MERIPLEX

Tips and Traps When it Comes to Securing a Cyber Insurance Policy

Understanding cyber insurance can feel overwhelming so we asked our own executives to come up with a list of the top tips to follow and pitfalls to steer clear of to ensure your success.

Tips

These tips will ensure you position your business as a safe bet for insurers and secure the most favorable rates.

Understand the Objectives

Recognize that cyber insurance aims to present your risk favorably to insurers.

Engage Proactively

Ensure engagement and alignment between insurance broker, leadership, IT, and MSPs.

Identify Top Exposures

Identify critical assets cybercriminals may target and assess potential financial losses for each.

Quantify Coverage Needs

Run models to quantify required coverage based on exposures.

Know Your Cybersecurity Level

Understand your cybersecurity posture relative to industry standards and the market.

Implement Security Measures

Allocate sufficient time to address identified security gaps.

Collaborate with MSPs

Work closely with MSPs to complete the insurance application and leverage their expertise.

Provide Detailed Responses

Avoid binary answers; provide detailed explanations and examples to showcase proactive cybersecurity efforts.

Prepare a Comprehensive Narrative

Develop a detailed narrative including cybersecurity practices, initiatives, and outcomes.

Conduct Third-Party Security Risk Assessments

Undertake third-party assessments to supplement external scans and demonstrate proactive risk management to insurers.

Review Before Submission

Ensure the application is comprehensive, accurate, and reflective of your organization's cybersecurity posture.

Be Honest and Proactive

Disclose security gaps and outline plans to address them proactively within a specified timeframe.

Traps

These traps highlight the importance of thorough understanding, clear communication, and proactive risk management to avoid pitfalls in insurance coverage related to cyber incidents.

- **Misleading Cyber Application:** Ensure accuracy when filling out cyber applications, as they become warranties to the contract. Misrepresentation can lead to claim denials.
- **OFAC Sanctions:** Consider potential legal constraints on ransom payments. If the perpetrator is identified as a sanctioned organization by OFAC, extortion payments may be illegal, leaving you without coverage.
- **Post-Event Service Coverage:** Be aware that insurance may not cover post-event services not authorized by the insurer. Clarify what services are covered before engaging external providers.
- **Fraudulent Funds Transfers:** Beware of fraudulent schemes beyond ransomware, such as fraudulent funds transfers. Implement verification protocols for any changes in payment instructions to avoid financial losses and insurance coverage gaps.
- **War Exclusions:** Understand the implications of war exclusions in insurance policies. Despite past cases, interpretations can vary, necessitating a thorough understanding of your policy's terms.
- **Communication Verification:** Establish communication verification protocols to prevent falling victim to fraudulent schemes. Verify any changes in payment instructions through known contacts before proceeding with transactions to ensure coverage.

Cyber insurance is a crucial component to staying protected and can get complicated quickly. Our experts can help guide you through the process and help you make the best decisions for your company. Reach out to set up a consultation today.

Contact Us