Cyber Insurance

EXECUTIVE SUMMARY REPORT

Prepared for

CLIENT NAME HERE

Industry Vertical	Manufacturing
Region(s)	United States, Mexico, Central America, and Caribbean
Annual Revenue	$900,000,000
Type of Records	PII, PCI, PHI

July 27, 2020

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 CyberLossControl@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 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:

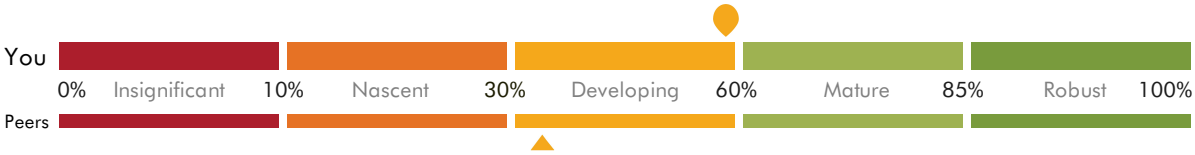
- Measuring threat likelihood monthly from both internal and external sources, and using the updated data in modeling.
- Measuring and modeling business impact and control strength.
- Concluding residual risk scores, top risk scenarios, control implementation, and prioritized remediation guidance.
-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

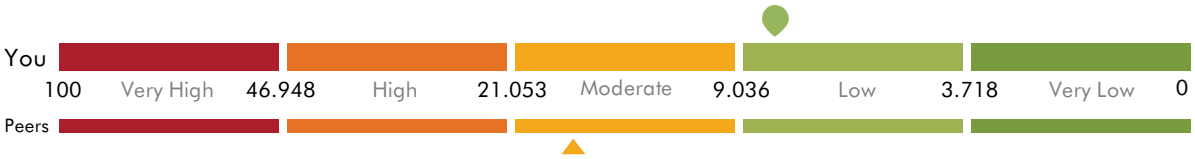
An organization's preparedness against cyber threats and its ability to protect its information assets.



58.83%
Developing
74% Better than Peers
33.89% Developing

Residual Risk

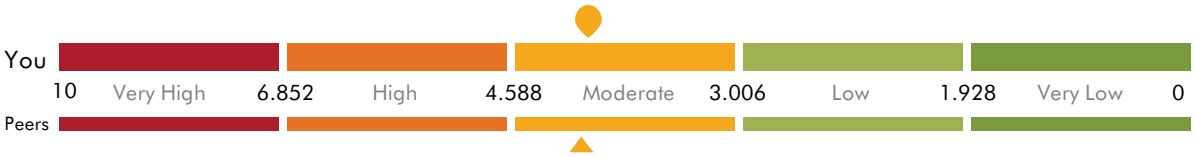
The remaining combination of threat and impact risk associated with an organization including benefits of cybersecurity controls.



8.252
Low
54% Better than Peers
17.803 Moderate

Threat Likelihood

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



4.057
Moderate
1% Better than Peers
4.106 Moderate

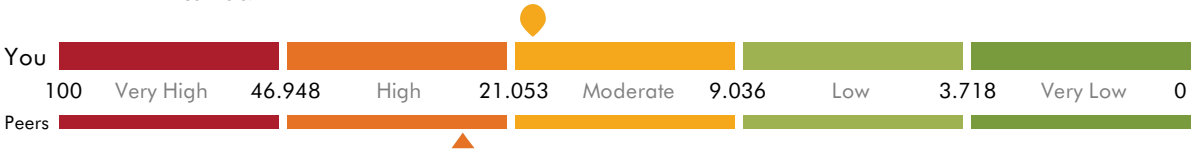
Control Effectiveness

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

55.48%
Substantial
65% Better than Peers
33.65% Partial

Implicit Risk

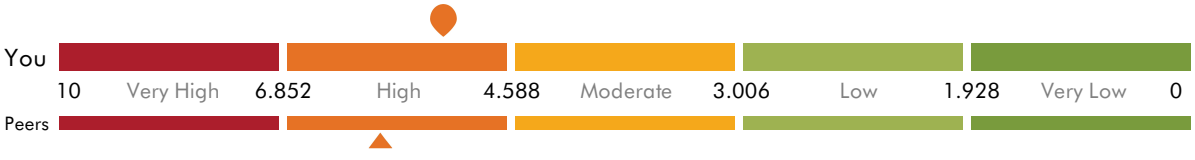
The combination of threat and impact risk associated with an organization not including benefits of cybersecurity controls.



