Cyberrisico's rapporteren aan Raden van Bestuur

CISO-uitgave

Controleren, meten, rapporteren, herhalen

Auteurs
Freddy Dezeure
George Webster
Jason Trost
Eireann Leverett
João Pedro Gonçalves
Patrick Mana
Greg McCord
Josh Magri

Reviewers
Lokke Moerel
Alex Iftimie
Chris Deverell
Greg Bell.
Jamie Hutchinson

Datum: 14 maart 2022
Versie: Definitief

Inhoudsopgave

INLEIDING 3

DOEL 4

VERWACHTINGEN VAN HET BESTUUR 4

HET GAAT ALLEMAAL OM RISICO 5

BELANGRIJKE KEUZES TE MAKEN 7

KWANTITATIEVE METRIEK 10

EEN METRIEKMODEL 12

INPUT VERZAMELEN - METEN WAT HET BELANGRIJKST IS 13

GEGEVENSBRONNEN - DE HARDE WAARHEID 20

TRANSFORMEREN - ZIJN ONZE CONTROLES GOED GENOEG? 20

CYBERRISICO'S RAPPORTEREN – BIEDEN VAN REDELIJKE ZEKERHEID 26

COMMUNICATIEKANALEN 28

WEERSTAND OVERWINNEN 29

TOEWIJZING VAN MIDDELEN AAN METRIEK EN RAPPORTAGE 30

BIJLAGE 1: WAAR TE BEGINNEN? 31

BIJLAGE 2: VOORBEELDEN UIT DE GEMEENSCHAP 32

BIJLAGE 3: VOORBEELD VAN EEN VERSLAG 37

Inleiding

Dit document biedt methoden en inspiratie voor Chief Information Security Officers (CISO) om kwantitatieve metrieken voor cyberbeveiliging te ontwerpen en te implementeren om het cyberrisico op bestuursniveau te rapporteren en redelijke zekerheid te verschaffen dat het risico binnen de aanvaarde risicobereidheid ligt.

Ooit kon je je geheimen beschermen door een sleutel in een gesloten deur te draaien. Voor je diepste geheimen heb je misschien een betere deur geïnstalleerd, misschien de muren verbeterd, of een paar bewakers gestationeerd. Wanneer je je geheimen moest verplaatsen, bundelde je ze in een zak en gebruikte je steganografie of cryptografie om het geheim voor nieuwsgierige ogen te verbergen. Dit sprookje was ook waar voor computers, maar die tijd is al lang voorbij. Onze samenleving, onze economie en ons dagelijks leven zijn afhankelijk van de uitwisseling van informatie die door onze onderling gekoppelde systemen stroomt. Het concept van een beschermende omheining behoort tot het verleden.

De moderne economie en haar afhankelijkheid van gegevens hebben onze geheimen steeds waardevoller gemaakt, en dit heeft de aandacht getrokken van de beroepscrimineel, die onze verdediging steeds verder aftast. Onze informatiesystemen vormen een aanzienlijk risico voor zowel overheden, bedrijven als individuen. In 2021 bedroegen de gemiddelde kosten van een datalek bij een doorsnee bedrijf 4 miljoen dollar. Een grote inbreuk kan zelfs oplopen tot meer dan 400 miljoen dollar[1]. De totale kosten voor alle incidenten op het gebied van cyberbeveiliging in 2020 worden geraamd op 1 miljoen dollar, een stijging van meer dan 50% in twee jaar tijd[2].

Het is geen wonder dat cyberbeveiliging voor de meeste organisaties en overheden een kwestie van het allerhoogste belang is, en deze aandacht is terecht. De nieuwe SEC-voorschriften met betrekking tot informatie-verstrekking over cyberbeveiligingsrisico's bevatten bijvoorbeeld bepalingen over het belang van het communiceren van cyberbeveiligingsrisico's aan Raden van Bestuur[3].

Maar het oor te luisteren leggen bij senior stakeholders lost de cyberbeveiligingsproblemen niet op en vermindert het risico niet. Onze bedrijfs- en regeringsleiders zijn slecht toegerust om met cyberbeveiliging om te gaan omdat cyberbeveiliging hun taal niet spreekt. Op zijn beurt is cyberbeveiliging slecht toegerust om met senior stakeholders om te gaan, omdat cyberprofessionals moeite hebben om de effectiviteit van hun programma te meten, het nut ervan te verwoorden of zelfs maar de successen ervan te communiceren. Dit onvermogen om de doeltreffendheid van cyberbeveiligingsmaatregelen te meten en de risicovermindering die zij opleveren aan de hogere belanghebbenden mee te delen, brengt cyberbeveiligingsmedewerkers in een positie waarin zij vechten om budget,

[1] https://www.ibm.com/security/data-breach
[2] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
[3] https://www.mofo.com/resources/insights/220311-sec-proposes-cybersecurity-disclosure-rules.html

terwijl zij niet weten of wat zij doen het risico op verliezen daadwerkelijk vermindert.

Nul risico is onbereikbaar en onrealistisch. Dat is altijd zo geweest. Maar de dynamiek is veranderd. Bovendien gaat de snelheid waarmee het dreigingslandschap voor cyberbeveiliging verandert, ons vermogen te boven om controles aan te passen aan risico's of zelfs maar vast te stellen welke controles van belang zijn voor het beperken van risico's. Een CISO moet het budget voor cyberbeveiliging verantwoorden en uitleggen waarom de gekozen aanpak aansluit bij de algehele risicobereidheid van de organisatie. Dit is een uitdagende taak, maar wel een waarvoor dit document inspiratie en materiaal wil bieden om pragmatische oplossingen te ontwerpen en te implementeren.

Doel

In dit document worden richtlijnen gegeven voor CISO's om cyberrisico's en de context ervan te rapporteren aan hun senior stakeholders, zoals hun Raad van Bestuur. Het beschrijft methoden die CISO's helpen bij cyberrisicomanagement, dit effectief te communiceren en goed toezicht te faciliteren. Hoewel dit niet de focus van dit document is, helpt de inhoud ervan ook bij het rapporteren van cyberrisico's aan andere belanghebbenden, zoals toezichthouders, verzekeraars en klanten.

Wij geloven dat metriek een noodzakelijk onderdeel is van elke succesvolle inspanning. De managementtheorieën van Peter Drucker zijn hiervan een bewijs en hebben het bedrijfsleven daardoor veranderd. Cyberbeveiliging is niet anders. Metrics zijn nodig om het beheer van risico's in organisaties te sturen, om de cyberweerbaarheid in de loop van de tijd te vergroten, en om compliance te tonen aan interne en externe belanghebbenden. U moet echter wel de juiste dingen meten en het probleem holistisch benaderen. Helaas is het meten van cyberbeveiligingsrisico's en het toepassen van een geschikte metriek net zoiets als het vinden van de heilige graal. Er zijn maar weinig goede praktijken voor meetmethoden, de verspreiding ervan in de gemeenschap is zeldzaam, en het meten van risico's in een niet-deterministisch landschap van cyberbeveiligings-dreigingen is een uitdaging.

Dit document is een samenvatting van de bevindingen en beste praktijken van een CISO-werkgroep. De deelnemers verdienen alle lof. Zonder hun inzichten, uitwisseling en interactie zou dit document niet mogelijk zijn geweest. Bij dit document zijn bijlagen gevoegd met voorbeelden uit de gemeenschap. We hopen nog meer bijdragen te genereren, zodat een nieuw corpus van werk en voorbeeldimplementaties ontstaat. Om de interactie en het delen met de gemeenschap te bevorderen, zijn we van plan om in de toekomst meer informatie te verspreiden.

Verwachtingen van het bestuur

Raden van bestuur geven meestal om:

- Strategische positionering en groei van de organisatie;
- Aandeelhouderswaarde, merkbescherming;

- Strategische plannen, toewijzing van middelen, managementcompensatie;
- Toezicht op naleving (overheids- en sectorvoorschriften, ESG);
- Kritieke bedrijfsrisico's - waaronder cyberbeveiliging;
- Vergelijking met sector/concurrenten;
- De fiduciaire aansprakelijkheid van individuele bestuursleden.

Voor de meeste van deze gebieden bestaat er een gevestigde praktijk om bewijsmateriaal te verzamelen en te rapporteren op een manier die nuttig is, met een passende mate van detail en verdeling van verantwoordelijkheid / delegatie.

Wat cyberbeveiliging betreft, is de gangbare praktijk in de sector minder volwassen. Vaak voelen Raden van Bestuur zich onvoldoende competent om cyberrisico's te begrijpen of vinden ze cyber te technisch, keuren ze middelen goed en delegeren ze dit risico.

Raden van bestuur zien vaak niet het voortdurende belang in van cyberbeveiliging en reageren met voorspelbare reacties op cyberverhalen in de media, waarna ze het snel weer vergeten tot het volgende grote cyberincident. Doorgaans wordt cyberbeveiliging pas een probleem als het al te laat is.

Dit wordt soms benadrukt door een ondoorzichtige managementcultuur, waarbij systematisch alles in orde / groen wordt gerapporteerd, terwijl de meeste Raden van Bestuur in werkelijkheid zouden willen horen welke lacunes er zijn en hoe deze kunnen worden verholpen.

In gevallen waarin cyberbeveiligingsrapportage aan het bestuur plaatsvindt, is er een grote verscheidenheid aan methoden, instrumenten en processen in gebruik. Organisaties worstelen met wat ze moeten rapporteren en hoe ze effectieve feedback van het bestuur kunnen krijgen.

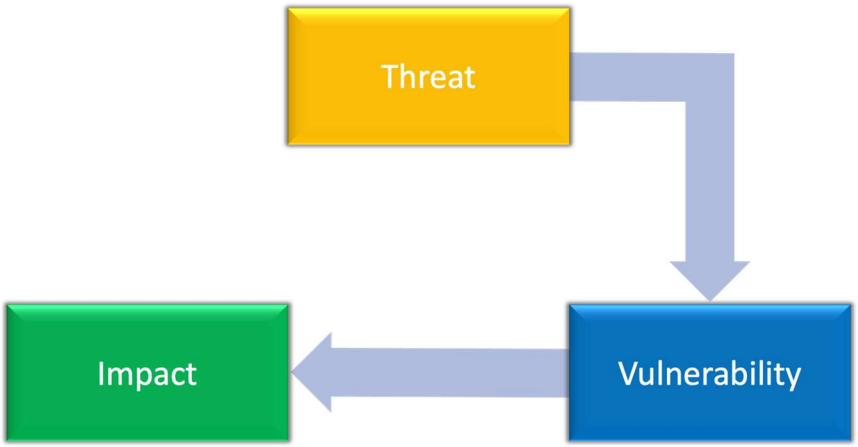
Het gaat allemaal om risico

Onze cyberomgeving dwingt ons keuzes te maken met betrekking tot wat te beschermen en hoe. Perfecte beveiliging is een illusie en de middelen zijn schaars. Beoordelingen en beslissingen over prioriteiten worden vergemakkelijkt en geobjectiveerd door gebruik te maken van de gevestigde praktijken van risicobeoordeling.

Er bestaan verschillende definities van risico, waarbij de nadruk ligt op de kans op een ongewenst resultaat als gevolg van een incident, gebeurtenis of voorval, bepaald door de **waarschijnlijkheid** en de bijbehorende **impact**[4]. Een reëel voorbeeld van risico is de mogelijkheid om te sterven of ernstig ziek te worden als gevolg van een pandemische virusinfectie.

Voor onze bespreking zullen wij het uitgebreide model gebruiken waarin risico is samengesteld uit drie factoren **Dreiging** x **Kwetsbaarheid** x **Impact**. In deze vergelijking wordt de waarschijnlijkheid uitgebreid tot een combinatie van dreiging en kwetsbaarheid, wat in de context van cyberbeveiliging nuttig is. We hebben het niet over toevallige gebeurtenissen.

[4] https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf

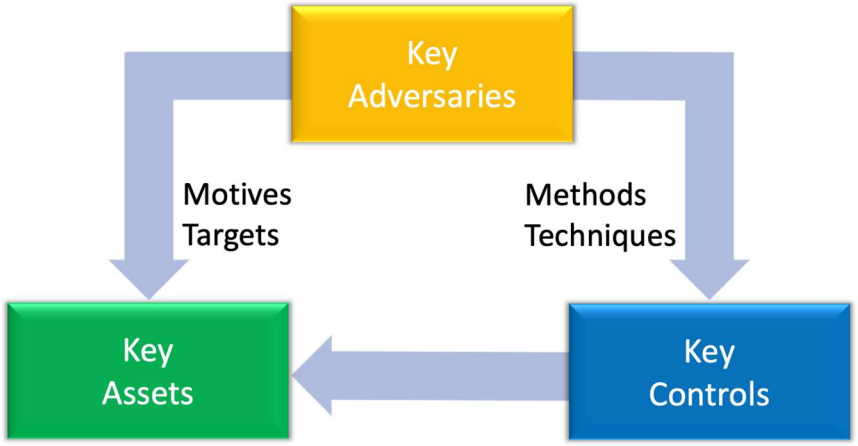


Figuur 1 Risico als een combinatie van dreiging, kwetsbaarheid en impact

Dreiging is meestal extern aan onze organisatie en is nauw verbonden met tegenstanders. Het identificeren van onze belangrijkste tegenstanders en hun motieven is belangrijk voor het stellen van prioriteiten. Wij kunnen huidige dreigingen observeren en toekomstige dreigingen proberen te voorspellen. Gespecialiseerde bedrijven en overheidsdiensten die inlichtingen over dreigingen verschaffen, kunnen helpen te begrijpen welke tegenstanders wij hebben, wat hun motieven zijn, welke instrumenten en methoden zij gebruiken en hoe zij te werk gaan om hun doelen na te streven.

De tweede factor is **kwetsbaarheid**, en dit is de factor waarop wij de meeste invloed kunnen uitoefenen door controles te ontwerpen en uit te voeren. Het identificeren van de belangrijkste controles, het in aanmerking nemen van onze belangrijkste activa en de motivatie en methoden van onze belangrijkste tegenstanders is belangrijk voor het stellen van prioriteiten.

