Cyber Insurance

EXECUTIVE SUMMARY REPORT

Prepared for

CLIENT NAME HERE

Industry Vertical	Finance and Insurance
Region(s)	United States, Canada, Europe, Russia and South Africa
Annual Revenue	$136,000,000
Type of Records	PII, PCI

June 18, 2018

Cyber Report Overview

Congratulations on becoming an AIG Cyber Insured. As a policyholder who has completed the cyber insurance application process, you and your organization have elected to receive the following Executive Summary Report. This report provides additional detail from AIG's underwriting assessment of your account based on both the application you submitted and AIG's understanding of the cyber risk landscape.

If you have any questions regarding your Executive Summary Report, please contact either your AIG cyber insurance underwriter or e-mail us at CyberRiskConsulting@aig.com.

AIG Cyber Risk Assessment

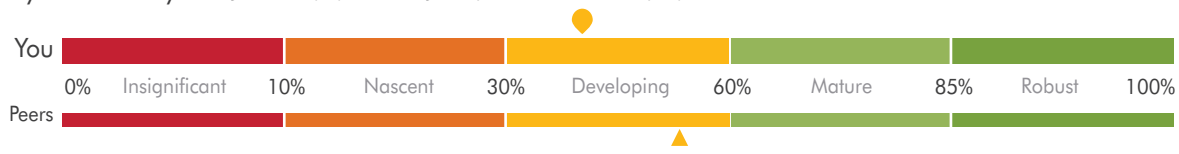
As a part of the underwriting process, AIG assesses cyber risk by utilizing a model that has at its core a patented method for which AIG has a license to and which measures and models cyber risk in economic terms. AIG extracts knowledge and insights from numerous datasets and client-specific answers (from the AIG Cyber Insurance Application) by:

- Measuring threat likelihood monthly from both internal and external sources, and using the updated data in modeling.
- Measuring and modeling business impact and control strength.
- Concluding residual risk scores, top risk scenarios, control implementation, and prioritized remediation guidance.
- Estimating cyber peril impact, probability, and expected loss ranges.

This report should not be viewed as a complete cyber risk assessment. Subjective answers, provided by the client within the AIG Cyber Insurance Application, may not be accurate. Due to emerging threats and other changing variables, the accuracy of this report diminishes over time. Additionally, impact values and probability values are calculated based on known ranges and representative and statistical curves. As such, there is a chance that a client falls outside of the range or curve due to uncertainty.

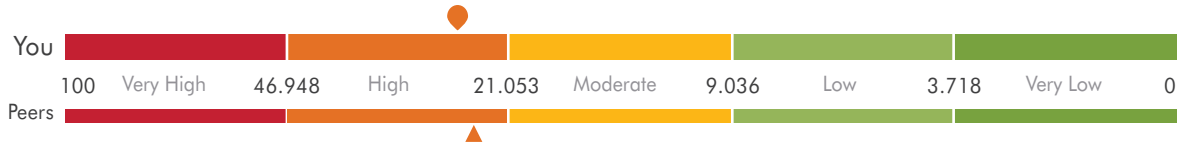
Cyber Risk Summary

Cyber Maturity
An organization's preparedness against cyber threats and its ability to protect its information assets.



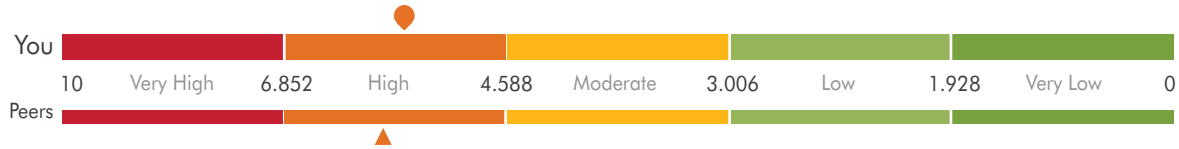
37.39%
Developing
▼ 14% Lower than Peers
54.84% Developing

Residual Risk
The remaining combination of threat and impact risk associated with an organization including benefits of cybersecurity controls.



