Cyberverzekering
Cyber Impact Analyse

Samengesteld voor
<Voorbeeld>

Sector	Mijnbouw en Delving
Regio's	Verenigde Staten
Omzet	€8.063.866
Type data	Persoonsgegevens (PII - Personally Identifiable Information including employee information), Creditcard informatie (PCI - Payment Card Information)

december 10, 2018

Voorwoord Cyber Impact Analyse

Gefeliciteerd met de AIG Cyber Verzekering. Dit rapport biedt aanvullende informatie over de manier hoe AIG naar ue risicoprofiel kijkt, gebaseerd zowel de door beantwoorde vragen als het inzicht van AIG in het cyberrisicolandschap. Als u vragen heeft over dit rapport, neem dan contact op met uw Verzekeringstussenpersoon, een AIG Cyber Risicospecialist of stuur een e-mail naar CyberRiskConsulting@aig.com.

AIG Cyber Impact Analyse

Als onderdeel van het acceptatieproces, gebruikt AIG een gepatenteerde methode voor het meten en modelleren van cyberrisico's uitgedrukt in economische waarden. AIG gebruikt kennis en inzichten van verschillende datasets en de specifieke antwoorden uit het vragenformulier op de volgende manieren:

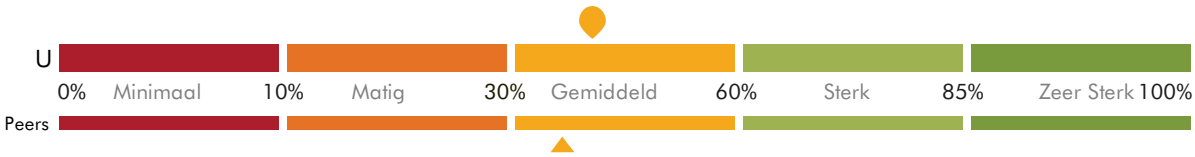
- Het meten van de (maandelijkse) kans op Cyberincidenten vanuit interne en externe bronnen, en het gebruik van de meest recente data in het model.
- Het meten en modelleren van de impact op de bedrijfsvoering en effectiviteit van beveiligingsmaatregelen.
- Weergave van de meest voorkomende scenario's en overgebleven risico's, implementatie en prioriteren van beveiligingsmaatregelen.
- Inschatting van de waarschijnlijkheid en impact van een Cyberincident, inclusief de te verwachten schade.

Het steeds veranderende Cyberlandschap en andere variabelen zorgt na verloop van tijd dat het rapport mogelijk minder accuraat wordt. De antwoorden in het vragenformier kunnen na verloop van tijd achterhaald zijn. Impact en kansbepalingen zijn een momentopname van data en statistische trends. De uitkomst van dit rapport geeft een goed beeld van de risico's die wij als AIG zien voor uw bedijf. Het rapport kan niet worden beschouwd als een volledige beoordeling van uw cyberrisico's.

Score Overzicht

Cyber Maturity

De mate waarin uw organisatie is voorbereid op cyberincindenten en in staat is om data te beschermen.



40,55%
Gemiddeld
11% sterker dan peers
36,67% Gemiddeld

Resterend Risico

Dit is het Cyberrisico, en de impact op de organisatie, na het toepassen van Cybersecurity maatregelen.

12,952
Gemiddeld
7% sterker dan peers
13,930 Gemiddeld

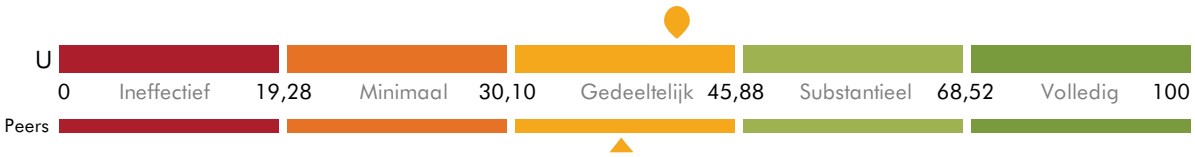
Cyberrisico

De kans dat onopzettelijke of kwaadwillige incidenten één of meer kwetsbaarheden in de IT-omgeving blootleggen.

