AANDACHTSPUNTEN BIJ STILLE DEKKINGEN IN TRADITIONELE POLISSEN

VERBOND VAN VERZEKERAARS

Oktober 2023

Het Platform Cyber van het Verbond van Verzekeraars heeft onder andere als doelstelling zijn leden en andere belanghebbenden te informeren over ontwikkelingen in cyberrisico's. In deze whitepaper zoomen we, aan de hand van voorbeelden, in op de zogeheten 'stille dekking' van cyberrisico's die het meest voorkomen in traditionele verzekeringen, zoals verzekeringen voor bedrijfs- en bestuurdersaansprakelijkheid, brand- en technische verzekeringen en motorrijtuigverzekeringen.

Dit document maakt onderdeel uit van een reeks van in totaal drie papers die ingaan op cyberrisico's en de verzekerbaarheid ervan. Eerder hebben we de paper over het systeemrisico in het cyber(verzekering)domein gepubliceerd. Daarin zijn we dieper ingegaan op enkele specifieke elementen van cyberdreigingen, die in belangrijke mate bijdragen aan het systeemrisico: ransomware, privacy en het gebrek aan incident data. Later dit jaar volgt de paper over 'marktontwikkelingen' waarin we stil zullen staan bij (inter)nationale ontwikkelingen binnen de cyberverzekeringsmarkt.

AANLEIDING

(Her)Verzekeraars maken zich zorgen over de aanwezigheid van onbedoelde dekking voor cyberrisico in hun portefeuilles. In mei 2017 deed zich een groot cyberincident voor: Wannacry. Het betrof een aanval met ransomware waarmee in korte tijd meer dan 230.000 computers in 150 landen geïnfecteerd raakten. De schade was groot. Het Deense containerbedrijf Maersk liep naar eigen zeggen een totale schade op van honderden miljoenen omdat de operatie wekenlang stil lag.

Dit incident was een 'eye opener' voor (her)verzekeraars. Het grootste deel van de verzekerbare schade was namelijk verzekerd op traditionele brand, transport en- aansprakelijkheidsverzekeringen (in plaats van de cyberverzekering)*. Dat dit zo zou kunnen gebeuren was door (her)verzekeraars nooit voorzien.

Dit cyberrisico, dat schuilt in de dekking van de traditionele verzekeringen, wordt silent cyber genoemd. Sindsdien is het aantal cyberincidenten in alle sectoren toegenomen. De impact van die aanvallen wordt almaar groter.

De COVID-19 pandemie heeft de afhankelijkheid van digitale infrastructuren verder versneld waardoor bedrijven ook nog eens meer blootstaan aan cyberdreigingen.

De Russische inval in Oekraïne zorgt bovendien voor geopolitieke instabiliteit waarbinnen zich verdere cyberincidenten kunnen voordoen.

* In 2018 deden zich nog twee grote cyberincidenten zich voor: Petya en NotPetya. Naar inschatting van verzekeraars en herverzekeraars bedroeg de schade voor verzekeraars in totaal $ 3 miljard waarvan ongeveer 90% silent cyber.

https://www.reinsurancene.ws/petya-cyber-industry-loss-passes-3bn-driven-by-merck-silent-cyber-pcs/

DEFINITIE SILENT CYBER: Dekking voor schade als gevolg van een cyberrisico op een traditionele verzekering. Het risico is niet in-of uitgesloten. Dit kan betekenen dat schade als gevolg van een cyberrisico onbedoeld gedekt is.

Vormen van stille dekking

De modelpolissen van traditionele verzekeringen zoals Gebouwen, Inventaris/voorraad, Bedrijfsschade en Aansprakelijkheid zijn in een tijd ontworpen waarin IT bij bedrijven geen (belangrijke) rol speelde. Daarom is bij het ontwerp en bij de verwerking van aanpassingen onvoldoende rekening gehouden met schade en gedekte gebeurtenissen die door een cyberincident kunnen ontstaan. Het risico dat hierdoor ontstaat, wordt ook wel "silent cyber" of "non-affirmative cyber coverage" genoemd.

Silent risk = stille dekking.

