DATA SHARING REPORT



Blind vertrouwen

Cybersecurity en de afhankelijkheid van IT-partners

58% vindt wat IT-partners met hun data doen een black box en vertrouwt er toch op

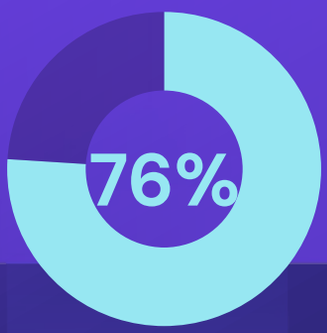
18% REGELT HET INFORMEEL OF NIET • p 15

Drie vragen voor je IT-partner • p 14

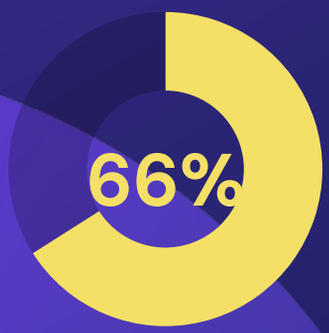
Onderzoek onder 433 beslissers bij Nederlandse organisaties (250+ medewerkers)

SureSync

Vier inzichten in één oogopslag



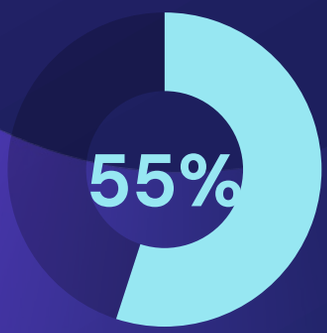
controleert bij contract-verlenging vrijwel altijd, regelmatig of vaak op certificeringen



voert minstens één keer per jaar een audit uit bij IT-partners



is voor toezicht op IT-partners afhankelijk van de expertise van een andere partij



heeft onvoldoende controle over waar de eigen data zich bevindt

SureSync

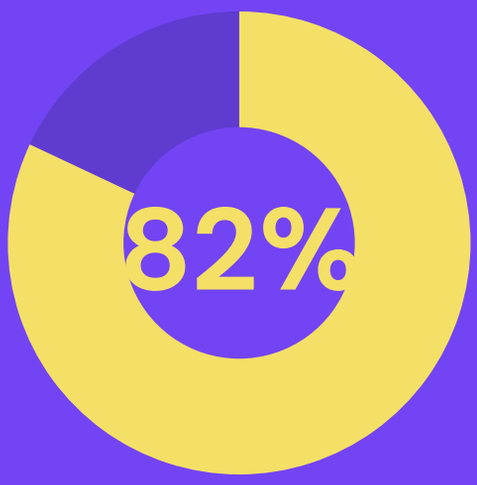
IT uitbesteden kan. De verantwoordelijkheid niet.

Of het nu gaat om het uitbetalen van salarissen, het versturen van facturen of het bewaren van klantgegevens: een organisatie doet dat vaak met systemen van externe partijen. Daarmee staat ook gevoelige data van medewerkers en klanten buiten de deur. IT uitbesteden kan, maar de verantwoordelijkheid voor de data blijft bij de organisatie zelf.

Hoe zorgvuldig met die data wordt omgegaan, hangt grotendeels af van de IT-partner, zeker wanneer die data ook nog eens met andere partijen in de keten wordt gedeeld.

Om in kaart te brengen hoe organisaties omgaan met die afhankelijkheid van IT-partners, deden wij onderzoek onder 433 beslissers en beïnvloeders op het gebied van IT, Finance, Data, Compliance en Legal, werkzaam bij organisaties met 250 medewerkers of meer. Drie hoofdvragen stonden centraal. Hoe goed is de afhankelijkheid van IT-partners geregeld, hoeveel grip houden organisaties in de praktijk op hun data, en hoe groot is het besef van de risico's die daarbij horen?

Victor den Bak, Portfolio Architect bij SureSync, leidt ons door de resultaten. Vanuit zijn werk aan datastrategie en systeemarchitectuur beantwoordt hij de vraag die onder deze cijfers schuilgaat: hoeveel kun je als organisatie overlaten aan een IT-partner, en welke verantwoordelijk-heden blijven altijd van jou?



van de ondervraagde organisaties heeft afspraken met IT-partners over data-veiligheid vastgelegd.

Maar bij **44%** is dat slechts deels, en 42% weet niet zeker of er de afgelopen twee jaar een incident was.

> *"Hoe de IT is ingericht, is het fundament van een organisatie."*
>
> **Victor den Bak**
> Portfolio Architect, **SureSync**

Dit rapport neemt je mee door vijf bevindingen. We beginnen bij de afspraken die organisaties met IT-partners maken, kijken daarna naar controle en zicht op data, staan stil bij incidenten en risicobesef, en sluiten af met wat organisaties nu zelf kunnen doen.



