USF | Muma Business Review
A publication of the Muma College of Business | University of South Florida

Volume 9, Number 14	Industry Analysis	21 NOVEMBER 2025

Cyber Insurance: Analyzing the Insurance Industry's Novel Coverage

By
Dalton Crabtree, University of South Florida

The cyber insurance market has rapidly evolved into a critical component of the global insurance industry, growing significantly in response to escalating cyber threats. In 2023, the market was valued at approximately $7 trillion, with cyber insurance emerging prominently, especially in the United States. The market operates through direct writing carriers of varying sizes and reinsurance carriers, catering to individual and commercial clients with tailored cyber insurance products.

Large carriers dominate, leveraging extensive marketing and financial capabilities to offer comprehensive coverage, while midsize and small carriers target specific market segments. Reinsurance carriers bolster market growth by providing capital, whereas InsurTechs introduce innovation and technology-driven solutions.

Despite considerable growth, the cyber insurance sector faces challenges such as a lack of extensive academic research, limited product diversity, and a high dependency on strategic partnerships. Nevertheless, opportunities abound with the rising demand for cyber insurance, driven by increased cybersecurity awareness, regulatory mandates, and the evolving nature of cyber risks.

This analysis is a cyber insurance industry analysis comparing cyber insurance with traditional lines of insurance. This paper utilizes a literature review of industry and academic publications and a SWOT analysis to understand the current state of the cyber insurance market.

The market's future is promising, with potential for significant expansion as cyber insurance becomes integral to risk management strategies akin to traditional insurance lines. The industry's progress hinges on bridging the academic-practitioner gap and adapting to dynamic market and risk landscapes. This executive summary underscores the cyber insurance market's trajectory, highlighting its growth potential, challenges, and the need for comprehensive research and strategic adaptation.

Keywords: Cyber insurance, insurance, reinsurance, risk management, cybersecurity, incident response

Copyright © 2025, *Dalton Crabtree*. This article is published under a Creative Commons BY-NC license. Permission is granted to copy and distribute this article for non-commercial purposes, in both printed and electronic formats

The Industry

The insurance industry, broadly, is a global industry comprised of insurance services ranging from property and casualty (P&C); life, health, and accident; medical, disability, financial instrument (credit, mortgage, etc.), cyber insurance, and niche (pet, travel, event, etc.) insurance products. According to the International Association of Insurance Supervisors (2023), the size of the global insurance market was approximately $7 trillion in gross written premium (GWP) (Figure 1) including emerging markets and developing economies (EMDE) and all advanced economies (AE). GWP is one main industry measure to determine the total premium paid by policyholders for insurance coverage. Within the global market, cyber insurance is the newest coverage, with the first cyber insurance coverages being sold in the United States in 2015 (Agrawal & Shivendu, 2016). Cyber insurance, insurance coverage for data security, network security, and the ensuing liability for security breaches has become a product of interest for both personal and commercial insurance policyholders. With the prevalence of cyber risk nationally and internationally, cyber insurance is quickly taking the forefront of the insurance market. Specifically, within the United States, cyber insurance has exponentially grown as international cyber insurance continues to develop. Developing an understanding of the current and future state of the cyber insurance market will allow for scholars and practitioners to better understand this line of insurance, and the implications of how cyber insurance contributes to risk management efforts.

The Cyber Insurance Product

Cyber insurance is a unique product and a novel form of coverage covering much of the minutia of cybersecurity and cybercrime. Cyber insurance has proven to be its own category of insurance as cyber encompasses elements from the more established lines of insurance such as property and casualty insurance. Cyber insurance acts like property insurance in some instances involving hardware. Cyber insurance acts like casualty insurance, as losses are often intangible and are of higher severity. Cyber insurance acts like commercial crime insurance, as cybercriminals often use tactics that would be addressed in commercial crime insurance. Lastly, cyber insurance acts like auto insurance as cyber for automotive products covers property and liability losses stemming from cyberattacks. Table 1 provides