2,767
Laag
0% gelijkwaardig aan peers
2,767 Laag

Effectiviteit van beveiligingsmaatregelen

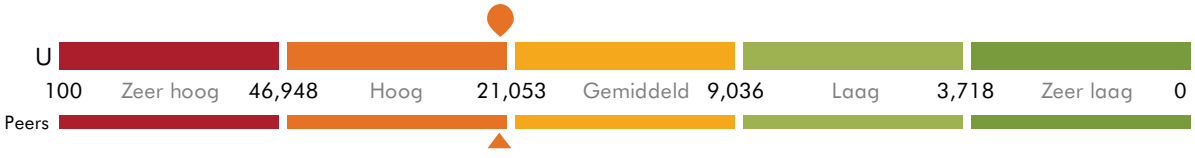
Geeft aan inhoevere de beveiligingsmaatregelen het Cyberrisico vermindertafhankelijk van hoe goed de maatregelen zijn geïmplementeerd.



41,77%
Gedeeltelijk
10% sterker dan peers
37,83% gedeeltelijk

Basis Risico

Het Cyberrisico en de impact op de organisatie, zonder de impact van Cybersecurity maatregelen.



21,786
Hoog
1% sterker dan peers
21,921 Hoog

Business Impact

De mate van impact op de vertrouwelijkheid, integriteit en beschikbaarheid van de bedrijfsmiddelen (o.a. data, IT infrastructuur, goederen, personeel etc.) van uw organisatie.

8,661
Zeer hoog
1% sterker dan peers
8,720 Zeer hoog

Uitleg vergelijking over vergelijking peers (andere ondernemingen)

Dit rapport bevat informatie over hoe <Voorbeeld> zich verhoudt tot vergellijkebare ondernemingen ten aanzien van het cyberrisicolandschap, inclusief de waarschijnlijkheid van dreiging, de impact op het bedrijf in het geval van een cyberincidenten de kracht van controlls. Elke groep waarmee een bedrijf wordt vergeleken, wordt bepaald door de primaire bedrijfstak van het bedrijf, het jaarlijkse omzetniveau, en het land waarin de aanvraag wordt ingediend bij AIG. De peergroepbevat de meest recente cyberrisicobeoordelingen die AIG heeft gedaan voor elk bedrijf in de afgelopenanderhalfjaar. De peergroep.<Voorbeeld > heeft 10 - 99 peers (AIG geeft niet het specifiekeaantal peers, maar biedt wel een range aan ter beeldvorming van het aantal peers).

Beveiligingsmaatregelen

De beveiligingsmaatregelen die het Resterend risico het meest effectief verlaagd. Een organisatie kan door implementatie van deze beveiligingsmaatregelen haar 'Resterend risico' - zoals vermeld in het score overzicht - verbeteren. Let op: elke verandering in het bedreigingslandschap kan aanbevelingen herschikken.
De indexwaarden aan de rechterkant geven de vermindering in het 'Resterend risico' aan. Daarnaast ook gerangchikt naar welke maatregel de grootste risicoverminderend effect heeft.

Rank	Vragen sectie	Specifieke subsectie	Vraag#	Beschrijving	Risicoreductie index
1	Rank	Small Business	24	Software management	*
2	Rank	Small Business	25	Untrusted parties - Employee awareness	0,711
3	Rank	Small Business	27	Multifactor authentication and password enforcement	0,662
4	Rank	Small Business	28	Online security	0,444
5	Rank	Small Business	29	Business continuity planning	0,428
6	Rank	Small Business	21	Phishing	0,417
7	Rank	Small Business	23	Removable media	0,402
8	Rank	Small Business	26	Pop-up blocking	0,266
9	Rank	Small Business	22	Business and personal use	0,142

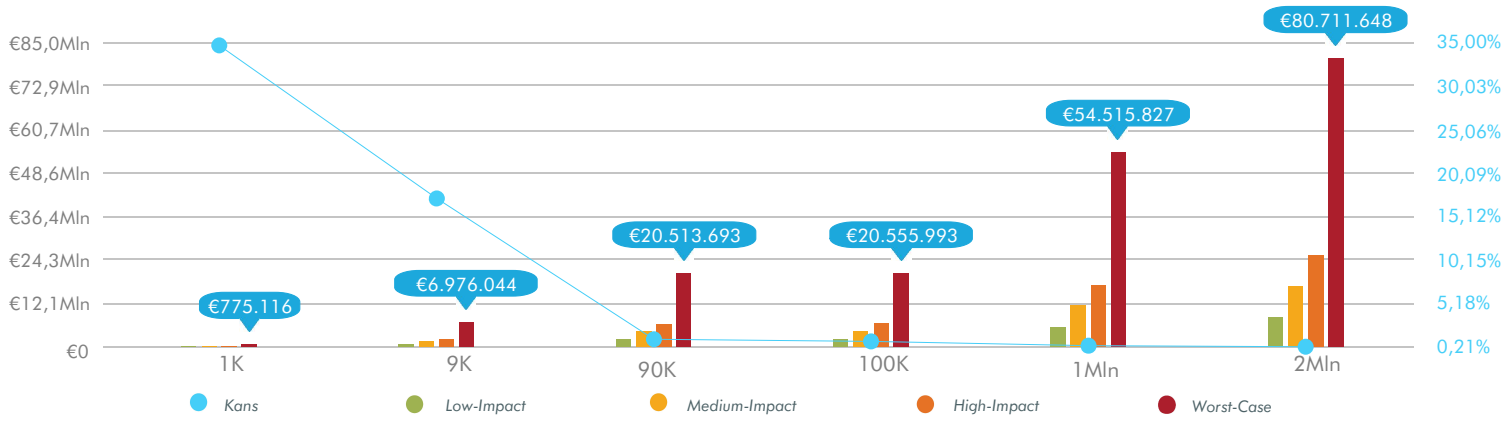
Opmerking: De bovenstaande uitkomsten/vragen zijn of niet beantwoord in het vragenformulier of dus dusdanig beantwoord dat de maatregelen niet zijn geimplementeerd.