Op papier is de afhankelijkheid geregeld

SureSync

Wanneer organisaties hun data uit handen geven, beginnen ze met het maken van afspraken. Daar zijn de meeste organisaties het over eens.

Acht op de tien (82%) hebben hun afspraken met IT-partners over dataveiligheid vastgelegd: bij 38 procent strikt en bij 44 procent deels. Bij bijna een op de vijf (18%) blijft het bij informele afspraken of is er niets afgesproken.

Grafiek 1

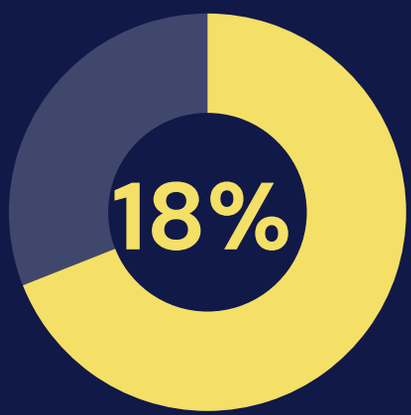
n = 433

Formele afspraken met IT-partners over dataveiligheid



Dat laatste valt Victor den Bak direct op. *"Dat bijna een op de vijf organisaties alleen informele afspraken heeft of helemaal niets heeft afgesproken, vind ik opvallend. Zeker omdat vrijwel iedereen ziet hoe afhankelijk hij is van zijn IT-leveranciers, bijvoorbeeld voor het versturen van facturen of het uitbetalen van salarissen."*

Ook bij de organisaties die wel afspraken hebben, is lang niet alles geregeld. De grootste groep (44%) heeft de afspraken maar deels vastgelegd. Wat organisaties vastleggen, hangt volgens Den Bak af van wat ze belangrijk vinden.



heeft alleen informele afspraken met IT-partners over dataveiligheid, of helemaal geen.

> *"Sommige organisaties letten vooral op gebruiksgemak of prijs. Anderen weer op de certificeringen die een IT-partner heeft. Soms gaan ze af op het imago en de naamsbekendheid van een partij."*
>
> **Victor den Bak**
> Portfolio Architect, **SureSync**

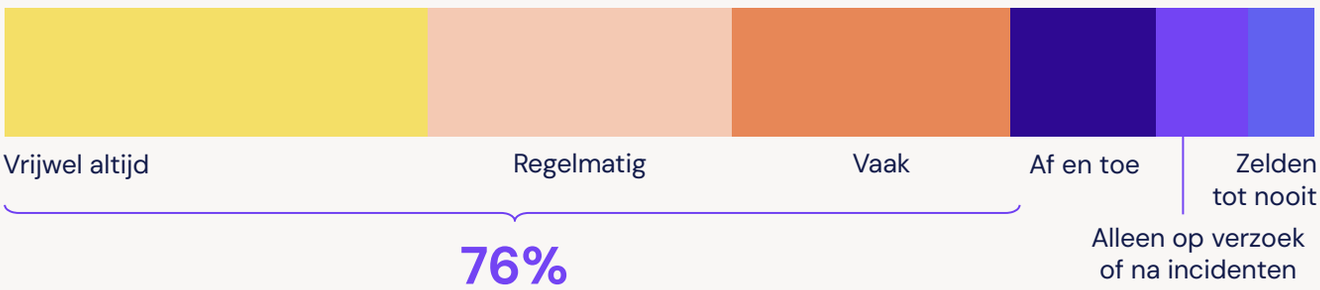
Een certificaat zegt niet alles

Op certificeringen letten de meeste organisaties in elk geval wel. Bij contract-verlenging controleert ruim drie kwart (76%) vrijwel altijd, regelmatig of vaak of de partner gecertificeerd is, bijvoorbeeld voor ISO 27001 of NEN 7510.

Grafiek 2

n = 433

Controle op certificeringen bij contractverlenging



Dat een partij een certificaat heeft, zegt niet alles. *"Een certificering betekent niet per se dat de hele organisatie of alle diensten eronder vallen,"* legt Den Bak uit. *"Een IT-bedrijf kan vijf producten hebben waarvan er maar één gecertificeerd is, en toch een certificaathouder zijn. In de kleine lettertjes staat dan om welke dienst het gaat. Bij grote aanbestedingen letten inkopers daar goed op, maar dat vraagt wel dat een organisatie moeite doet, in gesprek gaat met de aanbieder en bewijs opvraagt."*

Toch raadt Den Bak organisaties aan om altijd op certificeringen te letten. *"Certificeringen worden steeds gebruikelijker en het is geen eenmalige check. Elk jaar volgt er namelijk een deel-certificering en elke drie jaar een volledige. Zeker voor organisaties die weinig tijd of expertise hebben, geeft zo'n certificaat een duidelijke ondergrens aan de kwaliteit van een externe partner."* Ook voor een aanbieder kan het een voordeel opleveren. *"Een aanbieder hoeft niet in elk contract aparte afspraken te maken en kan makkelijker uitleggen wie waarvoor verantwoordelijk is bij een incident."*

> *"Een IT-bedrijf kan vijf producten hebben waarvan er maar één gecertificeerd is, en toch een certificaathouder zijn."*
>
> **Victor den Bak**
> Portfolio Architect, **SureSync**

Wat zijn ISO 27001 en NEN 7510?