20.045
Moderate
23% Better than Peers
26.178 High

Business Impact

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



5.236
High
11% Better than Peers
5.885 High

About Peer Benchmarking:

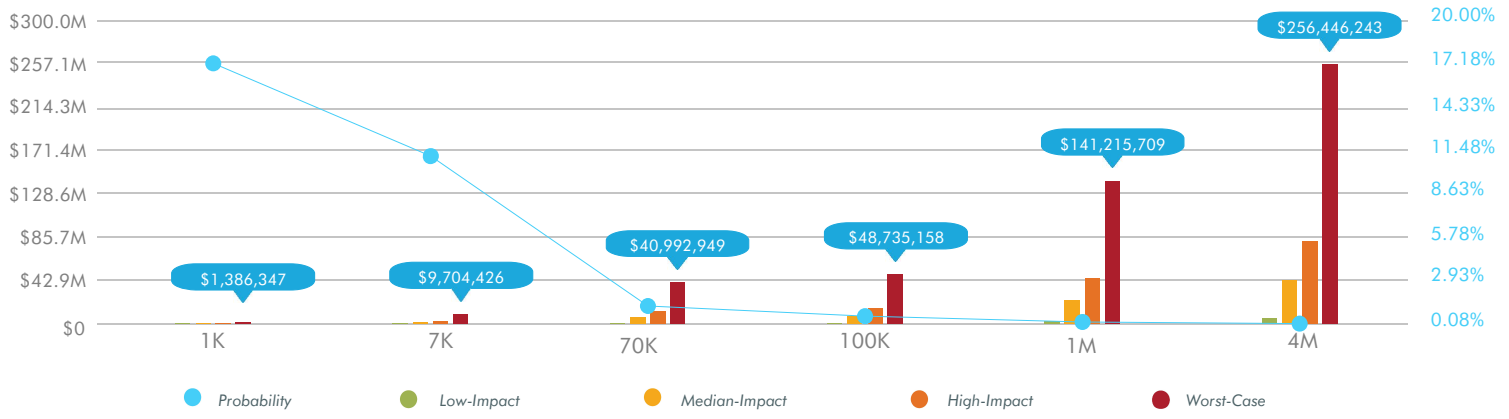
This report includes information about how <CLIENT NAME HERE> compares to its peers with respect to its cyber risk landscape, including threat likelihood, business impact in the event of a cyber incident, and control strength. Each peer group to which a company is compared is determined by the company's 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 HERE> has 10 - 99 peers within it (AIG does not provide the specific number of peers, but does provide a range for context).

Data Breach: Cyber Incident Probability and Impact

DATA BREACH EXPECTED LOSS
$3.31 million
(Breach – Median Impact Scenario)

DATA BREACH PROBABILITY
0.08%
(4 million records)

DATA BREACH WORST-CASE SCENARIO
$256.44 million
(4 million records)



