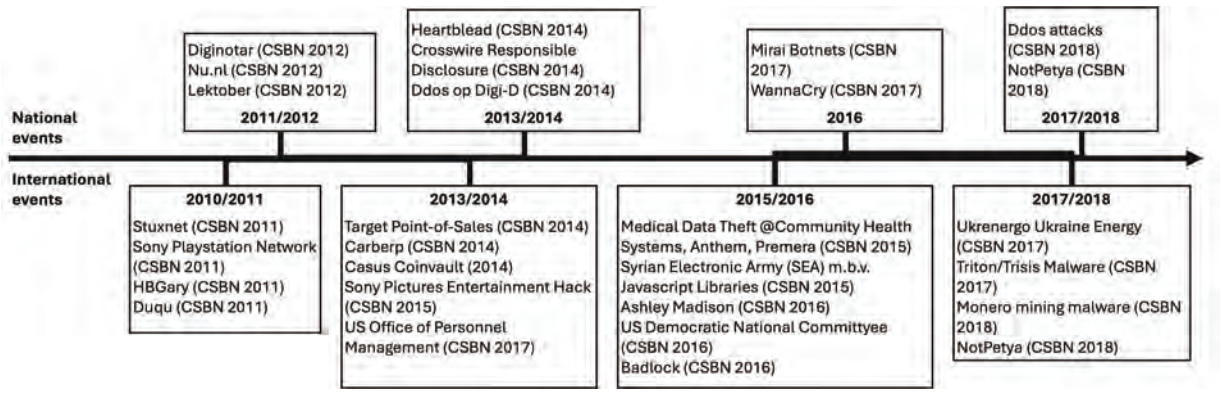
Auteur: Raymond Bierens is parttime promotieonderzoeker en docent bij het Amsterdam Business Research Instituut van de Vrije Universiteit van Amsterdam. Daarnaast is hij onafhankelijk strategisch adviseur en voorzitter van de stichting Connect2Trust die cross-sectorale dreigingsinformatie deelt uit open en gesloten bronnen. De focus van Raymond bij al deze activiteiten ligt op het beheersen van digitale risico's en cybersecurity bij grote digitale transformaties. Hij is bereikbaar via: raymond.bierens@connect2trust.nl.

Meten is weten… als je weet wat je meet

Cybersecurityincidenten spelen een belangrijke rol bij het schrijven van cyberstrategieën als onderbouwing voor de gevraagde investeringen. Het meten van de effectiviteit van diezelfde cyberstrategieën berust veelal op compliance raamwerken die weer worden bijgesteld aan de hand van diezelfde cybersecurityincidenten. Maar wat als de technologie zich sneller ontwikkeld dan die cyberstrategieën en raamwerken? Rekenen we ons dan niet veiliger dan we werkelijk zijn? Een kijkje in de keuken van een lopend promotieonderzoek.



Figuur 1: Analyse (inter)nationale incidenten in CSBN's Nederland t/m 2019.

In 2022 presenteerde de Nederlandse overheid haar meest recente nationale cybersecuritystrategie. Het jaarlijkse Cybersecuritybeeld Nederland (CSBN) vormt een belangrijk basiselement voor deze strategie en biedt inzicht in de ontwikkeling van dreigingen en risico's in Nederland. Het Cybersecuritybeeld Nederland wordt sinds 2011 uitgegeven wat samenviel met de eerste Nationale cybersecuritystrategie. Daarvoor (in 2007) was cybersecurity nog onderdeel van de Nationale Security Strategie. In 2014 verscheen de tweede cybersecuritystrategie, gevolgd door de Nederlandse Cybersecurity Agenda in 2019 en de nieuwste strategie in 2022.

Van cyberincident tot cyberstrategie

De ondertitels (1) van deze vier cybersecuritystrategieën laten zien hoe de focus van deze strategieën is verschoven van samenwerking en betere bekwaamheden, naar de gevolgen van de steeds sneller digitaliserende samenleving. Onderzoek (2), uitgevoerd in samenwerking met de universiteit ETH Zürich laat zien welke Nederlandse en internationale incidenten worden genoemd en uitgelicht in de diverse dreigingsbeelden. De opkomst van de aanvallen op procesautomatisering (startend met Stuxnet) hebben de noodzaak voor meer bekwaamheden gecreëerd, de gebruikmaking van IoT (o.a. Mirai Botnet) de risico's van het gebruik van IoT.