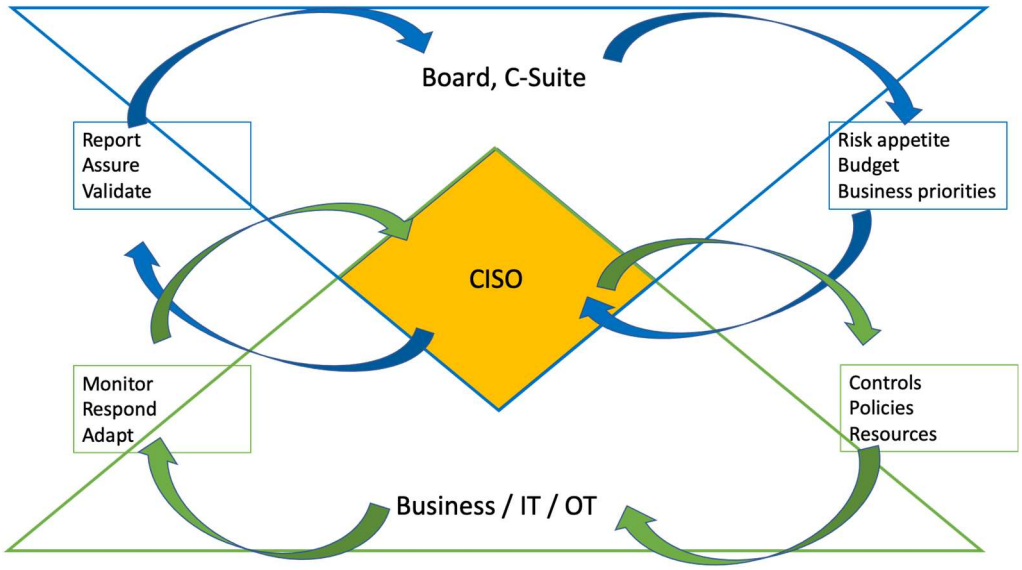
In termen van **impact** kunnen we denken aan diefstal van intellectueel eigendom, lekken van privégegevens, onderbreking van de dienstverlening, persoonlijke schade en reputatieschade. Impact is nauw verbonden met activa. Het identificeren van onze belangrijkste activa is belangrijk voor het stellen van prioriteiten.



Figuur 2 Cyberrisico door tegenstanders die zich richten op bedrijfsmiddelen door kwetsbaarheden uit te buiten

Wij zijn van mening dat we het cyberbeveiligingsprobleem moeten aanpakken als een risicobeheersingsprobleem en dat we op basis van geïnformeerd risicobeheer en risicobeperking voortdurend prioriteiten moeten stellen voor maatregelen. Cyber moet worden geïntegreerd in het algemene beheerssysteem, het moet niet worden beschouwd als iets speciaals/ geïsoleerds, maar als een integrerend deel van de organisatorische activiteiten en processen, met inbegrip van het risicobeheerproces. Dit vergt afstemming van methoden en vocabulaire.

Om de relevante informatiestromen in het huidige document te illustreren, maken wij gebruik van het schema in figuur 3, dat is geïnspireerd op het NIST Cyber Security Framework[5].



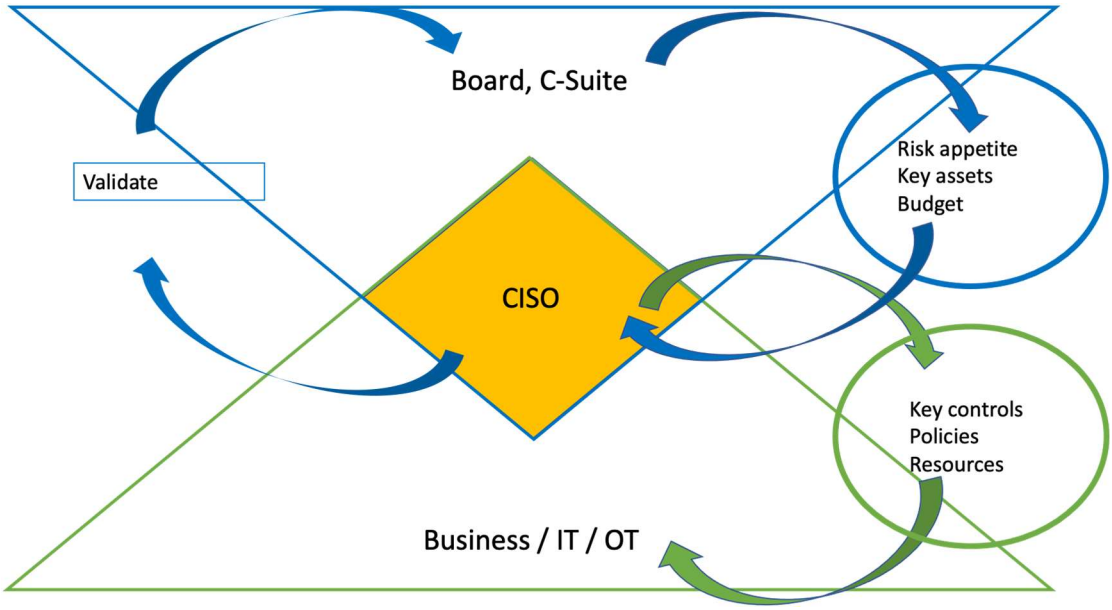
Figuur 3 Informatie- en beslissingsstromen. Geïnspireerd door NIST CSF

We kunnen een hoger, senior uitvoerend deel onderscheiden en een lager uitvoerend/operationeel deel met de CISO in de centrale overlappende zone, die het operationele cyberbeveiligingsniveau verbindt met het strategische niveau.

Belangrijke keuzes te maken

Het is noodzakelijk voor organisaties om fundamentele keuzes te maken voor cyberrisicobeheer. Deze worden geïllustreerd aan de rechterkant van het diagram: wat zijn de belangrijkste activa, wat is de risicobereidheid, en wat zijn de belangrijkste controles/mitigaties die moeten worden ingevoerd? En in verband daarmee, het budget en de toewijzing van middelen aan cyberbeveiligingsmiddelen en -personeel.

[5] https://www.nist.gov/cyberframework



Figuur 4 Te maken keuzes

Het is van cruciaal belang dat deze door de CISO voorgestelde keuzes in de hele organisatie (cyberbeveiliging, risico's, IT/OT, bedrijfsleven) worden goedgekeurd en op elkaar afgestemd, en dat zij op uitvoerend niveau worden begrepen/goedgekeurd en up-to-date gehouden.

Belangrijke activa - kroonjuwelen

In de meeste organisaties is het onbetaalbaar om alle bedrijfsmiddelen te beschermen tegen alle mogelijke cyberdreigingen. Er moeten prioriteiten worden gesteld en middelen worden toegewezen aan de meest relevante dreigingen voor de belangrijkste bedrijfsmiddelen. Het identificeren van deze belangrijkste bedrijfsmiddelen is een essentieel onderdeel van het beheer van bedrijfsrisico's in het algemeen en het beheer van cyberbeveiligingsrisico's in het bijzonder.

Het is een niet-triviale taak, die een functie overschrijdende analyse en beoordeling vereist, waarbij rekening moet worden gehouden met de potentiële gevolgen voor de bedrijfscontinuïteit, de privacy, de regelgeving en de concurrentiepositie op lange termijn (intellectuele eigendom).

Bij het vaststellen (en bijwerken) van de lijst van essentiële bedrijfsmiddelen moet een CISO verder kijken dan IT-bedrijfsmiddelen (datacentra, back-upsystemen, actieve map enz.) en ook relevante informatiebedrijfsmiddelen (opslagplaatsen, intellectuele eigendom), bedrijfs-assets (boekhouding, productiebeheer, logistiek, fysieke toegang) enz. in aanmerking nemen.

Er wordt veel gesproken over het identificeren van de belangrijkste activa of "kroonjuwelen", wat op zich een probabilistische risicobeoordeling is, een uitdrukking van de overtuiging dat een aanvaller meer kans heeft om x te stelen dan y. We zeggen hier probabilistisch (waarschijnlijk), omdat ervan wordt uitgegaan dat we sommige activa minder goed kunnen verdedigen dan andere. Een ander belangrijk element van probabilistisch redeneren is echter het bijwerken van die aannames op basis van actuele cyberdreigingen. Crypto-

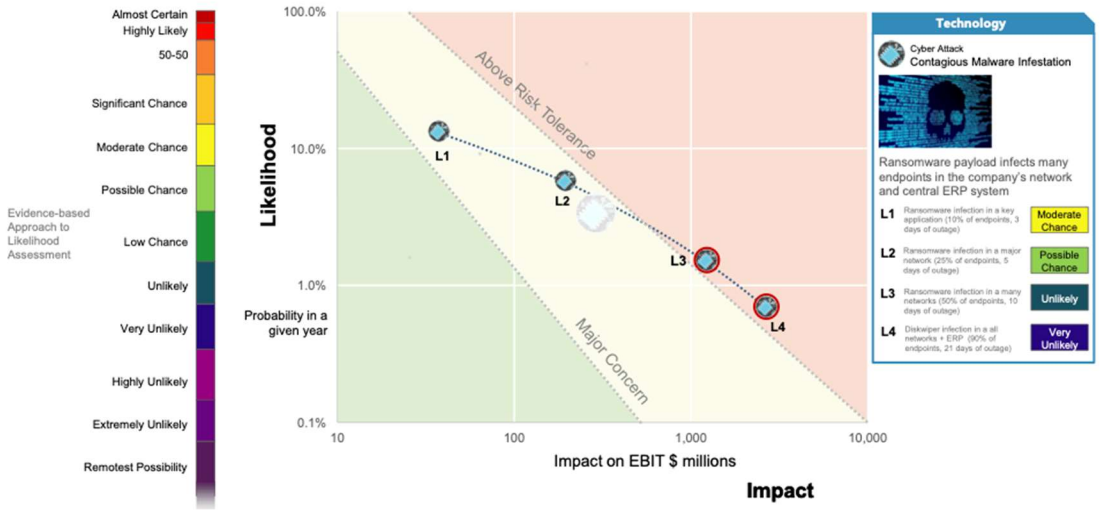
jacking, bijvoorbeeld, geeft er niet om wat uw kroonjuwelen zijn, en vindt het geen probleem om gewoon stil te staan bij minder belangrijke activa.

Het is belangrijk de waarschijnlijkheid van verschillende cyberdreigingen (DDoS, ransomware, gerichte IP-diefstal, opportunistische inbraak, phishing, fraude, malware-infectie - deze lijst is niet uitputtend) te evalueren in relatie tot de bespreking van de belangrijkste activa, het afval van de een is de schat van de ander.

Risicobereidheid

Om risicobeperkende en controlemaatregelen vast te stellen, moet een organisatie op directieniveau bepalen welk controleniveau "goed genoeg" is, of wat een aanvaardbaar risiconiveau is.

Daarbij moet de risicobereidheid op een kwantificeerbare manier worden uitgedrukt, met behulp van een drempelwaarde of een grafische voorstelling van aanvaardbare en niet-aanvaardbare situaties. Sommige organisaties gebruiken monetaire drempels voor risicobereidheid. Voor andere organisaties (vervoersector, ziekenhuizen, enz.) kan de drempel verband houden met het risico op letsel of het verlies van mensenlevens. In sommige gevallen kan de risicobereidheid verband houden met de bedrijfscontinuïteit of de aanvaardbare duur van een onderbreking van de dienstverlening.



Figuur 5 Voorbeeld van het in kaart brengen van risico's, credit Center for Risk Studies, Universiteit van Cambridge

Cyberbeveiligingsraamwerk(en) en essentiële controles

Cyberbeveiligingsraamwerken zijn een hulpmiddel om cyberbeveiligingsrisico's op een samenhangende manier te beheren en om een bedrijfsstrategie voor cyberbeveiliging uit te voeren. Veelgebruikte controleraamwerken zijn ISO/IEC 27001[6], NIST Cyber Security Framework (CSF)[7], het daarvan afgeleide CRI Profile[8], NIST SP 800-53[9] en de CIS Critical Security Controls[10]. Als alternatief,

[6] https://www.iso.org/isoiec-27001-information-security.html
[7] https://www.nist.gov/cyberframework
[8] https://cyberriskinstitute.org/
[9] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[10] https://www.cisecurity.org/controls/cis-controls-list/

of in combinatie, gebruiken veel organisaties ook het dreigingsgerichte MITRE ATT&CK® raamwerk[11]. Hoewel het overweldigend kan zijn om één enkel raamwerk te kiezen, hebben ze allemaal hun specifieke kenmerken, en maakt het niet veel uit welk raamwerk wordt gekozen omdat er koppelingen tussen de raamwerken zijn. Het is echter belangrijk er één te kiezen en daaraan vast te houden, zodat de organisatie de vooruitgang in de tijd kan meten.

Het is voor elke organisatie zeer raadzaam om intern overeenstemming te bereiken over het raamwerk dat moet worden gebruikt om de cyberbeveiligingsstrategie en risicobeperking in te kaderen. Zonder een dergelijke interne afstemming tussen CISO, IT/OT en risicobeheer is het moeilijk om het bestuur bij cyber te betrekken.

Een goed beginpunt voor het vaststellen en monitoren van essentiële controles is het in kaart brengen van de naleving van de basisrichtlijnen inzake cyberbeveiliging van de nationale cyberbeveiligingsautoriteiten. In bijlage 1 hebben wij een selectie van relevante bronnen opgenomen. Er is een grote mate van overlapping tussen deze verschillende reeksen basisrichtlijnen en ze moeten nog worden omgezet naar de specifieke situatie van een organisatie. Zij vormen echter wel een uitstekend, beknopt en praktisch uitgangspunt.

Enkele belangrijke controles die er altijd in zitten:

- K1: Een actuele inventaris bijhouden van alle (essentiële) activa en afhankelijkheden;
- K2: Betrouwbare, geldige, veilige en beveiligde back-ups maken van belangrijke activa;
- K3: Waar mogelijk afdwingen van multi-factor authenticatie;
- K4: Beperken van de toegangsrechten van gebruikers tot het strikt noodzakelijke;
- K5: Identificeren en tijdig patchen van belangrijke kwetsbaarheden;
- K6 Verzamelen en analyseren van logs van alle (belangrijke) activa;
- K7: Segmenteren van het netwerk om belangrijke activa te beschermen;
- K8: Verharden van systemen die op internet gericht zijn;
- K9: Een incidentenrespons- en herstelproces implementeren;
- K10: Bewustmaken van de gebruikers (met inbegrip van de leden van de Raad van Bestuur).

Wij zullen in de onderstaande voorbeelden van metriek naar deze belangrijkste controle-identificatoren verwijzen.

Kwantitatieve metriek

Het is zinvol om de selectie van een raamwerkprofiel te combineren met de definitie van kwantitatieve metrieken (KPI's, KRI's, KCI's, OKR [12]) met doelstellingen/resultaten en deze te koppelen aan de relevante processen/ systemen en proceseigenaars. Deze metrieken kunnen in de loop van de tijd worden afgemeten aan de aanvaarde doelstellingen, worden vergeleken binnen

[11] https://attack.mitre.org/
[12] Doelstellingen en belangrijkste resultaten, High Output Management, Andrew S. Grove.

het bedrijf en worden vergeleken met soortgelijke bedrijven. Enkele goede praktijken in de sector tonen het potentieel van deze aanpak aan:

- CIS-controlemaatregelen en metrieken[13];
- EPRI Cyber Security Metrics for the Electric Sector[14];
- De Cyber Resilience Metrics van de Nederlandse betalingsvereniging[15];
- De Duitse automobielsector KPI's gekoppeld aan ISO27001[16];
- Prestatie meetgids van NIST[17].

