



Cyber en Data Risks

Alles wat u moet weten om over cyberrisico's te adviseren



1. Alles wat u moet weten om over cyberrisico's te adviseren

Beste relatie,

Een groot deel van het MKB denkt dat zij geen cyberrisico's lopen. Maar het komt juist steeds meer voor. Hackers weten zich toegang te verschaffen tot persoonsgegevens, websites worden platgelegd door gerichte DDoS-aanvallen of ransomware gijzelt de bedrijfskritische data op computers.

Uit het onderzoek blijkt dat ondernemers veronderstellen dat deze problemen vooral spelen bij grotere bedrijven. Bijna elk bedrijf heeft een website, is afhankelijk van ICT en bijna elke ondernemer heeft een smartphone. Dit zijn allemaal risico's, vooral omdat het MKB vaak niet van de juiste beveiliging is voorzien.

Daarom is het de moeite waard om de beveiliging eens onder de loep te nemen en standaard procedures op te zetten bij verdachte mailtjes, brieven of telefoontjes. Uit onderzoek is namelijk gebleken dat een groot deel van de MKB bedrijven ooit slachtoffer wordt van cybercriminaliteit.

Reden te over voor uw relaties om een Cyber en Datarisks verzekering af te sluiten. Maar hoe brengt u aan uw relaties over hoe groot de risico's en gevolgen kunnen zijn ?

Wij hebben voor u op een rijtje gezet wat u mee kunt nemen in uw advies over dit onderwerp. Ook geven wij u handvatten om uw klanten te benaderen middels bijvoorbeeld een e-mailing.

Wij wensen u heel veel succes en voor vragen kunt u contact opnemen door een e-mail te sturen naar communicatie@turien.nl.

Turien & Co. Assuradeuren



2. Inhoudsopgave

1.	Alles wat u moet weten om over cyberrisico's te adviseren	1
2.	Inhoudsopgave	2
3.	Uw relatie vraagt 'waarom?'	3
4.	Oplossing: de Cyber en Datarisks verzekering?	4
5.	Niet goed gedekt binnen traditionele verzekeringen	6
6.	Meldplicht datalekken	8
7.	Cyberrisico's voor uw relaties	9
8.	Welke gegevens zijn blootgesteld aan risico's?	10
9.	Mogelijke oorzaken	11
10.	Mogelijke kosten	12
11.	Dekking door Cyber en Datarisks verzekeringen	13
12.	E-mailing – Do's & Dont's	16
13.	E-maling – Optie 1 Aansprakelijkheid	17
14.	E-mailing – Optie 2 Bedrijfsschade	19
15.	Social Media	21
16.	Meer informatie	23
17.	Praktijkvoorbeelden	23

3. Uw relatie vraagt 'waarom?'

"Het overkomt mij toch niet!", is een veelvoorkomende uitspraak in de markt. Helaas is de realiteit dat het iedereen kan overkomen! 98% van alle bedrijven zijn het slachtoffer van een datahacking of een poging daar toe. De Norton Symatec Security Survey toont aan dat:

- ✓ 29% op frequente basis onderhevig zijn aan een cyber aanval;
- ✓ 24% van de bedrijven schade en dataverlies oplopen;
- ✓ 20% van de aangevallen bedrijven hierna een inkomsten- of reputatieverlies ondervindt.

Waarom is het MKB juist een aantrekkelijke prooi voor cybercriminelen?

- ✓ Er valt bij het MKB meer te halen dan bij de gemiddelde consument, en de meeste ondernemers hebben hun cybersecurity niet beter geregeld dan de gemiddelde consument.
- ✓ Wanneer een kleinere organisatie bestolen of gehackt wordt, haalt dit niet vaak het nieuws, waardoor hackers rustig verder kunnen gaan zonder al te veel media-aandacht.



4. Oplossing: de Cyber en Datarisks verzekering?

De vier belangrijkste redenen voor uw relatie om een Cyber en Datarisks verzekering af te sluiten :

1. Cybercrime

Cybercrime is de snelst groeiende vorm van misdaad van de laatste jaren. Omdat ons leven zich meer en meer digitaal afspeelt, neemt ook de kans op online criminaliteit toe. Verlies van data en hacking zijn een paar voorbeelden en deze risico's zijn niet of maar voor een deel gedekt onder traditionele verzekeringen. De Cyber Data Risks verzekering van Turien & Co. biedt wel uitgebreide dekking voor deze risico's.