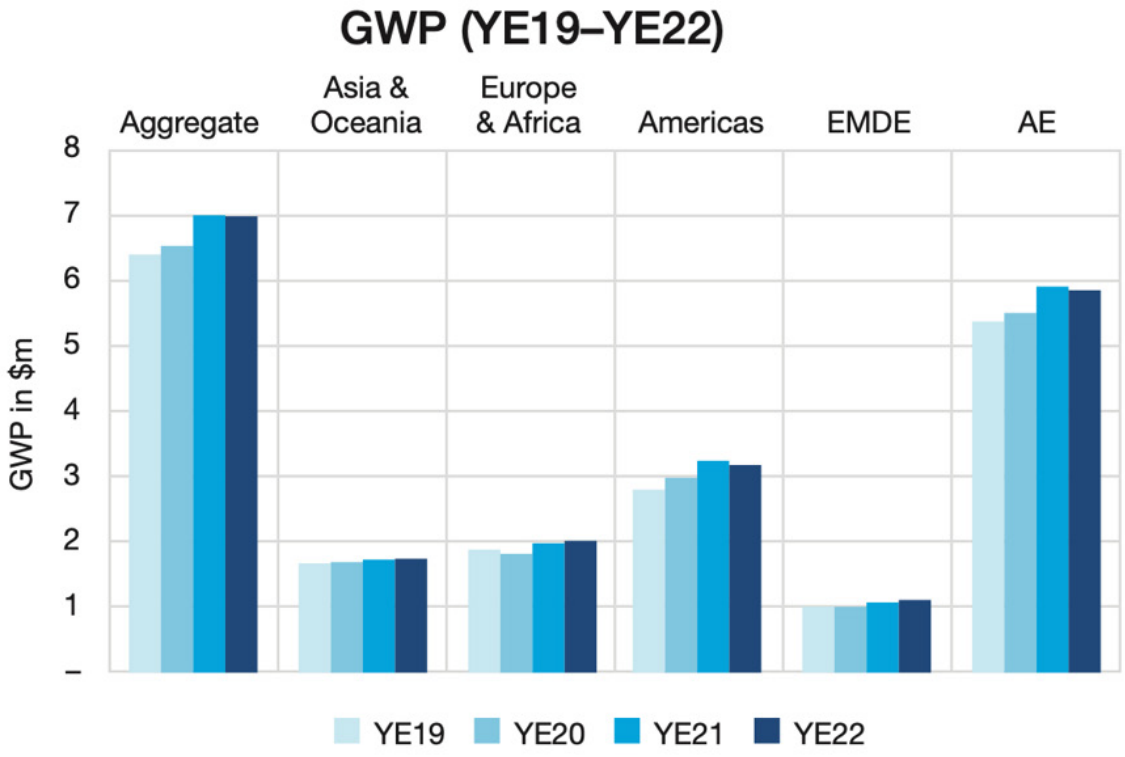

Figure 1: Cyber Insurance Gross Written Premium (2019 – 2022)

Table 1: Cyber Insurance Comparative Summary		
Line of Insurance	**Coverage Summary**	**Example of a Covered Loss**
Automotive	**Physical damages to the vehicle.** **Bodily injury to passengers or other drivers.**	**Being rear ended while stopped at a red light.** **Injury caused from hitting a pedestrian with a vehicle.**
Property and Casualty	**Property: Residential and commercial buildings, and personal property.** **Casualty: Legal responsibility claimed by a 3rd party against a person or business.**	**Property: Roof damage from a windstorm.** **Casualty: A customer slipped, fell, and become injured after slipping on a puddle in a store.**
Life, Disability, Health, Accident	**Life: The loss of life.** **Disability: Permanent or temporary loss of the ability to work.** **Health: Costs associated with illness and medical treatment.** **Accident: Costs associated with sudden and unforeseen injury or loss of life.**	**Life: The loss of an insured person's life due to age.** **Disability: Temporary injury resulting in a tradesperson being unable to complete manual labor.** **Health: Open heart surgery after a heart attack.** **Accident: The loss of life due to a car accident.**
Cyber	**First Party: Costs associated with addressing unauthorized access to computer systems.** **Third Party: Defense and settlement costs for 3rd party claims from a cyberattack.**	**First Party: A business being victimized by a ransomware attack resulting in theft of customer healthcare records.** **Third Party: Costs to settle a lawsuit for violating privacy law.**

a comparative view of cyber insurance and other standard lines of insurance, which demonstrates how cyber insurance is distinctive from the common lines of insurance individuals and businesspeople are more familiar.

As discussed above, cyber insurance contains elements of property and casualty insurance. From a property perspective, cyber insurance addresses the costs of lost and stolen data, network architecture, and extortion costs. Figure 2 provides an example of cyber insurance policy definitions for first party insuring agreements (Romanosky et al., 2019). Table 2 provides an example of common first party cyber insurance coverages (Munich Re, 2024a, 2024b). These first party coverages are costs cyber insurers reimburse policyholders for expenses paid that meet the insurance agreement's scope of coverage.

From a casualty perspective, cyber insurance responds to third party claims made against covered individuals or businesses for the failure to protect sensitive personally identifying or personal healthcare information. Figure 3 goes on to provide an example of cyber insurance policy definitions for third party insuring agreements (Romanosky et al., 2019). These third party coverages are costs cyber insurers reimburse policyholders for expenses incurred to legally defend and possibly settle claims made for violating data privacy laws.