De meeste raamwerken gaan ervan uit dat organisaties die ze toepassen zelfbeoordeling toepassen, eventueel in combinatie met een of andere vorm van externe toetsing door een certificatie- of auditinstantie. Ook zelfbeoordeling is in overeenstemming met de standaardpraktijken in bedrijfsrisicobeheer.

Monitoring door zelfbeoordeling heeft fundamentele nadelen om de status van de maatregelen ter beperking van cyberrisico's en de doeltreffendheid ervan te bepalen, waaronder:

- Het is subjectief (geen scheiding van plichten, zelfde niveau van kennis);
- Het is niet gedetailleerd genoeg;
- Het is tijdrovend;
- Het is in tijd losgekoppeld van de gebeurtenissen;
- Het kan niet worden gebruikt voor alarmering/escalatie/reactie;
- Er kan een onafhankelijke accountantscontrole nodig zijn om door regelgevers aanvaard te worden;
- Het kan beperkt blijven tot invoeringsindicatoren (wat is er uitgevoerd?).

Door machines gegenereerde gegevens kunnen een zeer nuttige aanvulling vormen op zelfevaluatie of deze zelfs grotendeels vervangen. Zij kunnen de rapportage over cyberbeveiligingsrisico's objectief, herhaalbaar en geautomatiseerd maken. Het bepalen van de bronnen van door machines gegenereerde gegevens en van de analyses die nodig zijn voor de metriek is een belangrijke stap in het proces van het ontwerpen en implementeren van een samenhangende, alomvattende en doeltreffende reeks van metriek.

Het grootste gevaar van meetmethoden voor cyberrisico's is dat ze een afspiegeling gaan vormen van verricht werk of geleverde inspanning, in plaats van risicobeperking. Een Raad van Bestuur of een uitvoerend team moet zich krachtig verzetten tegen het opnemen van dergelijke metrieken. Dat is een operationele kwestie, geen risicokwestie. Met andere woorden, vermijd statistieken over het aantal incidenten waaraan is gewerkt, of malware die in quarantaine is geplaatst. Dit zijn fantastische operationele statistieken, maar ze vertellen de Raad van Bestuur niet of het geld dat ze hebben uitgegeven om het risico te verminderen, effectief is. Een eenvoudig hulpmiddel is dat een risicometriek meestal de vorm heeft van een verhouding of ratio, zoals

[13] https://www.cisecurity.org/insights/white-papers/cis-controls-v7-measures-metrics
[14] https://www.epri.com/research/products/000000003002010426
[15] https://www.betaalvereniging.nl/wp-content/uploads/Library-of-Cyber-Resilience-Metrics-Shared-Research-Program-Cybersecurity.pdf
[16] https://www.vda.de/vda/en/News/publikationen/publication/vda-isa-catalogue-version-5.0.4
[17] https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft

ongevallen per 1000 gereden kilometers. Als er geen verhouding in een metriek staat, graaf dan wat dieper op de manier waarop de risicovariantie wordt gemeten.

Ook is het soms goed dat een metriek een verhoogd risico laat zien. Systemen voor vroegtijdige waarschuwing zijn een teken van een gezond risicoteam, en cyberrisico is dynamisch. Straf metrieken of teams die een verhoogd risico aangeven daarom niet af, ze kunnen een zeer tijdige boodschap aan u overbrengen.

Bij de vraag wat een goede metriek is, komen een aantal trefwoorden in gedachten:

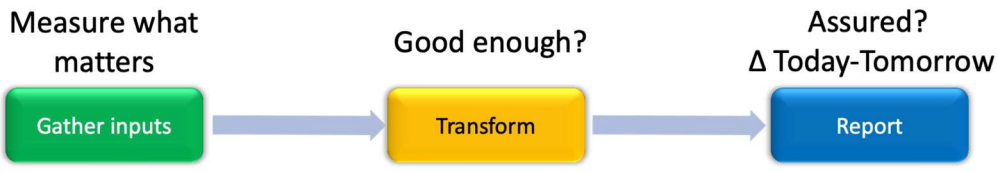
- Objectief
- Onveranderlijk
- Herhaalbaar
- Doorlopend
- Relevant
- Doeltreffend
- Geïnformeerd
- Geäccepteerd
- Uitvoerbaar

Een metriekmodel

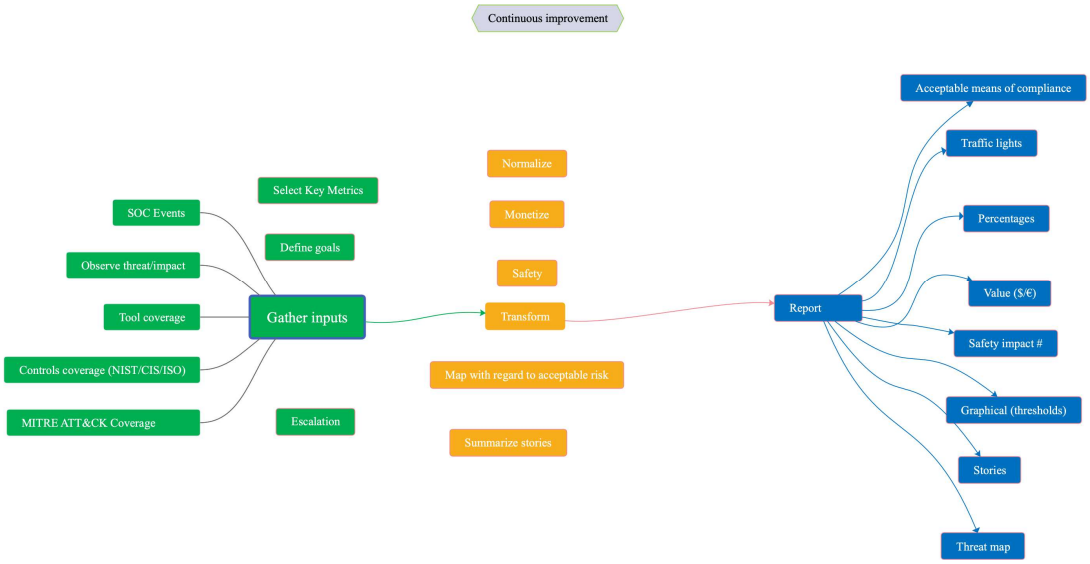
Wij stellen een metriekmodel voor met de volgende drie stappen:

1. Verzamelen van relevant cyberbewijsmateriaal;
2. Het bewijs omzetten in bedrijfsrisico[18];
3. Verslag uitbrengen aan de Raad van Bestuur, redelijke zekerheid verschaffen en lacunes aan het licht brengen.

In dit model wordt elke stap gedeconstrueerd in bouwstenen die wij hieronder zullen illustreren en becommentariëren, en waarvan voorbeelden uit de gemeenschap zijn opgenomen in bijlage 2. Het doel is inspiratie en inzichten te bieden voor organisatiespecifieke oplossingen, eerder dan te concluderen dat wij een perfecte oplossing voorstellen voor de uitdaging van het meten en rapporteren van cyberrisico's.



[18] Ondernemingsrisico is de blootstelling van een organisatie aan factoren die haar financiële doelstellingen zullen verlagen of tot mislukking zullen leiden. Een bedrijfsrisico kan van velerlei aard zijn, zoals strategisch, operationeel, reputatie, compliance of financieel.

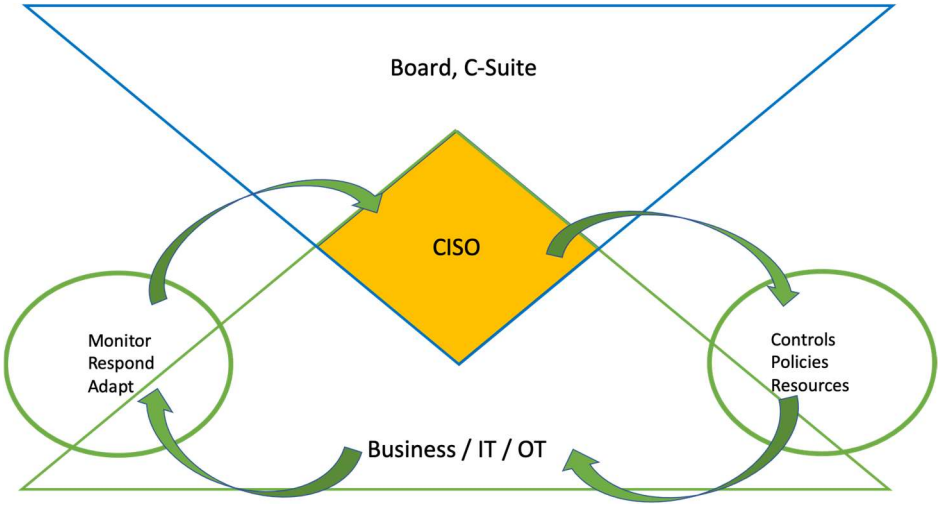


Figuur 6 Metriekmodel

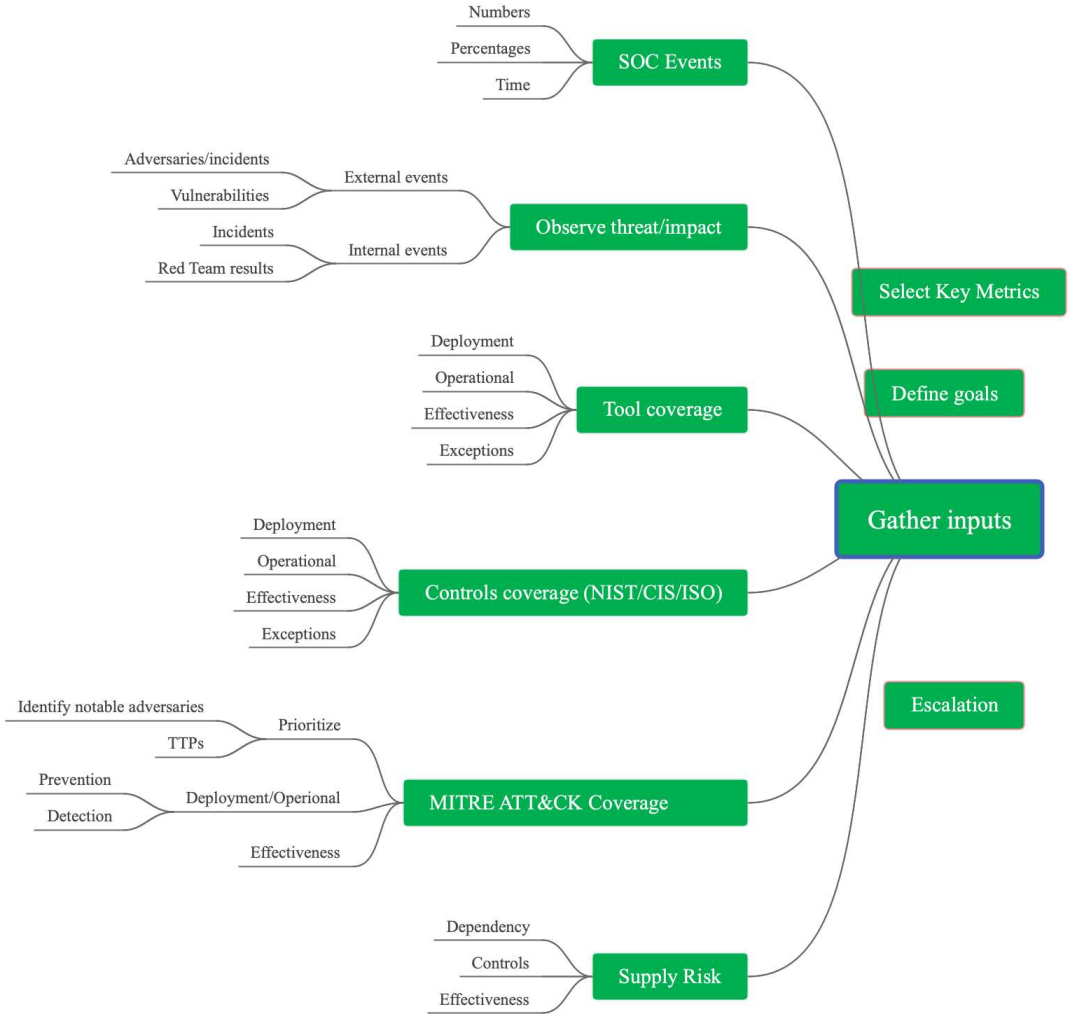
Verbeteringslussen (lokale en algemene) moeten worden opgenomen in het metriekmodel en de desbetreffende processen, waarbij het wordt aangepast aan veranderingen in de verwachtingen van de belanghebbenden en in de risicopositie (dreigingslandschap, kwetsbaarheden, afhankelijkheden). Inzichten en methoden die uit de gemeenschap naar voren komen, leiden ook tot verbeteringen.

Input verzamelen - meten wat het belangrijkst is

Aan de inputzijde van het Metriekmodel vinden we technische metrieken, die (een subset van) de metrieken moeten zijn die door het bedrijf/operations worden gebruikt om operationele cyberrisicobeperking te implementeren en te monitoren. In Figuur 7 vinden we deze technische metrieken linksonder in het diagram.



Figuur 7 Technische metriek - inputs



Figuur 8 Verzamelen van inputs - bouwstenen

Er kunnen verschillende families van operationele kengetallen worden onderscheiden, die worden gegroepeerd naar aard (**gericht op controle**, **dreiging**, **instrumenten** en **gebeurtenissen**).

Gericht op controle

In deze categorie vinden we metrieken die de organisatie vaststelt om de afstemming op een reeks essentiële controles te meten. Deze zijn gerelateerd aan een controleraamwerk (NIST CSF, ISO, CIS, enz.).

De op controle gerichte metriek zou kunnen omvatten:

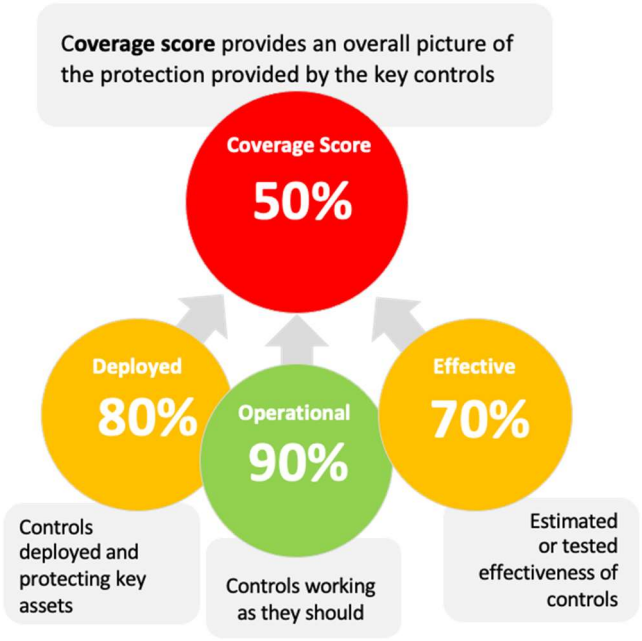
- Dekking van een controle - voor alle activa of een geselecteerde groep van (belangrijke) activa;
- Effectiviteit van een controle;
- Gegevensbron en updatefrequentie;
- Drempelniveau.