ISO 27001 is een internationale norm voor het managen van informatiebeveiliging. Een organisatie die zich laat certificeren, heeft haar beveiliging structureel georganiseerd en laat die periodiek door een onafhankelijke partij toetsen. NEN 7510 is de Nederlandse norm voor informatiebeveiliging in de zorg.

Beide normen komen vaak terug bij aan-bestedingen en bij de inkoop van IT-diensten. Een certificaat geldt altijd voor een afgebakend deel van de dienst-verlening, en dus niet automatisch voor de hele organisatie. Het is geen een-malige keuring: elk jaar volgt een deel-certificering en elke drie jaar moet een organisatie de volledige certificering opnieuw doorlopen.

Check, check, dubbelcheck

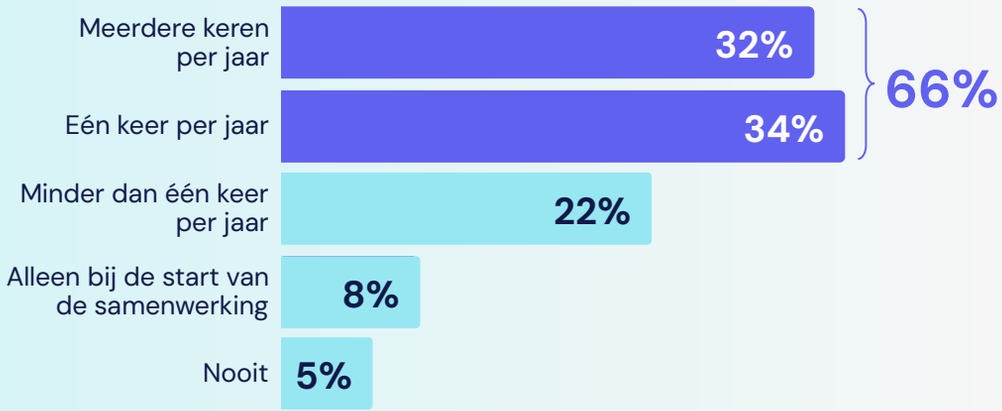
Afspraken en certificeringen laten zien wat een IT-partner belooft. Maar hoe weet een organisatie of die belofte ook in de praktijk wordt waargemaakt?

Twee derde voert minstens één keer per jaar een audit uit bij IT-partners. Een derde doet dat zelfs meerdere keren per jaar. Daartegenover staat 35 procent die minder vaak dan jaarlijks controleert, alleen bij de start van de samenwerking of nooit.

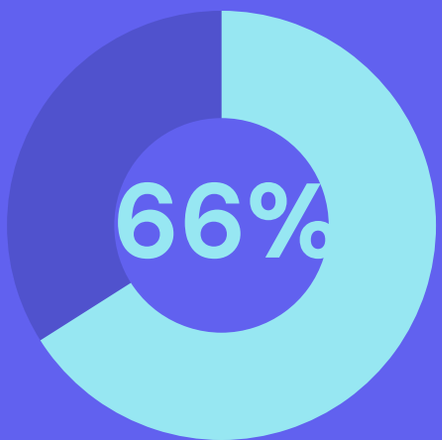
Grafiek 3

Hoe vaak organisaties audits uitvoeren bij IT-partners

n = 433



Den Bak noemt het een goed teken dat zoveel organisaties minstens jaarlijks een audit laten uitvoeren bij hun partners. *"Informatiebeveiliging is iets wat organisaties in de praktijk moeten doen,"* zegt hij. *"Daar hoort controle bij. Een audit kan bijvoorbeeld nagaan of er goede back-ups worden gemaakt en of die ook kunnen worden teruggezet. Ook kan een audit nagaan of de data wordt verwijderd als de samenwerking stopt, op wat wettelijk bewaard moet blijven na."*



voert minstens één keer per jaar een audit uit bij IT-partners. 13% controleert alleen bij de start of nooit.

Dat maar een klein deel alleen bij de start van een samenwerking controleert, komt mede door de groeiende aandacht van het management voor IT. "Iedereen ziet hoe afhankelijk bedrijfsprocessen zijn van IT, zeker sinds de coronapandemie," zegt Den Bak. *"Hoe de IT is ingericht, is het fundament van een organisatie."*

Voor de organisaties die alleen aan het begin van een samenwerking controleren, ziet Den Bak een risico. Een IT-partner kan na verloop van tijd iets veranderen in zijn processen of in de partijen waarmee hij samenwerkt. Dat merkt de organisatie dan niet.

