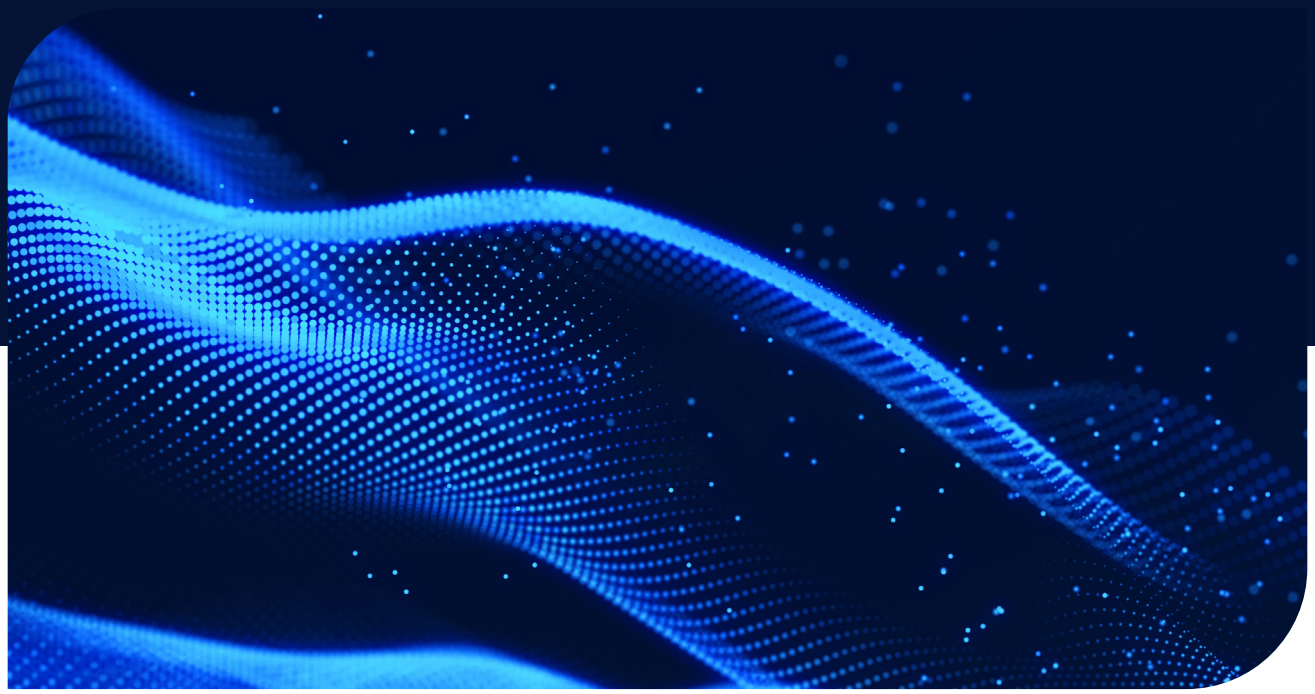
Teneo | TAG CYBER

Teneo Cyber Insights Series for CEOs

How Cyber Insurance is Transforming Enterprise Cyber Risk Management

Teneo Insights / June 2023



Every business understands the importance of managing risk. Larger and more complex organizations and their risk management teams have always had to manage multiple risk categories, including financial risk, compliance and legal risk, geopolitical and regulatory risk, and operational risk – among others. More recently, however, new forms of risk have emerged. In this article, we focus on how cyber insurance is transforming the management of enterprise cyber risk.

Introduction

Our ongoing Cyber Insights Series for CEOs has explored the growing complexity of cyber risk management, with a particular focus on AI, geopolitical risk and the demands placed on the professionals in charge of cybersecurity, namely the CISO. It is no secret to any modern CEO or their executive team that cyber threats pose significant risks to their enterprise. Malicious actors, often funded by adversary nation states, can easily disrupt operations, compromise sensitive data and erode customer trust. All business leaders have been forced to understand their grave responsibility to address the evolving cyber risk landscape and to adopt working strategies that can identify and mitigate these new risks.

Since the late 1990s, the use of cyber insurance has evolved as a new approach to handling enterprise security risk. We call this "new" because of its relative recency in comparison to other insurance lines. Unlike most existing solutions that attempt to reduce risk through design, operations or other tangible risk mitigation means such as hardware, software or testing, cyber insurance involves the transfer of risk through a contractual arrangement from one entity (the customer) to another entity (the insurance company), often through an intermediary (the broker). In this article, we examine key aspects of this approach to cyber risk and the implications for CEOs.