Cyber insurance is not simply an iteration of existing line(s) of insurance. Rather, cyber insurance is its own unique line of insurance that has created one of the fastest growing insurance markets in the world. Even since its start as an identity theft-only service, cyber insurance carriers have quickly developed products and expand coverage to serve the dynamic landscape of cybersecurity and understanding cybercriminals. Cyber insurance is posed to continue this innovative and exponential growth in the insurance industry, becoming one of the world's largest markets within the industry.

U.S. Cyber Insurance Market

The cyber insurance market is facilitated by primary insurance carriers who offer policies to individual and commercial customers (transactional underwriting model) and reinsurance carriers who, through reinsurance agreement(s), assume the

Coverage area	Description
Data Compromise Response	"Provides coverage for specified expenses arising from a personal data compromise involving personally identifying information of affected individuals. Affected individuals may be customers, clients, members, directors or employees of the insured entity."
Identity Recovery	"Provides coverage for Identity Recovery caused by an identity theft of an identity recovery insured first discovered during the policy period."
Computer Attack	"Provides coverage for specified expenses arising from a computer attack on the computer system."
Cyber Extortion	"Provides coverage for the cost of an investigator retained in connection with the extortion threat and coverage for any amount paid by the insured in response to the threat."

Figure 2: Summary of First Party Commercial Cyber Insurance Coverages

risk of primary insurance carrier's cyber insurance portfolio in exchange for reinsurance premium (reinsurance underwriting model).The US market is segmented based on the size of the organization in terms of gross written premium and active policies ranging from large carriers licensed and conducting business in all fifty states to midsized carriers licensed and conducting business in a particular region and small carriers that are licensed and conduct business in one state. In the US, cyber insurance is not a mandatory coverage businesses or individuals must secure to purchase property (i.e. a house or commercial building) or automobiles.

Direct Writing Carriers

Direct writing carriers were P&C carriers licensed to conduct business in at least one, but often several, states and offer a portfolio of insurance products to individuals, small and medium businesses, and corporations containing automobile, property, and liability products. Direct writing carriers represent the main means cyber insurance is distributed to individuals (personal lines cyber insurance) and companies (commercial lines cyber insurance).

Large Direct Writing Carriers

Large carriers were direct writing carriers with total annual gross written premium above $10,000,000 (A.M. Best, 2022). Large carriers include State Farm, Progressive, AIG, and Liberty Mutual (A.M. Best, 2022). These carriers used mass marketing efforts such as telephone and online sales agents, primetime television advertisement, mass mailers, and professional event and sport sponsorship to maintain and grow their national customer base. Large carriers service millions of individual policyholders, and underwrite standardized and customized products for small, medium, and large businesses with the financial capacity to underwrite more complex risks such as utility providers and renewable and non-renewable energy providers. These large direct writing carriers are responsible for placing millions of personal and commercial cyber insurance policies. By leveraging capital and financial capacity, these carriers have the ability to underwrite, whole or part, of large risk accounts such as municipalities, government programs, and Fortune 500 enterprises. Specifically, State Farm, the nation's largest insurance carrier by policies in force, has the most active personal lines cyber policyholders amongst all competitors.

Midsize Direct Writing Carriers

Midsize carriers were direct writing carriers with total annual gross written premium between $5,000,000 and $10,000,000. (A.M. Best, 2022). Midsize carriers included Auto-Owner's, Cincinnati Insurance, Tokio Marine, and Erie Insurance (A.M. Best, 2022). Midsize carriers used a regional approach leveraging brokerages and independent agents to solicit business following common sales practices such as cold calling, referral networking, and internet lead generation. Midsize carriers serviced hundreds of thousands of personal policyholders and primarily underwrite standardized

Table 2: Summary of First Party Personal Cyber Insurance Coverages	
Coverage Area	**Description**
Online fraud	**Pays for financial losses resulting from identity theft, phishing schemes, illegal bank and credit card transfers, and other deceptions**
Computer attack	**Removes malware and reprograms computers and tablets, Wi-Fi routers, or other internet access points**
Home systems attack	**Restores devices connected to the internet, including smartphones, thermostats, smart appliances, and security and monitoring systems**
Cyber extortion	**Provides professional assistance to respond to a ransomware attack and payment of the ransom (when pre-approved)**
Data breach	**Pays for notification costs and recovery services when private non-business data entrusted to an individual is lost, stolen, or published**
Identity recovery	**Pays for the costs of recovering from an identity theft as well as full-service ID theft restoration services**
Home title fraud	**Provides coverage for home title fraud costs resulting from an identity theft, including attorney and court filing fees for the recovery of the title**
Cyber bullying	**Pays for the costs of recovering from a cyber bullying attack, from psychiatric counseling services and legal expenses to temporary relocation expenses, social media monitoring software, and more**
Social media income interruption	**Includes coverage for social media income loss resulting from a cyber attack or the account takeover of a social media influencer**

small and medium businessowner products with less exposure to large and complex commercial risks. These midsize direct writing carriers mainly distribute mid-market (moderate to low risk, more limited coverage) commercial and specialized cyber insurance products. As an example, Cincinnati insurance targets high net worth homeowners and small businessowners.