Het onderzoek, uitgevoerd met ETH Zürich, vergeleek de ontwikkeling van nationale cybersecuritystrategieën in diverse landen (3) en concludeert dat deze strategieën zich hoofdzakelijk reactief ontwikkelen, gedreven door (inter)nationale incidenten. Nieuwe technologische ontwikkelingen worden veel genoemd, maar de meeste aandacht gaat toch naar het voorkomen van deze incidenten. De bestuurlijke inrichting van een land blijkt van grote invloed op de uitvoering van deze strategieën in de onderzochte landen. Een voorbeeld hiervan is de scheiding in Nederland tussen nationale en economische veiligheid, die heeft geleid tot het ontstaan van het Digital Trust Center bij het Ministerie van Economische Zaken en Klimaat, naast het Nationaal Cyber Security Center. Ook al worden deze twee organisaties in de toekomst gebundeld tot één, de bestuurlijke verdeling tussen nationale en economische veiligheid blijft in stand in de vorm van twee opdrachtgevers. In andere landen is deze veiligheidsscheiding er niet en wordt dit ook vertaald in een andere inrichting of ophanging van het Nationaal Cyber Security Center.

De incidenten, en daarmee de nationale cybersecuritybeelden die door veel landen jaarlijks worden gepubliceerd, hebben ook een ander doel. Door de aandacht te vestigen op deze incidenten ontstaat er sociale druk op een overheid om richting te geven aan het voorkomen (of verminderen) van deze incidenten. Dit is tenslotte de basis van ons democratisch bestel en is verankerd in allerlei sociale contracten, zoals bijvoorbeeld de Nederlandse grondwet en het Internationaal Verdrag voor de Rechten van de Mens. Onderzoek (4) toont aan dat de dynamiek van het sociaal contract, of het sociaal cyber contract, ook in de digitale wereld onverminderd van toepassing is. In dat onderzoek werd duidelijk dat dit zich niet alleen beperkt tot de relatie tussen de overheid en de maatschappij, maar ook dat er sprake is van een indirect sociaal cyber contract waarbij de markt enerzijds, en de overheid anderzijds, gezamenlijk proberen organisaties in de private sector te dwingen om maatregelen te nemen om cybersecurity incidenten te voorkomen. Om meer kracht bij te zetten in

De focus van cybersecuritystrategieën is verschoven van samenwerking en betere bekwaamheden, naar de gevolgen van de steeds sneller digitaliserende samenleving

de uitvoering daarvan, werken overheden internationaal samen zoals in Europe rondom de AVG, de CER en de NIS2. Wel blijft er altijd sprake van een zekere geopolitieke spanning, omdat het internet nu eenmaal wereldwijd is en er geen sprake is van een wereldwijde governance.

De NIS scope voor de strategie

De NIS richtlijnen zijn om meerdere redenen een interessant en actueel onderwerp. Niet alleen biedt de NIS door de vorm van een Directive (in plaats van een Act) landen de gelegenheid voor een nationale invulling, waarmee de verschillen in bestuurlijke inrichting kunnen worden gehandhaafd en tegelijkertijd ook het effect daarvan zichtbaar maken. Maar ook omdat de scope van de NIS richtlijn de trend volgt die we ook terugzien in de ondertitels van de nationale cybersecuritystrategieën in Nederland. Deze scope uit de eerste richtlijn (uit 2016) in het kader, inclusief de definitie, van de doorverwijzing naar het elektronisch communicatienetwerk. De richtlijn spreekt in lid b nadrukkelijk over apparaten, groep van apparaten en communicatienetwerken, waarmee zowel de traditionele kantoorautomatisering (IT), als IoT en procesautomatisering (ook wel OT of Operationele Technologie genoemd) binnen de scope valt. Ook de NIS richtlijn speelt daarmee in op de steeds digitaler wordende samenlevingen.

NIS1 (richtlijn (EU) 2016/1148) gebruikt de volgende definitie (in art. 4) als scope:

Netwerk- en informatiesysteem:

a) Een elektronisch communicatienetwerk in de zin van artikel 2, onder a), van richtlijn 2002/21/EG;

b) Een apparaat of groep van geïnterconnecteerde of bij elkaar behorende apparaten, waarvan een of meer, overeenkomstig een programma, digitale gegevens automatisch verwerkt of verwerken, of:

c) Digitale gegevens die via in de punten a) en b) bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan.