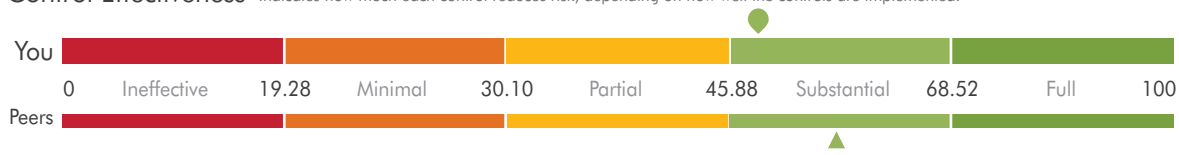
35.75
High
▲ 10% Higher than Peers
22.302 High

Threat Likelihood
The likelihood of a malicious or unintended action that may expose one or more weaknesses within an organization's IT ecosystem.



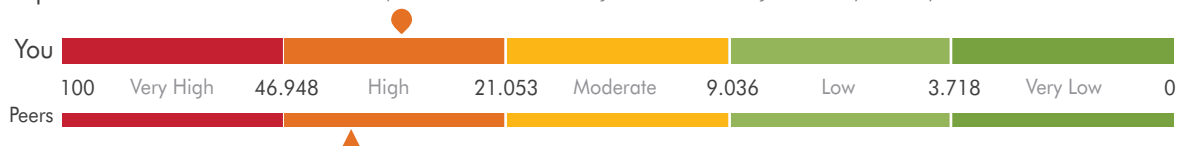
5.052
High
▼ 20% Lower than Peers
5.023 High

Control Effectiveness
Indicates how much each control reduces risk, depending on how well the controls are implemented.



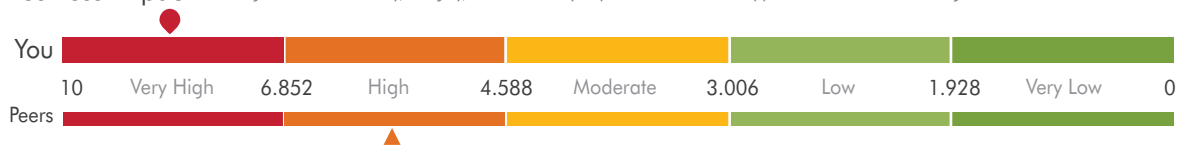
48.75
Substantial
▼ 30% lower than Peers
59.53 Substantial

Implicit Risk
The combination of threat and impact risk associated with an organization not including benefits of cybersecurity controls.



37.749
High
▲ 8% Higher than Peers
38.077 High

Business Impact
The degree of confidentiality, integrity, and availability impact associated with applicable assets within an organization.



7.952
Very High
▼ 11% Higher than Peers
6.023 High

About Peer Benchmarking:

This report includes information about how <Client Name> compares to its peers with respect to its cyber risk landscape, including threat likelihood, business impact in the event of a cyber incident, and control strength. Each peer group to which a company is compared is determined by the company's primary industry vertical, annual revenue tier, and the country in which the application is submitted to AIG. The peer group contains the most recent cyber risk assessments AIG has done for each company which matches those firmographic specifications in the past eighteen months. The peer group <Client Name> has 100 - 499 peers within it (AIG does not provide the specific number of peers, but does provide a range for context).

Prioritized Practices

This is a listing of the top risk reducing practices in AIG's Cyber Insurance Application which the client has not already implemented. This list is based upon the current threat likelihood as outlined in the Threat Likelihood Details section of this report, and may change with a shift in threat landscape. The index values to the right measure the reduction in residual risk associated with the implementation of each practice relative to the practice with the greatest risk reducing quality.

