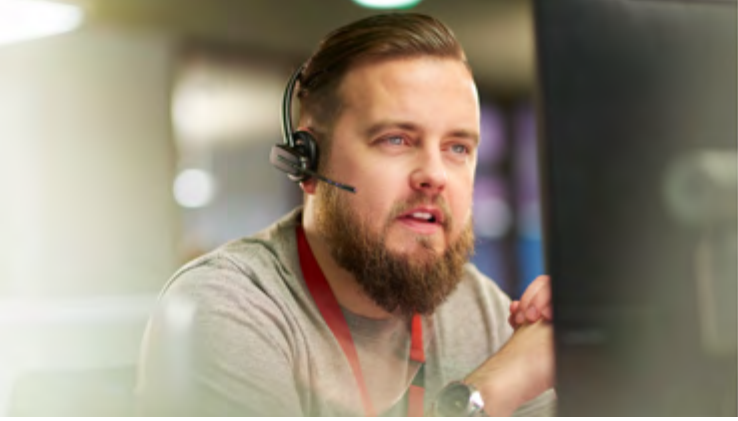
SOMPO



NORTH AMERICA

Tabletop Exercises

Enhance cybersecurity posture while maximizing the value of your insurance investment with tabletop exercises. Tabletop exercises help organizations simulate threats to improve incident response and enhance preparedness. The tabletop exercises described below are available to Primary Sompo Cyber Policy holders and will be paid for by Sompo provided they are completed within 120 days of the start of the policy period.

Email cyberservices@sompo-intl.com for more information on how to access tabletops.

Mullen Coughlin

Cyber Law Firm

OPTION 1	OPTION 2	OPTION 3
For Cyber insureds with premium > $25,000	**For Cyber insureds with premium > $50,000**	**For Cyber insureds with premium > $100,000**
• Following an introductory call to better understand your company's background, we will develop and conduct a tabletop exercise up to two (2) hours in length that will simulate a data security event and challenge your incident response readiness and compliance with industry best practices.	• We will conduct one information-gathering call to better understand: 1. Your objectives for the exercise. 2. Pertinent details regarding the structure and scope of your network environment and critical information/operations systems. 3. The personal information you hold and/or process that may be subject to U.S. state and/or federal data privacy and information security laws and other regulations. 4. Your current posture with respect to existing data privacy and information security policies and procedures. • Following this call, we will conduct a review of your existing and pertinent policies and procedures to incorporate into the exercise as appropriate. • We will then develop and conduct a tabletop exercise up to three (3) hours in length.	• We will conduct multiple information-gathering calls to better understand: 1. Your objectives for the exercise. 2. Pertinent details regarding the structure and scope of your network environment and critical information/operations systems. 3. The personal information you hold and/or process that may be subject to U.S. state and/or federal data privacy and information security laws and other regulations. 4. Your current posture with respect to existing data privacy and information security policies and procedures. • Following these calls, we will conduct an in-depth review of your existing and pertinent policies and procedures to incorporate into the exercise as appropriate. • We will then develop and conduct a tabletop exercise up to five (5) hours in length tailored to your organization and objectives that will simulate a data security event and challenge your incident response readiness and compliance with industry best practices.

>

NORTH AMERICA

Tabletop Exercises

SOMPO

CyberClan

Cyber Security Vendor

OPTION 1	OPTION 2	OPTION 3
For Cyber insureds with premium > $25,000	**For Cyber insureds with premium > $50,000**	**For Cyber insureds with premium > $100,000**
Live, virtually delivered two and half (2.5) hour presentation, focused on a thought-provoking experience to consider the what if's, blind spots, and elements of a breach (Ransomware attack). • Presentation and walk through of a mock incident. • Threat Intelligence and Case Study. • Audience – Senior Leadership. • Q&A.	Customized, virtual tabletop exercise four (4) hours in length, focused on identifying gaps, blind spots, and weaknesses within an organization, in the event of a breach. • Includes a simulation of an active incident with the opportunity for breakout sessions to form responses, on-the-spot strategies and an adaptive approach while dealing with threats. • Includes an in-depth written report. • Includes a summary recommendation report. • Audience – C-Suite & Board Members. • Q&A.	Customized, in-person tabletop exercise focused on identifying gaps, blind spots, and weaknesses within an organization, in the event of a breach. • Includes an in-person simulation of an active incident with the opportunity for breakout sessions to form responses, on-the-spot strategies and an adaptive approach while dealing with threats. – On-site at the insured's office – six (6) hours. • Includes an in-depth written report. • Includes a summary recommendation report. • Audience – C-Suite & Board Members. • Q&A.

"Top" Benefits

- **Improve Incident Response Preparedness:** Develop and refine incident response plans to ensure all team members understand their roles and responsibilities during a Ransomware attack.
- **Identify Gaps and Weaknesses:** Reveal vulnerabilities in an organization's current cybersecurity posture and incident response strategies to allow for targeted improvements.
- **Enhance Coordination and Communication:** Practice and improve coordination with Ransomware attack simulation.
- **Increase Awareness and Training:** Regularly conducting tabletop exercises raises awareness of Ransomware threats and reinforces the importance of cybersecurity best practices among employees.
- **Evaluate Technical Capabilities:** Assess the effectiveness of technical defenses, such as intrusion detection systems, antivirus software, and backup solutions, in a controlled environment.
- **Validate Policies and Procedures:** Ensure that policies and procedures related to Ransomware attacks are effective.
- **Mitigate Risks:** Identify and address potential weaknesses before an actual attack occurs to significantly reduce risk of a successful incident.
- **Ensure Regulatory Compliance:** Meet regulatory requirements and industry standards for cybersecurity preparedness and incident response.
- **Improve Stakeholder Confidence:** Demonstrate a proactive approach to Ransomware preparedness to enhance the confidence of stakeholders, including customers, partners, and investors, in the organization's ability to manage cyber threats.
- **Reduce Costs:** Address vulnerabilities proactively to improve response capabilities and prevent the costly consequences of an attack.