De doorverwijzing naar richtlijn 2002/21/EG definieert dan: Elektronisch communicatienetwerk: de transmissiesystemen en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen, waaronder netwerkelementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele terrestrische netwerken, elektriciteitsnetten, voor zover deze voor overdracht van signalen worden gebruikt, netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de over gebrachte informatie;

Het is interessant om de scope uit de definitie van de eerste NIS richtlijn uit 2016 te vergelijken met die uit de tweede NIS richtlijn uit 2022. Ook deze definitie is, net als de doorverwijzing voor een elektronisch communicatienetwerk, opgenomen in het kader. Er vallen daarin een aantal veranderingen op:

- De definitie van een elektronisch communicatienetwerk is aangepast en lijkt nu beter aan te sluiten op de cloud-ontwikkelingen;
- Het is niet meer één (groep van) apparaten, maar elk apparaat (of groep) en
- Het doel van de (groepen van) apparaten en/of elektronische communicatienetwerken is verwijderd. Dit betreft de zinsnede: 'met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan'.

NIS2 (richtlijn (EU) 2022/2555) gebruikt de volgende definitie (in art. 6) als scope:

Netwerk- en informatiesysteem:

a) Een elektronisch communicatienetwerk in de zin van artikel 2, punt 1), van richtlijn (EU) 2018/1972;

b) Elk apparaat of elke groep van onderling verbonden of verwante apparaten, waarvan er een of meer, op grond van een programma, een automatische verwerking van digitale gegevens uitvoeren, of

c) Digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b).

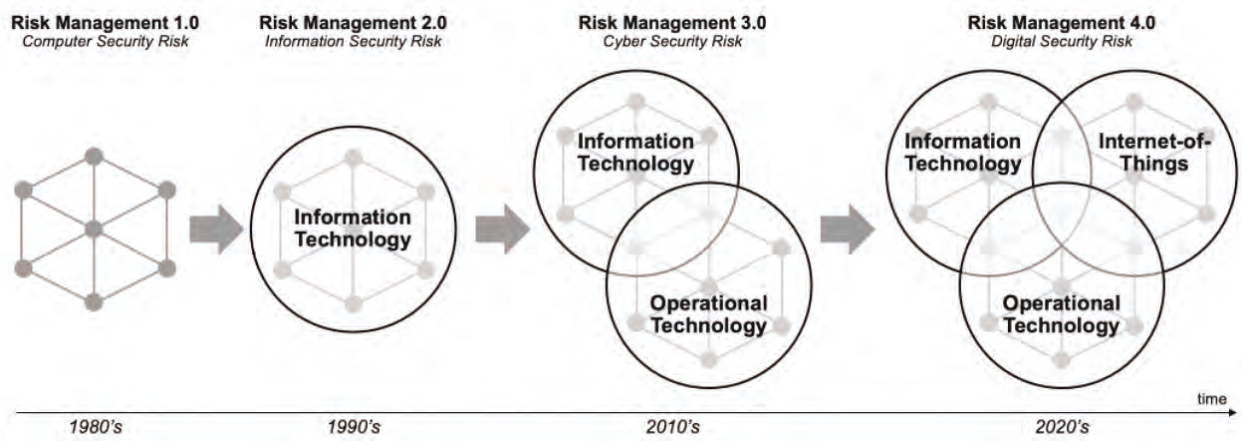
De doorverwijzing naar 2018/1972, artikel 2, punt 1), definieert dan:
Elektronisch communicatienetwerk: de transmissiesystemen, al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit, en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen, waaronder netwerkelementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele netwerken, elektriciteitsnetten voor zover deze voor overdracht van signalen worden gebruikt, netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie;

Hiermee is de scope nog iets groter geworden: waren in de NIS1 alle vormen van technologie (IT, OT en IoT) in scope, is dat voor de NIS2 van toepassing op ieder apparaat ongeacht het doel en al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit. Het is deze definitie die de scope vormt van de uitwerking in ieder land naar de nationale wetgeving.