Rank	Questionnaire Section	Questionnaire Subsection	Question Number	Question Description	Index of Relative Risk Reducing Quality
1	Control	General	15	Change Control	*
2	Control	DoS	1	DoS Mitigation	0.202
3	Control	Server/Apps	2	DLP Solution	0.148
4	Control	n/a	11	PCI DSS Certification	0.147
5	Control	WebApp	13	Incident Response	0.129
6	Control	WebApp	12	Application Lifecycle and Code Review	0.112
7	Control	WebApp	9	Multifactor Authentication and Least Privilege Access	0.105
8	Control	WebApp	1	Asset Discovery	0.102
9	Control	General	16	Multifactor Authentication	0.100
10	Control	Server/Apps	7	Multifactor Authentication	0.096

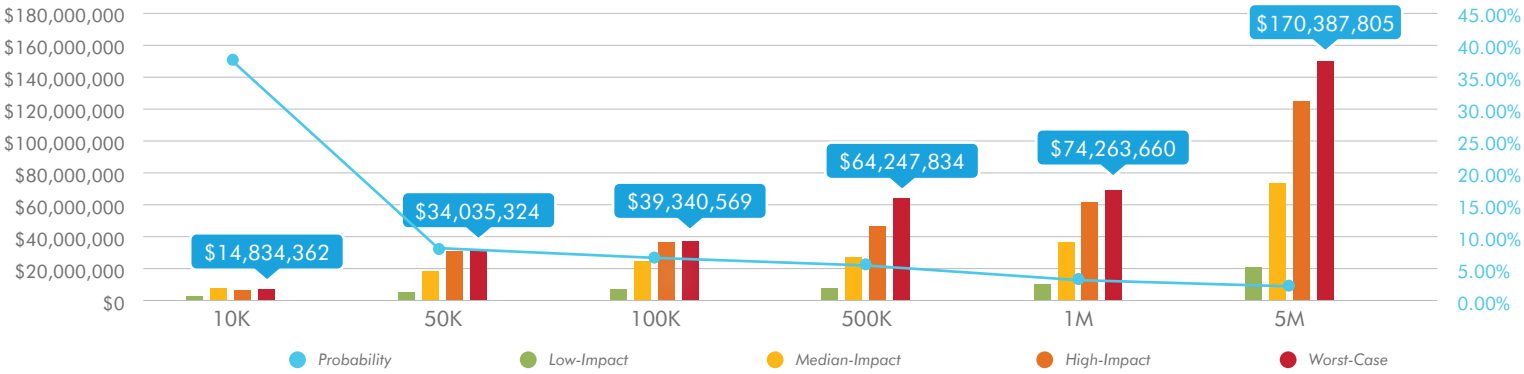
Note: The above questions were either not answered during the application process or were answered in a way that suggests the practice(s) may not be fully implemented.

Data Breach: Cyber Incident Probability and Impact

DATA BREACH EXPECTED LOSS
$15.3 million
(Breach - Median Impact Scenario)

DATA BREACH PROBABILITY
0.23%
(5 million records)

DATA BREACH WORST-CASE SCENARIO
$170.38 million
(5 million records)



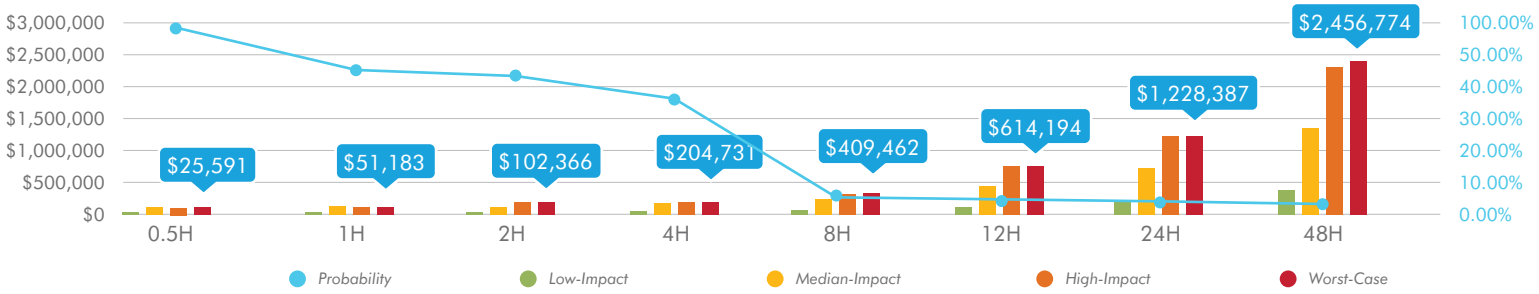
Breach Volume (Records)	Probability	Low-Impact Breach	Median-Impact Breach	High-Impact Breach	Worst-Case Breach
10K	38.288%	$579,187	$2,647,998	$4,716,808	$14,834,362
50K	8.432%	$1,328,862	$6,075,452	$10,822,043	$34,035,324
100K	1.935%	$1,535,998	$7,022,461	$12,508,925	$39,340,569
500K	1.057%	$3,524,170	$11,976,367	$20,428,564	$64,247,834
1M	0.756%	$4,073,566	$13,843,406	$23,613,246	$74,263,660
5M	0.235%	$9,346,240	$31,761,801	$54,177,362	$170,387,805