Een (meer gedetailleerde) variant van deze controlegerichte benadering splitst de dekking van een controle op in drie componenten: ingezet, operationeel en doeltreffend. Het is belangrijk op te merken dat deze metingen continu moeten zijn, omdat het dreigingslandschap en de mogelijkheden voor de controle om

risico's te beheersen in de loop van de tijd zullen verschuiven. Deze drie controles worden als volgt gedefinieerd:

- Ingezet - de controle wordt ingezet op de plek waar het moet zijn;
- Operationeel – de controle functioneert zoals ontworpen;
- Doeltreffend - de controle is doeltreffend, een metriek ("bewijs") om aan te tonen of een bepaalde controle over een bepaalde periode bijdraagt tot de beperking van het risico.

Op elk van deze drie gebieden wordt een score vastgesteld door bewijsmateriaal te verzamelen. Een gecombineerde score van de drie gebieden levert een "Dekkingsscore" op.



Figuur 9 Voorbeeld van een op controle gerichte metriek bij een pandemische infectie

Een real-life voorbeeld van dit concept is te vinden bij pandemische infecties, waarbij een vaccin een van de mogelijke belangrijkste controlemiddelen is;

- De inzet zou het gevaccineerde deel van de bevolking zijn (in dit voorbeeld 80%);
- Indien het vaccin pas na een bepaalde periode een immuunrespons genereert, leidt dit tot een verschil in het aandeel van de ingezette vaccins dat operationeel is (in dit geval 90%);
- Een vaccin is slechts tot op zekere hoogte werkzaam (in dit geval 70%);
- In dit geval is de totale dekkingsgraad dus 50% (een combinatie van de drie factoren).

$$\eta = \frac{70}{100} \times \left(\frac{90}{100} \times 80\right)$$
$$\eta = 50{,}4$$

De doeltreffendheid van de controles kan worden getest op afzonderlijke controles (pentest) of op alle ingezette controles (Red Teaming). In het laatste geval kan het resultaat worden gebruikt om het algemene niveau van cyberrisicobeperking in te schatten.

Een op controles gerichte aanpak zal meestal worden aangetroffen in sterk gereguleerde omgevingen. Van overheidsdiensten in de VS wordt bijvoorbeeld verwacht dat zij NIST 800-53 implementeren, dat ongeveer 1000 controles en controleverbeteringen omvat.

Maar zelfs in gereglementeerde omgevingen met verplichte controles is het zinvol de essentiële controles te identificeren die het meest van belang zijn voor de beperking van het huidige cyberrisico. De selectie van essentiële controles kan worden bevorderd door inzicht te krijgen in de belangrijkste dreigingen (motieven en technieken) en de belangrijkste activa die het doel zijn.

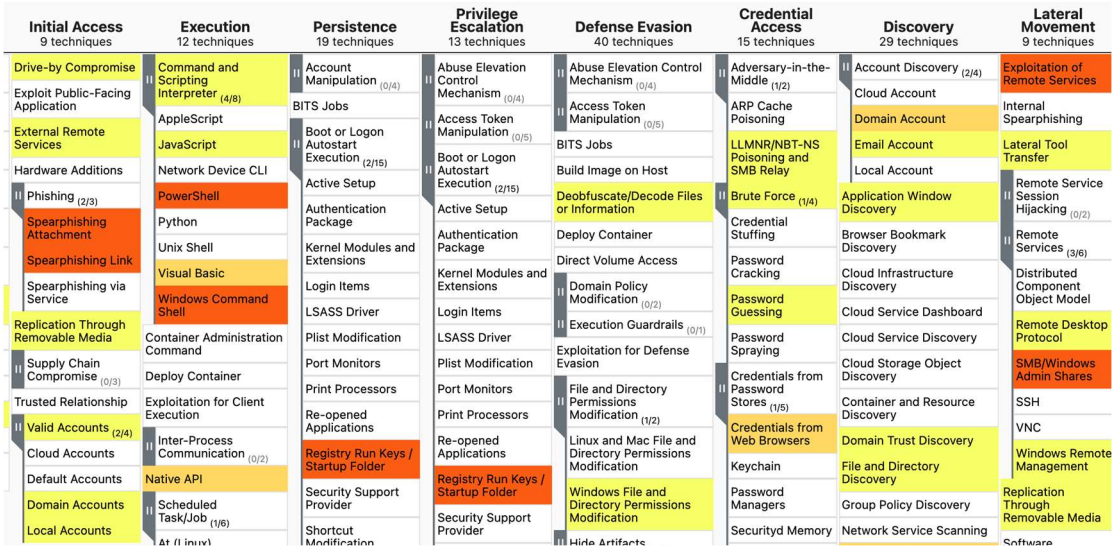
Enkele voorbeelden van op controle gerichte metriek

- K1: Percentage geïnventariseerde (belangrijke) activa (eindpunten, netwerk, servers);
- K1: Onversleutelde databanken waarin persoonlijk identificeerbare informatie wordt opgeslagen;
- K2: Percentage belangrijke activa dat voldoet aan het back-upbeleid;
- K4: Percentage eindpunten zonder lokale beheerdersrechten;
- K4: Percentage eindpunten waar witte lijsten worden geïmplementeerd;
- K4: Percentage bevoorrechte rekeningen dat wordt beheerd door een oplossing voor toegangscontrole;
- K8: Percentage (belangrijke) activa die naar het internet zijn gericht, dat wekelijks op kwetsbaarheden en verkeerde configuratie wordt gescand;
- K9: Percentage kritieke toepassingen zonder bedrijfsimpact analyse;
- K10: Percentage van het personeel dat in het afgelopen jaar een cyberbeveiligingsopleiding heeft gevolgd (inclusief bestuursleden);
- de doeltreffendheid van essentiële controles die door het Red Team of geautomatiseerde tests zijn vastgesteld.

Gericht op dreiging

In deze categorie vinden we metrieken waarin de organisatie haar belangrijkste tegenstanders identificeert en de TTP's (Techniques, Tactics, Procedures) bijhoudt waarvan bekend is dat ze worden ingezet met behulp van het MITRE ATT&CK® Framework. Mitigerende maatregelen worden tegen deze technieken op een vergelijkbare manier in kaart gebracht als bij de controlegerichte aanpak. Deze kennis moet up-to-date worden gehouden met de meest recente informatie over bekende tegenstanders en relevante incidenten.

In de onderstaande figuur is het gebruik van technieken door verschillende relevante groepen tegenstanders in kleur aangegeven, van geel (minder vaak voorkomend) tot rood (technieken gebruikt door alle relevante tegenstanders).



Figuur 10 Voorbeeld van het gebruik van een heatmap om de prevalentie van technieken aan te tonen

Een dreigings- en een controlegerichte aanpak kunnen worden gecombineerd door gebruik te maken van koppelingen tussen controle- en dreigingsraamwerken[19] om relevante dreigingen en risicobeperkende controles te identificeren en om te zetten in belangrijke statistieken.

Enkele voorbeelden van op dreigingen gerichte metriek:

- Percentage van de mitigatietechnieken waarvan bekend is dat ze door bekende groepen tegenstanders worden gebruikt;
- Percentage van de dekking van belangrijke inperkingen door een actief testprogramma (geautomatiseerd of Red Team);
- Percentage van de dekking van opmerkelijke tegenstanders en hun technieken met SOC-playbooks en jachtprogramma's.

Gericht op instrumenten

In deze categorie vinden we metrieken waarin de organisatie zich richt op de inzet van specifieke cyberbeveiligingstools (EDR, perimeter defenses, MFA, etc.) om risicobeperking te bereiken. De gegevensverzameling over de inzet van tools is rechttoe rechtaan en het in kaart brengen van de effectiviteit van elke tool tegen bekende dreigingen is ook goed gedocumenteerd.

Er zou gebruik kunnen worden gemaakt van soortgelijke beginselen als in de controlegerichte aanpak, met gebruikmaking van dekking/effectiviteit of inzetbaar/operationeel/actiegericht. Een op instrumenten gerichte aanpak zou een opstap kunnen zijn naar een meer samenhangende en volledige aanpak op basis van een raamwerk (controlegericht of dreigingsgericht).

Enkele voorbeelden van instrumentgerichte metrieken zijn:

- K3: Percentage van implementatie van multifactorauthenticatie (MFA);
- K6: Percentage systemen met een volledig pakket beveiligings-instrumenten en -beleid (EDR, logging, goudstandaardsoftware en -configuratie, beleid, enz;)
- K6: Percentage (belangrijke) activa met logboekzichtbaarheid;

[19] https://github.com/center-for-threat-informed-defense/attack-control-framework-mappings

- K8: Percentage activa dat gedwongen wordt via een proxy verbinding te maken met het internet;
- Percentage activa dat onder geautomatiseerde controles en herstelmaatregelen valt.

Gericht op gebeurtenissen

Veel organisaties verzamelen gegevens over cyberbeveiligingsgebeurtenissen (#alerts, #incidents, #false positives, #vulnerabilities, enz.) Dergelijke statistieken kunnen waardevolle input leveren voor het beheer van cyberbeveiligingsrisico's, maar ze moeten wel worden geïnterpreteerd. Is het goed of slecht als er meer kwetsbaarheden worden gevonden of meer incidenten plaatsvinden? Zijn de opsporingsmethoden verbeterd, of zijn de systemen verslechterd?

Enkele voorbeelden van gebeurtenisgerichte metrieken zijn de:

- K1: Aantal geïmplementeerde beveiligingssystemen afgezet tegen de dekking van de activa;
- K4: Aantal problemen dat is aangetroffen bij het monitoren/screenen van geprivilegieerde activa;
- K5: Percentage systemen dat binnen de SLA is gepatcht;
- K6: Aantal fout-positieven in het Security Operation Center;
- K8: Aantal gevonden (extern gerichte) verweesde activa;
- K9: Aantal kritieke incidenten/gemiddelde tijd tot ontdekking/opsluiting;
- K9: Percentage kritieke en zeer ernstige beveiligingswaarschuwingen dat binnen de SLA wordt beoordeeld;
- K10: Aantal bedrijfsreferenties in het wild (Account Take Over);
- Jaarlijkse kosten van cyberincidenten;
- Aantal openstaande beveiligings- en privacykwesties met een hoog risico die de SLA overschrijden en waarvoor geen herstelplan is opgesteld.

Tijdsgegevens over incidenten en kwetsbaarheden kunnen nuttige informatie opleveren over de prestaties van de cyberbeveiligingsorganisatie en -systemen. Op dit gebied is goede vooruitgang geboekt in de First Metrics SIG[20].

Risico in de toeleveringsketen

Steeds meer bedrijven ondervinden de gevolgen van cyberincidenten bij hun leveranciers, hetzij direct via netwerkverbindingen of producten, hetzij indirect via onderbrekingen van de toeleveringsketen die van invloed zijn op de bedrijfscontinuïteit. Het in kaart brengen van de afhankelijkheid van leveranciers, het verkrijgen van inzicht in hun cyberbeveiligingspositie en het implementeren van passende controles wordt een integraal onderdeel van cyberrisicobeheer en moet daarom ook in de metriek worden opgenomen.

Het toezicht op het cyberrisico van leveranciers kan worden toevertrouwd aan gespecialiseerde bedrijven en mitigaties kunnen, tot op zekere hoogte, de vorm aannemen van contractuele voorwaarden en verzekeringsdekking. Er moet echter een duidelijk beeld van de afhankelijkheden en scenario's voor detectie

[20] https://www.first.org/global/sigs/metrics/events

en respons worden opgesteld. Aanvullende richtlijnen zijn te vinden in de NIST-publicatie Key Practices in Cyber Supply Chain Risk Management[21].

Enkele voorbeelden van metrieken in de toeleveringsketen zijn:

- Percentage essentiële verkopers/leveranciers waarvoor een inventaris van de activa, de afhankelijkheid, de risicobeoordeling en de risicobeperking is uitgevoerd;
- Percentage essentiële verkopers/leveranciers met veiligheidsbijlagen;
- Percentage essentiële verkopers die aan een audit zijn onderworpen;
- Aantal essentiële verkopers/leveranciers met openstaande auditbevindingen inzake beveiliging en privacy met een hoog risico, zonder gedocumenteerd risicobeheersplan.

Effect waarnemen - Stories

Veel organisaties documenteren relevante incidenten (intern, met gevolgen voor collega's, sector of regio) met behulp van verhalen in "stories". Dit soort anekdotisch bewijs is zeer aantrekkelijk voor niet-technische C-Suite en bestuursleden omdat ze een voorbeeld zijn van wat er kan gebeuren (of is gebeurd) in de organisatie. Ze stellen de CISO ook in staat de aandacht te vestigen op trends in frequentie, impact en methoden in het dreigingslandschap, en ondersteunen de prioritering van actie in termen van controles en toewijzing van middelen.

Kies de essentiële criteria en doelstellingen zorgvuldig

Men moet de belangrijkste metrieken zorgvuldig kiezen, want de selectie en rapportage van metrieken stuurt een organisatie. De keuze van metrieken geeft aan wat de leiding het belangrijkst vindt en de mensen zullen zich daarop afstemmen. Het meten van de verkeerde dingen zal op zijn beurt de gewenste cyberbeveiligingsdoelstellingen tegenwerken en leiden tot verkeerde veronderstellingen over de risicopositie. Bovendien kan het zijn dat het bestuur zijn aandacht wil richten op het verbeteren van de indicatoren in plaats van op de onderliggende houding tegenover cyberrisico.

De belangrijkste metrieken moeten in de loop van de tijd evolueren met de toenemende maturiteit van de organisatie, veranderingen in de regelgeving, bedrijfsdoelstellingen en veranderingen in het landschap van cyberdreigingen. Voor de geselecteerde metrieken moeten doelstellingen worden vastgesteld en overeengekomen binnen de organisatie. Deze moeten zinvol zijn in termen van risicobeperking en risicobereidheid. Ze kunnen een tijdscomponent bevatten voor het geval de organisatie in de loop van de tijd een ontwikkeling in maturiteit wil opnemen.

Escalatieproces

Aanbevolen wordt een proces/drempel te definiëren waarbij afwijkingen/ontwikkelingen tussen twee rapportageperioden in een noodsituatie aan het leidinggevend niveau worden gemeld. Hierbij kan uiteraard worden gedacht aan essentiële incidenten/overtredingen, maar de trigger kan ook komen van essentiële kwetsbaarheden of ontwikkelingen in het

[21] https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

dreigingslandschap die onmiddellijke aandacht van het leidinggevende niveau vereisen. Een recent voorbeeld van zo'n geval was de Log4j-kwetsbaarheid en de afhankelijkheid van veel organisaties van producten die dit softwareonderdeel gebruiken.

