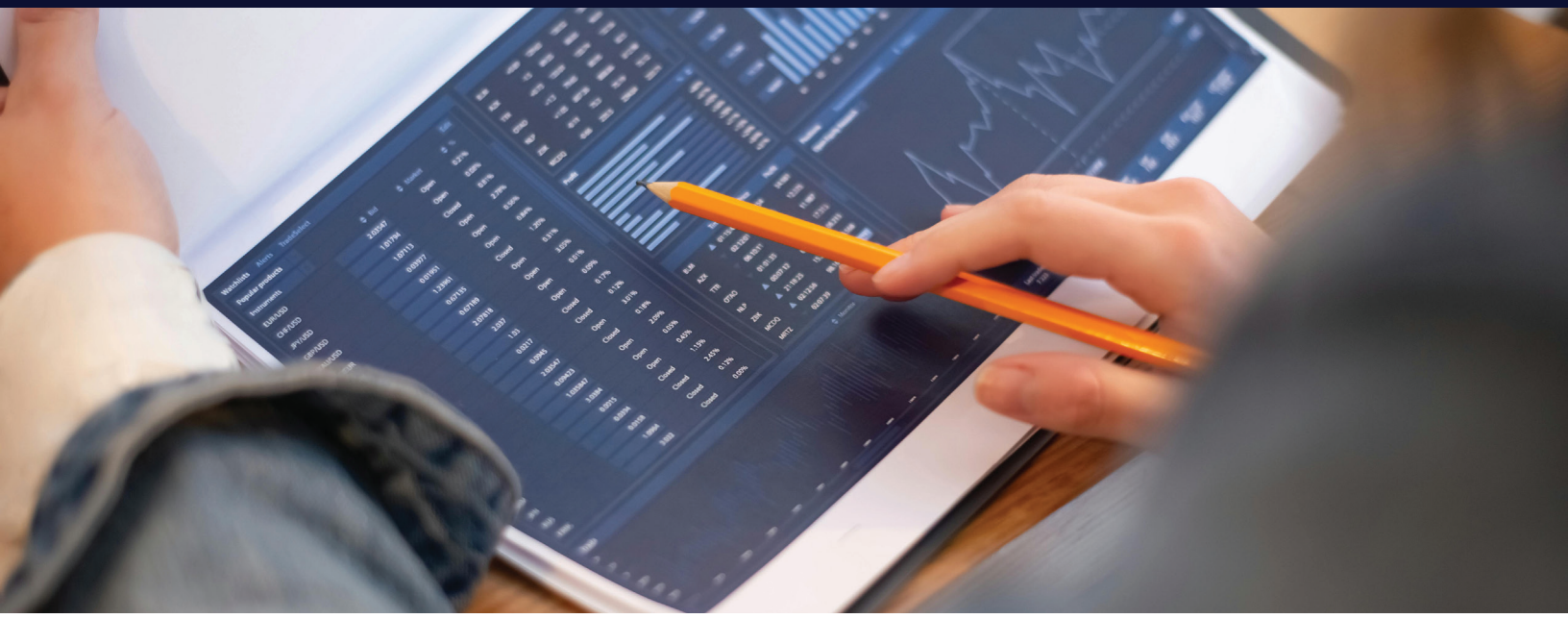
tien security

Onderzoek

Digitale Paraatheid: Inzichten van CFO's in Cybersecurity risico's binnen het MKB



Strategiën voor de moderne CFO

“Het onderzoek biedt inzicht in de perspectieven van CFO’s op digitale veiligheid, de bijbehorende risico’s en hun kwantificering.”

De intentie van ons onderzoek naar het kwantificeren van digitale risico’s was helder: inzicht krijgen in de specifieke uitdagingen en behoeften waarmee u als CFO’s wordt geconfronteerd.
Dit onderzoek is niet alleen waardevol voor u, om uw organisaties beter te beschermen tegen digitale dreigingen, maar ook van groot belang voor tien security.

Door uw motieven en behoeften te doorgronden, kunnen wij onze visie en missie verfijnen en onze diensten beter afstemmen op de markt. Uw medewerking stelt ons in staat om effectieve, schaalbare en kostenefficiënte oplossingen te ontwikkelen die niet alleen de huidige, maar ook toekomstige bedreigingen het hoofd kunnen bieden.