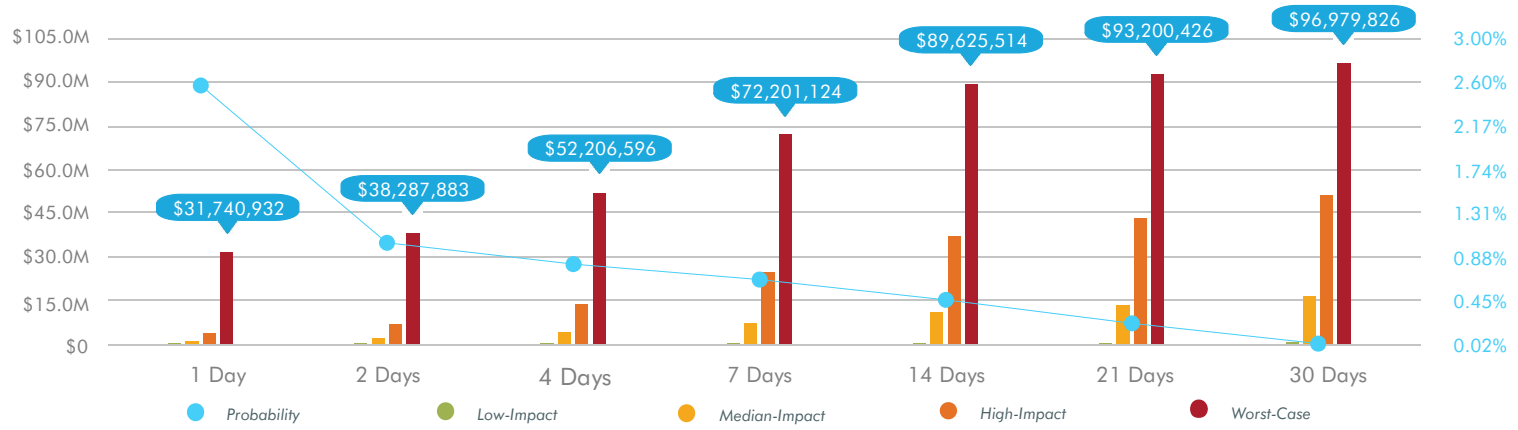
Breach Volume (Records)	Probability	Low-Impact Breach	Median-Impact Breach	High-Impact Breach	Worst-Case Breach
1K	17.13%	$37,177	$238,993	$440,810	$1,386,347
7K	11.07%	$260,236	$1,672,952	$3,085,668	$9,704,426
70K	1.25%	$946,304	$6,990,314	$13,034,324	$40,992,949
100K	0.57%	$985,919	$8,240,997	$15,496,076	$48,735,158
1M	0.21%	$2,614,722	$23,758,189	$44,901,656	$141,215,709
4M	0.08%	$5,478,448	$43,509,692	$81,540,936	$256,446,243

Ransomware: Cyber Incident Probability and Impact

RANSOMWARE EXPECTED LOSS
$3.49 million
(Ransomware Attack -Median Impact Scenario)

RANSOMWARE PROBABILITY
0.02%
(Ransomware Attack- 30 days)

RANSOMWARE WORST-CASE SCENARIO
$96.97 million
(Ransomware Attack- 30 days)



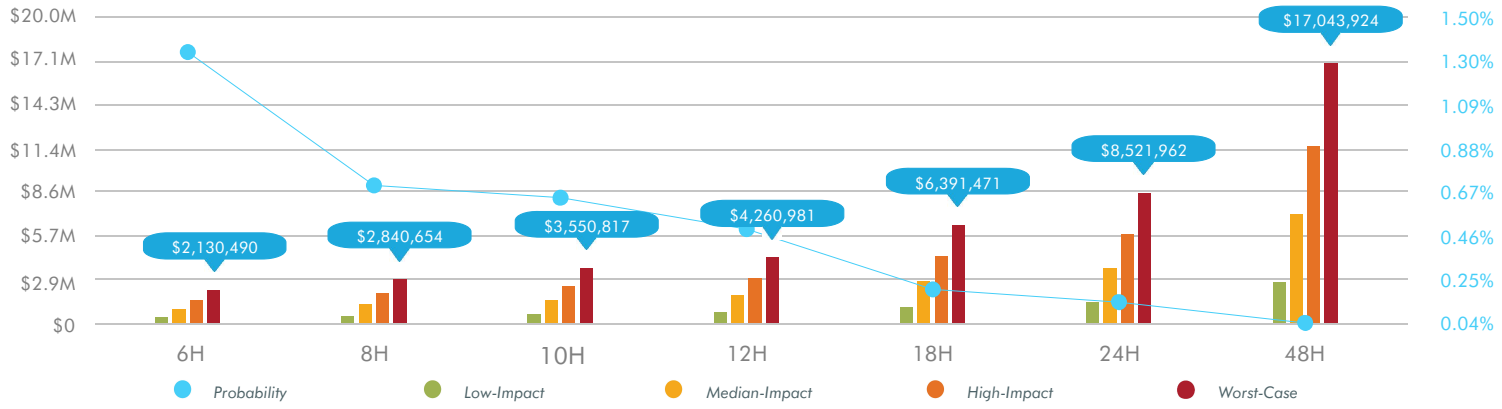
Ransomware Duration (Days)	Probability	Low-Impact Ransomware	Median-Impact Ransomware	High-Impact Ransomware	Worst-Case Ransomware
1 Day	2.55%	$14,088	$1,029,549	$3,618,914	$31,740,932
2 Days	1.01%	$25,353	$1,961,977	$6,877,811	$38,287,883
4 Days	0.80%	$48,921	$3,926,317	$13,726,421	$52,206,596
7 Days	0.65%	$94,659	$7,154,606	$24,740,579	$72,201,124
14 Days	0.45%	$188,280	$11,142,649	$37,097,534	$89,625,514
21 Days	0.22%	$267,907	$13,435,306	$43,376,868	$93,200,426
30 Days	0.02%	$370,061	$16,370,376	$51,425,255	$96,979,826