> *"Aan het begin nemen organisaties alle hindernissen. Er wordt een partner gekozen en er worden afspraken gemaakt. Daarna kijkt men er niet meer naar, totdat ze ineens tegen de ijsberg aan varen. Dan vraagt men zich af waarom er niet eerder is gecontroleerd. Vaak is het dan te laat om een incident te voorkomen."*
>
> **Victor den Bak**
> Portfolio Architect, **SureSync**

Wie controleert de partner van de partner?

Een audit bij de eigen IT-partner is één ding, maar data blijft zelden bij die ene partij. Neem een HR-softwarepakket. De leverancier brengt zijn hosting onder bij een andere partij, die op haar beurt misschien een derde inschakelt voor back-ups. Met die laatste schakels heeft de organisatie zelf geen contract, terwijl haar data daar wel terechtkomt. Gaat daar iets mis, bijvoorbeeld een datalek bij de hostingpartij, dan merkt ook de organisatie de gevolgen.

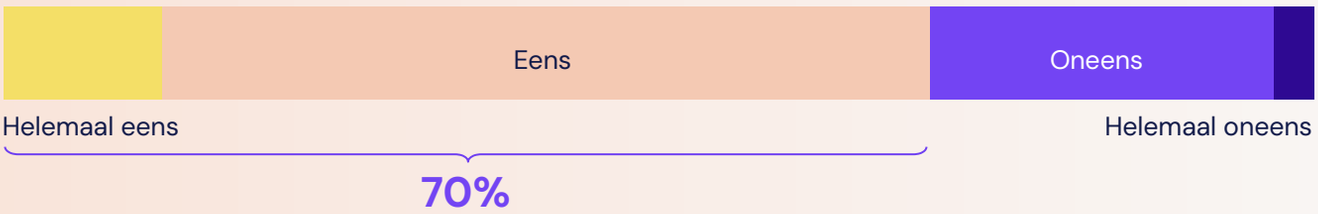
Zeven op de tien organisaties zeggen dat ze regelmatig ketenbrede audits uitvoeren.

"Organisaties zijn zich steeds meer bewust van wat er kan gebeuren als er slecht met data wordt omgegaan. Zeker als data wordt gedeeld met IT-partners, willen ze kunnen laten zien dat ze daar verantwoord mee omgaan."

Grafiek 4

n = 433

Onze organisatie voert regelmatig ketenbrede audits uit op datadeling.



70%

Toezicht dat je niet zelf inricht

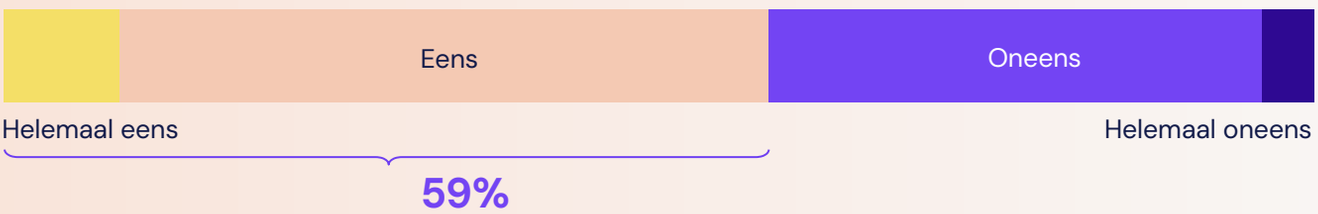
Zelf een audit uitvoeren is niet voor elke organisatie weggelegd. 59 procent geeft aan voor het toezicht op IT-partners af te hangen van de expertise van een andere partij, zoals een toezichthouder, koepel of brancheorganisatie.

"Vooral kleinere organisaties hebben vaak geen eigen IT-afdeling. Zij besteden dit soort diensten uit aan de bekendere partijen en gaan ervan uit dat de toezichthouder of koepelorganisatie de juiste eisen stelt. Dat is een redelijk gebruikelijke situatie," zegt Den Bak. *"Vooral in de zorg of accountancy. Daar hebben ze vaak niet de capaciteit om zich te verdiepen in zaken als dataveiligheid. Dan kan het lastig zijn de kwaliteit van een partner zelf te beoordelen. Hulp inschakelen is dus een logische keuze voor veel organisaties."*

Grafiek 5

n = 433

Wij zijn afhankelijk van de expertise van een andere partij (toezichthouder, koepelorganisatie) voor toezicht op onze IT-partners.



59%

Waarom krachten bundelen logisch is

Stel: een goede audit kost meer dan € 10.000. Een softwarepakket kost per jaar tussen € 1.500 en € 5.000. Voor één afnemer staat een audit dan zelden in verhouding tot de baten. Daarom bundelen organisaties hun krachten, bijvoorbeeld via raamcontracten van een koepelorganisatie, of laten ze de controle door een gezamenlijke partij uitvoeren. In de zorg gebeurt dat via regionale samenwerkingsverbanden, bij accountants en notarissen via de beroepsorganisatie.