Samen bouwen we aan een toekomst waarin digitale veiligheid voor iedereen bereikbaar en betrouwbaar is.

Rogier van Agt
CEO tien security

Van resultaat naar inzichten

De resultaten laten zien hoe CFO’s digitale risico’s beoordelen en hoe zij strategieën voor digitale beveiliging afwegen. Dit omvat zowel het vertrouwen in interne en externe expertise als hun bereidheid tot uitbesteding van cybersecurity-diensten.

De criteria die bedrijven hanteren bij het evalueren van investeringen in digitale beveiliging benadrukken het belang van kosteneffectieve oplossingen, toekomstgerichte strategieën en effectieve bescherming tegen bekende dreigingen.

Deze bevindingen onderstrepen de toenemende behoefte aan gespecialiseerde partners in cybersecurity. Door samen te werken met dergelijke partners kunnen mkb-bedrijven hun digitale weerbaarheid versterken en hun bedrijfscontinuïteit waarborgen. Dit stelt bedrijven in staat om effectieve strategieën te ontwikkelen voor het beheren van digitale risico’s en het beschermen van hun bedrijf tegen cyberdreigingen.

Impact van Digitale Risico's

Hoewel veel CFO's digitale risico's als 'gemiddeld' inschatten, kunnen zij daarmee de ernstige gevolgen van deze risico's onderschatten. Bewustzijn van de werkelijke bedreigingen en mogelijke financiële schade is cruciaal.

Dit belang blijkt uit verschillende factoren:

Toename van cyberaanvallen: Het aantal en de complexiteit van cyberaanvallen neemt toe, waardoor bedrijven kwetsbaarder worden voor gegevensdiefstal, fraude en bedrijfsverstoring.

Financiële gevolgen: Cyberaanvallen kunnen leiden tot aanzienlijke financiële verliezen, zoals herstelkosten.

Strengere regelgeving: Bedrijven moeten voldoen aan strengere cybersecurity-eisen van leveranciers, overheden en toezichthouders, wat niet-naleving strafbaar stelt.

Schade aan reputatie: Cyberincidenten kunnen het vertrouwen van klanten en partners schaden, wat leidt tot omzetverlies en een afname van merkwaarde.

Risico op bedrijfsstilstand: Ernstige cyber-aanvallen kunnen leiden tot tijdelijke of permanente bedrijfsstilstand, wat een directe impact heeft op de winstgevendheid.

Deze factoren onderstrepen de noodzaak van een grondige risico-evaluatie en de implementatie van sterke cybersecuritymaatregelen. Dit verkleint de kans op aanzienlijke verliezen en waarborgt de financiële stabiliteit van het bedrijf.

"Als CFO bent u de bewaker van de financiële gezondheid van uw organisatie."

tien security

Verkrijgen van Inzichten over Digitale Risico's

Veel bedrijven vertrouwen op hun interne of externe IT-teams voor cybersecurity inzichten. Dit is zorgelijk omdat dergelijke IT georiënteerde teams niet altijd op de hoogte zijn van de nieuwste ontwikkelingen en geavanceerde aanvallen die buiten hun directe ervaring vallen. Bovendien kunnen ze moeite hebben met het detecteren van kwetsbaarheden in hun eigen systemen vanwege hun betrokkenheid bij de dagelijkse operaties.

Echter, het integreren van externe experts kan een meer objectief en volledig beeld bieden van de cyberdreigingen. Dit is vooral belangrijk in een landschap waar nieuwe bedreigingen voortdurend ontstaan.

Het is gebleken dat externe experts met hun frisse blik en actuele kennis een nauwkeuriger risicoanalyse kunnen bieden. Dit is van cruciaal belang voor het ontwikkelen en implementeren van effectieve beveiligingsstrategieën.

Het toenemend belang van pro-actief handelen

De focus ligt op de aanpak van toekomstige dreigingen, wat aantoont dat proactieve beveiliging van toenemend belang is. Tegelijkertijd is het beheersen van kosten een cruciale factor voor het MKB. Dit wijst erop dat MKB-bedrijven behoefte hebben aan betaalbare en eenvoudig te implementeren cybersecurity-oplossingen.

