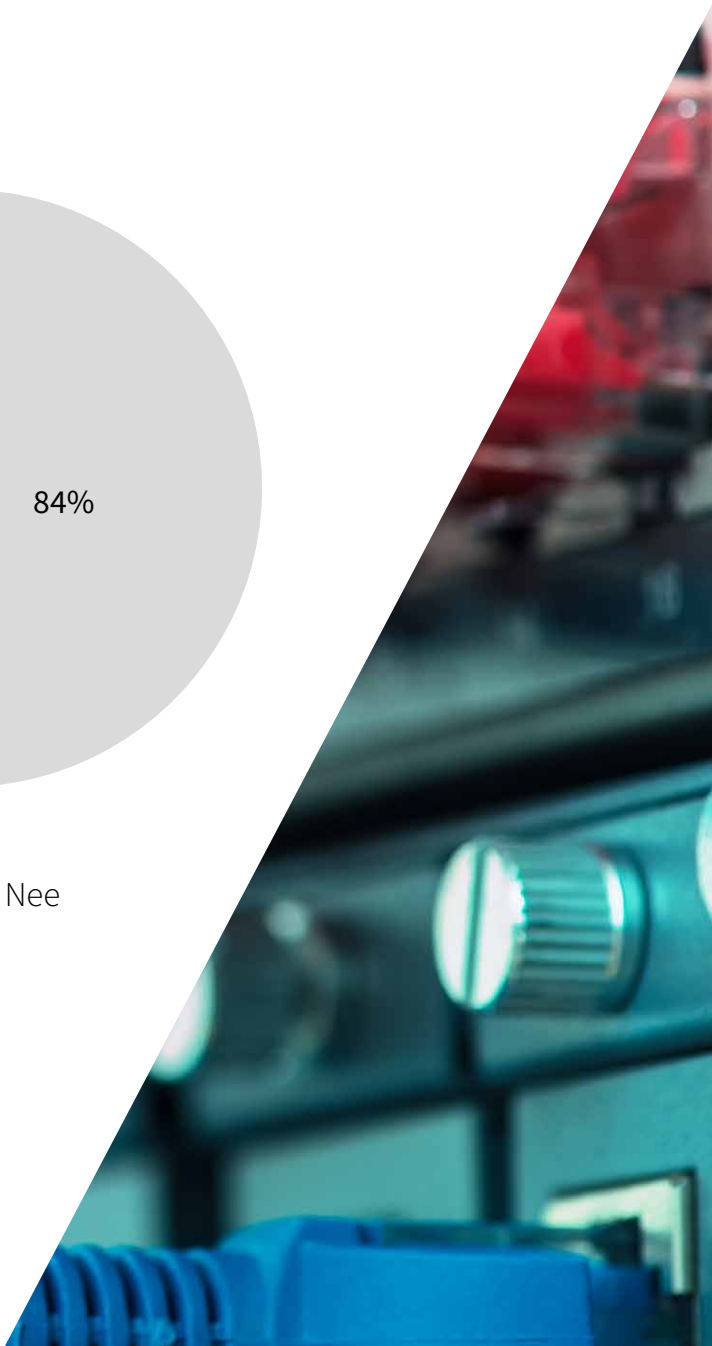
Volgens 84% van de respondenten zijn de ICT-risico's goed in kaart gebracht in de organisatie. Zij beargumenteren dit onder meer als volgt:

- "Audits, plannen en ICT staan prominent op de agenda bij IT-ers die met klanten praten. Ik c.q. mensen van mij zit(ten) vrijwel altijd bij dit soort gesprekken."
- "Dat is één van de eisen die onze accountant stelt."
- "Er wordt veel binnen de internationale organisatie samengewerkt op dit gebied, zodoende is er veel kennis en veel ervaring."
- "Jaarplannen, ISO-audit en accountants-audits en de aandacht die daar voor is. Dit in combinatie met de continuïteit van de organisatie."
- "Omdat wij zelf met onze IT kritisch kijken, van buiten af worden scans uitgevoerd."
- "We hebben audits en kijken zelf ook kritisch naar de organisatie ook samen met onze partners."