Denial of Service Interruption: Cyber Incident Probability and Impact

INTERRUPTION EXPECTED LOSS
$102,000
(DoS Attack - Median Impact Scenario)

INTERRUPTION PROBABILTY
2.31%
(DoS Attack - 48 hours)

INTERRUPTION WORST-CASE SCENARIO
$2.45 million
(DoS Attack - 48 hours)



Interruption Duration (Hours)	Probability	Low-Impact Interruption	Median-Impact Interruption	High-Impact Interruption	Worst-Case Interruption
0.5H	98.70%	$2,083	$5,606	$9,130	$25,591
1H	45.19%	$4,166	$11,212	$18,259	$51,183
2H	43.83%	$8,331	$22,425	$36,518	$102,366
4H	38.43%	$16,663	$44,849	$73,036	$204,731
8H	4.42%	$33,325	$89,699	$146,072	$409,462
12H	3.34%	$49,998	$134,548	$219,108	$614,194
24H	2.75%	$99,975	$269,096	$438,216	$1,228,387
48H	2.31%	$199,951	$538,191	$876,432	$2,456,774

Residual Risk Details

Residual risk is the remainder of risk associated with an organization. It accounts for the benefits of implemented risk reducing cybersecurity controls.
The Residual Risk score for <Client Name Here> is 35.75, which is HIGH.

	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	29.100	16.205	14.213	8.955	0.389	13.580	0.530	10.580	28.664	8.445
Network	6.900	6.429	9.597	4.995	0.393	7.702	0.512	6.142	22.118	4.569
End-User Systems	11.706	15.819	11.330	6.179	10.578	11.268	6.638	8.932	6.654	6.961
Terminal	19.825	16.098	11.652	1.370	0.339	6.358	24.014	6.992	5.452	4.196
ICS/SCADA/OT	23.533	0.000	16.057	10.665	0.398	15.849	0.633	12.515	26.387	10.136
Healthcare Devices	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Onboard Systems	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Critical IoT	9.318	14.696	12.907	2.374	3.162	12.720	6.596	7.652	6.451	4.694
Non-Critical IoT	4.840	0.000	5.373	0.566	0.145	2.788	0.215	3.394	2.538	1.963
Media & Offline Data	0.677	2.570	10.042	3.856	4.567	0.711	0.651	1.181	0.797	0.889
People	11.287	4.561	13.890	8.707	5.411	9.845	0.844	6.337	6.867	6.824

Note: In the above chart, 0.000 values represent that the risk scenario is not applicable for the client's profile. The color of the cell represents the degree of residual risk. The darker the cell, the greater the residual risk.