Er zou ook een escalatieproces kunnen worden ontworpen voor metrieken die alleen op het niveau van de Raad van Bestuur worden gerapporteerd indien een vooraf bepaalde drempel wordt overschreden. Dit zou de overvloed aan irrelevante informatie die aan de Raad van Bestuur wordt verstrekt, kunnen verminderen.

Gegevensbronnen - de harde waarheid

Gegevens verzameld van binnenuit

Technische metriek moet bestaan uit gegevens die automatisch worden verzameld uit de broninfrastructuur, met minimale menselijke tussenkomst, waaronder:

- Systemen voor activabeheer en opsporing (volledigheid, kriticiteit);
- Systemen en consoles voor het beheer van tools (inzet);
- Logs en SIEMs (inzet en werking);
- Scannen van software (versies, kwetsbaarheden, configuraties, beleidslijnen);
- Identiteits-, privilege- en toegangsbeheer (controles en beleids-maatregelen);
- Netwerksporen (volledigheid, controles).

De meeste van deze gegevens hebben betrekking op de invoering van controles, instrumenten en beleidsmaatregelen. De doeltreffendheid van de risicobeperking kan op theoretische wijze worden afgeleid op basis van de verwachte beperking door een specifieke controle.

Bij het testen verzamelde gegevens

Extra inzicht in de uitvoering (invoering en werking), en met name in de doeltreffendheid ervan, kan worden verkregen door de controles te testen. Dergelijke tests van controles kunnen doorgaans worden uitgevoerd door een handmatige pentest/Red Teaming of geautomatiseerde test waarbij gebruik wordt gemaakt van specifieke instrumenten of bug bounty-programma's. Deze categorie van meetgegevens zal vooral zinvol zijn in een organisatie die reeds beschikt over een volwassen beheerssysteem voor informatiebeveiliging ([22]).

Gegevens verzameld van buiten de infrastructuur

Sommige gegevens over bevestigde infecties en kwetsbaarheden kunnen van buiten de infrastructuur van een organisatie worden verzameld door netwerksporen te scannen of te observeren die naar bekende kwaadaardige infrastructuur verwijzen.

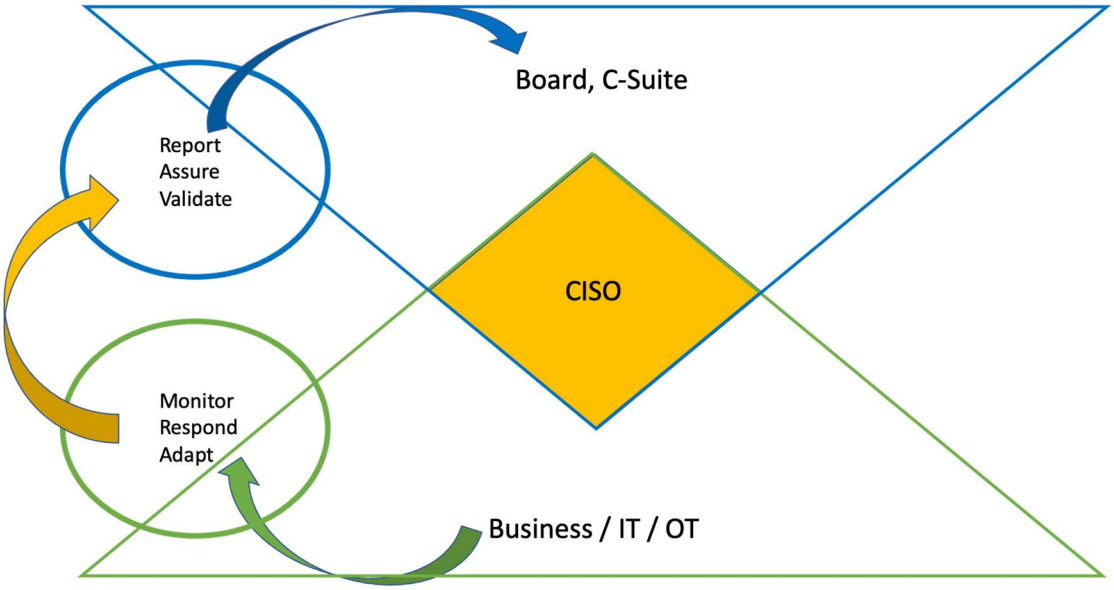
Transformeren - Zijn onze controles goed genoeg?

Terwijl operationele kengetallen belangrijk zijn voor de CISO om de uitvoering van de cyberbeveiligingsstrategie te sturen en de controles over de hele linie

[22] https://www.iso.org/isoiec-27001-information-security.html

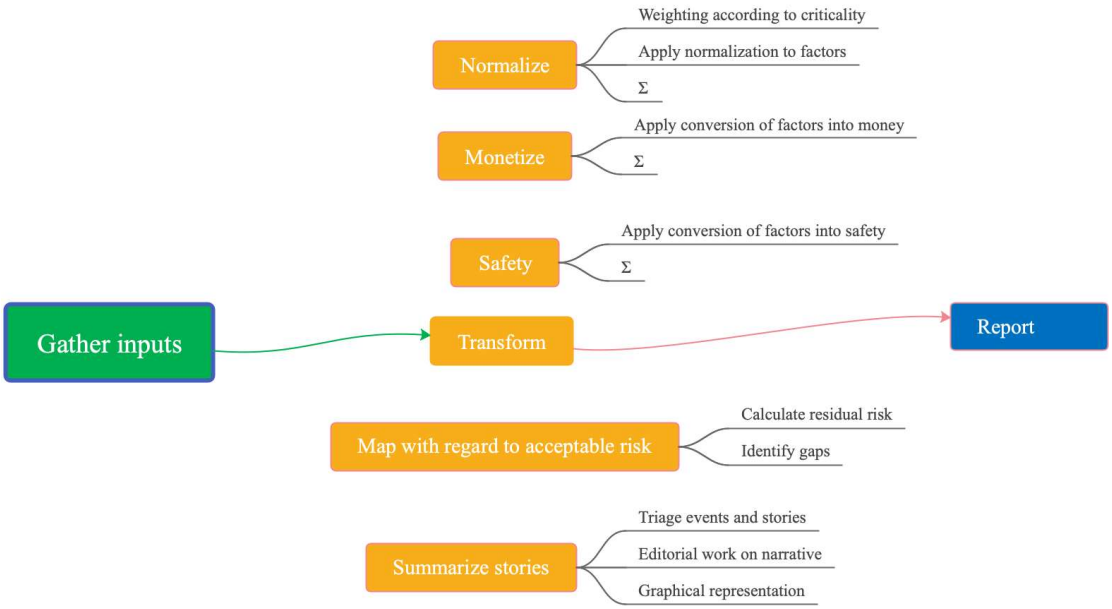
op een gedetailleerde manier te monitoren, zijn deze niet geschikt voor rapportage aan de leiding, het bestuur en andere strategische belanghebbenden. Ze zouden worden ervaren als overweldigend, cryptisch en losgekoppeld van het bedrijfsrisico.

Om ervoor te zorgen dat de cijfers over cyberrisico's weerklank vinden op bestuursniveau, moeten ze worden omgezet in zinvolle bedrijfsrapportage (geld, veiligheid, merkwaarde, enz.) en worden vergeleken met de risicobereidheid. Is onze risicobeperking goed genoeg? Kunnen we redelijke zekerheid bieden? Kan de Raad van Bestuur onze aannames en uitgangspunten valideren? In de volgende figuur tonen wij de informatiestroom van technische/operationele metingen naar metingen voor de Raad van Bestuur.



Figuur 11 Technische metriek omzetten in strategische metriek

Ook hier onderscheiden we een aantal bouwstenen in de Transform-stap. Deze zetten operationele kengetallen om in waarden die kunnen worden vergeleken met aanvaardbaar risico, kunnen worden geïntegreerd in het bedrijfsrisico, en kunnen worden gerapporteerd aan de Raad van Bestuur.



Figuur 12 Transformeren - bouwstenen

Normaliseren

In elke organisatie kan er een groot aantal metrieken zijn om de stand van de controles en de prestaties van de organisatie te beschrijven. Dit kan een negatief effect hebben wanneer belanghebbenden overweldigd worden door details. Een ander probleem is dat de waarde van één meting op zich betekenisloos kan zijn wanneer deze onafhankelijk wordt bekeken, maar van cruciaal belang wordt wanneer deze over een reeks metingen wordt bekeken.

Als u bijvoorbeeld de gezondheid van uw endpoints tegen malware wilt begrijpen, is het niet voldoende om alleen de inzet van antivirussoftware op een bepaald besturingssysteem te bekijken. U zou de verschillende metingen over de verschillende besturingssystemen moeten bekijken. Bovendien zal antivirussoftware alleen niet het antwoord geven. U zult de metingen van andere hulpmiddelen moeten bekijken, zoals Event Detection Response (EDR).

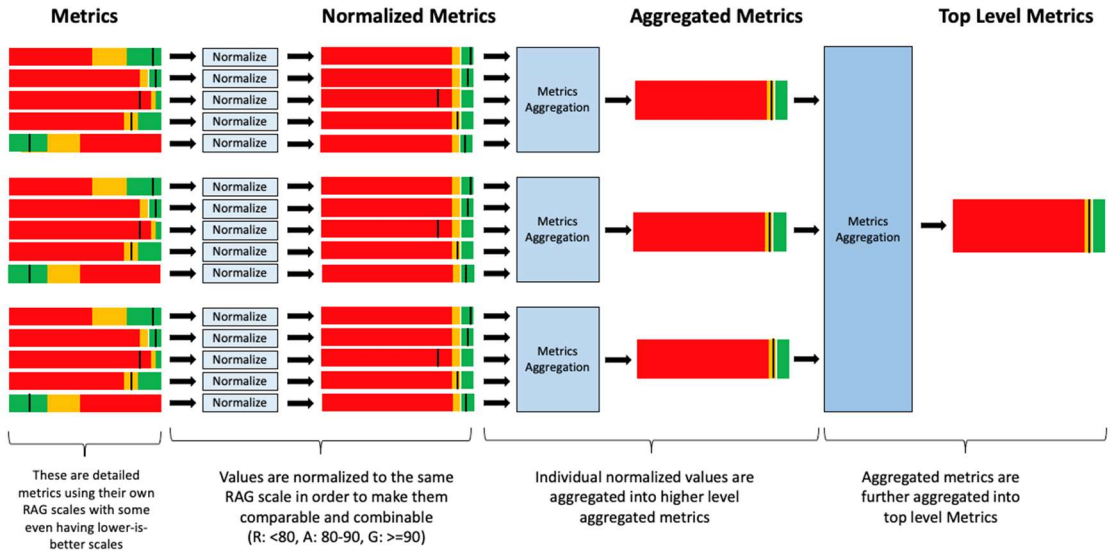
Om deze uitdaging het hoofd te bieden, kunnen reeksen metrieken, ook al zijn zij verschillend van aard, worden genormaliseerd of geharmoniseerd om een meer holistisch beeld te krijgen. Een dergelijke normalisatie moet een vereenvoudigd beeld opleveren van een groot aantal verschillende controledomeinen en tegelijk inzicht verschaffen in belangrijke leemten die door consolidatie ondoorzichtiger zouden kunnen worden.

Normalisatie zou ook een wegingscomponent kunnen omvatten om rekening te houden met verschillende niveaus van kriticiteit van activa. Zo zou bijvoorbeeld de dekking van controles op zeer essentiële activa als belangrijker kunnen worden beoordeeld dan op andere activa. In een geconsolideerde metriek zou dit kunnen worden verwerkt door middel van weging.

Door gebruik te maken van een normalisatie met drie schalen (rood/amber/groen) min/max, is het mogelijk de metriek aan een nieuwe schaal aan te passen, terwijl de exacte verhouding binnen elke schaal

behouden blijft (d.w.z. een input-metriek die bovenaan in rood staat, blijft bovenaan in rood staan, ook al kan de numerieke waarde veranderen).

In deze grafiek worden verschillende metrieken op laag niveau genormaliseerd tot een gemeenschappelijke schaal. Eenmaal genormaliseerd op een gemeenschappelijke schaal, kunnen deze metingen op zinvolle wijze worden geaggregeerd of gecombineerd en kunnen deze aggregaties worden gecascadeerd om slechts een paar samengevatte metrieken op topniveau te verkrijgen.



Figuur 13 Drielagige (rood/amber/groen) min/max normalisatie van de schaling

Monetariseren (value at risk)

In organisaties wordt de risicobereidheid uitgedrukt in monetaire termen. Als zodanig is het noodzakelijk te trachten de metriek om te zetten zodat ook de voornaamste belanghebbenden de stof begrijpen en er binnen de normale bedrijfsprocessen kan worden gewerkt. Dit is met name van belang wanneer om financiering wordt gevraagd. Als cyberbeveiliging bijvoorbeeld 10 miljoen dollar nodig heeft om een nieuw EDR-systeem te implementeren, is het een sterke rechtvaardiging om aan te geven dat het huidige risico voor de organisatie met 12 miljoen dollar zal afnemen en het bedrijf weer binnen de risicobereidheid zal brengen.

In deze stap worden individuele of geaggregeerde operationele kengetallen omgezet in de waarde van het beheerde risico. In termen van waarde moeten we rekening houden met de directe impact van het incident op het bedrijf (continuïteit van de activiteiten, geschillen door klanten, nalevingsstraffen, kosten van de reactie op het incident, ransomware-betalingen) en met de indirecte impact (schade aan het merkimago, aandelenkoers).

Een van de methoden om geld te verdienen is Factoranalyse van informatierisico's (FAIR™)[23], een model om cyberrisico's en operationele risico's in financiële termen te begrijpen, te analyseren en te kwantificeren. Deze methode is goed ingeburgerd en er is veel over gepubliceerd. Voor kleinere of

[23] https://www.fairinstitute.org/what-is-fair

minder volwassen organisaties kan zij echter te uitgebreid en te moeilijk te onderhouden zijn.

De PHOSI-calculator (Potential Harm of Security Incident) van de Nederlandse telecomaanbieder KPN is een alternatief met een lage instap, dat beschikbaar is als app op smartphones[24][25]. Met deze app kan aan de hand van een klein aantal vragen de risicowaarde worden berekend. Deze PHOSI-schattingen kunnen worden gecombineerd met afzonderlijke dreigingen/controles of ook met resultaten van Red Teaming (welke potentiële schade werd vermeden door een kritieke kwetsbaarheid tijdig te patchen of door een Red Team-oefening uit te voeren?) of blootstelling door belangrijke kwetsbaarheden.

Een bredere en eenvoudigere manier om belangrijke operationele metriek te monetariseren is het resultaat van de normalisatie/consolidatie te gebruiken als de matigingsfactor die moet worden vermenigvuldigd met de gemiddelde frequentie en impact van een in de gemeenschap waargenomen cyberincident. Onderzoek naar de frequentie en impact van ransomware-incidenten heeft interessante voorbeelden opgeleverd voor dergelijke benaderingen[26]. Recent academisch werk op dit gebied is ook te vinden in "A System to Calculate Cyber-Value-at-Risk"[27].