Stille dekkingen kunnen op de volgende drie manieren terug te zien zijn in verzekeringspolissen:

1. Cyberrisico wordt als mogelijke oorzaak voor schade niet expliciet in- of uitgesloten;
2. Cyberrisico wordt als mogelijke oorzaak voor schade uitgesloten maar de verwoording is dubbelzinnig of onvolledig;
3. Cyberrisico wordt als mogelijke oorzaak voor schade expliciet ingesloten maar de bewoording is dubbelzinnig of conflicteert met andere voorwaarden.

Belangen

Verzekeraars lopen ongemerkt cyberrisico's in de traditionele verzekeringsproducten. Het is in het belang van de klant én in het belang van verzekeraars daar iets aan te doen.

BELANG VAN VERZEKERAARS

Productontwikkeling/pricing/acceptatie

- Er wordt onvoldoende rekening gehouden met cyberrisico van organisaties.
- Producten zijn niet altijd goed genoeg geprijsd.

Accumulatierisico managen

- Er is een potentieel accumulatierisico omdat een wereldwijd cyberincident (systemic risk) door één gebeurtenis mogelijk voor veel claims kan zorgen. Denk aan het voorbeeld van Wannacry en NotPetya.

Stakeholders vinden het belangrijk

- Het onvoldoende aanpassen van het productaanbod brengt een reputatierisico met zich mee.
- Herverzekeraars eisen van verzekeraars om silent cyber risico's aan te pakken of sluiten het zelf (deels) van de dekking uit (actueel!).
- Rating agencies nemen de aanpak van silent cyber op in hun rating .*

Het onderwerp staat op de agenda van de toezichthouders. Zo heeft De Nederlandse Bank in 2022 een studie gedaan waarin ze het risico op schadeclaims voor onvoorziene cyberincidenten heeft benoemd. En in december 2022 bracht EIOPA een supervisory statement uit.

BELANG VAN VERZEKERDE

De verzekerde denkt goed verzekerd te zijn, maar is dat mogelijk toch niet

- Door het gebrek aan expliciete insluitingen of uitsluitingen in traditionele verzekeringsproducten is het voor veel bedrijven onduidelijk of en door welke producten schade door cyberincidenten gedekt is. Bij schade kan dit leiden tot teleurstellingen.

Discussie voorkomen

Onduidelijkheden in de voorwaarden kunnen bij schade leiden tot disputen. Deze betekenen vertraging en onzekerheid voor alle betrokken partijen. Daar is niemand bij gebaat.

* Bron:
https://www.captive.com/news/fitch-cyber-risk-analysis-inhibited-by-silent-cyber-risk-exposure

Verzekeraars in een veranderende wereld (dnb.nl)

Welke maatregelen nemen verzekeraars zoal?

1

SCHADE DOOR CYBERRISICO WORDT EXPLICIET INGESLOTEN. SOMS GELDEN SUBLIMIETEN.

Voordelen

- Ruime dekking, nauwelijks hiaten:
  - Geen verminderde dekking voor verzekerde of noodzaak voor alternatief.
  - Geen disputen over definitie van cyberincidenten.
- Duidelijkheid voor de verzekerde.

Nadelen

- Complex/kostbaar in de uitvoering.
- Mogelijke discussie of hogere premie kan worden gevraagd.

2

SCHADE DOOR CYBERRISICO WORDT EXPLICIET UITGESLOTEN.

Voordelen

- Duidelijkheid voor de verzekerde.
- Goedkoop en eenvoudig in de uitvoering.

Nadelen

- Niet klantvriendelijk:
  - Het cyberrisico van klanten wordt niet weggenomen.
  - Risico op hiaten in de dekking.
- Staat haaks op de maatschappelijke rol van verzekeraars bij het mitigeren van cyberrisico's.

3

SCHADE DOOR CYBERRISICO WORDT EXPLICIET UITGESLOTEN MET UITZONDERING VAN EEN AANTAL SPECIFIEK OMSCHREVEN TYPE CYBERINCIDENTEN.