Denial of Service Interruption: Cyber Incident Probability and Impact

INTERRUPTION EXPECTED LOSS
$3.62 million
(DoS Attack – Median Impact Scenario)

INTERRUPTION PROBABILITY
0.04%
(DoS Attack - 48 hours)

INTERRUPTION WORST-CASE SCENARIO
$17.04 million
(DoS Attack - 48 hours)



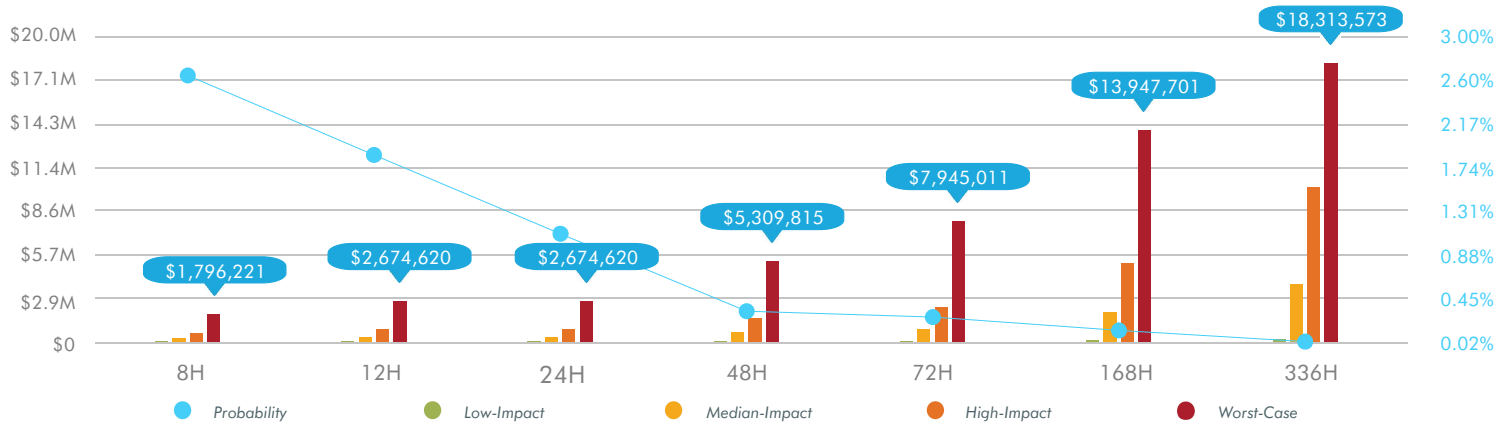
Interruption Duration (Hours)	Probability	Low-Impact Interruption	Median-Impact Interruption	High-Impact Interruption	Worst-Case Interruption
6H	1.34%	$331,027	$891,000	$1,450,973	$2,130,490
8H	0.70%	$441,370	$1,188,000	$1,934,630	$2,840,654
10H	0.64%	$551,712	$1,485,000	$2,418,288	$3,550,817
12H	0.49%	$662,055	$1,782,000	$2,901,945	$4,260,981
18H	0.20%	$993,082	$2,673,000	$4,352,918	$6,391,471
24H	0.14%	$1,324,110	$3,564,000	$5,803,890	$8,521,962
48H	0.04%	$2,648,219	$7,128,000	$11,607,781	$17,043,924

Other Business Interruption: Cyber Incident Probability and Impact

INTERRUPTION EXPECTED LOSS
$307,324
(Other Attack - Median Impact Scenario)

