AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

A Strategic Third-Party Risk Assessment:

Fortune Insurance Organization

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

About the Client

The client is one of the largest mutual life insurance firms headquartered in New York. It offers a broad range of financial products, including life, dental, vision, and disability insurance, as well as retirement and investment services. With a strong focus on innovation and client support, the client aims to provide comprehensive, personalized coverage to meet the evolving needs of its diverse clientele.

Requirement

The client relied on numerous third-party agencies for tools, services, and operational support, raising concerns about potential exposure to third-party data breaches. As third-party service providers posed significant risks, the organization required a robust strategy to safeguard its operations and maintain regulatory compliance.

The following were the key requirements:

- The firm sought a Third-Party Risk Assessment (TPRA) in accordance with NYDFS (New York Department of Financial Services) and AMSIS (Agency Minimum Implementation Standard) regulations.

- With global operations and a growing number of vendors, the organization had limited visibility into vendor-related risks. Therefore, it required a strong evaluation, risk prioritization, and mitigation process for all third-party service providers.

02

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Key Highlights

Critical Vulnerabilities Identified

10

Medium-Severity Vulnerabilities Identified

6

Risk Visibility Achieved

Up to 95%

Assessment Completion Timeline

30 Days

Solution

To meet the client's regulatory and security objectives, Ampcus Cyber implemented a comprehensive Third-Party Risk Assessment framework. The approach was designed to align with existing enterprise risk methodologies while integrating the specific requirements of NYDFS and AMSIS.

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

The Ampcus Cyber Approach

Risk Assessment Methodology Review and Alignment

- Assessed the organization's existing Enterprise Risk Management (ERM) methodology and incorporated applicable regulatory standards, including NYDFS and AMSIS, into the risk assessment framework.
- Developed a clear and mutually agreed-upon scope and approach document to define the boundaries and expectations of the assessment.

Contract Review and Third-Party Classification

- Assisted in creating a Third-Party Information Register that included the classification of vendors based on service type and data access.
- Reviewed contracts and service agreements to identify security and compliance gaps.

04

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Risk Assessment and Risk Prioritization

- Conducted due diligence to document the necessity of each third-party relationship within the Third-Party Information Register.
- Followed a stringent risk assessment procedure to identify potential threats across all systems and processes handling sensitive data.
- Developed a risk matrix (e.g., very low, low, moderate, high, critical) to quantify the likelihood and impact of identified risks.

Risk Treatment and Documentation

- Developed a risk treatment plan documenting the findings and recommended remediation measures to address identified gaps.
- Shared the findings and recommendations with the client to support informed decision-making and remediation planning.

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Outcomes

With Ampcus Cyber's structured and regulatory-aligned Third-Party Risk Assessment (TPRA) engagement, the client successfully achieved the following:

Regulatory Compliance:

Successfully met the Third-Party Risk Assessment requirements mandated by NYDFS and AMSIS, reducing regulatory exposure and strengthening audit readiness.

Improved Risk Visibility:

Through a centralized third-party risk register and vendor classification system, the client gained a clearer view of vendor-related risks across global operations.

Enhanced Data Protection:

Identified gaps in existing controls protecting PII/SPI and recommended mitigation strategies, resulting in stronger safeguards for sensitive data.

Informed Decision-Making:

The comprehensive risk assessment report and tailored risk matrix enabled the organization to make more informed, data-driven decisions regarding vendor partnerships.