2. Afhankelijkheid van systemen

Systemen zijn cruciaal voor het bedienen van klanten, maar hun downtime is niet gedekt door de standaard verzekeringen. Alle bedrijven vertrouwen op systemen om hun core business te kunnen verrichten. Een hackaanval, computervirus of kwaadaardige handeling van een werknemer kan voor onderbreking van business zorgen. Online en/ of offline omzetzijning wordt door de Cyber en Data Risks verzekering van Turien & Co. vergoed.



4. Waarom een Cyber en Datarisks verzekering?

3. Draagbare apparaten

De komst van draagbare apparaten en de mogelijkheid om thuis te werken heeft het leven een stuk makkelijker gemaakt voor velen van ons. Echter, deze nieuwe manier van werken betekent ook dat belangrijke en vertrouwelijke gegevens kunnen worden gestolen of gemakkelijker verloren. Een laptop achtergelaten in een trein, een gestolen iPad in een restaurant of een verloren USB stick zijn allemaal goede voorbeelden. Bovendien zijn de apparaten zelf het doelwit met een groeiend aantal virussen. De Cyber en Data Risks verzekering van Turien & Co. dekt de kosten en aansprakelijkheid die gepaard gaan met een data-inbreuk via draagbaar apparaat.

4. Data zijn waardevol

We hebben meer data dan ooit tevoren en vaak zijn deze gegevens van onze klanten en leveranciers. Non-disclosure overeenkomsten en commerciële contracten, garanties en vrijwaringen besteden steeds meer aandacht aan beveiliging van data. Gegevens van derden zijn waardevol en u kunt aansprakelijk worden gesteld als u het verliest ongeacht de oorzaak. De Cyber en Data Risks verzekering van Turien & Co. vergoedt de eigen kosten en de schade van derden als gevolg van verlies van data en/ of inbreuk op privacy.



5. Niet goed gedekt binnen traditionele verzekeringen

Verhouding tot traditionele verzekeringen *

De indruk bestaat dat sommige cyberrisico's al gedekt zijn op enkele traditionele verzekeringen. Zo kan een bestaande bedrijfsschadeverzekering een deel van de gevolgschade dekken die door een cyberincident ontstaat. De belangrijkste bestaande verzekeringen die dit al dekken, zijn de brand- en technische verzekeringen (machinebreuk/computer), de aansprakelijkheidsverzekering en de fraudeverzekering.

Brand- en technische verzekeringen*

Brand- en technische verzekeringen in de zakelijke markt bieden ofwel een allrisk dekking ofwel een dekking waarbij alleen specifieke schadeoorzaken verzekerd zijn. De allrisk dekkingen komen veel voor in de grootzakelijke markt, de specifieke oorzaken variant komt veel voor in de MKB-markt. In beide gevallen zal de overlap met Cyber en Datarisk verzekering doorgaans klein zijn. Bij een allrisk dekking is in principe alle materiële schade gedekt. In het geval dat een cyberincident dus ook materiële schade tot gevolg heeft, dan kan voor die materiële schade dekking worden gevonden bij de brandverzekering. Denk bijvoorbeeld aan de hacker die via een computerverbinding een lopende band of machine hackt, waardoor deze in elkaar draait. Verzekeraars beschouwen schade aan data echter zelden als materiële schade. Voor de schade aan data is dan ook een Cyber en Datarisk verzekering van belang. Bij een verzekering die alleen specifieke schadeoorzaken verzekert wordt tot op heden cyberschade zelden meeverzekerd. De overlap is daarom in beide dekkingsvarianten minimaal.



MALWARE

INFECTED

UNAUTHORIZED

INTRUDER

TROJAN

De algemene aansprakelijkheidsverzekering biedt in de regel alleen dekking voor zaak- en letselschade. Financieel nadeel valt hier niet onder, dus schade door cyberrisico ook niet. Ook een beroepsaansprakelijkheidsverzekering biedt onvoldoende dekking voor cyberincidenten. Toch kan het in sommige gevallen onderdeel uitmaken van de dekking. Dit is echter eerder uitzondering dan regel.