INTERRUPTION PROBABILITY
0.02%
(Other Attack- 336 hours)

INTERRUPTION WORST-CASE SCENARIO
$18.31 million
(Other Attack- 336 hours)



Interruption Duration (Hours)	Probability	Low-Impact Interruption	Median-Impact Interruption	High-Impact Interruption	Worst-Case Interruption
8H	2.63%	$7,140	$226,007	$576,241	$1,796,221
12H	1.85%	$10,607	$317,002	$820,449	$2,674,620
24H	1.08%	$10,607	$317,002	$820,449	$2,674,620
48H	0.32%	$21,008	$589,989	$1,553,073	$5,309,815
72H	0.26%	$31,410	$862,976	$2,285,698	$7,945,011
168H	0.13%	$73,015	$1,954,925	$5,216,194	$13,947,701
336H	0.02%	$145,194	$3,781,340	$10,176,207	$18,313,573

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	5	Administrative privileges	*
2	Control	General	1	Hardware inventory	0.852
3	Control	General	21	Access management	0.718
4	Control	Error	1	Employee behavior monitoring	0.664
5	Control	General	17	Network Segmentation	0.557
6	Control	General	11	Malware defense	0.352
7	Control	Server/Apps	12	Penetration testing	0.326
8	Control	General	13	Risk Assessment	0.309
9	Control	General	12	Port security	0.309
10	Control	General	20	DLP solution	0.307

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.

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 8.252, which is Low.

	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	10.897	2.643	12.114	12.123	0.993	12.000	0.328	5.822	10.652	9.776
Network	2.807	1.514	6.166	7.182	0.928	8.696	0.328	3.729	9.899	6.819
End-User Systems	5.759	2.574	8.938	7.691	4.984	9.251	1.285	3.990	3.726	5.742
Terminal	9.515	2.574	7.242	1.848	0.732	6.561	1.509	3.674	7.778	5.767
ICS/SCADA/OT	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
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	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Non-Critical IoT	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Media & Offline Data	0.804	0.000	11.171	4.476	2.411	2.008	0.000	2.929	0.359	3.484
People	3.325	0.000	9.868	9.846	1.581	5.861	0.000	2.909	2.954	7.891

Note: In the above chart, 0.00 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.