De criteria voor investeringen in digitale beveiliging komen dus voort uit een zorgvuldige afweging tussen proactieve bescherming en kostenbeheersing. Ondanks beperkte budgetten moeten mkb-bedrijven kostenefficiënte oplossingen kiezen die effectief zijn in het voorkomen van dreigingen.

De criteria houden in dat mkb-bedrijven de beschikbare cyber expertise optimaal benutten en inzetten op betaalbare, schaalbare beveiligingsoplossingen, zoals Cloud-gebaseerde diensten. Daarnaast investeren ze in werknemersopleiding om hun bewustzijn en verantwoordelijkheid te vergroten.

Het onderzoek onderstreept dat het vinden van een evenwicht tussen proactieve beveiliging en financiële haalbaarheid van groot belang is voor de digitale veiligheid en financiële gezondheid van mkb-bedrijven.

Uitbesteding van Digitale Risicobeheer

De belangrijkste reden voor het uitbesteden van cybersecurity door mkb-bedrijven is kostenbesparing. Het gaat hierbij niet alleen om het kopen van een licentie, maar ook om de bijkomende kosten van implementatie, configuratie, beheer en ondersteuning. Daarnaast vereist het een gedegen investering in interne cybersecurity expertise, om gegevens te kunnen interpreteren en adequaat te kunnen reageren op bedreigingen.

Door cybersecurity uit te besteden aan een cyberspecialist, kunnen mkb-bedrijven profiteren van duidelijke afspraken over service en ondersteuning, waardoor continuïteit wordt gewaarborgd. Dit geeft de directie een regisserende rol en stelt hen in staat om op strategisch niveau te opereren. Hierdoor kan men zich richten op langetermijndoelen en risicobeheer, terwijl de dagelijkse operationele beveiligingstaken worden verzorgd door experts. Dit leidt tot meer efficiëntie en betere bescherming van het bedrijf.

De toenemende complexiteit en impact van digitale dreigingen

De overwegingen voor het uitbesteden van cybersecurity-diensten door mkb-bedrijven komt voort uit de snel toenemende complexiteit en impact van digitale dreigingen. Veel bedrijven geven aan dat ze gewoonweg het inzicht missen om weloverwogen beslissingen te nemen over hun digitale beveiliging. De interne kennis is vaak onvoldoende om snel in te spelen op moderne dreigingen, en in sommige gevallen beschikken ook hun IT-partners niet over de expertise om deze dreigingen af te wenden, te interpreteren of te adresseren.

Het onderzoek heeft vijf belangrijke redenen geïdentificeerd waarom mkb-bedrijven cybersecurity-diensten uitbesteden:

1. Kostenbeheersing: Managed security services bieden een kosteneffectieve aanpak door schaalvoordelen en lagere operationele kosten.

2. Expertise: Externe specialisten brengen diepgaande kennis en ervaring met zich mee, waardoor bedrijven adequaat kunnen inspelen op bedreigingen.

3. Toegang tot geavanceerde technologieën: Door uitbesteding kunnen mkb-bedrijven profiteren van de nieuwste beveiligingstechnologieën zonder hoge investeringskosten.

4. Continue monitoring en support: Managed security services bieden 24/7 monitoring en ondersteuning, wat zorgt voor constante bewaking van dreigingen en snelle reacties.

5. Strategische focus: Door cybersecurity uit te besteden, kunnen mkb-bedrijven zich richten op hun kernactiviteiten en strategische doelen.

Een cyber expert kan deze hiaten effectief en efficiënt opvullen, wat mkb-bedrijven helpt om hun digitale veiligheid te verbeteren en de genoemde voordelen van uitbesteding te realiseren.

“Cyberbeveiligings-dreigingen vormen een belangrijke en veranderende uitdaging voor de verantwoordelijkheid”

tien security

Keuze van een Cybersecuritydienstverlener

Mkb-ondernemers kunnen een weloverwogen keuze maken voor een cybersecurity-dienstverlener door rekening te houden met belangrijke aspecten. Reputatie en ervaring zijn cruciaal, omdat dit vertrouwen in de betrouwbaarheid en deskundigheid van de dienstverlener wekt.