De andere 16% geeft aan dat dit niet goed in kaart is gebracht omdat er: 1) nog veel slordigheden en onvolledigheden zijn en 2) er een gebrek aan belangstelling voor is (het krijgt onvoldoende prioriteit).

- “Gebrek aan tijd en belangstelling.”
- “Vroeger stond het al helemaal niet op de agenda, tegenwoordig is het een voetnoot. Echt aandacht ervoor is er nog niet.”



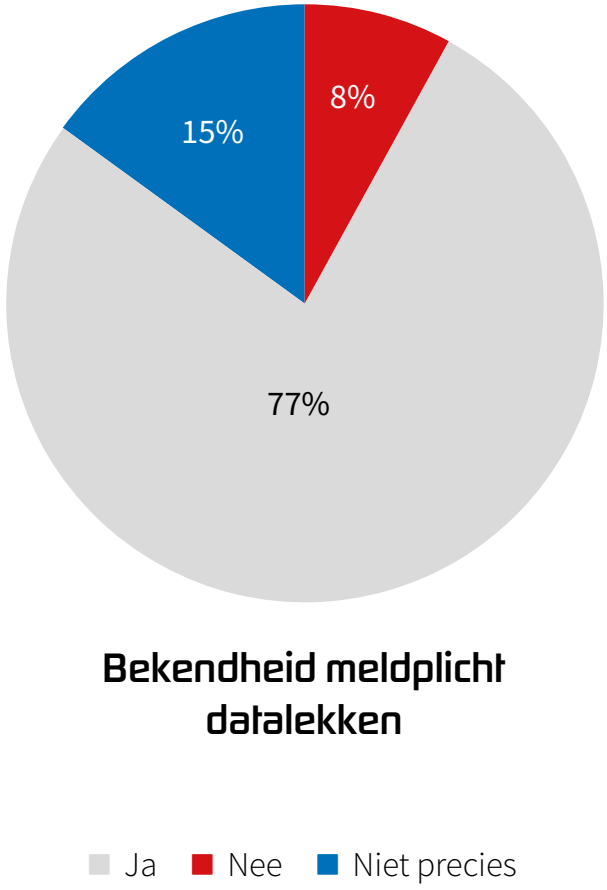
## 3.4 ICT in relatie tot security

### Bekendheid wetgeving meldplicht 1 januari 2016

Ruim drie kwart van de respondenten (77%) geeft aan bekend te zijn met de wetgeving meldplicht datalekken, die per 1 januari 2016 van kracht is gegaan. We zien hierbij dat meer eindverantwoordelijken (82%) dan medeverantwoordelijken (74%) hiervan op de hoogte zijn. Daarnaast blijkt de bekendheid van deze wetgeving beduidend lager te zijn onder bedrijven met minder dan 100 werkplekken (39% bekendheid versus ≥ 73% organisaties met 100 of meer werkplekken).

### Handelen volgens toegangs- en wachtwoordenbeleid

Als het gaat om het toegangs- en wachtwoordenbeleid zien we dat 97% van mening is dat medewerkers hier enigszins tot zeker naar handelen (afgedwongen).