Voordelen

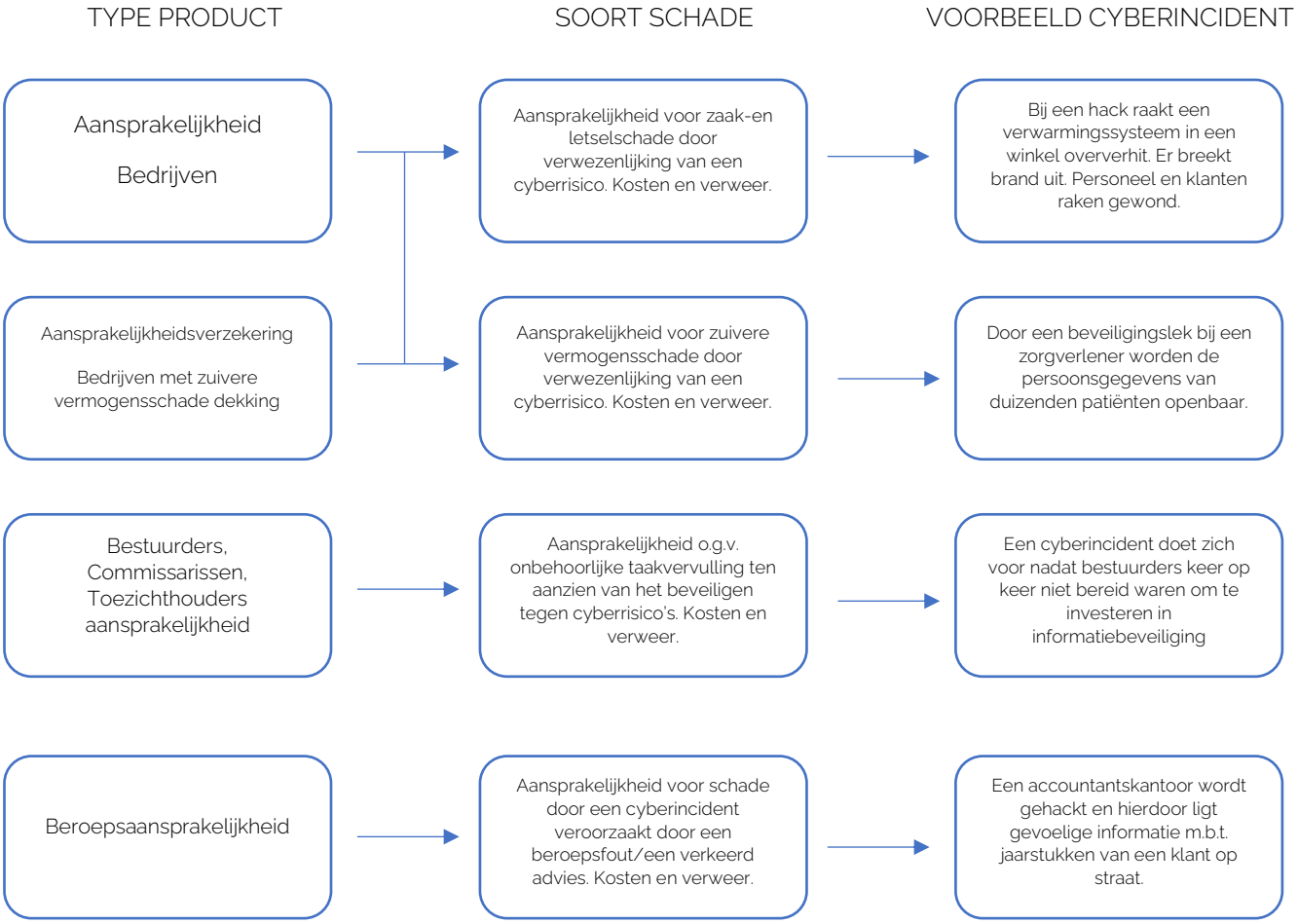
- Is voor de verzekerde beter dan alle cyberincidenten uitsluiten.

Nadelen

- Dekking blijft nog steeds beperkt.
- Kan mogelijk leiden tot onduidelijkheden en disputen over wat wel/niet gedekt is.

VOORBEELDEN van gedekte cyberschade op traditionele verzekeringen omdat een cyberschade niet expliciet is in- of uitgesloten

Aansprakelijkheidsverzekeringen en silent cyber risico's.



Beroepsaansprakelijkheidsverzekering

De beroepsaansprakelijkheidsverzekering is soms een vreemde eend in de bijt, gezien de ontwikkelingen op het gebied van cyberincidenten echter wel een zeer belangrijke verzekering. Om die reden gaan we hieronder nader in op deze verzekering.