Small Direct Writing Carriers

Small carriers were direct writing carriers with total annual gross written premium under $5,000,000. (A.M. Best, 2022). Small Carriers included Church Mutual, Auto Club Group (AAA), Farm Bureau, and FCCI. Small carriers focused on servicing local policyholders through insurance agents involved in communities, trade or professional associations, and industry groups such education, agriculture, or religious organizations. Small carriers serviced tens of thousands of individual policyholders and selectively underwrite specialized commercial products based on the target market. Due to limited financial capacity and the volatility of cyber risk, small direct writing carries offer very limited (low coverage and exposure) policies or do not currently have cyber insurance in their portfolio. As an example, Church Mutual and AAA do not currently offer personal or commercial cyber insurance.

Reinsurance Carriers

Reinsurers are licensed insurance carriers that provide insurance to other insurance companies (direct writing carriers) via reinsurance agreements. These agreements specify whether reinsurance is provided on a portfolio basis (covering a specific line of business) or on individual transactions, where the reinsurer underwrites a policy and assumes the risk of loss from the direct writing carrier in exchange for reinsurance premium.

Gross written premiums for the top 50 reinsurers ranged from $46 billion to $755 million (A.M. Best, 2022). Notable reinsurers included Munich Rein-

Liability	Description
Data Compromise	"[Provides] coverage for defense and settlement costs in the event that affected individuals or a government entity sue the insured because of a personal data compromise."
Network Security	"Provides coverage for defense and settlement costs in the event that a third party claimant sues the insured because of: • The breach of third party business information • The unintended propagation or forwarding of malware • The unintended abetting of a denial of service attack • The inability of an authorized third party user to access the insured's computer system."
Electronic Media	"Provides coverage for defense and settlement costs in the event that a third party claimant sues the insured alleging that the insured's electronic communications resulted in defamation, violation of a person's right of privacy, interference with a person's right of publicity or infringement of copyright or trademark."

Figure 3: Summary of Third Party Cyber Insurance Coverages

surance, Swiss Re, Berkshire Hathaway, and Lloyd's (A.M. Best, 2022). Reinsurers' customers range from large to small direct-writing carriers and, in some instances, other reinsurers. Reinsurers often provide coverage in the property, casualty, life, and health insurance markets but have specialized in smaller segments to create competitive advantages. In the past decade, established and new reinsurers, such as Beazley, have facilitated the growth of the cyber insurance market by providing additional capital to direct-writing carriers, allowing these carriers the financial capacity to develop cyber insurance products and expand their book of business.

InsurTechs

The rapid growth of the cyber insurance market combined with the novel coverage addressing the cybersecurity and computer science subject matters has created a sub-economy within the industry which has incubated multiple startup businesses. Like FinTechs within the finance industry; the insurance industry, these businesses are known as InsurTechs (insurance technology) which provide innovative insurance technology solutions. InsurTechs have disrupted the insurance industry and increased the rate of innovation and digitization for an industry that was still largely dependent on facsimile prior to the Covid-19 Pandemic. These startups often operate solely on venture capital during until the firm becomes self-sustaining or is acquired by a traditional insurance carrier. InsurTechs often have several hundreds to thousands of policies in place and complete on innovation to attract more capital or an acquirer.

Table 3 provides a summary of cyber security insurance carriers.

Stakeholders

Like the stakeholders of the general insurance industry, the stakeholders within the cyber insurance industry have a different set of interests, as these interests pertain specifically to cyber risk compliance with state and federal data privacy laws while managing the unpredictable nature of cybercriminals. Specifically, these stakeholders are concerned with global cybercrime trends, the effects of cyberterrorism, and the impact the insurance mechanism has

Table 3: Comparative Summary of Insurance Carriers Within the Cyber Insurance Market			
Carrier	**Number of Policies**	**Gross Written Premium**	**Market Segment**
Large Direct Writing	**Hundreds of Thousands**	**$10,000,000+**	**Large Enterprise**
Midsize Direct Writing	**Tens - Hundreds of Thousands**	**$5,000,000+**	**SME / High Net Worth Individuals**
Small Direct Writing	**Tens of Thousands**	**<$5,000,000**	**Small Business / Individuals**
Reinsurers	**Hundreds of Thousands**	**$10,000,000+**	**All of the above**
InsurTechs	**Hundreds -Thousands**	**>$2,500,000**	**Niche**

on encouraging cybercrime visa vi reimbursing cybercrime victims.