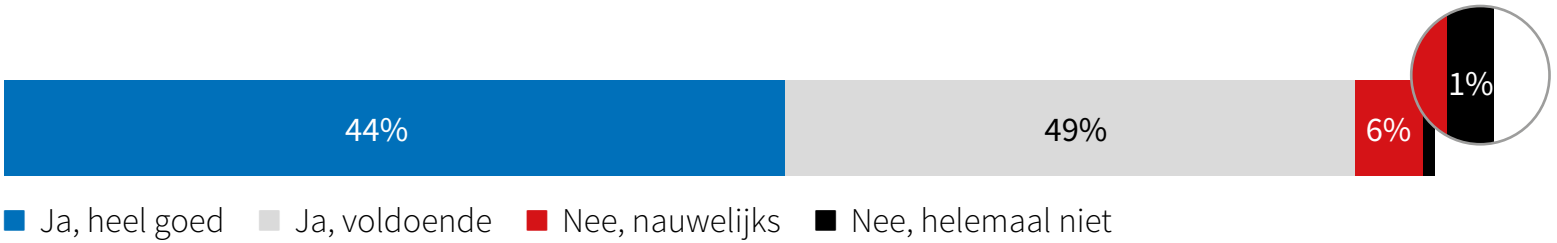


# Vrijwel alle organisaties vinden dat zij een goed toegangs- en wachtwoordenbeleid hebben.

Bij doorvragen blijkt dat veel medewerkers toch nog steeds wachtwoorden onderling doorgeven en gele post-its plakken op hun beeldscherm met data-gegevens…

## Bewapend tegen malware

Ruim twee vijfde (44%) van de respondenten acht zich heel goed bewapend tegen malware, bijna de helft (49%) acht dit voldoende.

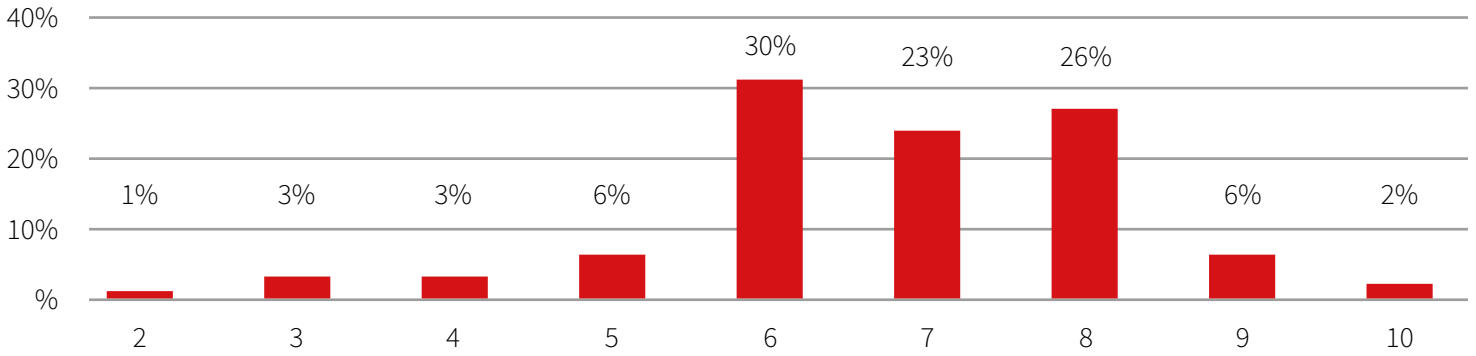



## Omgang medewerkers met security

Als respondenten een cijfer moeten geven op een schaal van 1 t/m 10 aan de manier waarop medewerkers omgaan met security in de organisatie, zien we een gemiddeld cijfer van 6,7.
Meest gegeven cijfer is een 6 (30%), 14% geeft de medewerkers een onvoldoende en 8% geeft een 9 of een 10.
Organisaties die aangeven dat het ICT-beleid niet voldoende prioriteit krijgt zijn een stuk kritischer (5,6) dan organisaties die aangeven dat het ICT-beleid wel voldoende prioriteit krijgt (7,0).

## Hoe goed gaat men om met security?

1 staat voor helemaal niet goed, 10 staat voor heel erg goed



# Organisaties geven de manier waarop medewerkers omgaan met data-security slechts een 6,7

## Beargumentering

Wanneer we vragen het gegeven cijfer te beargumenteren, zien we onder meer de volgende antwoorden.