Impact Datalek

Verwachte schade
€3,37 Miljoen
(Datalek – Medium Impact Scenario)

Kans op een datalek
0,21%
(2 Miljoen records)

Worst-Case Scenario
€80,71 Miljoen
(2 Miljoen records)



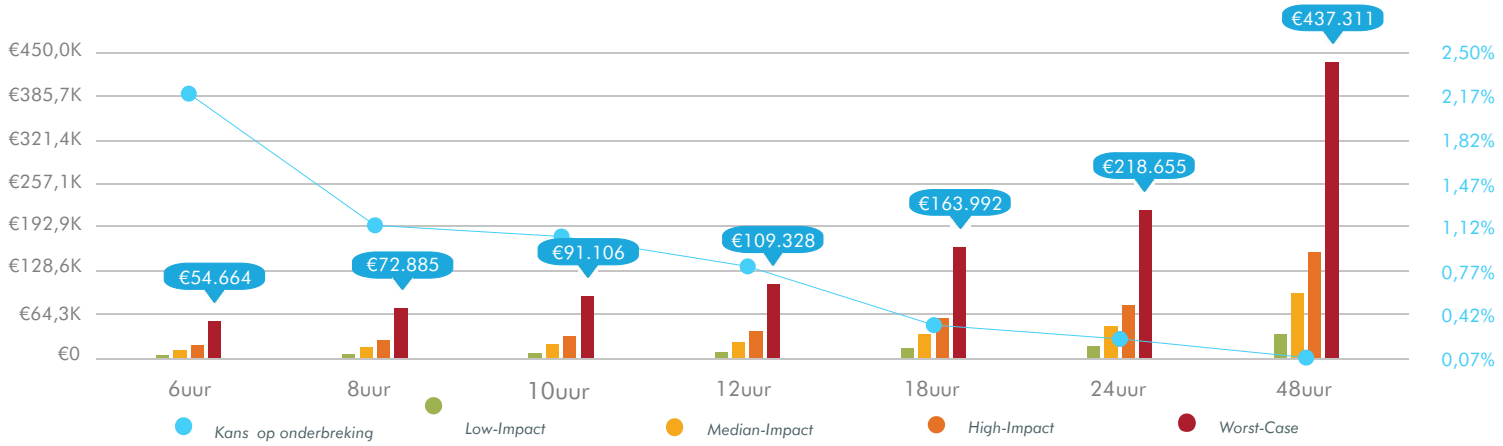
Omvang datalek (Records)	Kans	Low-Impact Datalek	Medium-Impact Datalek	High-Impact Datalek	Worst-Case Datalek
1K	34,69%	€79.920	€163.190	€246.460	€775.116
9K	17,19%	€719.282	€1.468.710	€2.218.138	€6.976.044
90K	1,07%	€2.115.113	€4.318.875	€6.522.637	€20.513.693
100K	0,83%	€2.119.475	€4.327.781	€6.536.087	€20.555.993
1Mln	0,32%	€5.620.984	€11.477.555	€17.334.126	€54.515.827
2Mln	0,21%	€8.321.967	€16.992.724	€25.663.481	€80.711.648

Impact Netwerkonderbreking (bedrijfsschade)

Verwachte bedrijfsschade
€79.415
(DoS Attack – Medium Impact Scenario)

Onderbreking
0,07%
(DoS Attack - 48 uur)

worst-case scenario
€437.311
(DoS Attack - 48 uur)



