Cyber Insurance

SUMMARIZED ASSESSMENT REPORT

Prepared for

<Client Name Here>

Industry Vertical: Finance and Insurance
Region(s): United States, Canada, Europe and Russia, Australia and New Zealand, Central and Southern Asia, East Asia and the Pacific, Mexico, Central America, and Caribbean, South America, Middle East and North Africa
Annual Revenue: $52,000,000,000
Type of Records: PII, PCI, PHI

May 17, 2018

Cyber Report Overview

Thank you for your interest in becoming an AIG Cyber insured. This is a report applicants can receive in conjunction with the cyber insurance application process. This report only illustrates summarized results 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 choose to purchase cyber insurance from AIG, you have the option to receive a longer, more detailed report that includes benchmarking information and may help you indicate top risk reducing controls for your organization.

We look forward to the opportunity to connect you with some of the world's top cybersecurity, law, and public relations experts to help you safeguard your organization against sensitive data breaches, computer hacking, employee error, and the unknown. If a claim does occur, our in-house cyber claims specialists will be ready to assist you. From innovative loss prevention tools to breach resolution, we are dedicated to help you stay ahead of the curve.

AIG Cyber Risk Assessment

As 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 underwriting questionnaire) 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.

Quick Score Summary

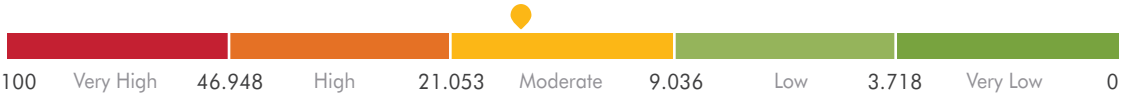
Cyber Maturity

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

42.53%
Developing

Residual Risk

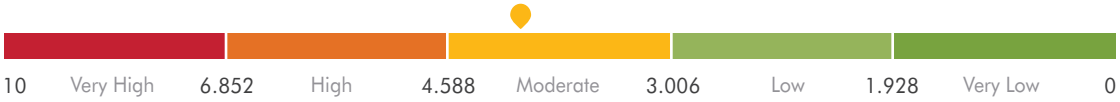
The remaining combination of threat and impact risk associated with an organization including benefits of cybersecurity controls.



13.757
Moderate

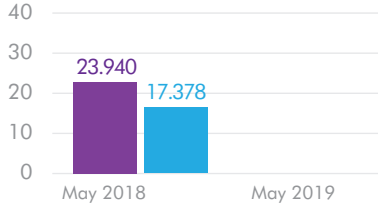
Threat Likelihood

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



3.887
Moderate

Baseline Risk Trending



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

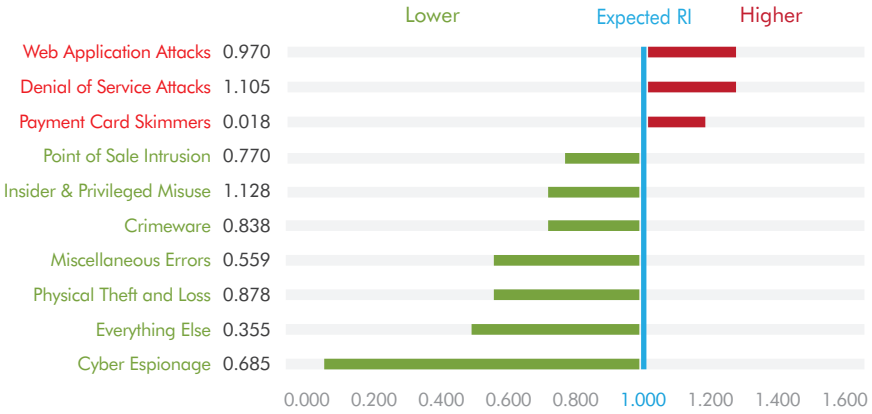
- Implicit Risk — The combination of threat and impact risk associated with an organization not including benefits of cybersecurity controls.
- Residual Risk

Top 5 Risk Scenarios

Rank	Risk Scenario
1	Insider and Privilege Misuse: Servers and Apps
2	Denial of Service Attacks: Servers and Apps
3	Denial of Service Attack: Network
4	Web Application Attacks: Servers and Apps
5	Physical Theft and Loss: End-User Systems

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 means an organization is at particular risk from that threat category. A Risk Index could be over 1.00 because it's a heightened threat for that organization's industry, the business is particularly sensitive to the impact of that threat, the organization's control implementation does not address that threat, or a combination of the three. By ranking threats by their Risk Index score from highest to lowest and comparing their relative magnitudes, an organization can better understand the threats against them.