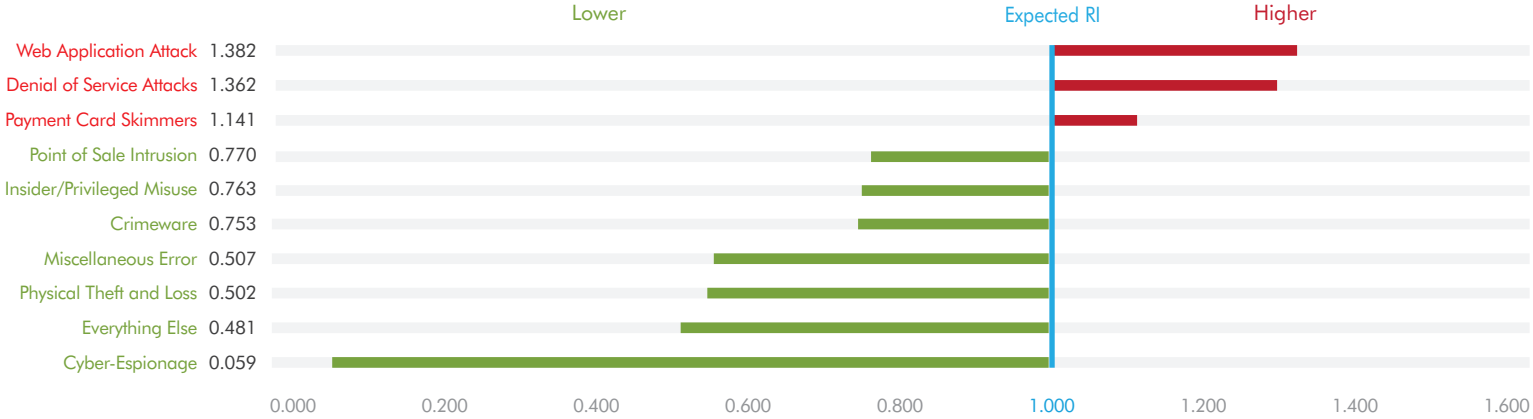
Top 10 Residual Risk Scenarios

Rank	Residual Risk Scenario	Residual Risk Score	Residual Risk Scale
1	Web Application Attacks: Servers and Apps	29.100	High
2	Denial of Service Attacks: Servers and Apps	28.644	High
3	Denial of Service Attacks: ICS/SCADA/OT	26.387	High
4	Payment Card Skimmers: Terminal	24.014	High
5	Web Application Attacks: ICS/SCADA/OT	23.533	High
6	Web Application Attacks: Terminal	19.825	Moderate
7	Point of Sale Intrusion: Servers and Apps	16.205	Moderate
8	Point of Sale Intrusion: Terminal	16.098	Moderate
9	Insider and Priviledge Misuse: ICS/SCADA/OT	16.057	Moderate
10	Crimeware: ICS/SCADA/OT	15.849	Moderate

Note: The top 10 residual risk scenarios are pulled directly from the Residual Risk Grid above and may be useful in prioritizing remediation and risk transfer decisions.

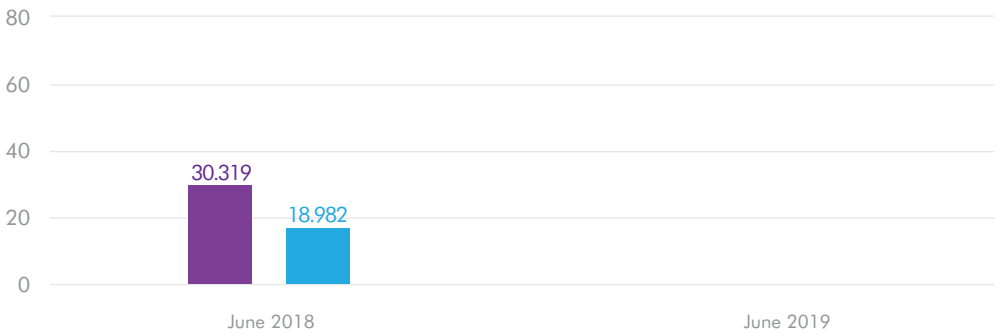
Risk Index per Threat Category

This is a measure of the organization's risk value associated with each of the applicable threat categories relative to the expected average risk value for that threat category amongst all organizations. A Risk Index greater than 1.000 indicates a heightened level of risk for an organization from that threat category. A Risk Index could be over 1.000 due to a heightened threat for that organization's industry, the business being particularly sensitive to the impact of that threat, weakness in the organization's control implementation as respects that threat, or a combination of all three. By ranking threats by their Risk Index score, from highest to lowest, and comparing their relative magnitudes, an organization can better understand the risk presented by different threats.