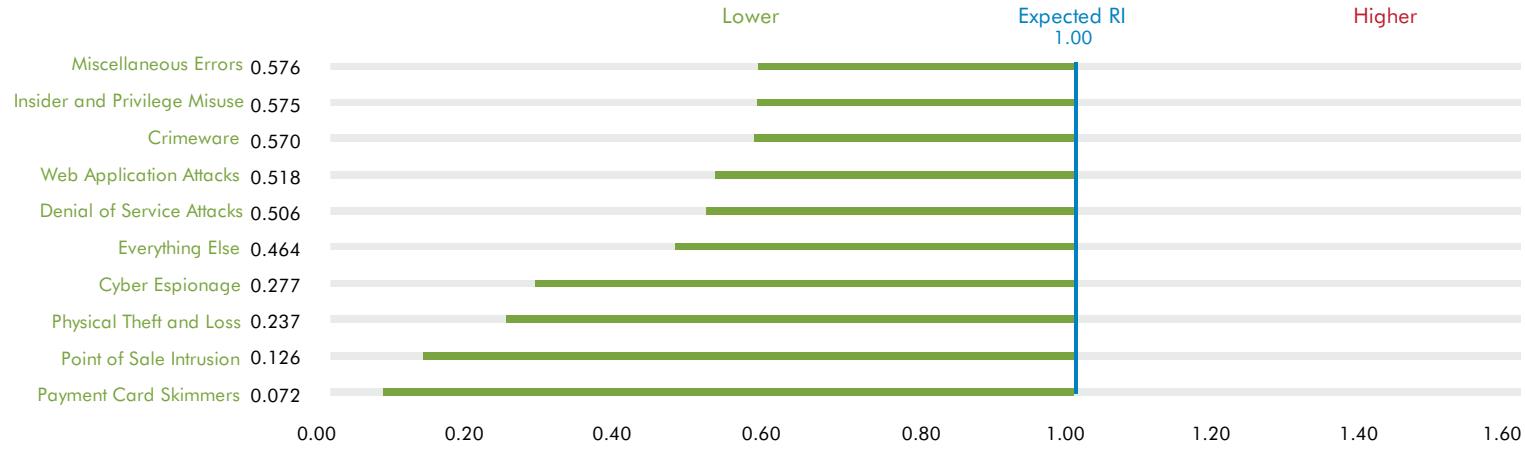
Top 10 Residual Risk Scenarios

Rank	Residual Risk Scenarios	Residual Risk Score	Residual Risk Scale
1	Miscellaneous Errors: Servers & Apps	12.123	Moderate
2	Insider and Privilege Misuse: Servers & Apps	12.114	Moderate
3	Crimeware: Servers & Apps	12.000	Moderate
4	Insider and Privilege Misuse: Media & Offline Data	11.171	Moderate
5	Web Application Attacks: Servers & Apps	10.897	Moderate
6	Denial of Service Attacks: Servers & Apps	10.652	Moderate
7	Denial of Service Attacks: Network	9.899	Moderate
8	Insider and Privilege Misuse: People	9.868	Moderate
9	Miscellaneous Errors: People	9.846	Moderate
10	Everything Else: Servers & Apps	9.776	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.

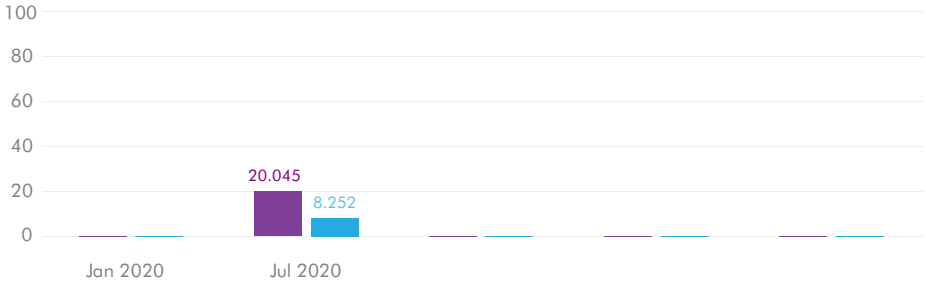
Risk Index per Threat Category

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 1.00 indicates a heightened level of risk for an organization from that threat category. A Risk Index could be over 1.00 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, 1.00 is the expected risk index value. If a risk index value is greater than 1.00, the risk is higher than expected. If a risk index value is lower than 1.00, 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 4.057, which is Moderate.

	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	6.315	3.557	3.408	4.084	0.193	5.463	0.065	2.065	6.637	4.280
Network	1.338	1.783	1.889	2.208	0.193	3.164	0.065	1.398	5.807	2.348
End-User Systems	2.569	3.557	3.413	3.906	2.611	5.463	0.266	2.075	1.659	4.255
Terminal	4.876	3.557	3.408	0.428	0.193	3.374	1.414	1.621	3.319	2.605
ICS/SCADA/OT	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
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	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Non-Critical IoT	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Media & Offline Data	0.237	0.465	4.018	2.089	1.378	0.521	0.065	0.760	0.128	0.904
People	3.425	1.532	4.131	4.087	1.255	3.633	0.065	1.649	1.452	3.443

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 HERE>.
3. Primary Threat: <PRIMARY THEAT> 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 55.48, 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	59.50	84.61	34.99	45.72		59.83		48.44	69.96	58.23
Network	51.80	82.64	37.70	37.92		47.55		49.09	68.65	44.57
End-User Systems	45.79	84.61	34.69	50.89	42.90	57.77		52.05	56.43	66.34
Terminal	56.03	84.61	50.72			54.91	77.33	47.43	54.53	48.66
ICS/SCADA/OT										
Healthcare Devices										
Onboard Systems										
Critical IoT										
Non-Critical IoT										
Media & Offline Data			27.88	44.41	63.68					
People	78.21		46.40	45.93	61.33	63.80		60.42	53.66	48.56

Note: A blank cell indicates that a risk scenario was not considered in determining control effectiveness because the asset is not applicable or the implicit risk associated with the scenario is "Very Low". A value of 0.00 indicates that there is at least "Low" implicit risk for a scenario, and the Applicant's profile does not include any cybersecurity controls to mitigate that scenario (based upon the Applicant's responses or lack of response to questions regarding controls AIG believes apply to the scenario).