Fraudeverzekerings*

De commerciële fraudeverzekering biedt dekking voor de directe financiële gevolgen van frauduleus handelen door werknemers en gespecificeerde soorten van frauduleus handelen door derden, waaronder afpersing, vervalsing van onder andere geld of documenten en computerfraude. Hierdoor kan er overlap ontstaan met de Cyber en Datarisk verzekering, aangezien deze eveneens dekking biedt voor financieel nadeel als gevolg van afpersing, bijvoorbeeld bij encryptie van gegevens. Daarnaast kan overlap bestaan binnen de computerfraudedekking. Voor deze uitkering moet binnen de fraudeverzekering echter wel sprake zijn van daadwerkelijk verlies van financiële middelen (verlies van saldo op bankrekeningen). De kosten om een aanval af te wenden vallen buiten veel verzekeringsdekkingen. Daarnaast worden deze dekkingen binnen de fraudeverzekering veelal beperkt.

Mind the gap*

Geen enkele traditionele verzekering biedt dus uitgebreide dekking in geval van cyberincidenten. Daarom heeft een Cyber en Datarisk verzekering in veel gevallen toegevoegde waarde. Analyseer de bestaande verzekeringen op mogelijke overlap, maar: **mind the gap!**

*Bron: Position Paper 'Virtuele risico's, echte schade'

6. Meldplicht datalekken

Heeft u uw relatie al geïnformeerd over de Meldplicht datalekken? Deze nieuwe wet zegt in vogelvlucht:

- ✓ **Boete van maximaal €820.000 of 10% van de jaaromzet**
- ✓ Voor commerciële instellingen en (semi-) overheid
- ✓ Binnen 48 uur melden bij falen van technische en organisatorische beveiliging met kans op verlies of onrechtmatige verwerking van persoonsgegevens
- ✓ Aard en vermoedelijke omvang van het datalek
- ✓ Inspanningen om de schade te herstellen
- ✓ Raadgevingen aan publiek en klanten

[Hier](#) vindt u de beleidsregels
Meldplicht datalekken



7. Cyberrisico's voor uw relaties

Waar moet uw klant zoal aan denken bij risico's voor zijn onderneming? Onderstaand treft u de meest voorkomende cyberrisico's in het MKB:

- ✓ Gehackte telefooncentrale
- ✓ Phising e-mails
- ✓ Politievirus / Locky ransomware
- ✓ DDOS
- ✓ Kwijtraken laptop of USB stick
- ✓ Datadiefstal



8. Welke gegevens zijn blootgesteld aan risico's?

- ✓ Persoonsgegevens
- ✓ Beschermde (gezondheid/zorg) gegevens
- ✓ Betaalkaart gegevens

Waarom worden persoonsgegevens gestolen?

Persoonsgegevens zijn simpelweg veel geld waard. Criminelen kunnen gestolen persoonsgegevens en vertrouwelijke informatie eenvoudig te gelde maken, bijvoorbeeld door fraude te plegen of door vertrouwelijke informatie te koop aan bieden.

Ter bescherming van persoonsgegevens zijn strenge regels opgelegd aan het bedrijfsleven; bedrijven die een fout maken of gehackt worden, moeten de kosten van de inbreuk betalen.



9. Mogelijke oorzaken

- ✓ Schadelijke of criminele aanvallen veroorzaken 44% van de inbreuken (grootste financiële schade)
- ✓ 31% van de inbreuken zijn te wijten aan de nalatigheid van personeel. Hieronder vallen ook gestolen, verloren , mobiele toestellen en fouten gemaakt door derden.
- ✓ 25% van de inbreuken worden veroorzaakt door een het falen van een IT-systeem



10. Mogelijke kosten

- ✓ Kosten van digitaal forensisch onderzoek
- ✓ Melden en inlichten van gedupeerden (kosten lopen uiteen van €1,25 tot €5,- p.p.)
- ✓ Kosten voor PR en crisismanagement
- ✓ Ransomware, betaling voor cyberafpersing
- ✓ Kosten voor herstel van ICT-systemen
- ✓ Bedrijfsschade



11. Dekking door Cyber en Datariskverzekering

Systeeminbraak: Deze dekking dekt eigen kosten als gevolg van inbraak op systemen of data:

- ✓ Kosten van forensisch onderzoek
- ✓ Kosten van communicatie met klanten, toezichthouders, justitie, creditmaatschappijen en andere belanghebbenden
- ✓ Kosten voor extra klantenondersteuning, bijvoorbeeld via een call centre
- ✓ Kosten van crisismanagement, reputatieherstel en pr-campagnes

Privacy: Deze dekking dekt gevolgen van gestolen privacygevoelige gegevens:

- ✓ Kosten van onderzoek door bijvoorbeeld justitie of creditcardmaatschappijen
- ✓ Claims van individuele personen
- ✓ Boetes opgelegd door toezichthouders, of andere verplichte vergoedingen

Digitale aansprakelijkheid:

- ✓ Deze dekking dekt voortvloeiende schade als bijvoorbeeld de website of e-mail onbedoeld het auteursrecht schendt, laster verspreidt of een virus bevat

Hacking: Deze dekking dekt de schade veroorzaakt door hackers:

- ✓ Reparatie, vervanging of herstel van websites, programma's of data
- ✓ Kosten van gestolen software of data
- ✓ Kosten van onderzoek en advies in systeembeveiliging
- ✓ Kosten van forensisch onderzoek naar de oorzaak van een hacking



11. Dekking door Cyber en Datarisks verzekering

Afpersing: Deze dekking beschermt uw relatie

Bescherm uw relatie tegen de schade van hackers die de website of data gijzelen. Uw relatie krijgt bijstand van security-adviesbureau NetDiligence en eventueel betaald losgeld wordt vergoed.

Omzet verlies door cyberaanvallen: Deze dekking dekt omzetverlies

Dekt omzetverlies door bijvoorbeeld een DDos-actie of andere aanval op de computersystemen van uw relatie wanneer deze leidt tot omzetverlies, bijvoorbeeld door uitval van een webwinkel .

Alle onderdelen zijn in één pakket verzekerd. Het is niet mogelijk om de onderdelen los van elkaar te verzekeren.

Gratis Security QuickScan!

Bij het afsluiten van onze Cyber en Datarisk verzekering wordt een gratis Security Quickscan aangeboden!

Naast de Quick Scan door ESET, biedt Hiscox ook een juridische check van de bewerkersovereenkomst aan. Dit betreft een scan en het aanpassen van bestaande bewerkersovereenkomsten ter waarde van 6 uur juridische dienstverlening; een controle van de bewerkersovereenkomst waarbij u wordt gewezen op mogelijke risico's, alsmede het aanpassen van de bewerkersovereenkomst. Deze check is van belang omdat je de medewerking van je ICT partner nodig hebt bij een incident.



12. E-mailing – Do's & Dont's

Een e-mailing is een snelle en persoonlijke manier om uw relaties te bereiken.



Do's bij een e-mailing

✓	Zorg dat de e-mail verstuurd wordt door een herkenbaar en persoonlijk e-mailadres
✓	E-mail op het juiste moment. Goede tijden zijn: tussen 10 en 12, en na 17 uur. Het weekend is vaak onbenut en voor u dus een kans!
✓	De eerste twee woorden van het onderwerp worden het beste gelezen
✓	Zet de belangrijkste informatie bovenaan
✓	Test uw e-mail incl. afbeeldingen en/of links in Gmail, Outlook en/of Hotmail
✓	Personaliseer de e-mailing waar mogelijk



Dont's bij een e-mailing

✓	Te veel tekst gebruiken
✓	Alleen afbeeldingen gebruiken
✓	Geen grote bijlagen toevoegen
✓	Privacy statement toevoegen
✓	Onderwerpregel vergeten

Mailmerge geeft u de mogelijkheid om in één keer al uw relaties tegelijk de e-mailing te versturen. Ook kan dit gepersonaliseert worden.

Klik [hier](#) voor een uitleg hoe u uw e-mailing kunt mergen.

13. E-mailing – Optie 1 Aansprakelijkheid

Naamloos - Bericht (HTML)

Bericht Invoegen Opties Tekst opmaken Adobe PDF

Verzenden Aan... CC... Onderwerp: Bent u verzekerd tegen cyberrisico's?

Beste <relatie>,

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. Soms moeten zij het datalek ook melden aan de personen van wie de gegevens zijn gelekt. Het onderzoeken van een datalek en de juridische afwikkeling hiervan kan aanzienlijke kosten met zich mee brengen.