Note: In the above chart, 1.000 is the expected risk index value. If a risk index value is greater than 1.000, the risk is higher than expected. If a risk index value is lower than 1.000, the risk is lower than expected.

Baseline Risk Trending



Note: Future reports will illustrate trending from one assessment to the next. Being the first assessment, only baseline trend from Implicit (Inherent) Risk to Residual Risk is shown.

Implicit Risk The combination of threat and impact risk associated with an organization not including benefits of cybersecurity controls.

Residual Risk The remaining combination of threat and impact risk associated with an organization including benefits of cybersecurity controls.

Threat Likelihood Details

Threat likelihood is the likelihood of a malicious or unintended action, which could expose weaknesses within an organization's information technology ecosystem.
The Threat Likelihood score for <Client Name Here> is 5.052, which is HIGH.

	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	9.991	2.979	4.470	2.755	0.102	4.457	0.128	3.427	9.000	2.772
Network	2.460	1.488	2.966	1.536	0.102	2.364	0.128	1.885	6.750	1.378
End-User Systems	4.769	2.978	4.367	2.320	3.506	4.457	1.655	3.532	2.250	2.753
Terminal	7.204	2.977	4.192	0.458	0.102	2.369	6.618	2.585	1.800	1.564
ICS/SCADA/OT	6.953	0.968	4.209	2.580	0.102	4.268	0.128	3.353	6.300	2.730
Healthcare Devices	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Onboard Systems	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Critical IoT	3.213	2.663	4.226	0.719	0.903	4.314	1.655	2.585	1.980	1.587
Non-Critical IoT	3.464	0.895	4.159	0.405	0.102	2.235	0.128	2.710	1.890	1.569
Media & Offline Data	0.251	0.647	3.988	1.642	1.771	0.157	0.128	0.447	0.174	0.336
People	4.016	0.951	4.900	2.765	1.736	3.127	0.128	2.013	2.430	2.168

Note: In the above chart, 0.000 values represent that the risk scenario is not applicable for the client's profile. The color of the cell represents the degree of threat likelihood. The darker the cell, the greater the threat likelihood.

Threat Summary:

1. Industry Baseline: The threat likelihood profile was built from an objective industry baseline (<CLIENT INDUSTRY>) and answers from AIG's Cyber Insurance Application.
2. Applicability: <NUMBER OF ASSETS> of the 11 asset groups pertain to <<CLIENT NAME>>.
3. Primary Threat: <PRIMARY THREAT> is the most likely threat category.

Note: AIG does not recommend making cyber risk remediation or transfer decisions solely from the threat details within this section of the report.

Control Effectiveness Details

Control effectiveness is the synergistic risk reducing benefit the cybersecurity controls have depending on how well the controls are implemented.
The Control Effectiveness score for <Client Name Here> is 48.75, which is SUBSTANTIAL.

	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	57.72	15.89	57.05	56.10	52.73	58.84	43.90	58.30	60.43	58.84
Network	58.91	32.55	54.75	54.51	52.20	54.45	43.90	54.44	57.29	53.64
End-User Systems	57.51	17.05	57.48	56.35	53.46	58.57	43.90	58.56	61.45	58.57
Terminal	57.04	15.57	57.03	53.69	52.73	58.51	43.90	58.17	60.51	58.51
ICS/SCADA/OT	57.33	15.86	56.82	53.20	52.73	57.97	43.90	57.76	58.12	57.97
Healthcare Devices	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Onboard Systems	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Critical IoT	57.27	15.57	57.03	53.55	52.73	58.51	43.90	58.34	60.51	58.38
Non-Critical IoT	57.27	15.57	57.03	53.55	52.73	58.51	43.90	58.34	60.51	58.38
Media & Offline Data	44.18	14.49	50.59	53.93	51.78	11.20	0.00	48.14	0.00	48.14
People	52.89	16.94	57.08	52.33	51.92	52.34	0.00	52.34	58.76	52.34

Note: In the above chart, 0.000 values represent that the risk scenario is not applicable for the client's profile. The color of the cell represents the degree of control effectiveness. The darker the cell, the greater the control effectiveness.