De ontwikkeling van risk management en compliance

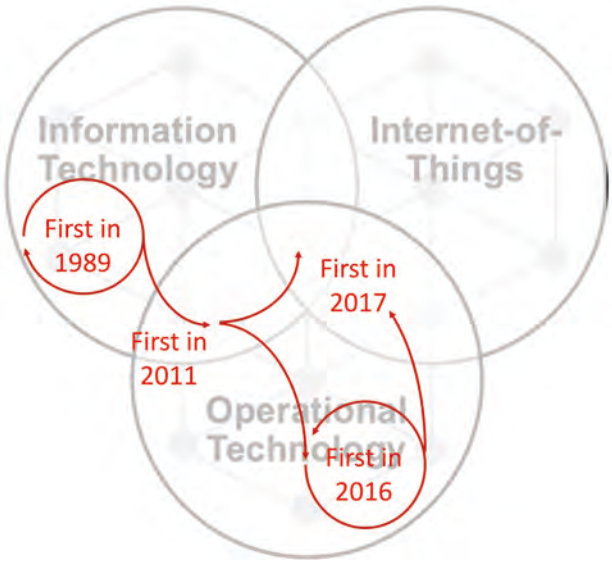
De vraag is nu of de ontwikkeling van compliance gelijke tred houdt met de trends in de internationale wetgeving en nationale cyberstrategieën. Immers, zonder compliance raamwerken, is het niet mogelijk om objectief te meten of er opvolging wordt gegeven aan de strategieën. Hiervoor moeten we kijken hoe, in navolging van de technologische ontwikkelingen en de risico's (en incidenten) die daaruit voortkwamen, compliance en security risk management zich hebben ontwikkeld. Onderzoek (5) naar wetenschappelijke literatuur die ten grondslag ligt aan moderne raamwerken, toont aan dat ook hier een relatie is te vinden met incidenten. Het vakgebied begon in de jaren 80 met het beveiligen van individuele computers. Naarmate deze met elkaar werden verbonden via elektronische communicatienetwerken ontstond een tweede fase van risk management (2.0) waarin nieuwe raamwerken werden ontwikkeld als vakgebied informatiebeveiliging die zich richtte op kantoorautomatisering. De bekendmaking van Stuxnet leidde er in 2011 toe dat er een nieuwe stroming ontstond van risk management (3.0). Deze richtte zich niet op het beveiligen van informatie, maar op het behoud van continuïteit en daarmee kwam ook procesautomatisering (OT) in scope erbij. Vanaf 2016 zijn we, vanuit de steeds digitaliserende samenleving, op weg naar de huidige fase van risicomanagement (4.0). Deze richt zich op elk verbonden apparaat overeenkomstig met de definitie van de NIS1 en NIS2. Figuur 2 (6), hieronder, toont deze ontwikkeling door de tijd, maar ook dat dit geen losstaande risico's zijn. Ze zijn tenslotte veelal aan elkaar verbonden en kunnen dan alleen via een integrale aanpak worden gemanaged.

De vraag is nu of de ontwikkeling van compliance gelijke tred houdt met de trends in de internationale wetgeving en nationale cyberstrategieën



Figuur 2: Transitie van Risk Management door de jaren heen.

Hetzelfde onderzoek (7) dat de ontwikkeling van security risk management heeft onderzocht, keek ook hoe compliance raamwerken zich ontwikkelen als gevolg van diezelfde technologische ontwikkelingen en de risico's (en incidenten) die daaruit voortkwamen. De transitie van risk management 2.0 naar 3.0 laat zien dat er vanaf 2011 sprake is van een 'tussenfase', als nieuwe incidenten bekend worden die worden veroorzaakt door nieuwe technologieën. In deze fase wordt, met behulp van 'oude' maatregelen, geprobeerd om ook deze nieuwe risico's te mitigeren. Een bekend voorbeeld is het omgaan met ransomware bij kantoorautomatisering versus procesautomatisering. Wat bij de ene technologie werkt, kan (veel) grotere gevolgen hebben bij een andere technologie. Pas na het ervaren, soms proefondervindelijk, ontstaan aangepaste of aanvullende raamwerken, als onderdeel van onderkende verschillen tussen de twee. Om die reden gebruiken veel organisaties zowel de ISO27000-serie voor kantoorautomatisering, of de IEC62443 voor procesautomatisering. Sommige sectoren kiezen er soms ook voor om dit nog verder te specificeren naar bijvoorbeeld de Baseline Informatiebeveiliging Overheid (BIO) op basis van ISO, en de Cyber Security Implementatie Richtlijn Objecten, op basis van de IEC62443. Vanaf 2017 zien we hoe, vanuit informatiebeveiliging enerzijds en continuiteitsrisico's anderzijds, er gekeken wordt hoe er met risico's uit andersoortige apparaten, IoT, moet worden omgegaan. Ook hier wordt er dus gestart vanuit de bestaande raamwerken. Figuur 3 geeft deze ontwikkeling grafisch weer.



Figuur 3: Ontwikkeling van compliance in navolging van nieuwe risico's.

