COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
Cyber Insurance Guidelines for Corporate Compliance and Ethics Executives and Boards of Directors

By Christine Marciano[1]

The impact of cyber and randsomware attacks can be devastating on companies, leading many seeking to mitigate these risks to purchase stand-alone cyber insurance polices. In today's internet-connected environment, companies are at risk for incidents both inside and outside the IT environment and can fall prey to a disruptive network intrusion or costly data breach at any time. Nonetheless, cyber insurance continues to be a hot topic across all companies, regardless of size and sector, as a way to combat the financial impact of these incidents when they happen.

Considering that today's cyber and data security threats are tomorrow's insurance claims, it is important that all companies review their current insurance policies to examine how and if such claims would be covered. Traditional insurance products, such as commercial general liability policies or property policies, are designed to cover bodily injury or damage to tangible property—*not* cyberattacks or data breaches. Most traditional insurance policies specifically exclude coverage for such losses. Specialized stand-alone cyber insurance policies are designed to protect your company in the event of unauthorized access, data theft, data loss, network intrusions, information security breaches, system downtime, and more.

While cyber insurance can't eliminate a data breach or be a replacement for data security, it can provide a backstop of financial relief, offering a budget dedicated to data breach preparedness and a comprehensive incident response plan solution to help minimize the financial damage of a data breach or cyberattack. Before purchasing a cyber insurance policy, companies need to consider the company's cyber and data risks to determine which risks to avoid, accept, mitigate, or transfer through insurance.

With many more insurance carriers now offering stand-alone cyber insurance policies, companies have many options to choose from and must carefully conduct their due diligence when reviewing varying policies and coverage options. In addition to the many insurance carriers offering cyber insurance, there are many new InsurTech start-ups that offer cyber insurance along with a complimentary risk assessment or cybersecurity tools and resources.[2] Note that these complimentary services do not directly decrease the premium of cyber insurance. When purchasing cyber insurance coverage, organizations would be prudent to check on the financial ratings and stability of the insurance provider.

Indeed, a company shouldn't just buy insurance to exonerate itself from its data security responsibilities, which is why it will want to ensure it implements data and cyber security protocols *before* applying for a cyber insurance policy. In fact, cyber insurance underwriters now expect that security measures such as multi-factor authentication be in place for remote access to all sensitve information to qualify for a new or renewal cyber insurance policy. Companies aren't typically awarded discounts for implementing security measures since they are now deemed to be an essential requirement to qualify for a cyber insurance policy.

When a company seeks cyber insurance, the insurance carrier will ask many questions about the company's operation, types of data collected, processed, and/or stored, data backup processes, data security controls, and third-party relationships. It is highly recommended that companies exploring the purchase of a cyber insurance

policy to first conduct a risk assessment to identify the company's cyber and data risks, third-party relationships, cybersecurity threats, and vulnerabilities. Risk assessments play a significant role in cybersecurity and can also help streamline the cyber insurance underwriting process; e.g., Where are the cybersecurity gaps? What are the company's cyber risk vulnerabilities? Which threats are most likely—and most serious? Which risks can be transferred to a cyber insurance policy to minimize losses when they occur?

By studying past data breaches and cybersecurity incidents that have occurred and considering the likely attack methods and routes of exploitation through a risk-assessment process, companies can be better positioned to mitigate the potential impact that data security breaches and other cyber events have on achievement of their objectives by transferring the associated risks to a cyber insurance policy.