Een dienstverlener die begrip heeft van ondernemerschap en leiderschap, kan oplossingen bieden die zijn afgestemd op de behoeften van het mkb. Ook zijn deskundigheid en eenvoud van samenwerking belangrijk, waaronder duidelijke communicatie, transparantie en toegankelijkheid.

Door aandacht te besteden aan deze aspecten, kunnen mkb-ondernemers een partner kiezen die aansluit bij hun digitale veiligheidsbehoeften en zakelijke doelstellingen.

Conclusie

De resultaten van het onderzoek suggereren dat mkb-bedrijven een sterkere focus moeten leggen op cybersecurity. Veel bedrijven vertrouwen op interne IT-teams voor risico-inzichten, hoewel het combineren van interne en externe expertise ook waardevol blijkt te zijn.
Dit benadrukt het belang van een weloverwogen aanpak om de complexiteit van digitale risico's effectief te beheersen.

De belangrijkste criteria bij investeringen in digitale beveiliging zijn het kunnen aanpakken van toekomstige bedreigingen, kosteneffectiviteit, integratie met bestaande systemen en effectiviteit tegen bekende bedreigingen.
Dit duidt op een behoefte aan doordachte, kosteneffectieve oplossingen die naadloos passen in de huidige bedrijfsomgeving.

Wat betreft het uitbesteden van digitale risicobeheer, noemen mkb-bedrijven kostenbesparing als belangrijkste reden, gevolgd door gebrek aan interne expertise en behoefte aan geavanceerde technologieën. De verdeling van meningen over het uitbesteden van cybersecurity-diensten toont dat er ruimte is voor overleg en afstemming van strategieën.

Aspecten zoals incidentrespons en -beheer, netwerkbeveiliging, endpointbeveiliging en gegevensbescherming worden gezien als het meest geschikt om uit te besteden. Dit onderstreept de voordelen van gespecialiseerde kennis en geavanceerde tools in deze kritische gebieden.

Het overwegen van uitbesteding van cybersecurity-taken kan mkb-bedrijven helpen hun digitale weerbaarheid te versterken en hun bedrijfscontinuïteit te waarborgen. Dit bevordert een strategische benadering van digitale veiligheid, waarbij bedrijven profiteren van deskundigheid, efficiëntie en geavanceerde oplossingen.

Het onderzoek en de resultaten

Vraag 1: Hoe schat u doorgaans de impact van digitale risico's op uw bedrijf in?

De meerderheid (56%) van de CFO's beoordeelt de impact van digitale risico's op hun bedrijf als 'gemiddeld'. Een klein percentage (11%) respondenten geven aan dat de impact 'hoog' is en een paar respondenten ziet deze als 'laag'.

De perceptie van een 'gemiddelde' impact kan wijzen op een zekere mate van bewustzijn van digitale risico's, maar mogelijk ook op een onderwaardering van de ernstige gevolgen die deze risico's kunnen hebben. De CFO's die de impact als 'hoog' inschatten, zijn mogelijk al geconfronteerd met incidenten die de financiële gezondheid van hun organisatie hebben beïnvloed, wat benadrukt hoe belangrijk het is voor alle MKB-bedrijven om hun cybersecurity serieus te nemen.

Vraag 2: Op welke manier verkrijgt u inzichten over digitale risico's in uw bedrijf?

Inzichten worden voornamelijk verkregen via interne IT-teams gevolgd door een combinatie van interne en externe ICT, en externe consultants of auditors.

Het vertrouwen op interne IT-teams is een goede eerste stap, maar het integreren van externe expertise kan bedrijven helpen een breder en mogelijk objectiever beeld te krijgen van de cyberdreigingen waaraan ze zijn blootgesteld. Het combineren van interne en externe inzichten kan een robuustere benadering van risicomanagement ondersteunen.

Vraag 3: Wat zijn voor u de belangrijkste criteria bij het evalueren van investeringen in digitale beveiliging?

De belangrijkste criteria die naar voren komen, zijn de 'mogelijkheid om toekomstige bedreigingen aan te pakken', 'kosten-effectiviteit 57%' en 'integratie met bestaande systemen 24%' en 'effectiviteit tegen bekende bedreigingen 19%'.