Afhankelijk van een black box

SureSync

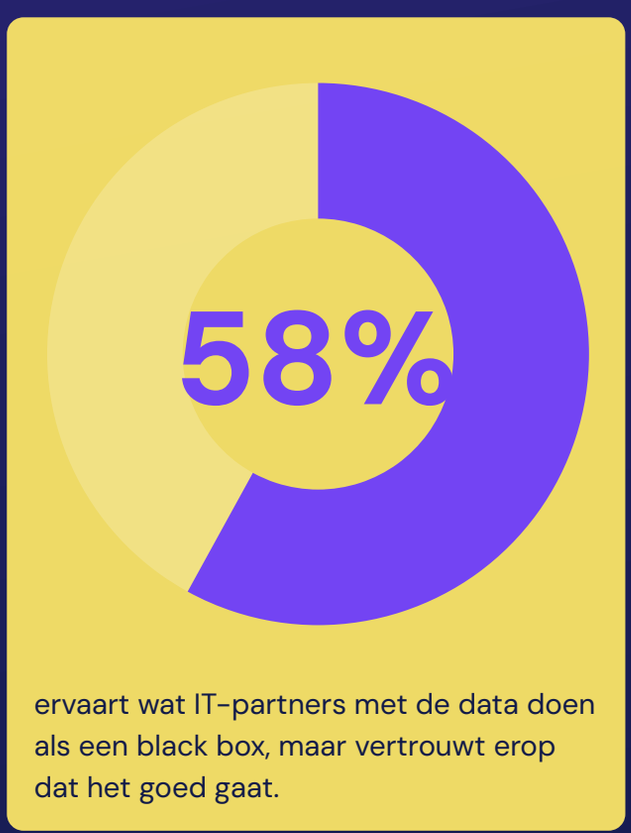
Ook organisaties die de juiste afspraken hebben gemaakt en met audits een oogje in het zeil houden, zien maar een deel van wat er bij hun IT-partner met hun data gebeurt.

Zolang de software of dienst werkt en de overzichten kloppen, heerst er vertrouwen dat het goed zit. Maar zeker weten wat de partner met hun data doet, doen ze niet. Ruim de helft (58%) herkent zich in de stelling dat wat partners met hun data doen als een black box voelt, maar vertrouwt er desondanks op dat het goed gaat.

"Als je zou vragen of een organisatie echt een beeld heeft van wat partners met hun data doen, zou ongeveer tachtig procent of meer aangeven dat ze geen idee hebben," schat Den Bak. *"Zeker wanneer ze veel zaken bij een partner hebben ondergebracht."*

Toch vertrouwen organisaties hun IT-partners. *"Dat komt omdat ze daar contextueel bewijs voor hebben."*

> *"Als een organisatie werkt met een factuursoftwarepakket, heeft ze een overzicht van hoeveel facturen er zijn verstuurd en naar wie. Worden er ineens geen facturen meer verstuurd of komen er opeens facturen bij, dan valt dat meteen op. Maar of er een goede back-up wordt gemaakt, kan de organisatie niet in dat overzicht zien. Dat gebeurt achter de schermen."*
>
> **Victor den Bak**
> Portfolio Architect, **SureSync**



ervaart wat IT-partners met de data doen als een black box, maar vertrouwt erop dat het goed gaat.

Zolang een systeem werkt zoals het hoort, hebben organisaties het idee dat het goed gaat.

Weten waar je data staat

Een vergelijkbaar beeld levert de stelling over controle op de plek van de data. Iets meer dan de helft van de Nederlandse IT-beslissers (55%) heeft het gevoel dat de organisatie onvoldoende controle heeft over waar de data zich bevindt.

"Moet je echt weten waar de data zich bevindt? Of is het gewoon belangrijk om te weten dat de data zich bevindt binnen de afspraken die je daarover hebt gemaakt?" vraagt Den Bak zich af. "Stel dat een zorginstelling met haar IT-partner afspreekt dat patiëntgegevens op twee aparte locaties worden bewaard, allebei binnen de Europese Unie. Zo gaat de data niet verloren als er op één locatie iets misgaat. Dan hoeft de instelling niet te weten welk datacenter dat is. Een goede dienstverlener kan aantonen dat de afspraken worden nageleefd."