Duur netwerkonderbreking	Kans op onderbreking	Low-Impact Onderbreking	Medium-Impact Onderbreking	High-Impact Onderbreking	Worst-Case Onderbreking
6uur	2,18%	€4.449	€11.975	€19.501	€54.664
8uur	1,13%	€5.932	€15.967	€26.001	€72.885
10uur	1,04%	€7.415	€19.958	€32.501	€91.106
12uur	0,80%	€8.898	€23.950	€39.002	€109.328
18uur	0,33%	€13.347	€35.925	€58.502	€163.992
24uur	0,22%	€17.796	€47.900	€78.003	€218.655
48uur	0,07%	€35.592	€95.799	€156.007	€437.311

Resterend risico

Het Cyberrisico en de impact op de organisatie, zonder de impact van Cybersecurity maatregeben. Dit geeft hiermee inzicht in de voordelen van geïmplementeerde Cybersecurity maatregelen.

Het resterende risico voor <Voorbeeld>. is 12,952, wat Gemiddeld is.

	Web Application Attacks	Point of Sale Intrusion	Insider and Privilege Misuse	Miscellaneous Errors	Physical Theft and Loss	Crimeware	Payment Card Skimmers	Cyber Espionage	Denial of Service Attacks	Everything Else
Servers & Apps	14,213	8,902	18,694	6,985	0,415	13,372	0,170	19,327	16,145	9,944
Netwerk	3,506	4,527	12,330	4,066	0,415	7,147	0,170	10,492	17,340	5,214
End-User Systemen	5,399	8,689	14,973	4,604	6,337	10,878	1,074	16,154	3,445	8,036
Terminal	10,159	8,979	16,033	1,996	0,368	6,689	4,683	13,244	4,209	5,279
ICS/SCADA/OT	11,409	0,000	20,594	7,736	0,432	15,464	0,199	22,012	10,758	11,827
Healthcare Systemen	6,994	0,000	17,501	2,180	0,391	6,706	0,167	14,490	4,602	5,822
Onboard Systemen	3,632	0,000	17,171	2,165	0,391	6,706	0,176	14,433	4,602	5,868
Critical IoT	4,709	9,317	17,965	3,486	3,430	13,537	1,128	14,642	9,204	5,862
Non-Critical IoT	2,474	0,000	6,859	0,762	0,157	2,722	0,068	5,956	3,964	2,248
Media & Offline Data	0,428	1,427	10,902	2,545	2,460	0,551	0,113	2,888	0,370	1,410
Mensen	4,985	2,634	14,269	5,679	2,896	7,354	0,147	8,726	2,971	6,095

Opmerking: in het bovenstaande diagram geven 0,000 waarden aan dat het risiconiet van toepassing is op het profiel van uw organisatie. De kleur van de cel geeft de mate van resterende risico weer. Hoe donkerder de cel, hoe groter het resterende risico.