Het is belangrijk op te merken dat dit een actief onderzoeksgebied is en dat de methoden om risico's te kwantificeren onvolmaakt zijn. Hoewel dit een na te streven doel is, en van essentieel belang voor de communicatie met de voornaamste belanghebbenden, moeten de resultaten met de nodige omzichtigheid worden behandeld.

Gevolgen voor de veiligheid (life at risk)

Sommige organisaties zijn door hun activiteit niet alleen begaan met de monetaire gevolgen, maar ook met de gevolgen voor de veiligheid. Dit zou het geval zijn voor luchtvaartmaatschappijen/luchtverkeersbeheer, auto-fabrikanten, ziekenhuizen, leveranciers van kernenergie, enz.

Cyberrisico's die tot verlies van mensenlevens kunnen leiden, zouden moeten worden ingeschat en de doeltreffendheid van controles en risicobeperking zou moeten worden gemeten en gecontroleerd. Op dit gebied is veel minder werk gepubliceerd, maar het onderliggende principe zou vergelijkbaar zijn met de berekening van de "value at risk".

Dit is zeker een gebied waarop organisaties zich minder op hun gemak zouden voelen om beoordelingen te delen of compromissen en berekende risico's bloot te leggen. Een externe perceptie van aanvaarding van risico's op verlies van mensenlevens door een organisatie zou zeer snel tot imagoschade kunnen leiden.

Aangezien het in geld uitdrukken van het verlies van mensenlevens niet aanvaardbaar is (althans in sommige regio's van de wereld), wordt het begrip aanvaardbaar risico van verlies van mensenlevens beoordeeld aan de hand van

[24] https://apps.apple.com/us/app/kpn-ciso/id1122223795
[25] https://play.google.com/store/apps/details?id=com.kpn.ksp&hl=en&gl=US
[26] https://www.youtube.com/watch?v=kSi-oXq4xV0
[27] https://www.sciencedirect.com/science/article/pii/S0167404821003692

een combinatie van kwantitatieve en kwalitatieve middelen om het risico te berekenen, waarbij ernaar wordt gestreefd geen verlies te veroorzaken voor zover dit redelijkerwijs uitvoerbaar is en door de regelgeving wordt getolereerd.

Risicobereidheid in kaart brengen

De resultaten van de tax/life at risk-beoordelingen moeten worden vergeleken met de risicobereidheid van de organisatie. In veel organisaties is deze risicobereidheid al vastgesteld in het raamwerk van de bedrijfsrisicoprocessen. Indien dit niet het geval zou zijn, moet de CISO de business/het bestuur ertoe aanzetten de risicobereidheid vast te stellen:

- Hoeveel zijn wij bereid te verliezen als het risico werkelijkheid wordt?
- In welke mate willen wij dat het risico wordt beperkt?
- Hoeveel middelen zijn wij bereid beschikbaar te stellen voor mitigatie?
- Verzekeren we een deel van het risico?

Sommigen zullen waarschijnlijk aanvoeren dat het niet mogelijk is de waarschijnlijkheid van een inbreuk te beoordelen. We mogen echter niet vergeten dat als er geen benchmark is voor risicobereidheid, niemand zal proberen de waarschijnlijkheid überhaupt te kwantificeren. Wij pleiten ervoor een discussie op gang te brengen over risicotolerantie zoals "minder dan 5% kans per jaar op een verlies door cyberinbreuken van meer dan 1 miljoen dollar". Hoewel we erkennen dat een dergelijke kwantitatieve benadering van cyberrisico's moeilijk te verwezenlijken is en eerder uitzondering dan norm is, is het doel ambitieus, niet alleen om risicokwantificering te stimuleren, maar ook om redelijke budgetten mogelijk te maken.

Vergist u zich eerst in deze getallen en laat de leidinggevenden werken aan het beantwoorden van de vraag in een herhaalbare methodologie. Als u geen idee hebt welke getallen u moet gebruiken, onderzoek dan enkele van de andere risico's binnen uw organisatie, zoals de risicotoleranties voor brand, overstroming of arbeidsongevallen. Het kan om heel verschillende risico's gaan, maar ze kunnen u een leidraad geven voor het uitdrukken van de risicotolerantie die u hoopt te bereiken. Misschien ontdekt u uiteindelijk dat uw organisatie in werkelijkheid dichter bij een kans van 10% zit, maar dan wordt de discussie wat de kosten zijn om die kans te verkleinen handelbaar en rationeel.

Het in kaart brengen van de risicowaarde en de risicobereidheid is noodzakelijkerwijs een multidimensionale analyse waarin verwachte frequentie en mogelijke impact worden gecombineerd en waarin de huidige situatie kan worden uitgedrukt in een aantal gegevenspunten op basis van hypotheses over de doeltreffendheid van de controles.

Het in kaart brengen kan ook worden gebruikt om te laten zien hoe de voorgestelde controles/investeringen tot verbeteringen kunnen leiden. Maar dat alles zal waarschijnlijk niet gebeuren, tenzij de Raad van Bestuur in de eerste plaats een risicotolerantie vaststelt. Alleen dan kan worden gediscussieerd over het realisme van de cijfers en de verwachtingen inzake de veerkracht van het cyberrisico.

Samenvatten van stories

Het selecteren van relevante stories (incidenten binnen en buiten de organisatie, informatie over cyberdreigingen, ontwikkelingen op het gebied van regelgeving) en het extraheren van de essentie (waarom is dit relevant?) is een essentiële aanvulling op de kwantitatieve metriek.

Het nauwkeurig vaststellen van het verhaal en een overtuigend verhaal opschrijven vergt specifieke vaardigheden van de CISO en het team. Geselecteerde stories moeten een extra context bieden voor het risicogedrag van de organisatie en een doel dienen. Anders dreigen ze de aandacht af te leiden en energie en middelen te kosten die elders beter zouden kunnen worden gebruikt.

Cyberrisico's rapporteren – bieden van redelijke zekerheid

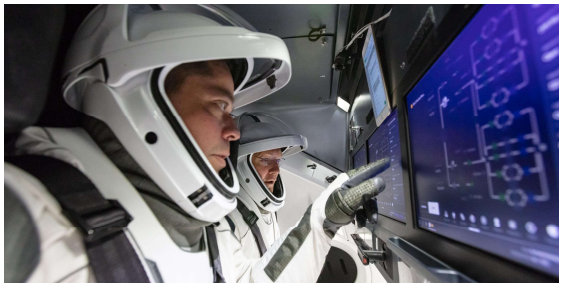
Cyberverslaglegging aan de Raad van Bestuur moet dienen om de Raad van Bestuur (opnieuw) te verzekeren dat het cyberrisico binnen de risicobereidheid valt, vandaag en morgen:

- Zijn we goed genoeg?
- Zijn de voor cyber toegewezen middelen adequaat en doeltreffend?
- Hoe verhouden wij ons tot onze collega's en onze sector?

Aangezien het bestuur en zijn comités niet gespecialiseerd zijn in cyber, zou het raadzaam zijn het bestuur te helpen de juiste vragen te stellen en ze niet te overstelpen met informatie. Om de situatie met beelden te vergelijken, toont de volgende figuur een "CISO"-cockpit met operationele instrumenten en consoles waarmee de piloten kunnen communiceren met het vliegtuig om de passagiers veilig en tijdig op hun bestemming te brengen.

Figuur 14 Krediet Luchtvaarders / Piloten van Zwitserland

De volgende figuur toont een "Board"-cockpit met verschillende instrumenten en zonder de mogelijkheid tot besturing, die volledig afhankelijk is van de grondcontrole.



Figuur 15 Krediet NASA/SpaceX

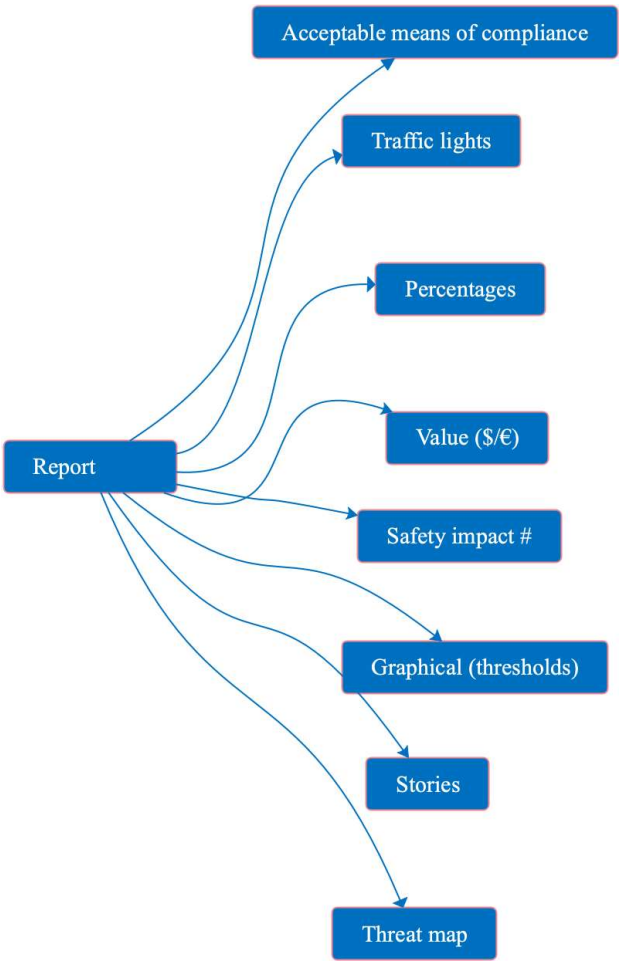
De Raad verwacht van de CISO dat hij ontwikkelingen signaleert die de situatie ten goede of ten kwade wezenlijk veranderen, en dat ze naar aanleiding daarvan relevante acties en middelen voorstellen.

Het vaststellen van een pakket cybermetriek en het consequent rapporteren van de context daarvan aan het bestuur, de individuele leden en de relevante comités (audit, compliance) kan een effectieve en betrouwbare manier zijn om cyberzekerheid te bieden.

Het kan worden gecombineerd/afgestemd met rapportage over andere soorten bedrijfsrisico's en met rapportage over de digitale transformatiestrategie.

Metriek en verhaal

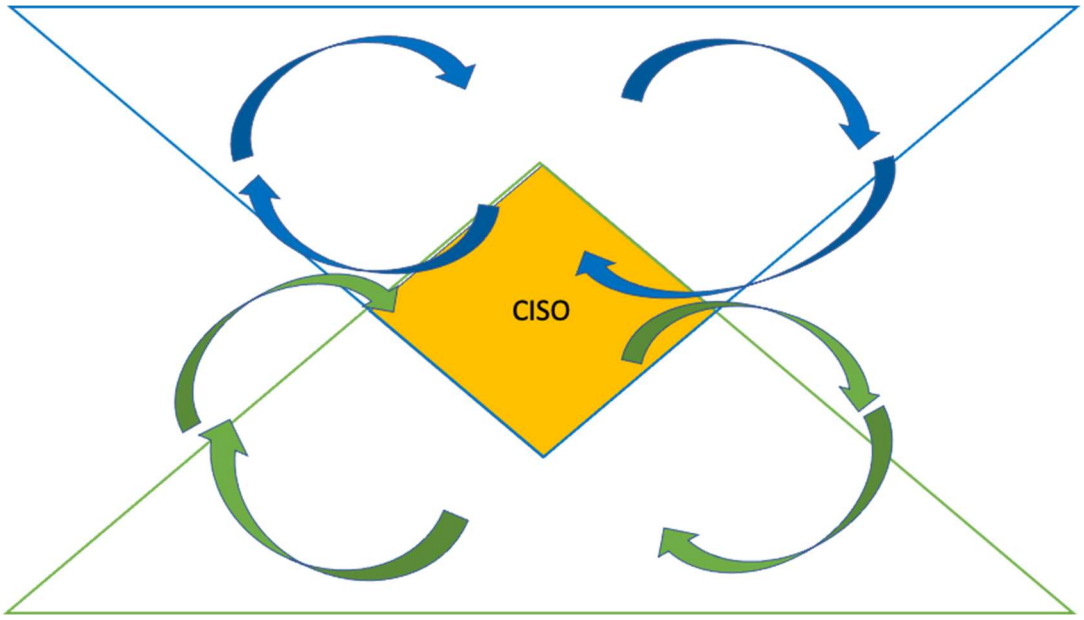
Het oude adagium "een beeld zegt meer dan duizend woorden" is ook waar in de context van cyber die uw Raad van Bestuur weet te betrekken. Er is een grote verscheidenheid aan grafische weergaven van cybercijfers in gebruik in de gemeenschap en het bekijken van dergelijke voorbeelden en de interactie met branchegenoten kan zeer inspirerend zijn voor het ontwerp van het rapportagepakket van een organisatie. In Figuur 16 hebben we een aantal bouwstenen opgenomen, gebaseerd op voorbeelden uit de gemeenschap zoals opgenomen in de bijlagen.



Figuur 16 Rapportering – bouwstenen

Communicatiekanalen

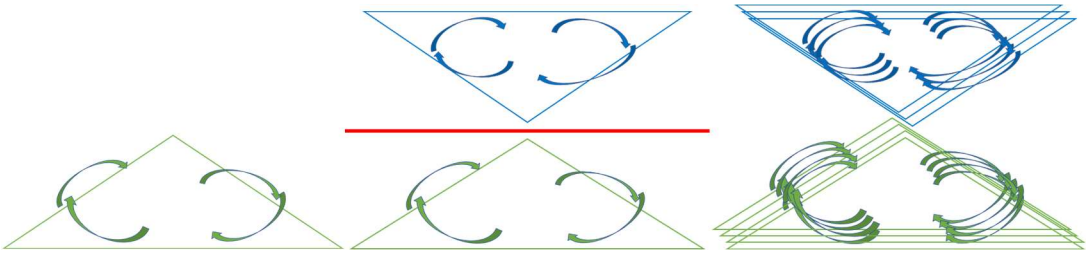
Idealiter zou een organisatie een coherent en geïntegreerd communicatie-kanaal tot stand brengen om input te verzamelen, om te zetten en vervolgens aan de Raad van Bestuur te rapporteren. De communicatiestromen in Figuur 17 zou worden uitgevoerd zoals bedoeld. Dit vereist dat verschillende functies samenwerken en op één lijn zitten wat betreft het raamwerk, de processen om de metriek te vullen, en de rollen en verantwoordelijkheden bij de rapportage.



Figuur 17 Optimale communicatiestroom

Ongeacht wie daadwerkelijk rapporteert aan de Raad van Bestuur, moet de CISO een sleutelrol spelen in het proces en zorgen voor een professionele en onafhankelijke kijk op het cyberrisico. In het optimale geval zou het de CISO zijn die persoonlijk verslag uitbrengt aan de Raad van Bestuur, zodat interactie mogelijk is en zekerheid wordt verschaft.