De nadruk op toekomstige bedreigingen toont aan dat CFO's vooruitkijken en zich willen voorbereiden op nieuwe soorten aanvallen. Kosten-effectiviteit blijft echter ook een belangrijke factor, wat aangeeft dat besluitvorming nog steeds sterk wordt beïnvloed door budgettaire overwegingen.

Vraag 4: Wat zou voor uw bedrijf de belangrijkste reden zijn om digitale risicobeheer uit te besteden aan een specialist?

De meest genoemde reden voor uitbesteding is 'kostenbesparing ten opzichte van het aannemen van interne specialisten 48%' gevolgd door 'gebrek aan interne expertise 37%' en 'toegang tot geavanceerde technologieën en tools 15%'.

Deze resultaten benadrukken dat veel MKB-bedrijven het moeilijk vinden om gespecialiseerde kennis intern te ontwikkelen of te behouden. Dit maakt uitbesteding een aantrekkelijke optie, niet alleen om kosten te besparen, maar ook om toegang te krijgen tot gespecialiseerde technologieën en kennis die intern moeilijk te verkrijgen is.

Vraag 5: In hoeverre overweegt uw bedrijf het uitbesteden van cybersecurity-diensten?

De meningen zijn verdeeld: 28% van de respondenten staan neutraal tegenover uitbesteding, meer dan de helft overwegen het matig 58%, en een paar is sterk voor uitbesteding 14%.
De uiteenlopende antwoorden kunnen wijzen op een variërende mate van bewustzijn en vertrouwen in eigen capaciteiten om cybersecurity te beheren. Bedrijven die het sterk overwegen, zijn mogelijk al geconfronteerd met de complexiteiten van cybersecurity en zien de voordelen van het inschakelen van specialisten.

Vraag 6: Welke aspecten van cybersecurity zouden volgens u het meest geschikt zijn om uit te besteden?

'Incidentrespons en -beheer' en 'Netwerkbeveiliging', 'Endpointbeveiliging, 'Gegevensbescherming', en één respondent heeft geen idee. Deze resultaten benadrukken de behoefte aan gespecialiseerde diensten op gebieden waar snel reactievermogen of technische expertise vereist is. Het uitbesteden van incidentrespons en netwerkbeveiliging kan bedrijven helpen om snel en effectief op incidenten te reageren, wat cruciaal is voor het minimaliseren van schade.

Vraag 7: Welke factoren zouden voor uw bedrijf doorslaggevend zijn bij het kiezen van een cybersecurity-dienstverlener?

'Reputatie en ervaring van de dienstverlener' wordt het vaakst genoemd, gevolgd door 'Prijs van de diensten' en daarna 'Klantenservice en ondersteuning'.

Reputatie en ervaring spelen een grote rol bij de keuze voor een dienstverlener, wat aangeeft dat vertrouwen en bewezen competentie belangrijk zijn voor CFO's. Dit suggereert dat dienstverleners die zich richten op het bouwen van een sterke reputatie en het tonen van hun expertise in specifieke cybersecurity-domeinen, meer kans hebben om gekozen te worden als partners.

Vraag 8: Hoe vaak voert uw bedrijf een formele evaluatie uit van de ROI voor cybersecurity-investeringen?

'Zelden 47%' en 'Nooit 51%' zijn de meest voorkomende antwoorden, met slechts een aantal respondenten die aangeven dit 'Af en toe (jaarlijks) 2%' te doen.

Deze resultaten wijzen op een mogelijk tekort aan formele beoordelingsprocessen voor cybersecurity-investeringen binnen MKB's. Het meten van ROI is cruciaal voor het rechtvaardigen van de investeringen en het optimaliseren van de strategieën, wat aantoont dat hier nog veel winst te behalen valt.

Vraag 9: Kunt u de potentiële kosten van een datalek of cyberaanval voor het bedrijf kwantificeren?

Meer dan 95% van alle CFO's geven aan dat ze moeite hebben met het bepalen van de kosten, of geen specifieke informatie hebben.