De beroepsaansprakelijkheidsverzekering biedt in de basis dekking voor de aansprakelijkheid van een verzekerde voor de door derden geleden schade als gevolg van een beroepsfout die wordt gemaakt in het kader van de beroeps-uitoefening. Onder deze aansprakelijkheid kan dus ook de aansprakelijkheid voor cyberincidenten vallen, mits er sprake is van een beroepsfout gemaakt in het kader van de beroepsuitoefening.

Steeds vaker krijgen verzekeraars dan ook de vraag of aansprakelijkheid ten gevolge van cyberincidenten verzekerd is op de traditionele beroepsaansprakelijkheids-verzekering. De vraag is dan met name of schade aan derden (lees o.a.: klanten) door bijvoorbeeld een tekortschietende beveiliging van de website, het netwerk, de opslag en/of de verwerking van digitale (persoons)gegevens is verzekerd op een beroepsaansprakelijkheidsverzekering.

Een voorbeeld is het lekken van financiële gegevens door een hack in het netwerk van de accountant, waardoor een fusie in gevaar komt. Dit voorbeeld kan – zeker zonder expliciete uitsluiting voor cyberincidenten - op een beroepsaansprakelijkheidsverzekering verzekerd zijn.

Een ander voorbeeld is het per ongeluk lekken van privacygevoelige informatie van een cliënt door zijn psycholoog. Of dit onder de beroeps-aansprakelijkheidsverzekering zonder expliciete in- of uitsluiting van cyberincidenten valt zal afhangen van het feit of er een beroepsfout is gemaakt.

Zo ja, dan zal een verzekeraar kijken of er sprake is van aansprakelijkheid en wat de schade is/of er schade is geleden door een derde.

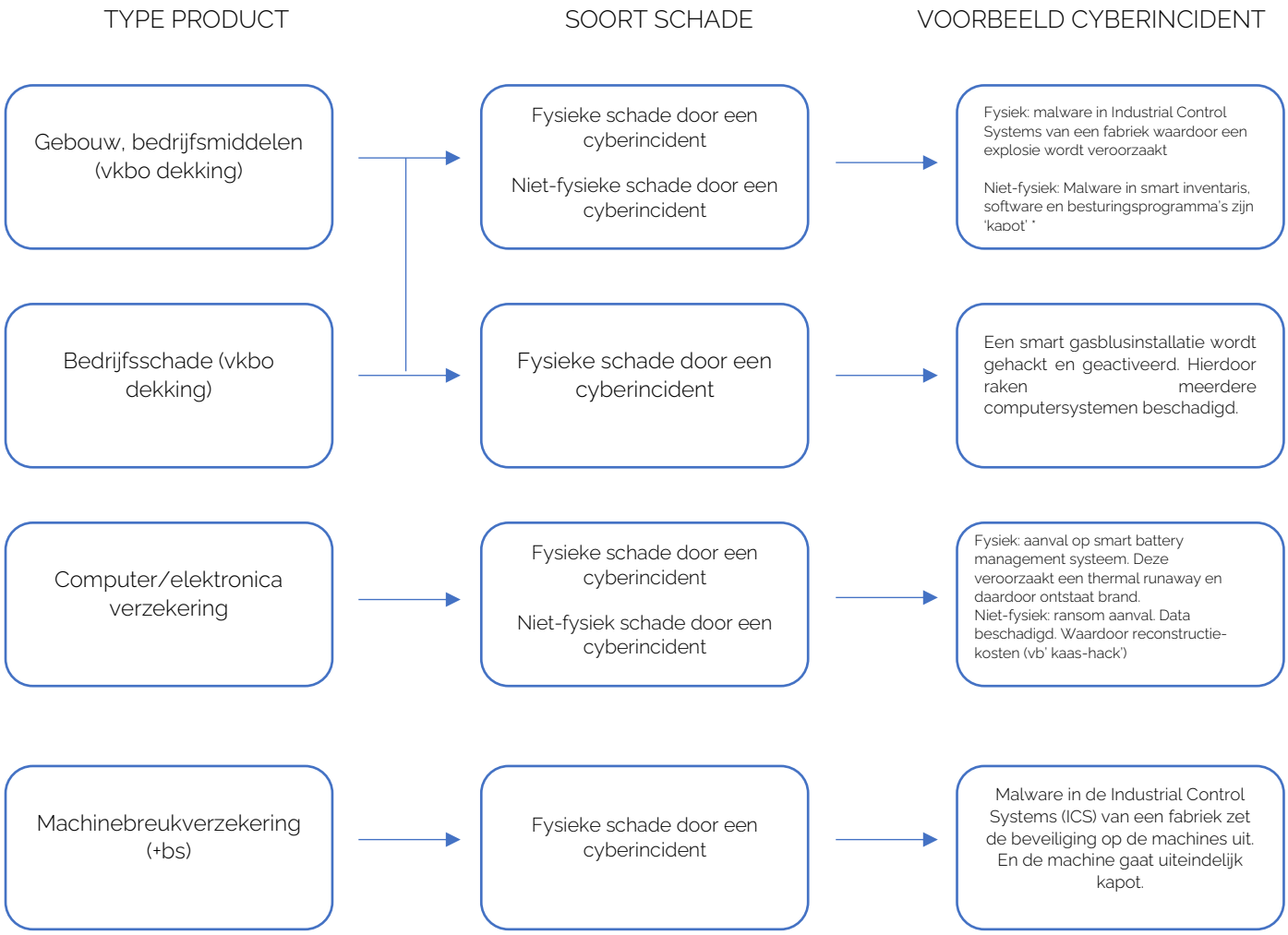
Grofweg zijn er twee soorten cyberincidenten welke voor beroepsaansprakelijkheid van belang kunnen zijn.
Ten eerste, nalatigheid, vergissing, verzuim, en/of onachtzaamheid ten aanzien van de netwerkbeveiliging van een verzekerde (beveiligingsfout). Ten tweede, nalatigheid, vergissing, verzuim, en/of onachtzaamheid ten aanzien van de bescherming van persoonsgegevens (privacyfout) van derden (ook van bijvoorbeeld werknemers).
Voor beide incidenten is niet altijd op voorhand duidelijk of deze meeverzekerd zijn op de beroepsaansprakelijkheidsverzekering aangezien niet alle verzekeraars een in- of uitsluiting hanteren met betrekking tot cyberincidenten, of een duidelijk standpunt hebben ingenomen over het wel of niet verzekeren van cyberincidenten.