CIS Critical Security Control (CSC) Alignment Score

The CIS Critical Security Control Alignment Score is a measure of an organization's implementation of the Center for Internet Security's (CIS') Critical Security Controls for Effective Cyber Defense combined with the synergistic risk reducing quality of those controls. This score is not a measurement of compliance. Please note that the alignment score for a particular control does not necessarily correlate to the individual scenarios that present the most residual risk to <CLIENT NAME HERE>. Implementing a control with the lowest alignment score may not provide the greatest reduction to remaining aggregated risk. Instead, <CLIENT NAME HERE> should consider prioritizing the controls with the most "remaining aggregated risk reducing quality".

Control	Score	Control Name	Control	Score	Control Name
1	48.32%	Inventory of Authorized and Unauthorized Devices	11	64.38%	Secure Configurations for Network Devices
2	68.22%	Inventory of Authorized and Unauthorized Software	12	53.59%	Boundary Defenses
3	48.32%	Secure Configuration for Hardware and Software	13	26.28%	Data Protection
4	59.09%	Continuous Vulnerability Assessment and Remediation	14	48.32%	Controlled Access Based on the Need to Know
5	58.49%	Controlled Use of Administrative Privileges	15	56.18%	Wireless Access Control
6	56.75%	Maintenance, Monotring, and Analysis of Audit Logs	16	56.45%	Account Monitoring and Control
7	64.96%	Email and Web Browser Protections	17	37.95%	Security Skills Assessment and Training to Fill Gaps
8	62.55%	Malware Defenses	18	52.38%	Application Software Security
9	63.76%	Limitation and Control of Network Ports	19	59.09%	Incident Response and Management
10	71.06%	Data Recovery Capability	20	42.21%	Penetration Tests and Red Team Exercises

Remaining Aggregated Risk Reducing Quality Index

This is a prioritized listing of the Center for Internet Security's (CIS') Critical Security Controls for Effective Cyber Defense in order of how much each security control would reduce the risk scores of the 110 risk scenarios applicable to <Client Name Here>, assuming the control was fully implemented, and there was no change in threat likelihood. The index values to the right provide a relative measurement of each security control's effect on residual risk. While this analysis does not include the cost to fully implement the controls, the organization can combine this data with relative cost to prioritize control improvements.

Rank	Control Name	Index
1	13. Data Protection	*
2	14. Controlled Access Based on the Need to Know	0.940
3	12. Boundary Defenses	0.762
4	19. Incident Response and Management	0.747
5	17. Security Skills Assessment and Appropriate Training to Fill Gaps	0.727
6	3. Secure Configuration for Hardware and Software	0.726
7	1. Inventory of Authorized and Unauthorized Devices	0.703
8	8. Malware Defenses	0.701
9	9. Limitation and Control of Network Ports	0.695
10	5. Controlled Use of Administrative Privileges	0.686
11	7. Email and Web Browser Protections	0.643
12	2. Inventory of Authorized and Unauthorized Software	0.634
13	20. Penetration Tests and Red Team Exercises	0.550
14	4. Continuous Vulnerability Assessment and Remediation	0.534
15	16. Account Monitoring and Control	0.510
16	6. Maintenance, Monitoring, and Analysis of Audit Logs	0.475
17	11. Secure Configurations for Network Devices	0.398
18	15. Wireless Access Control	0.370
19	10. Data Recovery Capability	0.367
20	18. Application Software Security	0.333

Implicit Risk Details

Implicit risk is the overall risk or inherent risk associated with an organization. It is purely a combination of threat and impact associated with an organization. It does not include the benefits of cybersecurity controls. The Implicit Risk score for <Client Name Here> is 37.749, which is HIGH.