Ook dan is een organisatie er volgens Den Bak nog niet. *"Vaak stopt een organisatie met doorvragen als ze weet waar haar data is. Dat is stap één. Maar stel ze weet waar de data staat en er is een incident. Wat doet de organisatie dan? Die vraag is vaak belangrijker."*

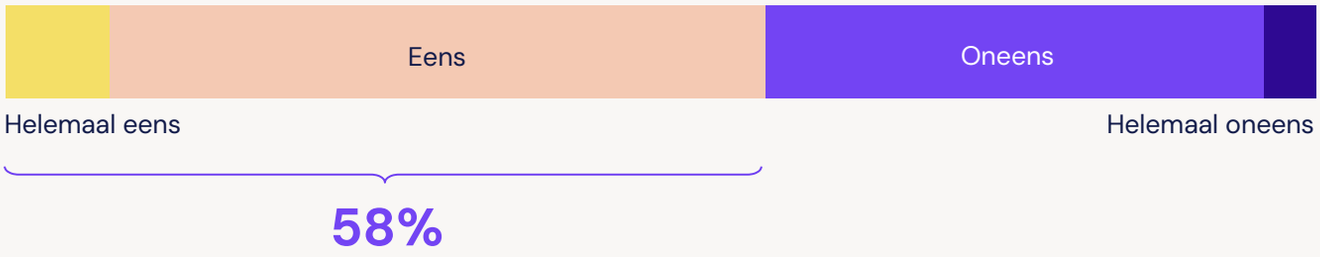
Controle over data houdt dus meer in dan weten waar die staat. Het gaat er ook om dat een organisatie kan laten zien dat de afspraken worden nageleefd, en dat ze weet wat ze kan doen als er iets misgaat.

Grafiek 6

n = 433

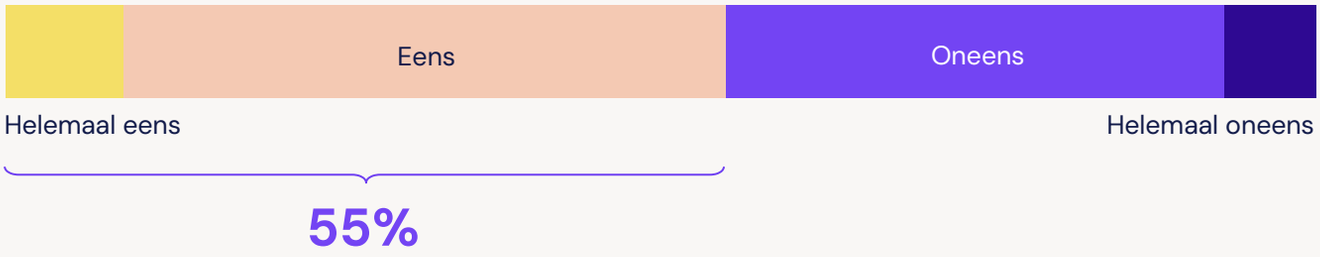
Zicht en controle op data bij IT-partners

Wat partners met onze data doen voelt als een black box, desondanks vertrouwen we erop dat het goed gaat.



58%

Ik heb het gevoel dat we binnen de organisatie onvoldoende controle hebben over waar onze data zich bevindt.



55%

> *"Wat voor herstelmogelijkheden heb je? Wanneer communiceer je met je klanten en ketenpartners? En met welke boodschap? Heldere communicatie is minstens even belangrijk voor het imago als de juiste acties nemen."*
>
> **Victor den Bak**
> Portfolio Architect, **SureSync**

Hoofdstuk 4

Een incident merken organisaties niet altijd

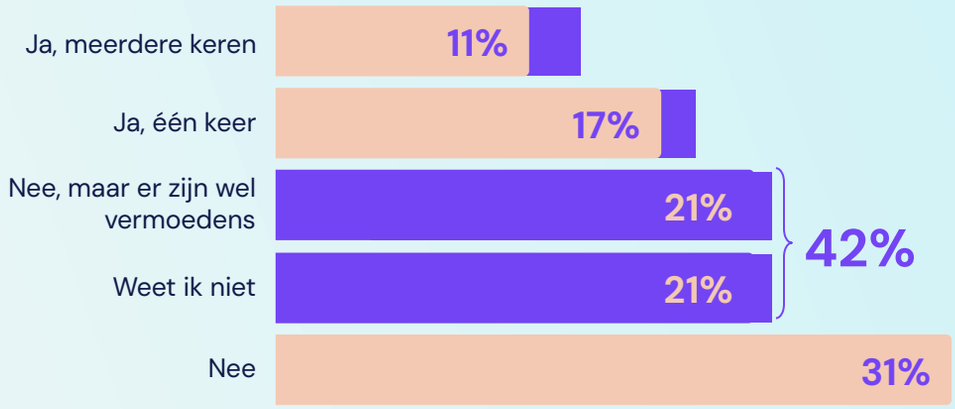
Vertrouwen op wat zichtbaar is, werkt zolang er niets misgaat. Maar hoe vaak gaat er iets mis?

Ruim een kwart van de organisaties kreeg de afgelopen twee jaar te maken met een incident rond data-uitwisseling met een externe partij, zoals een datalek bij een leverancier. Bijna een derde zegt dat dit niet is gebeurd. De grootste groep, 42 procent, weet het niet of heeft alleen vermoedens. Veel organisaties kunnen dus niet met zekerheid zeggen of er iets is misgegaan.