Alternatieve situaties, zoals geïllustreerd in Figuur 18 waarin in het eerste diagram geen informatie aan de Raad van Bestuur wordt verstrekt, in het middelste diagram de aan de Raad van Bestuur verstrekte informatie niet op de werkelijkheid is gebaseerd, of in het derde diagram tegenstrijdige informatie via verschillende kanalen aan de Raad van Bestuur wordt verstrekt, moeten worden vermeden of geleidelijk worden beëindigd.



Figuur 18 Inexistente, niet-aangesloten, parallelle communicatiestromen

Weerstand overwinnen

Hoewel de in dit document beschreven concepten tot op zekere hoogte al worden gebruikt door cyberbeveiligingsafdelingen, vormen ze ook een basis om cyberbeveiligingsrisico's te integreren als onderdeel van de bedrijfsrisico-beheerprocessen. Deze interacties vormen echter nog steeds een uitdaging in veel organisaties waar:

- Cyberbeveiliging en risico's worden beheerd door verschillende afdelingen/silos;

- Cyberbeveiliging wordt door de bedrijfsafdelingen beschouwd als een discipline voor ingewijden, een "zwarte kunst";
- Risicobeheersmodellen worden door de cyberbeveiligingsafdelingen als complex en abstract beschouwd;
- Cyberwoordenschat en -metriek worden niet vertaald in bedrijfstermen.

Om cyberbeveiliging als een terugkerend onderwerp op de agenda van de Raad van Bestuur te krijgen, zijn inspanningen en overtuigingskracht nodig, maar dit kan worden bevorderd door een aantal proactieve initiatieven:

- Inzicht in de verwachtingen van de Raad van Bestuur en de individuele leden en aanpassing aan veranderende verwachtingen;
- Bewustmakingssessies met de Raad van Bestuur, waarin dreigingen en risico's op een begrijpelijke manier worden uitgelegd;
- Incidentenbestrijdingsoefeningen waarbij de Raad betrokken is;
- De Raad van Bestuur maandelijks cyberbriefings sturen met relevante verhalen en context;
- Bilaterale briefings met individuele leden van de Raad van Bestuur die belangstelling tonen;
- Geleidelijk beginnen en het systeem in de loop van de tijd verbeteren (bijvoorbeeld beginnen met de uitvoering van een op een maturiteitsmodel gebaseerde aanpak alvorens een volwaardig kwantitatief model in te voeren);
- Transparante en positieve samenwerking met het Auditcomité.

Toewijzing van middelen aan metriek en rapportage

Het lijdt geen twijfel dat het implementeren en onderhouden van een metriek- en rapportagesysteem zoals in dit document beschreven, specifieke middelen vereist. Het bespaart echter ook middelen door interne afstemming/ stroomlijning, door het vermijden van nodeloze reactieve reacties in de media en uiteindelijk door de middelen te richten op wat echt belangrijk is om het cyberrisico tot een aanvaardbaar niveau terug te brengen, waardoor reacties op incidenten en negatieve gevolgen worden voorkomen.

Bijlage 1: Waar te beginnen?

Vragen voor de Raad

- Hebben we een inventaris van de belangrijkste activa?
- Wie heeft het op ons gemunt (belangrijkste tegenstanders) en waarom?
- Wat zijn onze belangrijkste controles en wat is hun status?
- Waar zitten de lacunes en hoe denken wij die te dichten?
- Hebben we een plan voor respons op incidenten / bedrijfscontinuïteit / veerkracht?
- Hoeveel staat er op het spel?
- Hoe verhouden wij ons tot onze gelijken?

Sleutelcontrole basislijnen

Hieronder volgt een (niet-uitputtende) selectie van basisaanbevelingen:

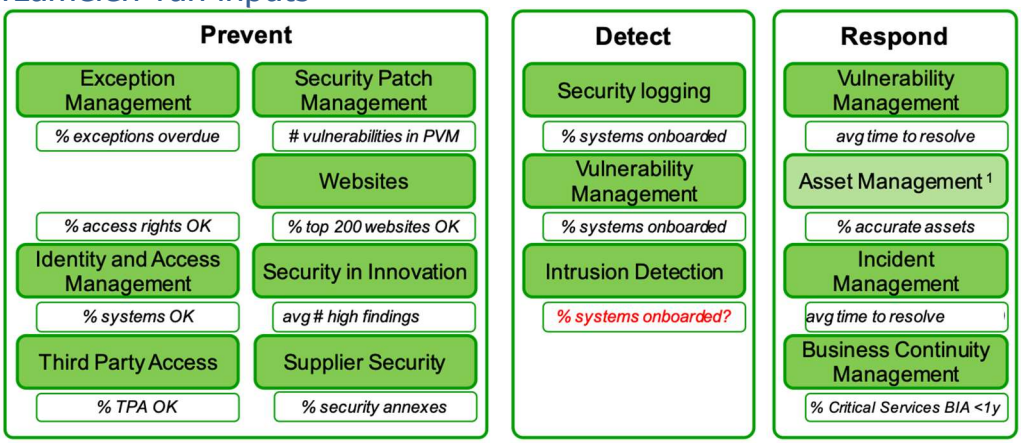
- Top zeven beveiligingsmaatregelen (Cybersecurity Centrum België)[28]
- Top tien (UK National Cyber Security Centre)[29]
- Essentiële acht (Australisch Cyberbeveiligingscentrum)[30]
- Top 42 van maatregelen voor een gezond netwerk (FR ANSSI)[31]
- Top acht beveiligingsmaatregelen (NL Nationaal Cyber Security Centrum)[32]

Deze autoriteiten zijn ook een bron van actuele informatie over het dreigingslandschap en de evoluerende aard van kwetsbaarheden en vijandige technieken.

[28] https://cyberguide.ccb.belgium.be/en/take-security-measures-0
[29] https://www.ncsc.gov.uk/files/2021-10-steps-to-cyber-security-infographic.pdf
[30] https://www.cyber.gov.au/acsc/view-all-content/essential-eight
[31] https://www.ssi.gouv.fr/en/guide/40-essential-measures-for-a-healthy-network/
[32] https://www.ncsc.nl/onderwerpen/basismaatregelen

Bijlage 2: Voorbeelden uit de gemeenschap

Verzamelen van inputs



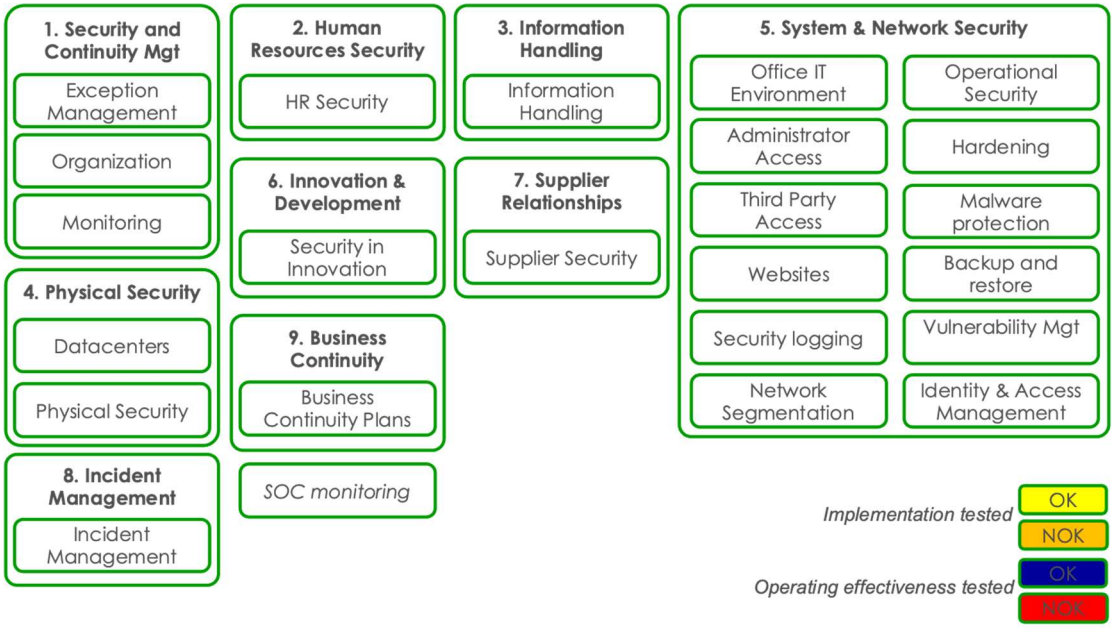
Figuur 19 Voorbeeld van gebeurtenisgerichte metriek

Incident Timeline	Applicability Level	Description
Time of First Activity	Recommended for significant incidents	This is the earliest event in a confirmed or potential chain of events, that caused the incident.
Time of Detection	All incidents	The time that a control (e.g. telemetry, technology) or another detection mechanism (e.g. a human) recognizes that something has occurred.
Time of Containment	All incidents that require Containment	Time of Containment is the point in time at which the incident can no longer spread nor do damage.
Time of Remediation	All incidents that require Remediation	Time of Remediation is the point in time at which an affected target asset is returned to its pre-incident state or removed from the environment permanently.

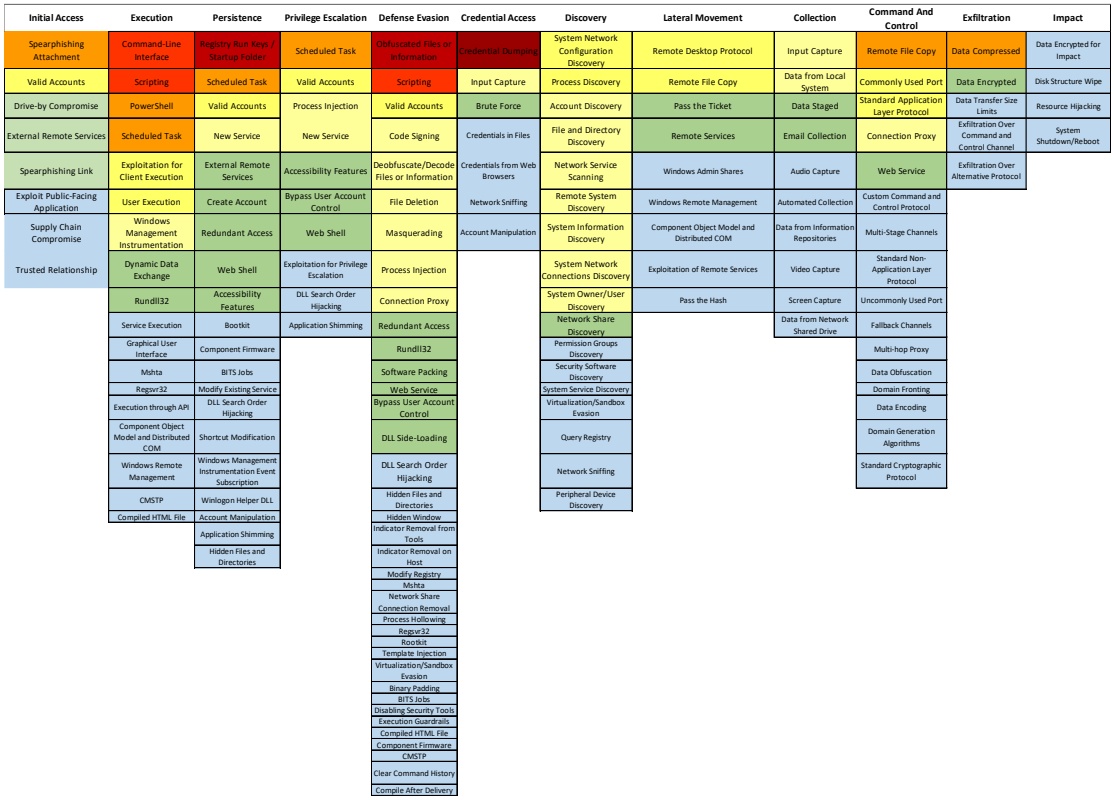
Figuur 20 Aanbevolen timingmetrieken. Bron FIRST Metrics SIG.

Function	Category	Subcategory	Subcategory Risk	Sub Cat Score	Subcategory Composite Risk Score
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	Critical	6	30
		ID.AM-2: Software platforms and applications within the organization are inventoried	Weighted Medium	4	
		ID.AM-3: Organizational communication and data flows are mapped	Weighted Medium	4	
		ID.AM-4: External information systems are catalogued	Critical	6	
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Critical	6	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Weighted Medium	4	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	Weighted Low	2	
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Low	1	
		ID.BE-3: Priorities for organizational mission, objectives			

Figuur 21 Een voorbeeld van de toepassing van aan de NIST-CFR gekoppelde metrieken

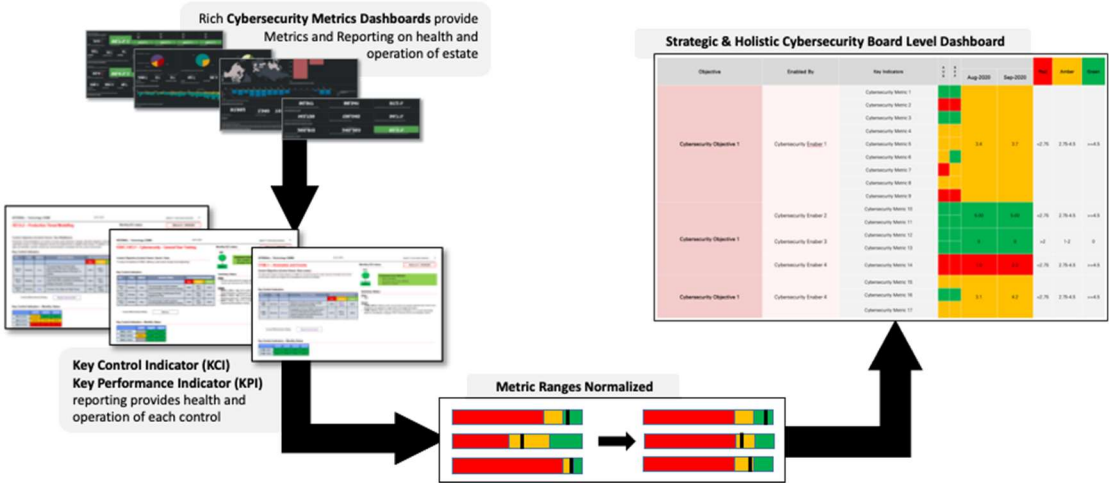


Figuur 22 Voorbeeld van metrieken uit tests

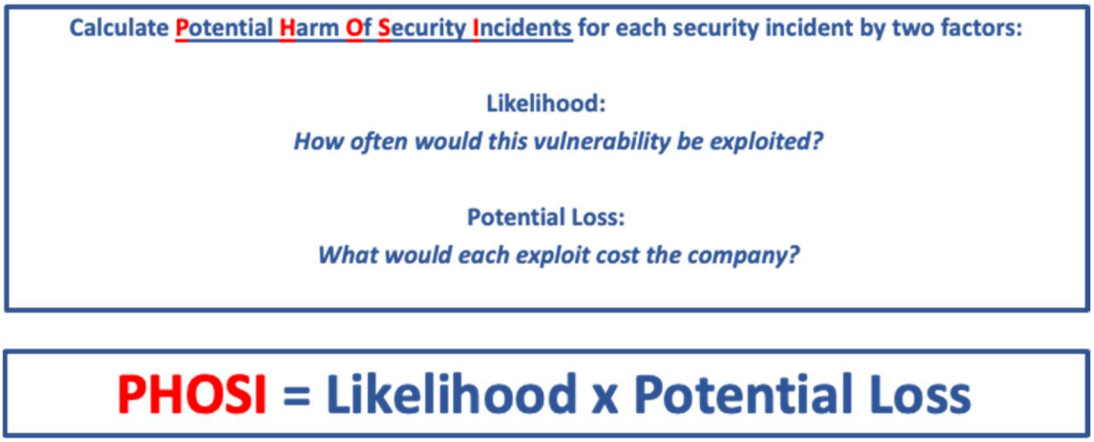


Figuur 23 Voorbeeld van het gebruik van een heatmap om de dekking van TTP's weer te geven