Stakeholders specific to the cyber insurance industry include:

- Regulators (attorney generals, Office of Civil Rights, Office of Health and Human Services, etc.)
- Policyholders
- Incident response firms
- Cybercriminals

Regulators

In the United States, data privacy is not a basic right guaranteed to US citizens. Outside of the Fourth Amendment which protects individuals from unlawful search and seizure, the federal government does not consistently recognize individual right to data privacy including how one's data is stored, used, and sold, and deleted (often called the right to be forgotten). At the federal level, some laws and regulation do govern how individual's data can and cannot be used. Laws like Health Insurance Portability and Accountability Act (HIPPA), Family Educational Rights and Privacy Act (FERPA), and Fair and Accurate Credit Transaction Act (FACTA) dictate how certain industries and business use and store data. Outside of operations within the scope of these federal laws, the individual right to data privacy is determined at the state level. States such as California, Washington, Florida, and Colorado lead the nation in comprehensive data privacy law that provides protection beyond healthcare, education, or financial data. These states have ratified law that outlined resident's individual right to control how their data is collected, used, and stored and provides legal remedies to individuals when their data privacy rights have been violated. In addition to the state and federal agencies that enforce data privacy laws, state insurance commissioners and departments of insurance are interested in the frequency in which cyber coverage and premiums change as these agencies and regulators are tasked with protecting consumers from unfair insurance carrier practices.

Policyholders

Insurance policyholders, both personal and commercial, have a vested interested in cyber insurance. Many individuals and businesses are not aware of the availability of cyber insurance, or what types of losses cyber insurance addresses. Broadly, the insurance market customer base needs to educated on the availability and scope of cyber insurance so they can discuss their cyber risks when buying insurance like they discuss more common risks such as losses of property, automobiles, or life.

For those who are currently aware of cyber insurance or have even bought cyber insurance, there is an on-going concern regarding the cost of cyber insurance, the limits of cyber insurance coverage, and evolutions in cyber threats that create new gaps in coverage that current polices either exclude or do not address. Emerging trends in the past 24 months like artificially generated media, social media account takeover, and cyberattacks on automobiles have created the need for cyber insurers to innovate faster than traditional lines of insurance due to the rapid rate cybercriminals evolve.

Incident Response Firms

The complexity of managing commercial cyber insurance claims requires expertise from several areas to ensure a comprehensive, timely, and effective recovery from a cyberattack. Cyber insurance companies assemble a team of external data privacy attorneys (1-2), digital forensic investigators (1-2), an identity protection firm, IT professionals specializing in data and system recovery, and a digital negotiator and payment vendor in the event of cyber extortion matters.

Incident response firms are interested in developing cyber insurance coverage as many of these firms depend on referral businesses from cyber insurers to provide a consistent source of clients and reliable payments. Without cyber insurance referrals, incident response firms are left to compete for business and seek reimbursement from clients. Both attracting clients and receiving payments from general clients are more complex than receiving a consistent stream of new clients financially supported by a cy-

ber insurance policy that will pay the firms within the firm's desired billing cycle. Incident response firms are vested in the success of the cyber insurance market and commercial policy attachment as less uninsured clients stabilize the business model and financial health of incident response firms.

Cybercriminals

The cyber insurance market has caught the attention of cybercriminals keen to understand how insurers respond to their attack tactics. Before the rise of cyber insurance, cybercriminals had to deal with a broader range of victims' financial positions and the ability to meet demands. However, with more people and organizations insured, the costs of cybercrime are now shifted to the insurance mechanism rather than being borne by the victim. Cybercriminals view cyber insurance as a means to gain financial stability for themselves and their targets. One strategy cybercriminals and cybercrime syndicates suggest to their victims is to file an insurance claim if they cannot meet the cybercrime demands. They also advise victims to purchase cyber insurance in the event of any future cyberattacks. With the cyber insurance market expanding and more policies being made available, cybercriminals now have a larger pool of potential victims to defraud or extort for money covered by the policy. This notion is one that cyber insurance critics point to when arguing that cyber insurance is harmful to the insurance and cybercrime markets as cyber insurance further motivates cybercriminals to target traditionally unappealing victim groups like individuals and small and micro-businesses.