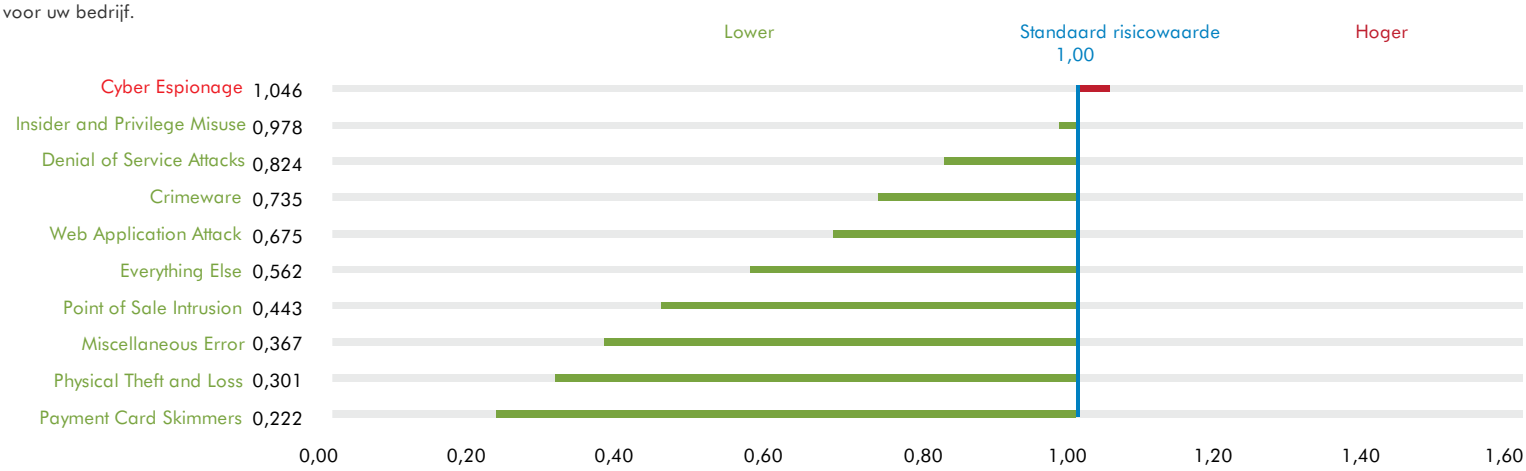
Top 10 resterende Cyberrisico's

Rank	Cyberrisico	Score	classering
1	Cyber Espionage: ICS/SCADA/OT	22,012	Hoog
2	Insider and Privilege Misuse: ICS/SCADA/OT	20,594	Gemiddeld
3	Cyber Espionage: Servers & Apps	19,327	Gemiddeld
4	Insider and Privilege Misuse: Servers & Apps	18,694	Gemiddeld
5	Insider and Privilege Misuse: Critical IoT	17,965	Gemiddeld
6	Insider and Privilege Misuse: Healthcare Devices	17,501	Gemiddeld
7	Denial of Service Attacks: Network	17,340	Gemiddeld
8	Insider and Privilege Misuse: Onboard Systems	17,171	Gemiddeld
9	Cyber Espionage: End-User Systems	16,154	Gemiddeld
10	Denial of Service Attacks: Servers & Apps	16,145	Gemiddeld

Opmerking: de bovenstaande top 10 Cyberrisico's kunnen nuttig zijn bij het nemen van beslissingen om het meest effectief in beveiligingsmaatregelen te investeren.

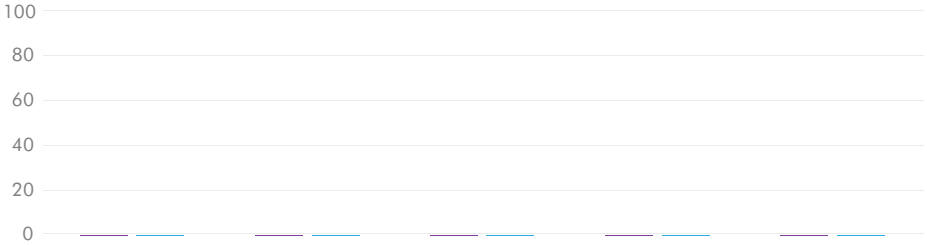
Risico index per categorie

Dit is een meting op basis van de van toepassing zijnde risicocategorieën met als uitgangpunt de gemiddelde risicowaarde. Een index groter dan 1,00 betekent dat uw bedrijf een specifiek risico loopt in die categorie. Dit is gebaseerd op de sector waarin uw bedrijf actief is en de kwetsbaarheden voor een specifieke dreiging. Ook ontoereikende beveiligingsmaatregelen beinvloeden de index. Door bedreigingen te rangschikken van laag naar hoog en te vergelijken kunt u een beter inzicht krijgen in de specifieke bedreigingen voor uw bedrijf.



Let op:in bovenstaande grafiek is 1,00 het verwachte risico. Als de waarde groter is dan 1,00, is het risico groter dan verwacht. Als de waarde lager is dan 1,00, dan is het risico lager dan verwacht.

Cyberrisico Trending



Basis risico Het Cyberrisico en de impact op de organisatie, zonder de impact van Cybersecurity maatregelen.

Resterend risico Dit is het Cyberrisico, en de impact op de organisatie,na het toepassen van Cybersecurity maatregelen.

Kans op een Cyberincident

De kans op Cyberincindenten betekent de waarschijnlijkheid dat een kwaadwillende of onbedoelde actie zwakheden binnen de informatietechnologie van een organisatie kan blootleggen.
De kans dat <voorbleeld> wordt getroffen door een Cyberincindent is 2,767, wat Laag is.