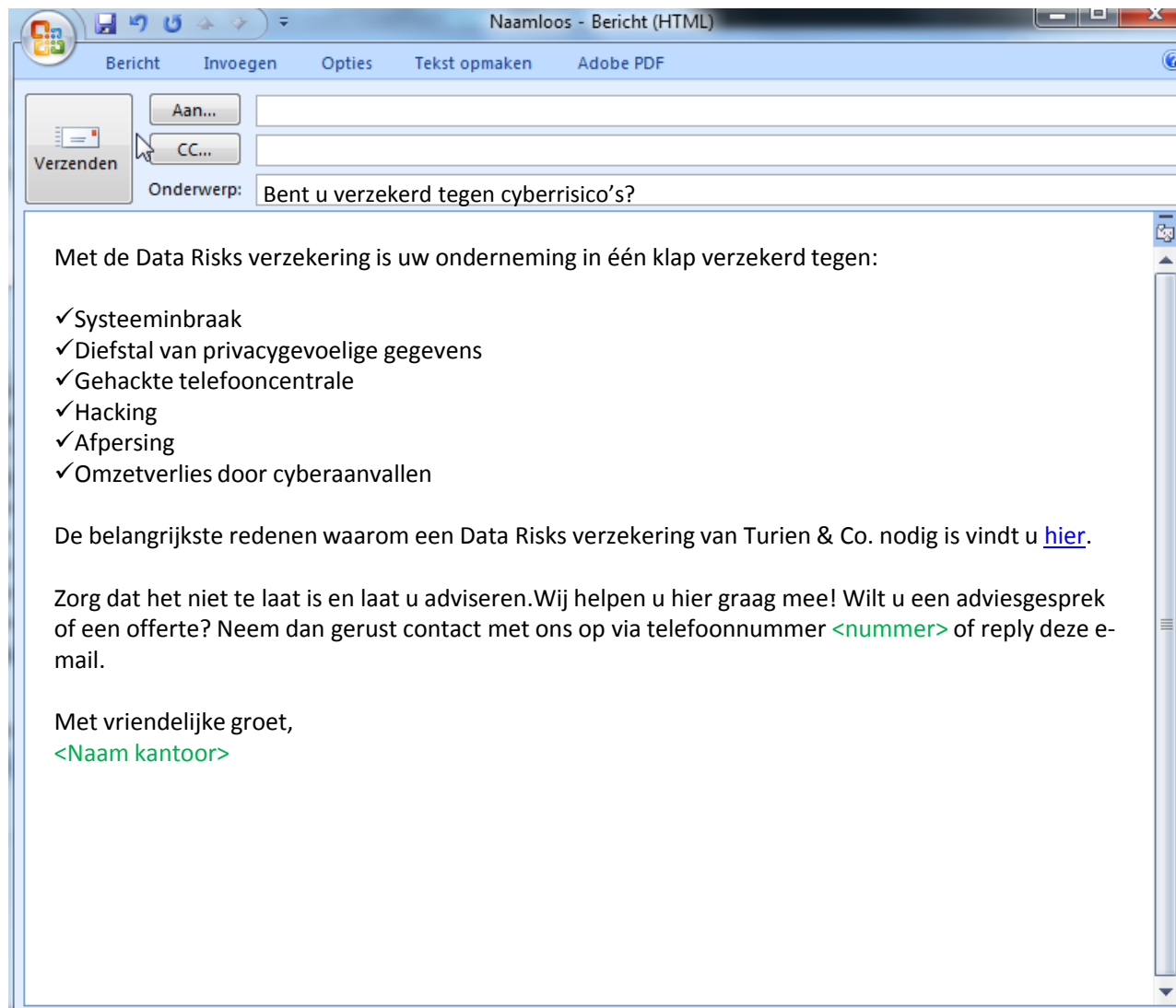
MKB'ers vormen een aantrekkelijke prooi voor cybercriminelen omdat er meer bij hen te halen valt dan bij de gemiddelde consument. De meeste ondernemers hebben hun cybersecurity echter niet beter geregeld dan de gemiddelde consument!

Beschikt u over persoons- of betaalkaartgegevens van uw relaties of verwerkt u grote hoeveelheden gegevens van derden? Beschikt u over medische gegevens? Of zijn uw systemen gekoppeld met die van andere organisaties? Dan loopt u waarschijnlijk aansprakelijkheidsrisico's die op de traditionele aansprakelijkheid verzekeringen niet of nauwelijks zijn gedekt. U doet u er verstandig aan om in kaart te (laten) brengen welke aansprakelijkheidsrisico's u loopt en in hoeverre deze risico's zijn afgedekt met een verzekering.