Method

The investigator's background includes direct experience as a practitioner and scholar in the cyber insurance industry. Professionally, the investigator has several years of experience managing cyber insurance claims, incident response, and developing personal and commercial lines of cyber insurance products. Information used in this report is a combination of the investigator's firsthand experience, industry reports, public records, and academic literature.

To analyze the cyber insurance industry, the researcher defined the scope of academic and industry reports to specify those related to cyber insurance rather than the broader insurance industry. From there, relevant artifacts were identified and marked for review to conduct a literature review. This review summarizes the current scope of cyber insurance-specific literature to accompany the industry overview grounded in the investigator's experience, industry reports, and other industry media.

Specifically, this literature review reviews the gap in academic literature pertaining to cyber insurance and incident response. Throughout the review of P&C insurance and cybersecurity literature, the investigator has identified that both disciplines have not conducted research into the use, effectiveness, or efficiency of cyber insurance. This gap not only represents a gap in business and risk management literature but also in computer science and cybersecurity literature.

After this literature review was completed, an industry analysis was conducted which addressed how the cyber insurance industry stakeholders are impacted by the presence, or lack thereof, of coverage but also identified additional opportunities for practitioners and scholars to investigate cyber insurance and raise awareness of this coverage type to match the interest that exists with tenured lines of coverage. This analysis includes a market summary of the industry in which strengths, weaknesses, opportunities, and threats will be identified.

Analysis

Two main analyses are complete in this section. First, a literature review is completed to identify and summarize all relevant academic and industry publications pertaining the current state of the cyber insurance industry. After this review is complete, a Strength, Weakness, Opportunity, and Threat (SWOT) analysis will be presented to summarize how cyber industry professionals can leverage internal strengths and weaknesses while addressing external opportunities and threats.

Literature Review

Cybersecurity, computer science, and computer are the foundation of cyber insurance including understanding and mitigating cyber risks, post-breach incident response, and the active criminals involved in perpetrating cybercrime. With an understanding of the underlying subject matter, a detailed review of the current state of the cyber insurance will be provided.

Cybersecurity

Much of the academic literature on cybersecurity focuses on the technical application of computer science and engineering theory and skills to proactively prevent cyber breaches. Regarding cybersecurity framework and processes, academics and practitioners spend much time researching and experimenting with ways to identify cyber threats and prevent cyber losses (Balzacq & Cavelty, 2016). Specifically, research focusing on using cybersecurity tools and practices on pre-breach activites rather than developing robust incident respond capabilities (Balzacq & Cavelty, 2016). The gap in academic observation of post-breach cybersecurity practice has created a need to understand what other areas of cybersecurity frameworks, processes, and knowledge areas can be applied to cyber risk management.

Specifically, the role cyber insurance can provide to organizations and individuals that were unable to prevent a cyber breach.

Cybersecurity activities such as ransomware negotiation, digital forensics, and network architecture are all fundamental in every cyber insurance policy and most commercial cyber insurance claims. These activities are on-going and active ones that request subject matter experts versed in both cybersecurity and computer science to achieve optimal outcomes for the organization (Ryan et al., 2022). Cybersecurity professionals provide organizations with their networking and infrastructure while they also inform underwriters on the technical side of the risks they are reviewing.

Cyber Insurance

Cyber insurance is the most novel coverage in the insurance market, with the first modern cyber insurance policies being written in 2015 (Granato & Polacek, 2019). Within scholarly cyber insurance publications, most attention is given to explaining cyber insurance policy coverage and terms (Balzacq & Cavelty, 2016; Romanosky et al., 2019; Eling et al., 2021). The initial intent of cyber insurance was to assist policyholders with the increasing costs of the expenses associated with cyber losses. These losses typically include ransomware, social engineering, online fraud, and computer attacks (Wrede et al., 2020). These policies ranged in size from $25,000 to several million dollars in coverage. The availability of larger policies most often requested additional underwriting review and requirements of the applicant.

Cyber insurance continued to gain traction rapidly from 2015 to a peak in 2020 due to the COVID-19 pandemic (Deloitte, n.d.). After the Pandemic, cyber insurers realized net income from policies became undesirable as rapidly evolving cybercriminals, elevated geopolitical tensions, and rapid deployment of new technology expanded the vulnerable digital surface (Granato & Polacek, 2019). Post-pandemic, cyber insurers faced a demand from policyholders to soften and make the market more favorable to buyers regarding expanding coverage availability and insurance limits (Mott et al., 2023). However, prices must be increased by two to threefold to accommodate the market coverage increase. Surprisingly, the buyers responded so positively to the availability of larger policies that they paid the premium without complaint (Mott et al., 2023).