	Web Application Attacks	Point of Sale Intrusion	Insider and Privilege Misuse	Miscellaneous Errors	Physical Theft and Loss	Crimeware	Payment Card Skimmers	Cyber Espionage	Denial of Service Attacks	Everything Else
Servers & Apps	3,377	1,489	4,325	1,724	0,052	3,116	0,022	4,417	3,307	2,317
Netwerk	0,831	0,744	2,869	0,961	0,052	1,653	0,022	2,430	3,382	1,152
End-User Systemen	1,612	1,489	4,225	1,451	1,798	3,116	0,147	4,553	0,780	2,302
Terminal	2,435	1,489	4,056	0,286	0,052	1,656	1,165	3,331	0,929	1,307
ICS/SCADA/OT	2,350	0,484	4,073	1,614	0,052	2,984	0,023	4,322	1,858	2,282
Healthcare Systemen	1,536	0,608	3,965	0,280	0,052	1,487	0,023	3,264	0,929	1,291
Onboard Systemen	0,798	0,608	3,890	0,278	0,052	1,487	0,023	3,251	0,929	1,301
Critical IoT	1,086	1,487	4,089	0,450	0,463	3,016	0,146	3,331	1,858	1,327
Non-Critical IoT	1,171	0,447	4,024	0,254	0,052	1,563	0,023	3,492	1,858	1,312
Media & Offline Data	0,085	0,323	3,859	1,027	0,908	0,110	0,023	0,576	0,072	0,281
Mensen	1,358	0,475	4,741	1,730	0,890	2,187	0,023	2,595	0,929	1,812

Opmerking: in het bovenstaande diagram geven 0,000 de waarden aan dat het risico niet van toepassing is op het profiel van uw organisatie, De kleur van de cel geeft weer hoe vaak het risico zich kan voordoen. Hoe donkerder de cel, hoe groter het risico dat zich daardwerkelijk een incident voordoet.

Samenvatting van het Cyberrisico

1. Industrie: het risicoprofiel is gebaseerd op een objectieve industrie standaard(Mijnbouw en Delving) en de antwoorden ingevuld In het vragenformulier.
2. Toepasselijkheid: 11 van de 11 risico's behoren tot het risicoprofiel van< Voorbeeld>
3. Primaire risico: Insider and Privilege Misuseis de meest waarschijnlijke risicoscenario.

Opmerking: AIG raadt het af om, uitsluitend op basis van dit rapport, een beslissing te nemen over het afnemen van cyberverzekering of andere manier van het afdekken van de risico's.

Effectiviteit van de beveiligingsmaatregelen

Effectiviteit van de beveiligingsmaatregelen is het risicoverminderende voordeel dat de beveiligingsmaatregelen zouden hebben, afhankelijk van hoe goed de maatregelen worden geïmplementeerd.
De core voor <voorbeeld>. is 41,770, wat gedeeltelijk is.

	Web Application Attacks	Point of Sale Intrusion	Insider and Privilege Misuse	Miscellaneous Errors	Physical Theft and Loss	Crimeware	Payment Card Skimmers	Cyber Espionage	Denial of Service Attacks	Everything Else
Servers & Apps	41,73	11,01	42,92	46,48		43,33		42,22	42,06	43,33
Netwerk	41,61	10,26	43,25	44,10		42,91		42,97	39,14	40,23
End-User Systemen	44,04	11,48	43,49	49,42	44,57	44,34		43,42	45,79	44,34
Terminal	40,15	11,07	43,30			42,07	42,31	42,97	46,23	42,07
ICS/SCADA/OT	41,58		42,76	45,73		41,34		42,36	42,10	41,34
Healthcare Systemen	40,15		43,30			42,07		42,97	46,23	42,07
Onboard Systemen	40,15		43,30			42,07		42,97	46,23	42,07
Critical IoT	42,08	11,07	43,30			42,07		43,27	46,23	42,98
Non-Critical IoT	42,08		43,30			42,07		43,27	46,23	42,98
Media & Offline Data			43,65	50,60	48,16					
Mensen	40,51		53,86	49,68	48,84	48,44		48,44	53,33	48,44

Opmerking: een lege cel geeft aan dat een risicoscenario niet is meegewogen voor het bepalen van de effectiviteit van de maatregel. Dit is gedaan omdat die niet van toepassing is, of het Basis risico dat aan het scenario is verbonden, "Zeer laag" is. Een waarde van 0,00 geeft aan dat er ten minste een 'laag' risico is voor een scenario, en het profiel van uw organisatie cyberbeveiligingsmaatregelen bevat om dat scenario te beperken. Dlt is gebaseerd op basis van de antwoorden van uzelf of juist het ontbreken van antwoord op vragen.

De kleur van de cel geeft de mate van effectiviteit van de maatregel weer. Hoe donkerder de cel, hoe groter de effectiviteit van de maatregel.

CIS Critical Security Control (CSC) Alignment Score

CIS Critical Security Control (CSC) Alignment Score is een maatstaf voor implementatie van kritieke beveiligingsmaatregelenen gecombineerd met de de kwaliteit van deze maatregelen. Deze score is geen maatstaf voor compliance. Houd er rekening mee dat de maatregel niet noodzakelijkerwijs hoeft samen te hangen met het individuele scenario's voor <Voorbeeld>. Met andere woorden, het implementeren van onderstaande beveiligingsmaatregel met de laagste score, levert waarschijnlijk de minste reductie op voor het risicoprofiel. In plaats daarvan zou <Voorbeeld> juist de prioriteit moeten geven aan de maatregelen met de hoogste score.