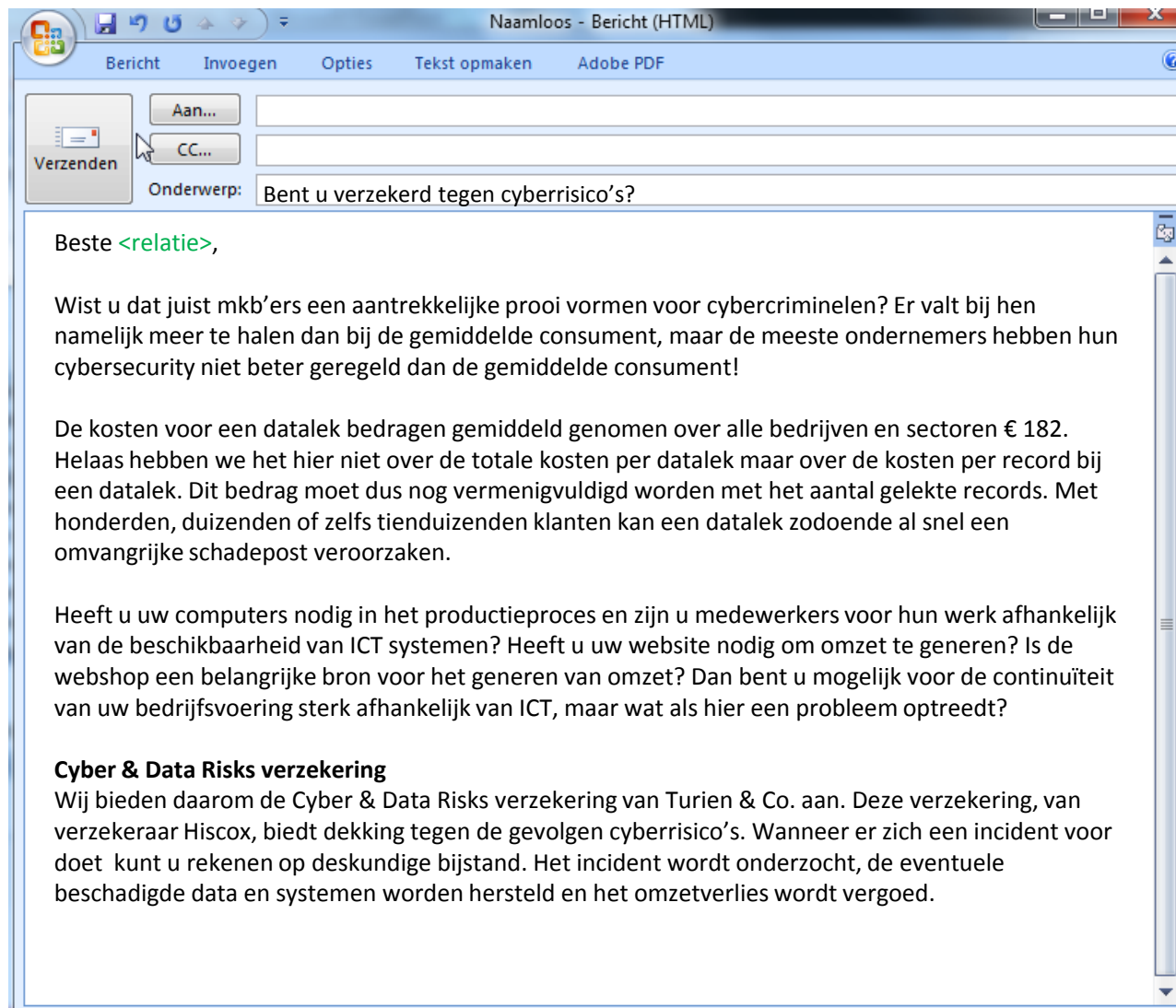
Cyber & Data Risks verzekering

Wij bieden daarom de Cyber & Data Risks verzekering van Turien & Co. aan. Deze verzekering, van verzekeraar Hiscox, biedt dekking tegen de gevolgen van inbreuk op data. Een incident waarbij gevoelige, beschermde of vertrouwelijke gegevens gekopieerd, overgedragen, gestolen of gebruikt worden door een persoon die niet bevoegd is om deze handelingen uit te voeren.