Dit onderstreept een significant probleem in risicobeheer; zonder duidelijk begrip van de financiële impact, kunnen bedrijven niet adequaat plannen voor of investeren in cybersecurity. Het verbeteren van deze kennisbasis zou een prioriteit moeten zijn voor elk bedrijf.

Vraag 10: Hoe kunt u de directiekamer het beste overtuigen van de noodzaak van investeringen in cybersecurity?

34% van de responsenten gaven aan alle genoemde overtuigings-methoden te gebruiken. 28% van de respondenten geven de voorkeur aan het wijzen op recente cyberincidenten bij vergelijkbare bedrijven, terwijl 8% de financiële impact van een cyberaanval benadrukt en 8% de vergelijking maakt met kwaliteitsvraagstukken. Resterende hadden geen mening.

Deze resultaten tonen aan dat een gecombineerde aanpak waarbij meerdere argumenten worden aangedragen vaak als meest effectief wordt gezien. Dit suggereert dat een multifaceted presentatie die zowel de financiële, operationele als vergelijkende aspecten belicht, waarschijnlijk de meest overtuigende manier is om leidinggevenden te beïnvloeden. Het wijzen op concrete voorbeelden van recente incidenten biedt tastbare bewijzen die de urgentie en relevantie van cybersecurity-investeringen benadrukken. Deze aanpak kan directieleden helpen de verborgen kosten en risico's van onvoldoende beveiliging te begrijpen

Stelling 11: Investeringen in cybersecurity kunnen hoog zijn en er zijn andere prioriteiten die dringender lijken.

Meerderheid 68% is 'een beetje eens' met deze stelling, terwijl een 24% 'eens' zijn en 8% 'oneens'.

Deze stelling toont de uitdaging waarmee veel bedrijven geconfronteerd worden: het balanceren van noodzakelijke investeringen in cybersecurity met andere zakelijke prioriteiten. Het feit dat de meeste respondenten het er enigszins mee eens zijn, suggereert dat hoewel ze het belang van cybersecurity erkennen, het vaak als minder urgent wordt gezien in vergelijking met andere bedrijfsbehoeften. Dit kan leiden tot uitgestelde of onvoldoende beveiligingsmaatregelen.

Stelling 12: Ik heb onvoldoende kennis over de risico's en gevolgen van cyberaanvallen.

De meningen zijn gemengd: 45% zijn 'een beetje eens', 33% 'beetje oneens', en 22% zijn expliciet 'eens' of 'oneens'.

De verdeeldheid onder de respondenten benadrukt een variërende mate van begrip en bewustzijn van cybersecurity binnen het MKB. Dit kan wijzen op de noodzaak voor betere educatieve programma's en trainingen om de kennis van besluitvormers te vergroten.

Stelling 13: Ik vertrouw op mijn huidige beveiligingsmaatregelen om mijn bedrijf te beschermen.

De meningen zijn ook hier gemengd, met een lichte overweging naar 'beetje eens'.

Hoewel sommige CFO's vertrouwen hebben in hun huidige maatregelen, toont de aanwezigheid van 'geen mening 28%' en 'beetje oneens 24%' aan dat er twijfel bestaat over de effectiviteit van bestaande beveiligingsmaatregelen. Dit kan wijzen op een kans voor cybersecurity-dienstverleners om de voordelen van hun diensten beter te communiceren.

Stelling 14: De implementatie van cybersecuritymaatregelen kan complex en tijdrovend zijn.

Een meerderheid is het 'eens 42%' of 'beetje eens 39%' met deze stelling.

Dit toont aan dat de complexiteit en tijdsinvestering die gepaard gaan met het implementeren van cybersecurity als aanzienlijke hindernissen worden gezien. Het onderstrepen van de noodzaak voor vereenvoudigde oplossingen of managed services kan een belangrijke marketingstrategie zijn voor aanbieders van cybersecurity.

Stelling 15: Ik geloof dat cyberaanvallen voornamelijk grote bedrijven treffen en mijn bedrijf minder kwetsbaar is.