Rank	Score	Beveiligingsmaatregels	Rank	Score	Beveiligingsmaatregels
1	20,00%	Inventarisatie van geautoriseerde en niet-geautoriseerde apparaten	11	20,00%	Veilige configuraties voor netwerkapparaten
2	20,00%	Inventarisatie van geautoriseerde en niet-geautoriseerde software	12	20,00%	Netwerk segmentatie
3	45,00%	Continue testen en beheersen van kwetsbaarheden	13	60,00%	Gegevensbescherming
4	20,00%	Gecontroleerd gebruik van administratieve privileges	14	55,00%	Gecontroleerde toegang tot systemen
5	30,00%	Veilige configuratie voor hardware en software	15	70,00%	Draadloze toegangscontrole
6	70,00%	Onderhoud, Monitoring en Analyse van Audit logs	16	65,00%	Account Monitoring and Control
7	45,00%	Bescherming van e-mail en webbrowser	17	55,00%	Beveiligingsvaardigheden toetsing and training
8	70,00%	Malware afweer	18	20,00%	Applicatie beveiliging
9	45,00%	Beperking en controle van netwerkpoorten	19	45,00%	Incident Response and Management
10	60,00%	Data Recovery-mogelijkheid	20	20,00%	Penetratietests en Red Team oefeningen

Resterende risicoverminderende kwaliteitsindex

Dit is een lijst met beveiligingsmaatregelendie het Resterend risico het meest effectief verlaagd. Een organisatie kan door implementatie van deze beveiligingsmaatregelenhaar Resterend risico - zoals vermeld in het score overzicht - verbeteren. De lijst is gebaseerd op een totaal aantal van 110 risicoscenarios die van toepassing zouden kunnen zijn op <Voorbeeld>. ‚Hierbij is het uitgangspunt dat de maatregel volledig is geïmplementeerd en er geen verandering in het risicolandschap optreed. De indexwaarden aan de rechterkant bieden een meting van het effect van elke beveiligingsmaatregel op het resterende risico. Hoewel deze analyse niet de kosten bevat om de maatregelen volledig te implementeren, kan uw organisatie deze gegevens gebruiken om prioriteit te geven in uw budget.

Rank	Maatregel	Index
1	12. Netwerk segmentatie	*
2	1. Inventarisatie van geautoriseerde en niet-geautoriseerde apparaten	0,875
3	4. Gecontroleerd gebruik van administratieve privileges	0,873
4	2. Inventarisatie van geautoriseerde en niet-geautoriseerde software	0,787
5	19. Incident Response and Management	0,691
6	13. Gegevensbescherming	0,685
7	20. Penetratietests en Red Team oefeningen	0,681
8	9. Beperking en controle van netwerkpoorten	0,676
9	14. Gecontroleerde toegang tot systemen	0,596
10	5. Veilige configuratie voor hardware en software	0,535
11	17. Beveiligingsvaardigheden toetsing and training	0,490
12	11. Veilige configuraties voor netwerkapparaten	0,473
13	3. Continue testen en beheersen van kwetsbaarheden	0,467
14	7. Bescherming van e-mail en webbrowser	0,441
15	18. Applicatie beveiliging	0,337
16	8. Malware afweer	0,329
17	16. Account Monitoring and Control	0,309
18	6. Onderhoud, Monitoring en Analyse van Audit logs	0,243
19	10. Data Recovery-mogelijkheid	0,192
20	15. Draadloze toegangscontrole	0,146

Basis risico - details

Het 'Basis risico' is het het Cyberrisico en de impact op de organisatie, zonder de impact van Cybersecurity maatregelen. De score voor <voorbeeld>. is 21,786, wat Hoog is.