Grafiek 7

n = 433

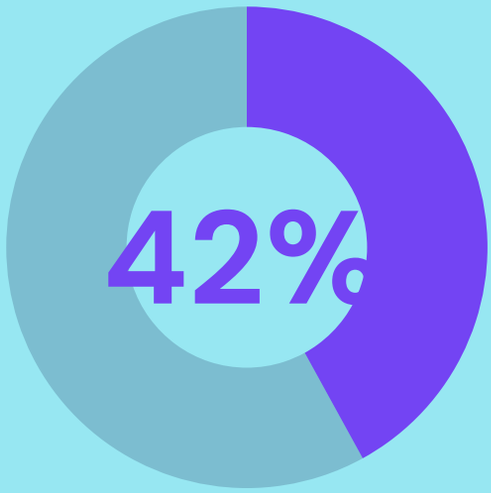
Incident rond data-uitwisseling met een externe partij in de afgelopen twee jaar



De cijfers zeggen nog niets over de ernst van een incident. Een incident hoeft geen grootschalige hack te zijn. "Het kan bijvoorbeeld ook gaan om een e-mail die per ongeluk naar de verkeerde persoon is gestuurd," vertelt Den Bak.

> *"Je merkt pas iets van zo'n incident als het een directe impact heeft. Soms merk je het pas maanden later. Zoals wanneer er fraude wordt gepleegd met een creditcard. Dan heb je geen idee waar of hoe die gegevens zijn gelekt."*
>
> **Victor den Bak**
> Portfolio Architect, **SureSync**

Dat zoveel organisaties niet weten of er een incident is geweest, vindt hij niet vreemd.



weet niet of er de afgelopen twee jaar een incident is geweest, of heeft alleen vermoedens.

SureSync

Wie ziet hoe afhankelijk organisaties zijn?

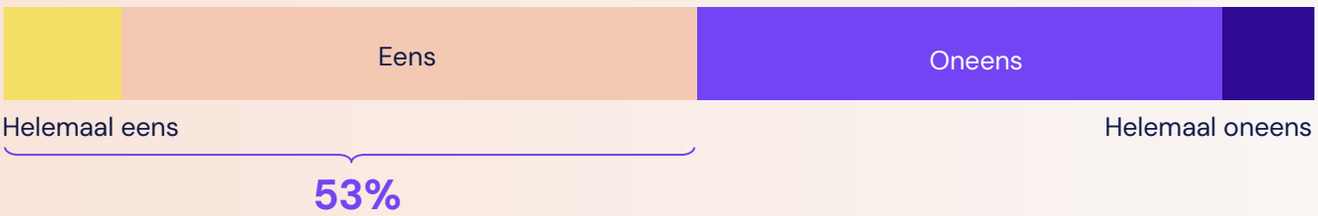
Stel dat de partij die het salaris- of factuurproces draait plotseling niet meer kan leveren. Door een faillissement, een grote hack of een leverancier die zijn eigen koers vaart. Kan de organisatie dan nog mensen betalen en facturen versturen?

Veel organisaties geven zelf aan dat ze de ernst van dit soort risico's niet voldoende inzien. Ruim de helft (53%) zegt dat de eigen organisatie de risico's van afhankelijkheid van IT-partners onderschat.

Grafiek 8

n = 433

Onze organisatie onderschat de risico's van afhankelijkheid van IT-partners.



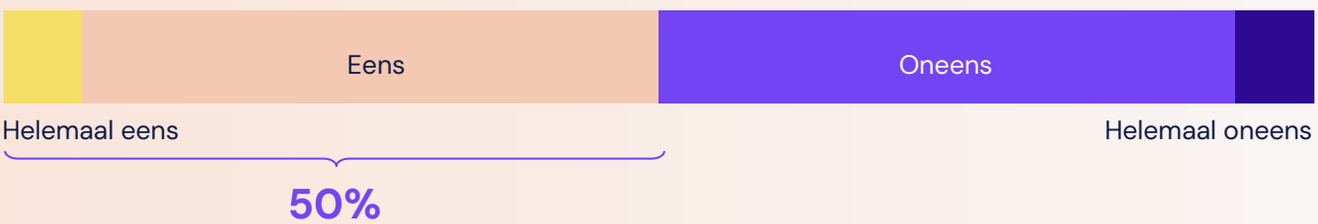
Het gaat hier dus om beslissers die zelf aangeven dat ze iets over het hoofd zien. Volgens Den Bak past dat bij een groeiend besef. "Ook hier zie je dat het bewustzijn van risico's rond data groeit. IT is in steeds meer processen cruciaal geworden, bijvoorbeeld in financiële en HR-processen. En organisaties zijn steeds afhankelijker van een kleiner aantal partijen."