12. E-mailing – Optie 1 Aansprakelijkheid



14. E-mailing – Optie 2 Bedrijfsschade



14. E-mailing – Optie 2 Bedrijfsschade



Naamloos - Bericht (HTML)

Bericht Invoegen Opties Tekst opmaken Adobe PDF

Verzenden Aan... CC... Onderwerp: Bent u verzekerd tegen cyberrisico's?

Met de Data Risks verzekering is uw onderneming in één klap verzekerd tegen:

- ✓Systeeminbraak
- ✓Diefstal van privacygevoelige gegevens
- ✓Gehackte telefooncentrale
- ✓Hacking
- ✓Afpersing
- ✓Omzetverlies door cyberaanvallen

De belangrijkste redenen waarom een Data Risks verzekering van Turien & Co. nodig is vindt u [hier](#).

Zorg dat het niet te laat is en laat u adviseren. Wij helpen u hier graag mee! Wilt u een adviesgesprek of een offerte? Neem dan gerust contact met ons op via telefoonnummer <nummer> of reply deze e-mail.

Met vriendelijke groet,
<Naam kantoor>

15. Social Media

Social media is één van de meest effectieve manieren om uw bedrijf en uw producten en diensten te promoten op internet.

Post een casus!

Om het risico voor uw relaties te duiden kunt u elke week een casus posten op social media waaruit blijkt wat de gevolgen/kosten kunnen zijn als uw relatie ten prooi valt aan cybercriminaliteit.

Naar je eigen site!

Post een bericht die ervoor zorgen dat er doorgeklikt wordt naar je eigen internetpagina over de Cyber en Datarisk verzekering.



Turien & Co. Assuradeuren

Gepubliceerd door Stephan de Wit [?] · 24 februari · 🌐

Een hotelketen wordt gehackt. De credit card gegevens van 700 klanten vallen in verkeerde handen. Wat zijn de te verwachten kosten? [<link naar casus>](#) #cyber



Turien & Co. Assuradeuren

Gepubliceerd door Stephan de Wit [?] · 24 februari · 🌐

Wist u dat het MKB 2 keer zo vaak het slachtoffer wordt van cybercrime dan grotere ondernemingen? <link over cybercrime op uw site> #cybercrime

Klik [hier](#) voor casussen



15. Social Media



“ Een update delen Foto uploaden

Veel MKB-ers onderschatten het gevaar van cybercrime. Terwijl juist zij veel gevaar lopen. Ook alle branches lopen gevaar. Hier een casus van een overslagbedrijf <link> [#cybercrime](#)

Delen met: openbaar Delen



Status Foto/video Aanbieding, Evenement +

 Weet u al hoe groot de risico's en gevolgen kunnen zijn van een datalek?
<link website>



Status Foto/video Aanbieding, Evenement +

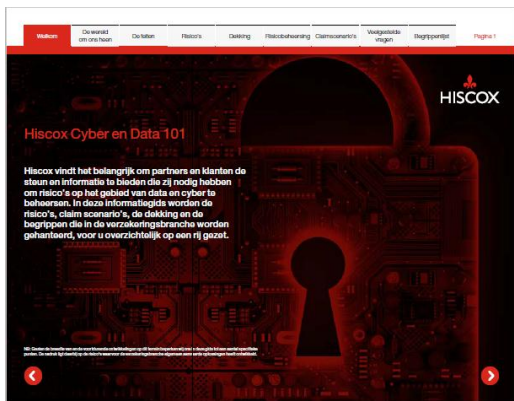
 MKB'ers vormen een aantrekkelijke prooi voor cybercriminelen omdat er meer bij hen te halen valt dan bij de gemiddelde consument. De meeste ondernemers hebben hun cybersecurity echter niet beter geregeld dan de gemiddelde consument. U wel? <link website>



16. Meer informatie

Download dan [hier](#) de brochure 'Hiscox Cyber en Data'

Download dan [hier](#) de Position Paper 'Virtuele risico's, echte schade'



17. Praktijkvoorbeelden

Voor praktijkvoorbeelden klikt u [hier](#)