Ook op de ontwikkeling van een compliance raamwerk voor het managen van risico's is de werking van het sociaal cybersecurity contract zichtbaar in bij de totstandkoming, de implementatie en handhaving van nationale cybersecuritystrategieën. Bij het schrijven van iedere Nederlandse cybersecuritystrategie is een grote groep bedrijven, non-profit organisaties en overheidsinstel-

lingen betrokken. Bij de ontwikkeling van de CSIR voor procesautomatisering, maar ook bij andere certificeringsprogramma's, is het uitgangspunt 'de markt tenzij' cultureel bepaald. Maar ook bij de ontwikkeling van internationale raamwerken zoals het NIST-raamwerk zijn veel organisaties betrokken, maar volgt het NIST-raamwerk de herkenbare Amerikaanse cultuur; waarbij de president directief (in 2013 en 2021) een opdracht geeft tot het ontwikkelen van een raamwerk en daar dan opvolging aan wordt gegeven. Dit is een duidelijk cultureel verschil met de aanpak in Europa waarbij een richtlijn lokaal wordt vertaald op basis van lokale culture aspecten en kenmerken.

Wat in figuur 3 het meest opvalt, is dat er geen pijltjes voorkomen in de cirkel IoT. We spreken daarom over een vakgebied in ontwikkeling. Het is geen kantoorautomatisering, het is geen procesautomatisering, de risico's en incidenten die het veroorzaakt zijn nog niet grootschalig, en dus is de aandacht voor digital of beter digital-by-design security risk management beperkt. De gevolgen van deze beperking is echter groot: hoeveel cybersecurityoplossingen zijn in staat om alle apparaten zoals de NIS2 voorschrijft: 'elk apparaat of elke groep van onderling verbonden of verwante apparaten' die verbonden zijn met de elektronische communicatienetwerken realtime te inventariseren? En hoeveel organisaties zijn in staat om opvolging te geven aan iedere binnenkomende melding van een kwetsbaarheid en dreiging van al die apparaten?

Ben je dan niet NIS2 compliant als je dat niet kunt? Op dit moment is het antwoord daarop: nee. Want als er geen compliance raamwerk is dat kan worden toegepast of er ontbreken technische oplossingen die het mitigeren van risico's mogelijk maken dan kan een organisatie daar niet verantwoordelijk of aansprakelijk voor worden gehouden. Maar hoeveel bestuurders weten dat ze met compliance op basis van de genomen maatregelen slechts voor een deel hun risico's meten? Om dat te begrijpen moet je weten wat je meet en kun je beginnen met het inschatten wat je restrisico's zijn. En als de geschiedenis van cybersecurity-incidenten ons iets heeft geleerd, is dat er altijd nieuwe incidenten zullen voortkomen vanuit die restrisico's en dat die zullen leiden tot bijgewerkte cybersecurity-strategieën en nieuwe of updates van compliance raamwerken. Maar tegelijkertijd moeten we ons beseffen dat reactiviteit in het proces is ingebakken en we dus altijd achter de feiten aanlopen met restrisico's als onvermijdelijk gevolg. Dat is de prijs die we betalen voor de toenemende afhankelijkheid van technologie in onze maatschappij.

Referenties

(1) 2011: Slagkracht door samenwerking, 2014: Van bewust naar bekwaam, 2019: Nederland digitaal veilig, 2022: Ambities en acties voor een digitaal veilige samenleving

(2) Bierens/Castellon, National Cybersecurity and Cyberdefense - Policy Snapshot of The Netherlands - National Cybersecurity and Cyberdefense Policy_Snapshot of The Netherlands, Center for Security Studies (CSS), ETH Zürich University of Science and Technology, 2019

(3) Oostenrijk, Finland, Frankrijk, Duitsland, Italië, Nederland, Verenigd Koninkrijk en Singapore

(4) Bierens/Van den Berg/Klievink, A Social Cyber Contract Theory Model for Understanding National Cyber Strategies a Social Cyber Contract Theory Model for Understanding National Cyber Strategies, Springer, 2017

(5) Raymond/Shahim, Are We Ready to Manage Digital Risks Today and Tomorrow? Are We Ready to Manage Digital Risks Today and Tomorrow?, Journal of Information Security, 2023

(6) Bierens/Nieuwmeijer, Digital Security Risk Management for data centers, International Federation for Information Processing, 2023

(7) Bierens/Shahim, Are We Ready to Manage Digital Risks Today and Tomorrow? Are We Ready to Manage Digital Risks Today and Tomorrow?, Journal of Information Security, 2023