Men is grotendeels 'beetje eens 39%' of 'oneens 37%'. Deze resultaten wijzen op een gevaarlijke misvatting dat kleinere bedrijven minder risico lopen. Het is cruciaal voor cybersecurity-aanbieders om de realiteit te benadrukken dat MKB's vaak doelwit zijn, juist omdat ze als minder goed beveiligd worden gezien.

Stelling 16: Ik vertrouw op mijn externe IT-dienstverlener om eventuele problemen op cybersecurity gerelateerd domein op te lossen als ze zich voordoen.

De meeste respondenten zijn 'beetje eens 44%' of 'eens 32%'.

Dit toont een afhankelijkheid van externe dienstverleners voor cybersecurity, wat de waarde van managed security services benadrukt. Het biedt een kans voor dienstverleners om hun rol als een betrouwbare partner te versterken.

Stelling 17: Ik ben bereid om mijn bestaande processen en systemen aan te passen om cybersecuritymaatregelen te integreren.

Een mix van 'eens 28%' en 'beetje eens 31%', met enkele 'geen mening 41%'.

Hoewel er een algemene bereidheid is om aanpassingen te maken, toont de aanwezigheid van 'geen mening' dat sommige besluitvormers mogelijk nog steeds niet overtuigd zijn van de noodzaak of haalbaarheid van dergelijke veranderingen.

Stelling 18: Het vaststellen van een specifiek budget voor cybersecurity is een essentiële stap om de algehele digitale weerbaarheid van een organisatie te versterken.

Veel 'beetje eens 29%' en 'eens 38%', met enkele 'geen mening 33%'.

De consensus over het belang van een specifiek cybersecuritybudget toont het groeiende besef dat gerichte investeringen nodig zijn om weerbaarheid tegen digitale bedreigingen te verhogen.

Stelling 19: Uitbesteding van cybersecurity-taken aan gespecialiseerde dienstverleners kan leiden tot een hoger rendement op investeringen vergeleken met interne beheermodellen.

Men is verdeeld, met sommigen die 'eens 22%' zijn, anderen 'beetje eens 31%', en 'geen mening 47%'.

De gemengde meningen wijzen op onzekerheid of gebrek aan bewijs over de voordelen van uitbesteding voor ROI. Dit biedt een kans voor dienstverleners om case studies en bewijzen van succes te delen die de waarde van hun diensten aantonen.

Stelling 20: Het IT-budget van een organisatie zou idealiter moeten toenemen naarmate de omzet groeit.

Een mix van meningen met 'eens 24%', 'oneens 29%' en 'hangt af van andere factoren 47%'.

Dit toont de complexiteit van budgettering in relatie tot bedrijfsgroei. Het benadrukt de noodzaak voor flexibele en schaalbare cybersecurity-oplossingen die kunnen meegroeien met het bedrijf.

Dankwoord

Wij willen graag onze oprechte dank uitspreken aan alle CFO's die hun inzichten en expertise hebben gedeeld in ons onderzoek naar het kwantificeren van digitale risico's. Uw bereidheid om deel te nemen heeft een essentiële bijdrage geleverd aan de kwaliteit en diepgang van onze bevindingen.

Indien u de enquête niet heeft ingevuld, willen we benadrukken dat dit geen probleem is. We hopen dat u ons rapport toch als een waardevol naslagwerk zult beschouwen en het kunt gebruiken om uw eigen strategieën en beslissingen te ondersteunen.

De conclusies en inzichten uit ons onderzoek sluiten nauw aan bij wat **tien security** reeds in gang heeft gezet. We waarderen het niet alleen om deze inzichten te delen, maar ook om te zien dat onze bestaande initiatieven in lijn liggen met de behoeften van de markt. Dit bevestigt de waarde van onze inspanningen en motiveert ons om verder te gaan met de ontwikkeling en optimalisatie van onze missie en visie, zodat deze nog beter aansluiten bij de verwachtingen van het MKB.

Onze ambitie is duidelijk: we willen het marktalternatief zijn voor ondernemend Nederland (MKB en ZZP) als het aankomt op het leveren van betaalbare en betrouwbare cybersecurity diensten.

Nogmaals, onze oprechte dank voor uw medewerking en betrokkenheid.

tien security

Veilig ondernemen, zonder gedoe

www.tiensecurity.nl | info@tiensecurity.nl