This has accounted for the large increase in cyber insurance applications and policies issued, continuing the trend of nearly doubling policies each year. This is a strong signal that the cyber insurance industry will only continue to develop rapidly and increase its overall share of the general insurance market (Dyson, 2021). At this rate, cyber insurance will become as large as automotive and property insurance. There is an opportunity for industry professionals and speculators to engage in the industry and cyber insurance market.

Key Findings

To fill the gap in academic literature, a review of industry literature highlights the themes of the cyber insurance market. These findings are presented in the SWOT analysis (Figure 4) as common themes in internal and external factors are highlighted.

Strengths

Cyber insurance firms can leverage deep cybersecurity expertise and artificial intelligence to enhance risk selection during underwriting. A hard market throughout the COVID Pandemic allowed insurers to impose strict underwriting guidelines, often requiring applications to make large investment to improve their security posture before a cyber insurance would be sold to the firm. Concurrently, underwriters continued to develop their cybersecurity knowledge supported with implementation of artificial intelligence tools to identify and select applications with favorable risk profiles (Ramachandran, 2025). These strengths support profitable risk selection as the market softens after the Pandemic in favor of lower premiums, higher limits, and less stringent underwriting requirements. Additionally, many insurers have developed in-house incident response solutions to create economy of scale and simplify the operationalization of incident responses processes and vendors.

Weaknesses

While growth in the cyber insurance sector has advantages, it can be hampered by a significant reliance

Strengths	Weaknesses
Cybersecurity Expertise (At-Bay,2024; Corvus, 2024; Elphasecura, 2024)	Limited Product Offering (CISA, 2024)
Strong Market Outlook (Adam & Emura, 2023)	High Dependency on Strategic Partners (Chubb, 2024)
Opportunities	**Threats**
Emerging Cyber Risks (Gartner, Inc. 2024)	Competitors (NAIC, 2022)
Increasing Product Diversification (Munich Re, 2024)	Regulatory Changes (McDonald Hopkins, 2024)

Figure 4: Cyber Insurance Industry SWOT Analysis

on external resources, such as third-party incident response firms. If the demand for cyber insurance rises more quickly than the availability of qualified incident response services, the claims handling may be delayed resulting in unfavorable claims outcomes and dissatisfied customers. Furthermore, the inherently risk-averse nature of insurers, coupled with conservative capital allocation, can create internal obstacles for those with an entrepreneurial mindset who aim to develop new products in response to a demand that often outstrips the available capital in the cyber insurance market.

Opportunities

Cyber risk is a dynamic and continuously evolving rugged landscape. The nature of this landscape generates new risks, sustaining the demand for cyber insurance. This dynamic environment enables insurers to diversify product offerings while the largely undeveloped or underdeveloped segments of the market—often described as a "Blue Ocean"—create space for innovation and growth. New InsurTech firms can also emerge to capitalize on unmet market needs and capture substantial market share before competition intensifies. Within the past decade, mainstay insurance firms have looked to venture capital investment and acquisitions of InsurTech firms as the most efficient way to enter the cyber insurance market through these agile firms with a profitable book of business and intellectual property valuable to claims and underwriting.

Threats

However, pursuing these Blue Ocean opportunities may require specialization or substantial capital investments that deter some insurers and new entrants from competing. As competition increases, it shifts toward more accessible segments of the market, which then become crowded with providers offering smaller-scale, less risky policies. Moreover, heightened regulatory scrutiny increases the cost and complexity of maintaining compliant products. These rising compliance obligations, coupled with competition in easier-to-enter market niches, can undermine growth potential and erode the optimism surrounding the cyber insurance sector.

Discussion

The outlook for the cyber insurance industry is robust, signaling considerable opportunities for growth through expanding policyholder bases, increased written premiums and net income, and ongoing development of innovative insurance products. Cyber insurance is well-positioned to become a leading segment within the insurance market by 2030, if not sooner, driven by heightened attention to cybersecurity, the proliferation of state and federal data privacy regulations, and the continuously evolving sophistication of cybercriminal activities.

As the demand for cyber insurance capacity and diverse coverage options continues to rise, contractual transactions—including those involving lending institutions—may increasingly incorporate mandatory cyber insurance requirements. Such mandates would elevate cyber insurance to a level of prominence comparable to traditional insurance products like automobile, homeowners, and commercial property insurance. Given the current trend where cyber-related losses surpass property and auto lines, the cyber insurance sector will evolve from a niche market into a fundamental pillar of the broader insurance landscape.