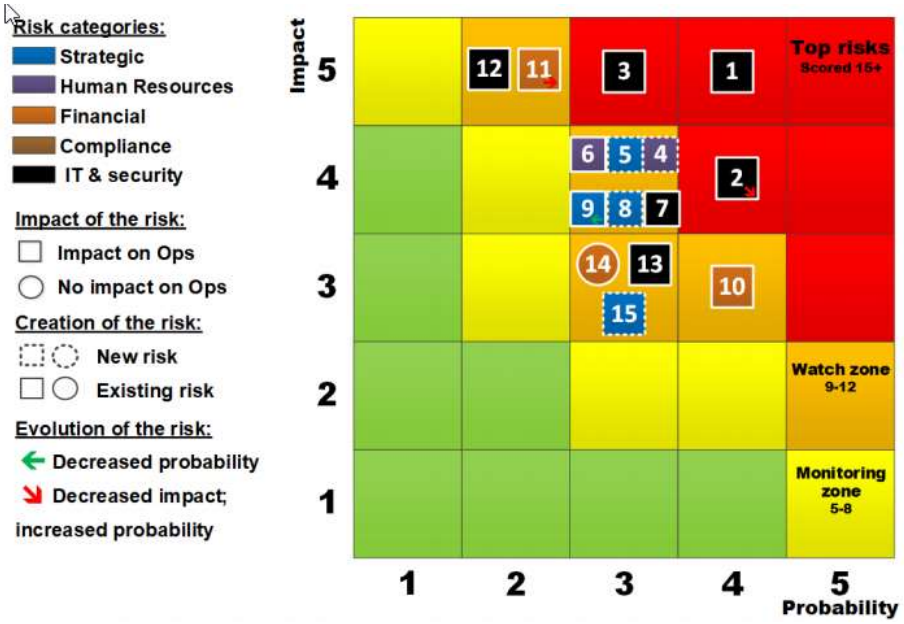
Transformeer



Figuur 24 Voorbeeld van normalisatie

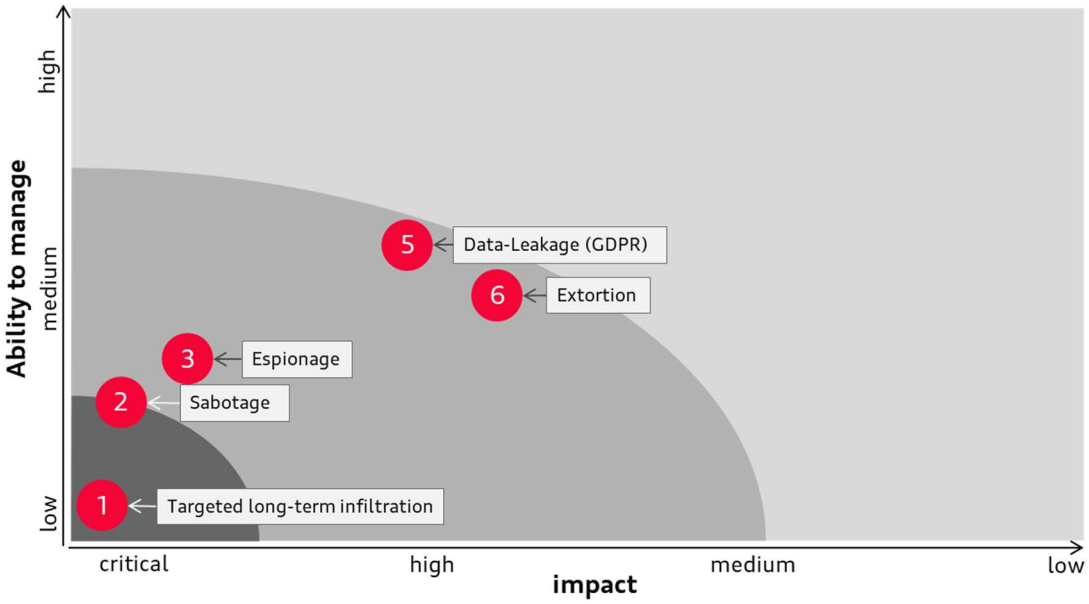


Figuur 25 Voorbeeld van monterarisatie



Figuur 26 Voorbeeld van het in kaart brengen van risico's

Melding van cyberrisico



Manufacturing industry or geographically close

When?	What?	Category	Group
Q1.2021	Hackers exploit IT tool Z to establish persistence	1	Unknown
Q4 2020	Ransomware attack at enterprise X	2 6	Cyber-Crime
Q4 2020	Enterprise Y hit by ransomware, data leaked	2 6	Cyber-Crime

Figuur 27 Voorbeeld van rapportage over het dreigingslandschap

When	Type	What?	Status	Group
4/2020	3	Spear phishing campaign with malicious Excel attachment.	Closed	APTX

Figuur 28 Voorbeeld van incidentenrapportage

Group	Motive	Trend
Adversary 1	Adversary known to steal intellectual property in high tech industry.	↗
Adversary 2	Adversary known to steal intellectual property in our sector.	→
Targeted Cyber-Crime	Ransomware actor increasingly prevalent and sophisticated	↑

Figuur 29 Voorbeeld van het opsporen van opmerkelijke tegenstanders

CERT-EU

TLP:WHITE

Threat Landscape Report 2021 Q3 - Executive Summary

Direct Threats to EU Institutions, Bodies, and Agencies

INCIDENTS

4 significant incidents affected EUIBAs this quarter.

In 3 cases the attack started with a compromise of a publicly accessible server (Oracle WebLogic, Microsoft Exchange).

In the other case, attackers obtained credentials via a phishing campaign.

In at least 3 significant incidents, threat actors successfully exfiltrated data.

Since the beginning of 2021, CERT-EU has already recorded 15 significant incidents, compared to 13 during the whole of 2020 and 8 in 2019.

THREATS

CERT-EU released 26 threat alerts (compared to 20 during Q1 and 22 in Q2).
The top 5 reasons for threat alerts were:

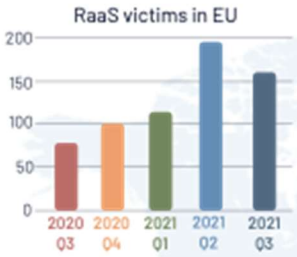
- Active exploitation of zero-days or n-days: Microsoft Exchange, VPNs, etc.
- Recent activity or new tools used by top threat actors
- Sharing actionable data related to TTPs used in significant incidents
- Spear-phishing campaigns directly affecting EUIBAs or sectors of interest
- Active use of commercial mobile spyware

Top threat actors: CERT-EU currently tracks 13 top threat actors. The level of exposure of EUIBAs has been high for 4 of them: two alleged Russian threat actors, one alleged Chinese, and one allegedly of North Korean origin.

Social media: The most frequently used social media network for impersonation of EU staff or the digital identities of EUIBAs has been Instagram, followed very closely by Facebook and at a distance by Twitter.

Malware and tools: The three most observed pieces of malware or malicious tools to which EUIBAs have been exposed were Cobalt Strike, Mimikatz, and Dridex. However, no infections have been confirmed.

Threats in Europe



Ransomware

A supply chain attack conducted by REvil against Kaseya VSA, software used by many MSPs, had a major impact on several organisations including in Europe, causing significant disruptions.

Taking into consideration the first 9 months of 2021, the average number of ransomware victims per month increased by 129% in 2021, compared to last year.

Nation-state activity

The EU has acknowledged and condemned Russian "Ghostwriter" cyberespionage / information operation activity against EU member states. The Russian APT29 threat actor targeted European governments with a zero-day exploit earlier in 2021. The EU, the UK, and the US attributed the Hafnium ProxyLogon attacks to China and are calling for an immediate stop to such adversarial activities. France reported a significant cyberespionage campaign by the Chinese Zirconium (aka APT31) threat actor. The NSO group and its Pegasus spyware have been used in several espionage cases against politicians and journalists.

Hacktivism

Belarussian hacktivists continue hack-and-leak operations against the Minsk regime.

Threats in the World

China: China is establishing full control over all domestic knowledge of software vulnerabilities. As always, China is active on social media, working to amplify pro-Chinese messages.

Russia: Political opposition and anti-corruption entities in Russia fall victim to DDoS attacks and data leaks. Stricter internet controls and censorship established before the September parliamentary election remain in place after the election. Proposed legislation prohibits foreign companies from processing biometric data of Russian citizens.

Iran: Iranian governmental websites were taken offline after a "cyber disruption".

North Korea: A North Korean cyber threat actor compromised a major South Korean major producer of combat ships & submarines.

CERT-EU, CERT for the EU Institutions, Bodies, and Agencies https://cert.europa.eu - services@cert.europa.eu

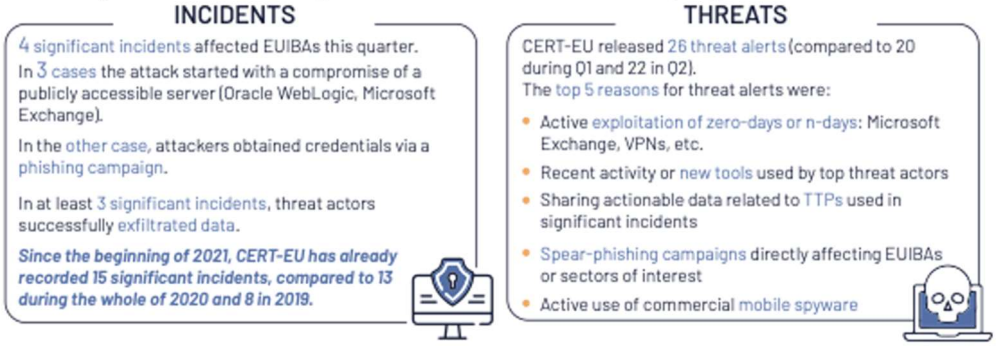
Figuur 30 Voorbeeld van metrieken en beschrijving, krediet CERT-EU

Bijlage 3: Voorbeeld van een verslag

Ontwikkeling van het dreigingslandschap

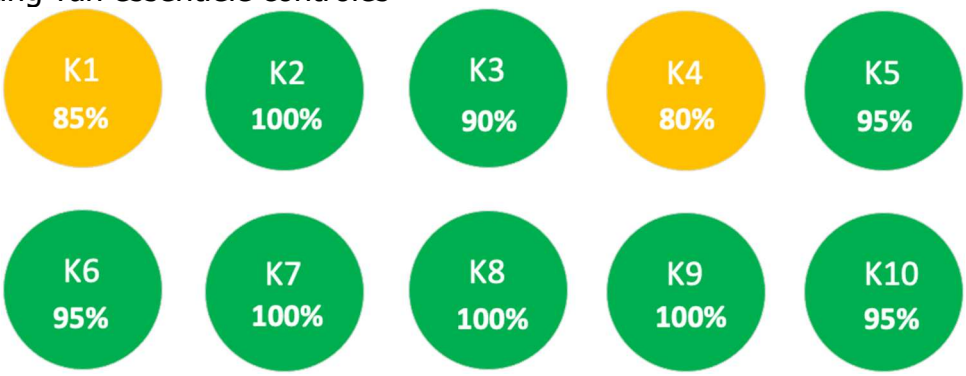
Who?	Group / Malware?	Why?	Trend
Adversary 1	APTX	Adversary known to steal intellectual property in high tech industry.	↗
Adversary 2	APTY	Adversary known to steal intellectual property in our sector.	→
Targeted Cyber-Crime	FIN11 (TA505)	Public and corporate IT-infrastructure is a growing market for ransomware	↑

Opmerkelijke ontwikkelingen in incidenten en dreigingen

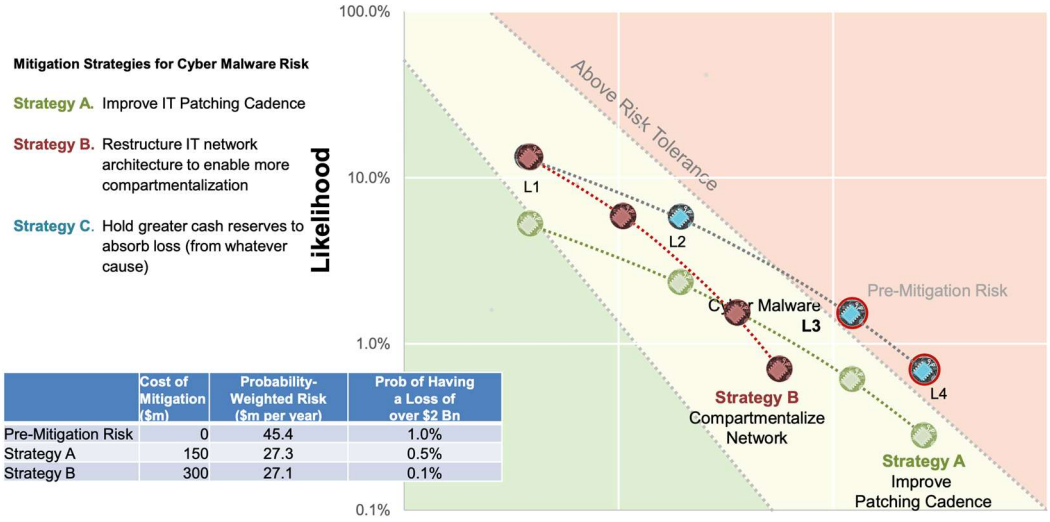


Figuur 31 Bron CERT-EU

Dekking van essentiële controles



Impact van aanvullende maatregelen op de beperking van het cyberrisico



Figuur 32 Bron Centrum voor risicostudies, Universiteit van Cambridge