	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	68.826	19.268	33.092	20.398	0.822	32.994	0.946	25.369	72.437	20.518
Network	16.792	9.532	21.209	10.982	0.822	16.908	0.913	13.481	51.781	9.854
End-User Systems	27.552	19.071	26.647	14.157	22.726	27.196	11.833	21.553	17.260	16.801
Terminal	46.143	19.066	27.113	2.959	0.717	15.323	42.807	16.716	13.808	10.113
ICS/SCADA/OT	55.156	0.000	37.186	22.788	0.842	37.707	1.128	29.626	62.999	24.115
Healthcare Devices	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Onboard Systems	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Critical IoT	21.807	17.406	30.034	5.112	6.688	30.657	11.758	18.366	16.338	11.278
Non-Critical IoT	11.326	0.000	12.502	1.219	0.307	6.720	0.384	8.145	6.429	4.716
Media & Offline Data	1.213	3.005	20.324	8.370	9.472	0.800	0.651	2.277	0.797	1.714
People	23.959	5.491	32.365	18.266	11.254	20.657	0.844	13.297	16.650	14.317

Note: In the above chart, 0.000 values represent that the risk scenario is not applicable for the client's profile. The color of the cell represents the degree of implicit risk. The darker the cell, the greater the implicit risk.

Implicit Risk Summary:

1. Implicit Risk Calculation: Implicit risk is purely the multiplication of threat likelihood and business impact.
2. Applicability: <<NUMBER OF ASSETS>> of the 11 asset groups pertain to <<CLIENT NAME>>.
3. Highest Risk Scenario: In terms of implicit risk, the scenario which poses the greatest risk to <CLIENT NAME> is the intersection of <ATTACK PATTERN OF HIGHEST RISK SCENARIO> and <ASSET OF HIGHEST RISK SCENARIO>.

Note: AIG does not recommend making cyber risk remediation or transfer decisions solely from the implicit risk details within this section of the report.

Business Impact Details

Business impact is the degree of confidentiality, integrity, and availability impact associated with applicable assets within an organization.
The Business Impact score for <Client Name Here> is 7.952, which is VERY HIGH.

	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	6.889	6.468	7.403	7.403	8.056	7.403	7.403	7.403	8.049	7.403
Network	6.826	6.405	7.151	7.151	8.056	7.151	7.151	7.151	7.671	7.151
End-User Systems	5.777	6.405	6.102	6.102	6.482	6.102	7.151	6.102	7.671	6.102
Terminal	6.405	6.405	6.468	6.468	7.030	6.468	6.468	6.468	7.671	6.468
ICS/SCADA/OT	7.932	0.000	8.834	8.834	8.252	8.834	8.834	8.834	10.000	8.834
Healthcare Devices	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Onboard Systems	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Critical IoT	6.787	6.535	7.106	7.106	7.408	7.106	7.106	7.106	8.252	7.106
Non-Critical IoT	3.270	0.000	3.006	3.006	3.006	3.006	3.006	3.006	3.402	3.006
Media & Offline Data	4.834	4.645	5.096	5.096	5.350	5.096	5.096	5.096	4.588	5.096
People	5.966	5.777	6.605	6.605	6.482	6.605	6.605	6.605	6.852	6.605

Note: In the above chart, 0.000 values represent that the risk scenario is not applicable for the client's profile. The color of the cell represents the degree of business impact. The darker the cell, the greater the business impact.

Business Impact Summary:

1. Business Impact Profile: The business impact profile was built from specific answers in AIG's Cyber Insurance Application.
2. Applicability: <NUMBER OF ASSETS> of the 11 asset groups pertain to <CLIENT NAME>.
3. Most Critical Asset Group: In terms of business impact, <MOST CRITICAL ASSET GROUP> is the most critical asset group.

Note: AIG does not recommend making cyber risk remediation or transfer decisions solely from the business impact details within this section of the report.