	Web Application Attacks	Point of Sale Intrusion	Insider and Privilege Misuse	Miscellaneous Errors	Physical Theft and Loss	Crimeware	Payment Card Skimmers	Cyber Espionage	Denial of Service Attacks	Everything Else
Servers & Apps	24,390	10,003	32,750	13,052	0,415	23,596	0,170	33,447	27,867	17,546
Netwerk	6,005	5,044	21,728	7,274	0,415	12,517	0,170	18,399	28,493	8,724
End-User Systemen	9,647	9,816	26,498	9,102	11,432	19,542	1,074	28,551	6,354	14,436
Terminal	16,975	10,097	28,274	1,996	0,368	11,547	8,118	23,222	7,828	9,113
ICS/SCADA/OT	19,530	0,000	35,980	14,256	0,432	26,364	0,199	38,186	18,580	20,162
Healthcare Systemen	11,687	0,000	30,864	2,180	0,391	11,576	0,167	25,407	8,559	10,049
Onboard Systemen	6,069	0,000	30,282	2,165	0,391	11,576	0,176	25,307	8,559	10,130
Critical IoT	8,129	10,477	31,681	3,486	3,430	23,368	1,128	25,808	17,118	10,280
Non-Critical IoT	4,270	0,000	12,097	0,762	0,157	4,698	0,068	10,498	7,372	3,943
Media & Offline Data	0,428	1,427	19,348	5,151	4,745	0,551	0,113	2,888	0,370	1,410
Mensen	8,380	2,634	30,925	11,284	5,661	14,263	0,147	16,925	6,366	11,821

Opmerking: in het bovenstaande diagram geven 0,000 de waarden aan dat het risico niet van toepassing is op het profiel van uw organisatie. De kleur van de cel geeft weer hoe vaak het risico zich kan voordoen. Hoe donkerder de cel, hoe groter het risico dat zich daardwerkelijk een incident voordoet.

Basis risico samenvatting

1. Basis risico: deze berekening is puur de vermenigvuldiging van de kans op het Cyberincindent en de impact van op uw organisatie.
2. Toepasselijkheid: 11 van de 11 risico's behoren tot het risicoprofiel van <voorbeeld>.
3. Hoogste Risico: wat betreft het 'Basis risico', is het scenario met het hoogste risico voor <voorbeeld> de co,binatie van Cyber Espionage en ICS/SCADA/OT.
Opmerking: AIG raadt het af om uitsluitend op basis van dit rapport een beslissing te nemen over het afnemen van cyberverzekering of andere manier van het afdekken van het risico.

Business Impact Details

Business impact de mate van impact op de vertrouwelijkheid, integriteit en beschikbaarheid van de bedrijfsmiddelen (o.a. data, IT infrastructuur, goederen, personeel etc.) van uw organisatie.
De Business Impact -score voor <voorbeeld> is 8,661, wat Erg hoog is.

	Web Application Attacks	Point of Sale Intrusion	Insider and Privilege Misuse	Miscellaneous Errors	Physical Theft and Loss	Crimeware	Payment Card Skimmers	Cyber Espionage	Denial of Service Attacks	Everything Else
Servers & Apps	7,222	6,719	7,572	7,572	7,932	7,572	7,572	7,572	8,426	7,572
Netwerk	7,222	6,782	7,572	7,572	7,932	7,572	7,572	7,572	8,426	7,572
End-User Systemen	5,984	6,594	6,271	6,271	6,358	6,271	7,321	6,271	8,143	6,271
Terminal	6,971	6,782	6,971	6,971	7,030	6,971	6,971	6,971	8,426	6,971
ICS/SCADA/OT	8,310	0,000	8,834	8,834	8,252	8,834	8,834	8,834	10,000	8,834
Healthcare Systemen	7,610	0,000	7,785	7,785	7,465	7,785	7,408	7,785	9,213	7,785
Onboard Systemen	7,610	0,000	7,785	7,785	7,465	7,785	7,785	7,785	9,213	7,785
Critical IoT	7,485	7,045	7,747	7,747	7,408	7,747	7,747	7,747	9,213	7,747
Non-Critical IoT	3,647	0,000	3,006	3,006	3,006	3,006	3,006	3,006	3,968	3,006
Media & Offline Data	5,041	4,412	5,014	5,014	5,226	5,014	5,014	5,014	5,154	5,014
Mensen	6,173	5,544	6,523	6,523	6,358	6,523	6,523	6,523	6,852	6,523

Opmerking: in het bovenstaande diagram geven 0.000 waarden aan dat het risicoscenario niet van toepassing is op het profiel van de klant. De kleur van de cel geeft de mate van bedrijfsimpact weer. Hoe donkerder de cel, hoe groter de impact van het bedrijf.

Business Impact Samenvatting

1. Business Impact profiel: is gebaseerd op specifieke antwoorden uit het ingevulde vragenformulier.
2. Toepasselijkheid: 11 van de 11 risico's behoren tot het risicoprofiel van <voorbeeld>.
3. Meest kritieke bedrijfsmiddel: in termen van business impact is ICS/SCADA/OT het meest kritieke bedrijfsmiddel.

Opmerking: AIG raadt het af om uitsluitend op basis van dit rapport een beslissing te nemen over het afnemen van cyberverzekering of andere manier van het afdekken van het risico.