The Role of Cyber Insurance

As one might expect, cyber insurance is intended as a financial safety net for enterprise teams, with the goal of reducing the impact of breaches and helping organizations recover more rapidly and efficiently. Furthermore, cyber insurance is designed to help an operational team better allocate their resources and avoid the stress and time required for dealing with financial risk calculations. In 2020, cyber research firm Cybersecurity Ventures noted that global cybercrime costs are expected to grow by 15% year over year, reaching $10.5 trillion USD annually by 2025[1], which more than makes the case for the necessity of this type of insurance. The recent spate of large-scale, highly public and highly disruptive cyber-attacks over the last several years has sent demand surging. Depending on the market research firm, the projected global cyber insurance market is valued anywhere from an estimated $64-$90 billion by 2030 (as of this writing, we found three different research firms with varying estimates, indicative of the lack of predictability in the sector). Whether one chooses $64 or $90 billion as the target, the delta between projected cyber disruption costs and projected market coverage only suggests an increasingly larger role for and focus on cybersecurity insurance as a risk and cost mitigation.

It is important to note, however, that cyber insurance – if it is provided properly by insurers – will serve to encourage better security decisions and behaviors within the insured entity. Insurance providers in the cybersecurity space are increasingly enabling access to experts to support clients with cybersecurity risk

and/or maturity assessments as part of prevention. They are also enabling access to experts to support technical incident response, public relations and crisis management partners in the event of a breach. This follows familiar practices in all types of insurance where the company accepting the risk is incentivized to guide the insured entity toward safer and more secure practices both within the organization and across its support landscape with third parties, suppliers and customers.

In 2020, cyber research firm Cybersecurity Ventures noted that global cybercrime costs are expected to grow by 15% year over year, reaching $10.5 trillion USD annually by 2025[1].

Risk Modeling Challenge for Insurance

The manner in which insurance companies write contracts has been a mature discipline for centuries, where maritime policies were based on an intuitive understanding of risk. Since then, the insurance industry has become one of the most quantitatively driven industries in the world, using empirical and predictive financial, operational and risk models to create offerings that have become part of the business and social fabric.

For cybersecurity insurance, the first challenge stems from the availability of empirical data to develop

1. Cybercrime Magazine, Nov 13, 2020

quantitative models. Only decades of data are available to model cybersecurity risk versus centuries of rich data available to other types of insurance, and much of the most relevant information exists in the proprietary environments of businesses who generally choose to keep evidence of minor breaches (and some major ones) largely unknown. This creates significant gaps in the empirical data required to develop standardized metrics and benchmarks to produce accurate insurance models. One other facet of the cyber threat landscape is its ever-evolving nature and the unpredictability in cyber-attack methods and threat actors. To underscore the point, AI is yet another development which may further exacerbate the complexity, scope and scale by which cyber-attacks can cause businesses disruption and thus complicate the ability to underwrite appropriate insurance against such a moving target.

The second challenge comes from the predictive models that can be applied to both offense and defense. The problem here is that offensive models are tough to bound. That is, could it be possible, for example, for a nation-state to identify all the customers of some insurance company, perhaps using artificial intelligence, and then develop a cyber weapon that attacks them all at once? It seems this would create an untenable payout situation for the insurance company.

Unfortunately, the skyrocketing cost of cybersecurity insurance has been yet another biproduct of high demand in recent years, making the buying process more frustrating and the business case harder.

Current Landscape for Cyber Insurance

Cyber insurance is popular, perhaps even required, for virtually all large commercial organizations. Senior leadership teams, boards and investors tend to demand the presence of a policy, so typically finance teams, in conjunction with in-house counsel and security leaders, generally engage a broker to help them locate and purchase a reasonable policy. Unfortunately, the skyrocketing cost of cybersecurity insurance has been yet another biproduct of high demand in recent years, making the buying process more frustrating and the business case harder. According to consulting firm Ankura, subsequent to major attacks of 2020 and 2021, insurance industry providers increased rates as much as 83.3% on average for the top 25% of companies.[2] In addition to the costs of a policy, providers stepped up requirements for buyers.

Acquiring cybersecurity insurance often includes lengthy review processes involving underwriters and can be an unpleasant experience for security teams given the pre-requisites to even obtain a policy. CISOs and security teams will often have to endure a pre-audit, which includes an assessment of current controls and security protocols and a review of any past incidents and outcomes. Companies will often be required to implement a range of controls or enhancements or demonstrate an implementation roadmap and commitment prior to being awarded a cybersecurity insurance contract.