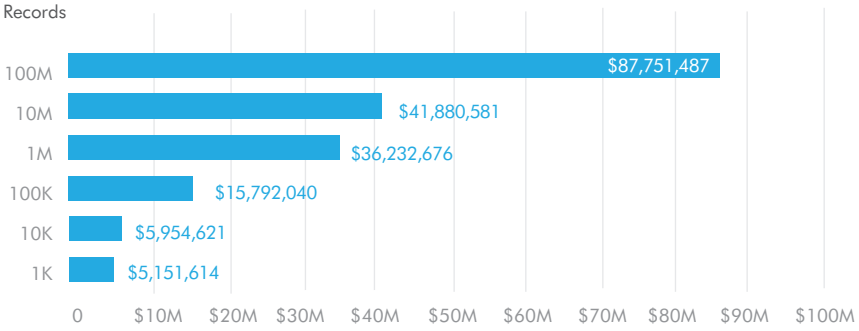
**Note: In the above chart, 1.0 is the expected risk index value. If a value is greater than 1.0, risk is higher than expected. If a value is lower than 1.0, then risk is lower than expected.*

Top 5 Risk Reducing Controls

This is a prioritized listing of the Center for Internet Security's (CIS) Critical Security Controls for Effective Cyber Defense, with the key actions that would most reduce the organization's overall Residual Risk score listed first. By implementing those controls which map to these key actions, an organization can better improve their Residual Risk score. Note that any change in the threat environment may re-prioritize these recommendations.

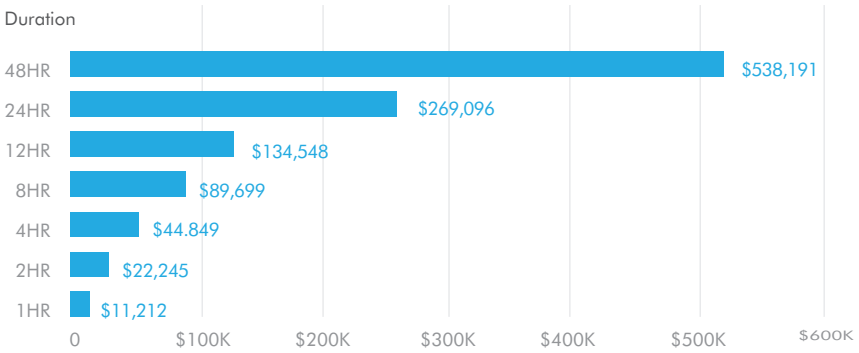
Rank	CIS Critical Security Control
1	19. Incident Response and Management
2	17. Security Skills Assessment and Appropriate Training to Fill Gaps
3	13. Data Protection
4	14. Controlled Access Based on the Need to Know
5	12. Boundary Defenses

Data Breach Impact (Median impact value per record volume)



Breach Volume (Records)	Low-impact Breach	High-impact Breach	Worst-case Breach
100M	$33,128,015	$174,201,553	$547,863,884
10M	$12,490,830	$92,277,608	$290,213,078
1M	$4,709,956	$34,795,404	$109,431,544
100K	$1,775,958	$13,120,118	$41,262,770
10K	$669,670	$4,947,274	$15,559,177
1K	$252,516	$1,865,495	$5,866,983

Denial of Service Interruption Impact (Median impact value per hour duration)



Interruption Duration	Low-impact Interruption	High-impact Interruption	Worst-case Interruption
48HR	$76,451,745	$335,106,366	$492,043,011
24HR	$38,225,873	$167,553,183	$246,021,505
12HR	$28,669,405	$125,664,887	$184,516,129
8HR	$19,112,936	$83,776,591	$123,010,753
4HR	$15,927,447	$69,813,826	$102,508,961
2HR	$12,741,958	$55,851,061	$82,007,168
1HR	$9,556,468	$41,888,296	$61,505,376