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>. Thus, 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	23.70%	Inventory of Authorized and Unauthorized Devices	11	79.97%	Secure Configurations for Network Devices
2	79.50%	Inventory of Authorized and Unauthorized Software	12	44.63%	Boundary Defenses
3	39.90%	Continuous Vulnerability Assessment and Remediation	13	48.50%	Data Protection
4	4.70%	Controlled Use of Administrative Privileges	14	24.22%	Controlled Access Based on the Need to Know
5	63.30%	Secure Configuration for Hardware and Software	15	79.97%	Wireless Access Control
6	62.54%	Maintenance, Monitoring, and Analysis of Audit Logs	16	9.52%	Account Monitoring and Control
7	82.14%	Email and Web Browser Protections	17	81.42%	Security Skills Assessment and Appropriate Training to Fill Gaps
8	36.13%	Malware Defenses	18	53.09%	Application Software Security
9	7.92%	Limitation and Control of Network Ports	19	57.44%	Incident Response and Management
10	80.36%	Data Recovery Capability	20	36.26%	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	14. Controlled Access Based on the Need to Know	*
2	13. Data Protection	0.856
3	16. Account Monitoring and Control	0.797
4	12. Boundary Defenses	0.777
5	4. Controlled Use of Administrative Privileges	0.697
6	19. Incident Response and Management	0.643
7	20. Penetration Tests and Red Team Exercises	0.611
8	1. Inventory of Authorized and Unauthorized Devices	0.593
9	6. Maintenance, Monitoring, and Analysis of Audit Logs	0.518
10	8. Malware Defenses	0.490
11	9. Limitation and Control of Network Ports	0.431
12	3. Continuous Vulnerability Assessment and Remediation	0.403
13	17. Security Skills Assessment and Appropriate Training to Fill Gaps	0.379
14	18. Application Software Security	0.294
15	5. Secure Configuration for Hardware and Software	0.215
16	7. Email and Web Browser Protections	0.150
17	15. Wireless Access Control	0.127
18	2. Inventory of Authorized and Unauthorized Software	0.120
19	11. Secure Configurations for Network Devices	0.114
20	10. Data Recovery Capability	0.098

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 control. The Implicit Risk score for <CLIENT NAME HERE> is 20.045, which is Moderate.

	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	26.909	17.173	18.634	22.331	0.993	29.870	0.328	11.291	35.459	23.402
Network	5.824	8.719	9.898	11.570	0.928	16.581	0.328	7.325	31.575	12.304
End-User Systems	10.625	16.725	13.686	15.662	8.728	21.905	1.285	8.322	8.552	17.060
Terminal	21.640	16.725	14.697	1.848	0.732	14.550	6.657	6.989	17.104	11.234
ICS/SCADA/OT	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
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	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Non-Critical IoT	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Media & Offline Data	0.804	0.000	15.490	8.052	6.640	2.008	0.000	2.929	0.359	3.484
People	15.260	0.000	18.409	18.211	4.089	16.191	0.000	7.349	6.374	15.341

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 HERE>.
3. Highest Risk Scenario: In terms of implicit risk, the scenario which poses the greatest risk to <CLIENT NAME HERE> is the intersection of <ATTACK PATTERN OF HIGHEST RISK SCENARIO> & <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 5.236, 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	4.261	4.827	5.468	5.468	5.153	5.468	5.082	5.468	5.343	5.468
Network	4.353	4.890	5.241	5.241	4.812	5.241	5.082	5.241	5.437	5.241
End-User Systems	4.136	4.702	4.010	4.010	3.343	4.010	4.830	4.010	5.154	4.010
Terminal	4.438	4.702	4.312	4.312	3.797	4.312	4.708	4.312	5.154	4.312
ICS/SCADA/OT	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
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	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Non-Critical IoT	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Media & Offline Data	3.397	0.000	3.855	3.855	4.819	3.855	0.000	3.855	2.801	3.855
People	4.456	0.000	4.456	4.456	3.258	4.456	0.000	4.456	4.390	4.456

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 HERE>.
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.