One unusual aspect of the cyber insurance landscape is that while security teams are often viewed as the beneficiaries of the risk transfer, the truth is that few security teams actually budget for and pay the premiums. These payments, and most of the financial negotiations, are handled by the finance team. This is potentially fraught with challenges in that CFOs, if not

2. The Cybersecurity Insurance Market: What to Expect in 2023, February 13, 2023

adequately informed of the scope and scale of potential cyber risk facing his/her business, may underestimate the need and coverage of a policy. One wonders what the impact might be if CISOs had to budget for insurance as part of their operational allocation? For smaller businesses, cyber insurance is often provided through bundled products, and in many cases just exists so that the smaller entity can claim that they have a policy. It is not uncommon for larger companies to require their smaller suppliers to have such a policy, so this drives the practice. Ask any business owner today if they have good cyber coverage and they will either not know or will point to a policy clause that in actuality may have little impact. This is particularly noteworthy since small and medium-sized businesses typically comprise an enterprise supply chain, not to mention customer rosters.

Three Cyber Insurance Observations for Senior Leaders

We recommend that senior leaders, especially CEOs and Board Directors, maintain a clear understanding of the present and likely future of cyber insurance as a key component of business cyber risk mitigation. To that end, we provide three observations that we believe are worth keeping in mind as executives make risk-related decisions for their organizations:

Observation 1: The cyber insurance industry will continue to grow, benefitting businesses

Our research clearly demonstrates future growth for the global cybersecurity insurance market. We see no evidence that cyber insurance products will become less popular in the coming years. In fact, we expect to see continued and even accelerated growth in this industry based on the evolving complexities in the cyber threat landscape, more education and hopefully awareness of the benefits of adopting cyber insurance as a mitigant. However, according to Michael Tagg, Senior Managing Director at Teneo specializing in insurance, "CEOs and CFOs may also need to consider alternative forms of risk management, including the use of captive insurers or risk retention groups to overcome potential capacity and/or restrictions on coverage for cyber risks." Certainly, as CISOs get more involved from a budget perspective, this could have a slight dampening effect on the growth slope, because financial trade-offs will have to be made between allocating budget for cyber insurance versus allocating budget for cybersecurity staff, consultants, services, products and platforms. Today, this is typically resolved at a higher level than the CISO, but it is possible that such decisions will move closer to the CISO in the future. When that happens, CEOs and CFOs in charge of signing off on CISO recommendations will have to work through the delicate balance of trusting the expertise and recommendations of the CISO subject matter expert versus the immediate reflex to manage costs.

Observation 2: The terms and conditions of cyber insurance policies will improve

Growth implies more players, new and hopefully more innovative contracts due to an enhanced understanding of the risk, access to better data and more accurate models. The convergence of these factors will likely drive down costs, opening the market and availability of more reasonable contracts and contract terms to global businesses. While it might be tempting to assume that with poor empirical data insurance companies would be motivated to drive less attractive terms for buyers, our view is that with competition will come policies with premiums, payouts, deductibles and terms that are more attractive to buyers. This will help to drive continued growth in the industry and will help smaller companies obtain policies that offer meaningful risk transfer (typically a supply chain security requirement for larger enterprise buyers).

Observation 3: Brokers will become more aggressive in offering cyber services

We see evidence that brokers have identified a key role for their teams to help drive better cybersecurity architectures, processes and operational deployments for buyers of insurance. Brokers are in a good position to assist with these areas of organizational protection, so executives should expect to see excellent offerings from these entities, probably starting with the larger brokers. Aforementioned competition for enterprise business will hopefully return the leverage to companies seeking insurance coverage, allowing purchasers to shop around, compare offerings and identify a policy ideally attuned to their specific business.

Next Steps for Executives

Our assumption is that readers of this note are likely already buyers of cyber insurance. That said, we recommend a few near-term actions. First, we strongly recommend an annual cyber insurance review, perhaps by a capable independent entity to provide expert guidance on the terms and conditions of existing policies, and any trend occurring in the cyber landscape.

Second, we encourage executives to develop good relationships with one or more of the best brokers in the industry. These companies can be effective partners and can offer guidance on developing the best roadmap toward cyber risk transfer. Even if a company has not done business with a given broker, creating a relationship is recommended. They will be motivated to spend the time and offer their perspective.

Finally, we must emphasize that cyber insurance is no substitute for operational excellence in preventing, detecting and responding to cyber threats. Ultimately, risk transfer is less attractive than risk reduction or avoidance, so executives must continue to support their CISO and to ensure that proper levels of budget, funding and support are in place to ensure the best cybersecurity outcome for the organization.

Authors

Ed Amoroso
Senior Advisor, Teneo
CEO TAG Infosphere, Inc., Research Professor, NYU and Senior Advisor to Teneo Risk

Courtney Adante
President, Teneo Risk Advisory
Teneo Cybersecurity Client Lead and Cyber Crisis Management Advisor

Michael Tagg
Senior Managing Director
Financial Advisory, Insurance Specialist

Teneo®
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions, and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 500 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth guidance, market analysis, consulting, and personalized content based on thousands of engagements with clients and non-clients alike—all from a practitioner perspective.

www.tag-cyber.com