In dat beeld past ook de uitkomst van de volgende stelling: de helft zegt dat de eigen organisatie niet altijd volledig transparant is over de risico's van data-uitwisseling met externe partijen. Dat kan van alles zijn. Een export met persoonsgegevens die per interne mail wordt rondgestuurd, of een verantwoordingsrapport voor de buitenwereld dat een rooskleuriger beeld geeft dan de praktijk.

Grafiek 9

n = 433

We zijn niet altijd volledig transparant over de risico's van data-uitwisseling met externe partijen.



> *"Het laat zien dat we allerlei risico's zien, en dat is bewustwording. Tien jaar geleden was een hack nauwelijks nieuws. Tegenwoordig opent het journaal er regelmatig mee. Dat komt niet alleen doordat het vaker voorkomt, maar ook doordat het als maatschappelijk relevanter wordt gezien."*
>
> **Victor den Bak,** Portfolio Architect, **SureSync**

Van afhankelijkheid naar regie

Hoeveel kun je als organisatie overlaten aan een IT-partner, en wat blijft altijd van jou? **De uitvoering ligt bij de partner, maar organisaties moeten zelf zorgen dat ze weten wat er gebeurt, goede afspraken maken en voorbereid zijn op een incident**. Dat zijn drie dingen waar elke organisatie zelf invloed op heeft.

01 Inzicht

Weet wat er met je data gebeurt, en zorg dat je kunt laten zien dat het gebeurt volgens de afspraken. Controleren is niet eenmalig.

Vraag voor je IT-partner

Kun je aantonen dat mijn data staat waar we dat hebben afgesproken?

02 Afspraken

Leg vast wat je van elkaar verwacht, ook bij een incident, en ga na waar een certificering precies voor geldt.

Vraag voor je IT-partner

Voor welk deel van je dienstverlening geldt je certificering, en hoe gaan we samen om met een incident?

03 Weerbaarheid

Wees voorbereid op het moment dat het misgaat, door het risico te spreiden en overstappen mogelijk te houden.

Vraag voor je IT-partner

Kan ik mijn data in een open formaat mee-nemen als ik moet overstappen?

Waar begin je?

Je hoeft niet alles tegelijk aan te pakken. Een goed begin is één scenario doorlopen met je IT-partner. Neem een belangrijk proces, zoals de financiële administratie, en bedenk wat er gebeurt als er een incident is. Wie doet wat, wie is bereikbaar, en waar staat de data? Zo zie je meteen waar het inzicht ontbreekt, welke afspraken nog niet zijn gemaakt en waar je te veel van één partij afhangt. Je hoeft ook niet alles te dekken. Wie de belangrijkste risico's aanpakt, is al een stuk verder dan wie niets heeft geregeld.

Methodologie

Onderzoekspopulatie	433 beslissers en beïnvloeders in IT, Finance, Data, Compliance en Legal
Organisatie	Nederlandse organisaties met 250 medewerkers of meer
Periode	23-02-2026 t/m 09-03-2026
Methode	Online survey, gesloten vragen (schalen en meerkeuze), anoniem
Werving	Panelprovider en eigen netwerk SureSync
Uitvoering	SureSync

De steekproef is niet representatief gestratificeerd naar sector of organisatiegrootte. De resultaten gelden voor de onderzochte populatie.

Kunnen we je ergens mee helpen?

Of je nu vragen hebt, advies zoekt of gewoon iets wil delen, onze experts luisteren graag. Neem contact op en we helpen je verder om je zakelijke leven gemakkelijker te maken.

www.suresync.nl

Dit Data Sharing Report is bedoeld voor informatieve doeleinden en bevat inzichten en aanbevelingen met betrekking tot gestructureerde gegevensuitwisseling en de technologieën die SureSync aanbiedt. De informatie in dit document is zorgvuldig samengesteld, maar SureSync kan niet garanderen dat alle gegevens volledig, accuraat of up-to-date zijn. De lezer is verantwoordelijk voor het verifiëren van de gepresenteerde informatie en het toepassen ervan in specifieke zakelijke contexten.

SureSync aanvaardt geen aansprakelijkheid voor eventuele schade die voortvloeit uit het gebruik van de inhoud van dit Data Sharing Report, inclusief maar niet beperkt tot verlies van gegevens, winst, of andere gevolgen die kunnen ontstaan door het implementeren van de besproken technieken of aanbevelingen.

Alle inhoud van dit Data Sharing Report, inclusief teksten, afbeeldingen, grafieken en andere materialen, is eigendom van SureSync of haar partners en is beschermd door auteursrechten en andere intellectuele eigendomsrechten. Het is verboden om de inhoud zonder expliciete toestemming te reproduceren of te distribueren.

De informatie in dit Data Sharing Report weerspiegelt de stand van zaken op het moment van publicatie en kan zonder voorafgaande kennisgeving worden gewijzigd.

© 2026 SureSync. Alle rechten voorbehouden.