**0-5**

Cijfer 5 of lager

- “De medewerkers houden zich niet aan regels, plakken post-it's op de monitor, gebruiken elkaars wachtwoorden enz.”
- “Onvoldoende, nog veel werk te verrichten. Denk aan: nonchalance, niet nadenken. Het is maar bedrijfsdata. Thuis zijn ze accurater.”
- “Onvoldoende awareness, de gebruiker vindt het allemaal lastig, nog geen mandaat. Nog steeds; geeltjes op beeldschermen.”
- “Veel gebruikers vinden security maatregelen erg lastig en vinden wegen om er omheen te werken. Sommige medewerkers gebruiken privé clouddiensten om bedrijfsgegevens (tijdelijk) op te slaan.”
- “Wachtwoorden doen ze goed, awareness is matig. Denk aan de geeltjes op beeldschermen.”
- “Wachtwoorden voor allerlei systemen worden te makkelijk gedeeld, werkstations nog lang niet allemaal gelocked bij weglopen, geen enkel document heeft beveiligingsclassificatie.”

**6-8**

Cijfer 6 t/m 8

- “Goeie en slechte gevallen tussen de mensen dat geeft een gemiddelde. Mentaliteit verschilt ook per land, onze Chinese vestiging is veel slordiger.”
- “Het wordt afgedwongen. Wachtwoord wijzigen moet, anders word je geblokkeerd.”
- “Matig, awareness is belangrijk. Nonchalance, paswoorden delen, geeltjes op schermen. Laptop op kantoor laten etc.”
- “Medewerkers realiseren zich onvoldoende wat de risico's zijn van onzorgvuldig handelen.”
- “Personeel volgt regelmatig een cursus waar ze voor moeten slagen, goed wachtwoordenbeleid.”
- “Voldoende, sommigen zijn makkelijk met paswoord of even inloggen en dan weglopen. Ik kom daar dan bij toeval achter.”

**9/10**

Cijfer 9 of 10

- “Dit is policy en er worden audits uitgevoerd.”
- “Er zijn regels en die worden nageleefd.”

# 4. Conclusie en advisering

De ICT-veiligheidsstatus van de Nederlandse industrie laat nog zeer te wensen over. De helft van de bedrijven vindt dat hun netwerken nog niet optimaal zijn beveiligd.

Het omgaan met data(-security) in de organisatie wordt door bedrijven zelf gewaardeerd met nog geen 7,0 gemiddeld. Organisaties die aangeven dat het ICT-beleid onvoldoende prioriteit krijgt, geven zelfs een onvoldoende.

Met name in de bewustwording bij medewerkers ligt een grote uitdaging. Het komt regelmatig voor dat wachtwoorden gedeeld worden of dat er gele post-its op de beeldschermen geplakt zijn met data-gegevens e.d. Bedrijven kunnen hierop inspelen door actief cursussen/trainingen aan te bieden om enerzijds de noodzaak van data-security duidelijk te maken en anderzijds medewerkers bewust te maken van de dagelijkse risico's die een bedrijf loopt als er niet nauwkeurig met data wordt omgegaan.

Daarnaast lopen organisaties aan tegen de integratie van verschillende systemen, het gebruik van mobiele devices en toegang tot netwerk en data. Maar liefst de helft van de organisaties besteedt nauwelijks tot enigszins ICT-zaken uit.

**De initiatiefnemers van dit representatieve onderzoek binnen de Nederlandse industrie zijn ICT-dienstverlener Simac en IT-wereldspeler Cisco. Samen bieden zij diverse oplossingen voor een optimale IT-security-omgeving en -netwerk. Voor vragen over dit onderzoek en specifieke security-vraagstukken kunt u direct contact opnemen met Simac op nummer 040 258 29 11 of kijk op www.simac.com.**

**SIMAC**
Postbus 340
5500 AH Veldhoven
T. +31 (0) 40 258 29 44
E. info@simac.com
F. +31 (0) 40 258 27 07