COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2024
Appendix 5-N: Common Cyber Insurance Mistakes to Avoid

Below is a list of common mistakes organizations make in relation to their cyber insurance coverage along with best practices they can use to avoid them.

Common Mistake	How to Avoid
Thinking all cyber insurance policies are the same	Do your research! There are more than 150 different insurance carriers offering some type of cyber insurance coverage, whether it be a standalone policy, a rider, or an add-on to another type of coverage. Coverage terms and amounts will vary widely by carrier and type. Be sure to look for differences in: • Incidence response coverage limitations, • Lack of coverage for incidents resulting from certain causes, • Denial of coverage for failure to notify the insurer of a breach or incident within a certain limited time period, and • Requirement to carry other types of insurance (e.g., business continuity or crisis response).
Assuming all incidents will be covered	Just like all other types of insurance, cyber insurance has a number of limitations, exclusions, and conditions. Pay careful attention to narrow policy definitions and limitations and maximum coverage amounts. Consider working with insurance coverage counsel and/or an experienced cyber insurance broker for assistance.
Comparing using only premium price	Organizations often make the mistake of using premium price as the primary comparison point when deciding between different insurance policies. An accurate comparison cannot be made using quoted premiums alone. Carefully consider: • Coverages being offered, • Policy exclusions and conditions, and • The financial ratings and claim-paying ability of the insurance carrier.
Failing to take advantage of tools and resources offered by your insurance carrier	Most insurance carriers offer value-added benefits to its policyholders, including risk mitigation tips, contract reviews, cyber security consultations, employee training materials, and more. Don't miss out on these extra benefits.

Common Mistake	How to Avoid
Not keeping your promises (i.e., failing to do what's expected/required)	The representations you make in your application for insurance are promises you must keep. The organization must understand and do what's expected and required of it by its insurance carrier in order to avoid claim disputes when an incident arises. For example, if the organization represents in its insurance application that it encrypts all sensitive data that resides on mobile devices, and months later an employee loses an unencrypted mobile device that contains sensitive data, the claim may be denied because the security standards on the device were not as they were represented to be in the cyber insurance application.
Not understanding your policy exclusions	Be aware that your cyber insurance policy will have some exclusions. Oftentimes, an insurance carrier will include exclusions that pertain specifically to the risk profile of your organization. You need to understand what will *not* be covered. Exclusions you should pay attention to and ask about include: • Terrorism and war, • Regulatory action, • Inadequate security, • Breach of contract, • Third-party vendor breaches, and • Unfair trade practices.
Not understanding your policy sublimits	Many cyber insurance policies, especially add-on cyber insurance coverage endorsements, offer coverage that is capped at a sublimit. This means the liability coverage amount for any one incident is most likely not as high as the policy's total aggregate liability limit. You may have a $1 million cyber incident coverage with a sublimit of $250,000, which could mean the maximum amount of coverage you have for a specific incident is only $250,000, not $1 million. Make sure you understand and are comfortable with the policy's sublimits (if this is applicable), otherwise you may not have as much liability coverage for a particular incident as you thought you did.

Common Mistake	How to Avoid
Not understanding what "panel" and "prior consent" provisions in your policy mean	Most cyber insurance policies include a panel of "preferred" data breach resolution consultants and legal counsel the insurance carrier has already contracted with that the insured company must use at the time of a claim if it wants the incident to be covered. Insurers will often "tie your hands" when responding to a breach and require you to obtain their prior written consent and approval before you can use anyone who is not included on their already approved panel of providers. Waiting for this approval can cause significant and costly delays when responding to a cyber incident. Make sure you understand whether you will be able to select your own vendors and/or counsel. Often, organizations have preexisting relationships with consultants and counsel they like to work with, but they may be barred from using them if they are seeking to have the incident covered by their cyber insurer.