In de praktijk zien wij twee oplossingen: 1.) verzekeraars nemen cyberincidenten expliciet in hun voorwaarden op of 2.) sluiten deze volledig uit. Uiteraard zijn er dus nog polissen waar niets expliciet geregeld is of wordt, maar de verwachting is dat verzekeraars een keuze zullen maken uit de genoemde twee opties. Een aantal verzekeraars maakt daarbij ook nog onderscheid tussen grootzakelijk en middelkleinbedrijf (MKB) waarbij de benadering ook binnen hun eigen beroepsaansprakelijkheidsproducten anders kan zijn.

Bij grootzakelijk zie je momenteel vaak een koppeling naar een cyberverzekering of specifieke in- en uitsluiting van cyberaansprakelijkheid. Bij MKB-polissen zien we momenteel dat er veelal nog geen duidelijk standpunt is ingenomen met betrekking tot cyberincidenten noch een verwijzing naar cyberincidenten / cyberaansprakelijkheid. De eerder genoemde voorbeelden kunnen dan nog steeds onder de dekking vallen, maar het zal dan meer afhankelijk zijn van hoe de aanspraak geredigeerd wordt en of er een beroepsfout is gemaakt.

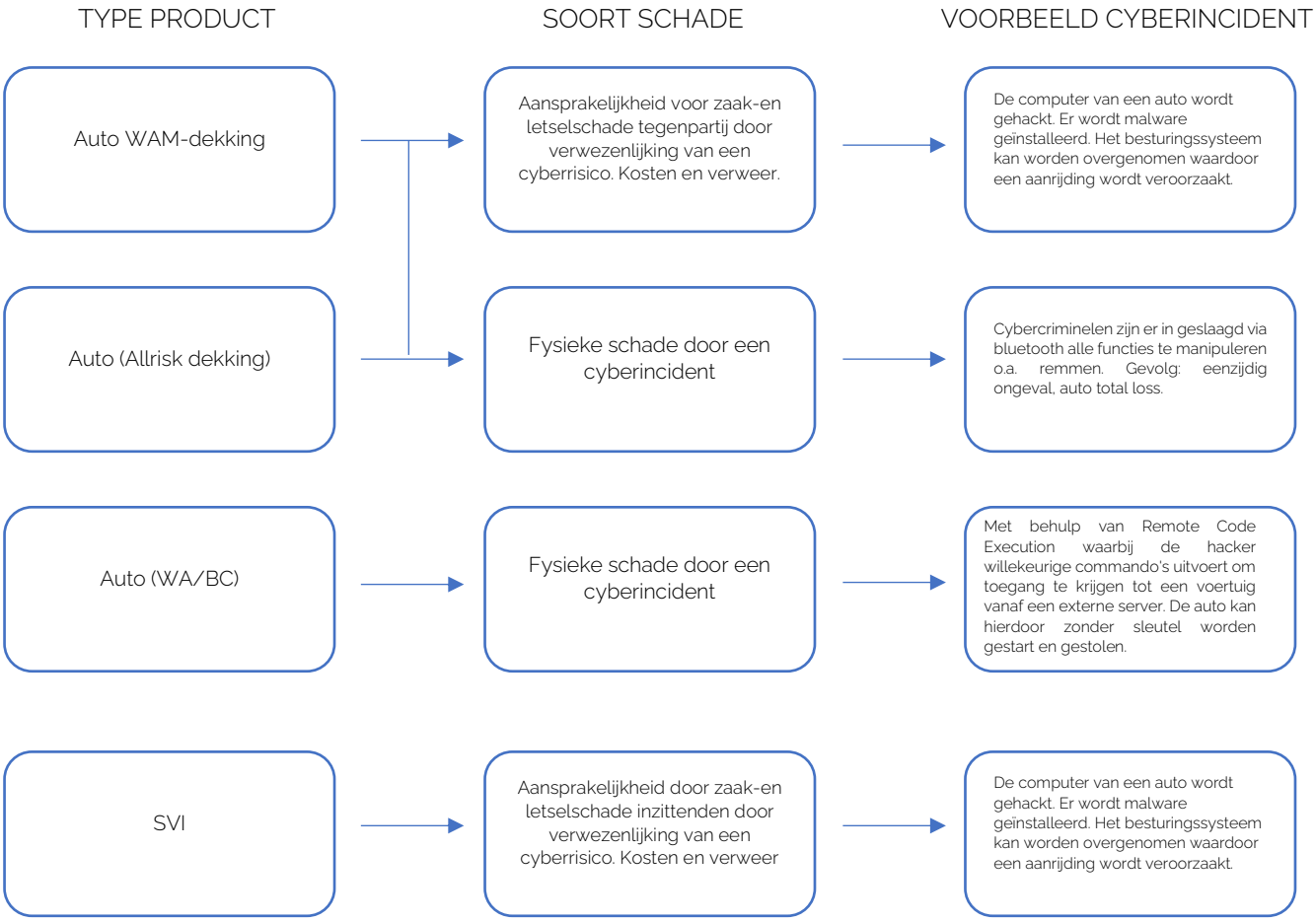
Kortom, voor wat betreft de huidige beroepsaansprakelijkheidsverzekeringen zijn de oplossingen op het gebied van cyberincidenten en cyberaansprakelijkheid nog uiteenlopend. De rol van verzekeringsadviseurs en verzekeraars is groot als het aankomt op het sluiten van een nieuwe verzekering of bij het controleren van een lopende verzekering. Zij dienen goed te kijken of de verzekering dekking biedt voor cyberincidenten en cyberaansprakelijkheid

Brand- en technische verzekeringen en silent cyber risico



* Bij ontbreken vereiste van materiële schade

Motorrijtuigverzekeringen en silent cyber risico



VOORBEELDEN VAN (MOGELIJKE) FYSIEKE SCHADE DOOR CYBERRISICO

BRONNEN:

German Steel Plant Suffers Significant Damage from Targeted Attack - Nouvelles de sécurité - Trend Micro FR | Coast Guard Details February Cyberattack on Ship - WSJ

Ransomware-aanval op Duits ziekenhuis leidde mogelijk tot dood patiënte - Computer - Nieuws - Tweakers | Medicijnrobot in apotheek Wilhelmina Ziekenhuis Assen gehackt - RTV Drenthe

Triton-malware infecteert opnieuw vitale infrastructuur - Security.NL | Hackers Remotely Kill a Jeep on a Highway | WIRED - YouTube