ALLIANZ COMMERCIAL

Cyber Risk Consulting Services

As confirmed by our [2024 Allianz Risk Barometer](link), the cyber risk has proven to be a prominent risk for businesses during several years. Entities across all industries and business segments now have this risk firmly on their radars. How can we get a comprehensive overview of these triggers and how can we enhance our preparedness?

With extensive experience in cyber insurance, Allianz leads in safeguarding businesses against evolving digital threats. Our global risk consulting team, in collaboration with trusted partners worldwide, specializes in identifying companies' cyber exposure. We offer a comprehensive suite of cyber services, including workshops, surveys, cyber 360° assessments, Business Continuity Management, risk scenario analyses, crisis training, ensuring transparency across the cyber value chain.

At Allianz Commercial, our solutions provide peace of mind by protecting against financial losses from cyber incidents. We go beyond mere compensation, recognizing that genuine cyber resilience demands proactive measures and swift responses. Through our global network of cyber risk consultants and industry partners, we offer clients invaluable prevention and response services, leveraging collective knowledge and insights for enhanced protection.

Our 5 Services Provided

Allianz Risk Consulting's Cyber Loss Control Services are offered in combination of free as well as fee-based structure.

1) Cyber E2E Transparency Assessment (free of charge)

This service delivers a comprehensive cyber risk profile through company-wide security reviews. Utilizing Business Model Canvases (BMC) workshops, it evaluates the end-to-end value chain, offering insights into cyber risks across various business operations. The assessment focuses on risk scenarios, attack vectors, and key performance indicators (KPIs) versus confidentiality, integrity, and availability (CIA) versus availability, integrity, and confidentiality (AIC) aspects. Key features include:

- Identification of cyber risk posture & security maturity level
- Prioritizing short, medium, long-term recommendations to improve the organization's security posture
- In-depth evaluation of information security
- programs mapped to compliance, security, and industry frameworks
- Proposal of risk reduction and security posture improvement processes

Allianz ⑪

2) Ransomware Preparedness Check (available at cost)

Beyond compliance insurance led evaluation of how comprehensive client's ransomware threat mitigation strategy is. Identify security weaknesses for the now prevalent ransomware threat against ARC's cyber hygiene checks and guide clients to understand, plan for, respond to and protect against ransomware attacks. Offer examples, recommendations and advice to ensure clients stay prepared by the constantly evolving ransomware menace.

- Review existing network and endpoint security monitoring solutions and processes. Review incident response policy
- Budget and resources skill sets
- Identify roles and responsibilities
- Effective crises comms plan Incident Response Plan

3) Cyber Security Training (free of charge)

Empower clients with dynamic 1-hour specialist webinars offered by ARC or trusted partners.

- Network access control
- Cyber Security Frameworks
- Social engineering
- Cyber Resilience Strategy
- Data loss prevention
- Vulnerability and Patch Management
- Multi-factor authentication
- Cyber Supply Chain Risk Management
- Data privacy regulations
- Network Security & Cryptography Personal data protection practices Application Security
- AI and security implications
- Identity and Access Management
- Cloud Containerization Basics
- Cyber Risk of Emerging Technologies
- Cookies basics
- Incident Management Recovery & Response
- Blockchain & Bitcoin basic concepts
- Backup Security
- Operational Technology Cybersecurity

4) Cyber Business Interruption exposure quantification (available at cost)

We assist clients in identifying cyber business interruption (BI) risks and quantifying potential financial losses resulting from cyber events. Quantifying cyber-BI enables:

- Enhanced risk management and understanding of potential outcomes
- Implementation of cybersecurity measures and risk mitigation strategies
- Resource allocation, budgeting, and risk prioritization
- Determination of appropriate coverage levels and clarity on what is covered

Through scenario-based workshops, we analyze cyber-BI exposures and assess the impact of incidents on business operations. This exercise helps estimate potential losses from cyberattacks, data breaches, or system outages. By actively engaging with clients, we identify mitigation strategies to minimise financial losses.

5) Breach Simulation, Cyber War gaming Exercices (available at cost)

Led by our select panel partners, clients participate in breach simulation and cyber war gaming exercises to bolster cyber defences, protect assets, and prepare for potential threats. These controlled exercises mimic real cyber breaches, including scenarios like data breaches, ransomware, or DDoS attacks. Participants, including IT, security, legal, and communication experts, assume various roles to simulate real incident responses, testing readiness, response, and recovery capabilities.

Key outcomes include:

- Improving incident response plans, policies, and procedures
- Enhancing cybersecurity posture and preparedness
- Identifying vulnerabilities and strengths in incident response
- Streamlining response times and mitigating potential damage during real incidents

Rishi Baviskar
Global Head of Cyber Risk Consulting

Rishi.Baviskar@allianz.com
+44 78815 80241

Rémy Jacquet
Key Account Manager

Remy.Jacquet@allianz.com
+33 6 48 56 63 75

Mehdi Meyer
Cyber Risk Consultant

Mehdi.Meyer@allianz.com
+33 6 58 64 36 11

More information on the Allianz Risk Barometer 2024

Commercial.allianz.com