Moreover, current trends suggest that the stabilization observed within the cyber insurance market will continue facilitating its transition into a softer market phase. As insurers accumulate larger datasets and strengthen analytical capabilities, underwriting practices, premium structures, and coverage limits are expected to become increasingly standardized. Concurrently, the industry trend toward partnerships between insurers, InsurTech companies, and cybersecurity providers indicates that cyber insurance policies will play a key role in enhancing the accessibility and affordability of cybersecurity solutions. In some cases, policyholders may receive complimentary services, including credit monitoring, dark web monitoring, and cybersecurity policy guidance, or benefit from discounted services such as data deletion and virtual private network (VPN) access. Consequently, more significant capital investment in cyber insurance will benefit consumers by reducing previously unaffordable premiums for limited coverage and lessening the need to incur substantial additional expenses to enhance their cybersecurity posture.

This industry analysis is consistent with conclusions from existing literature reviews, which indicate that cyber insurance remains under-researched within academic circles. Although scholarly interest is increasing, practitioners and industry advisory firms primarily drive current research and discussions regarding cyber insurance. The present analysis provides a valuable scholar-practitioner perspective, offering insight into the current state of the cyber insurance market and encouraging further scholarly exploration into the significant growth and future potential of cyber insurance.

Conclusions

The cyber insurance market has emerged as a significant segment within the global insurance industry, showing rapid growth and substantial market potential. The increasing cyber threats worldwide have led to a surge in demand for cyber insurance, as reflected by the exponential rise in policies and premiums, especially in the U.S. market. The evolution of cyber insurance from a niche offering to a mainstream

product shows the industry's response to the pervasive nature of cyber risks, which have been further magnified by the digital transformation accelerated by the COVID-19 pandemic.

Large direct writing carriers dominate the market, thanks to their financial capacity to underwrite complex risks and serve a diverse clientele. In contrast, midsize and small carriers cater to specific market segments. Reinsurance carriers and InsurTechs play crucial roles in supporting the industry's growth and innovation by facilitating the development and distribution of cyber insurance products.

Despite its rapid growth, the cyber insurance market faces challenges, including the need for more comprehensive academic research, product diversification, and adaptation to evolving cyber threats and regulatory landscapes. The industry's strength lies in its cybersecurity expertise and strong market outlook, but it must navigate the challenges of product limitations and dependency on strategic partnerships

Future growth will likely be driven by the increasing recognition of cyber insurance as a critical component of risk management strategies, driven by regulatory requirements and the intrinsic value of coverage in mitigating the financial impact of cyber incidents. This development positions cyber insurance as a cornerstone of the insurance market, paralleling traditional lines like auto and property insurance.

The current state of the cyber insurance market serves as a call to action for scholars and practitioners to engage more deeply in understanding and shaping the future of this vital industry. By bridging the gap between academic research and practical application, the industry can better navigate the challenges and opportunities ahead, ensuring cyber insurance's role as a pivotal element in the global insurance landscape.

References

Adam, M., & Emura, K. (2023). Global cyber insurance: Reinsurance remains key to growth. S&P Global. Retrieved from https://www.spglobal.com/ratings/en/research/articles/230829-global-cyber-insurance-reinsurance-remains-key-to-growth-12813411

Agrawal, M., & Shivendu, S. (2016). Cyber insurance at USF. Muma Case Review, 1(2). https://doi.org/10.28945/3554

At-Bay. (2024). Homepage. Retrieved from https://www.at-bay.com

Balzacq, T., & Cavelty, M. (2016). A theory of actor-network for cyber-security. European Journal of International Security, 1(2), 176-198. https://doi.org/10.1017/eis.2016.8

Cybersecurity and Infrastructure Security Agency (CISA). (2019). Cyber insurance market assessment. Retrieved from https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf

Chubb. (2024). Cyber partners for mitigation and response. Retrieved from https://www.chubb.com/us-en/business-insurance/products/cyber-insurance/cyber-partners-for-mitigation-and-response.html

Corvus Insurance. (2024). Homepage. Retrieved from https://www.corvusinsurance.com

Deloitte. (n.d.). Overcoming challenges to cyber insurance growth. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/4997_FSI-Cyber-insurance/DI_FSI%20Cyber%20Insurance.pdf

Dyson, B. (2021). Soft market for cyber insurance unlikely in foreseeable future – Gallagher Re. The SNL Insurance Daily.

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. Risk Management and Insurance Review. Advance online publication. https://doi.org/10.1111/rmir.12161

Elphasecure. (2024). Homepage. Retrieved from https://www.elphasecure.com

Gartner, Inc. (2024). Gartner predicts 30 percent of enterprises will consider identity verification and authentication solutions unreliable in isolation due to deepfakes by 2026. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2024-02-01-gartner-predicts-30-percent-of-enterprises-will-consider-identity-verification-and-authentication-solutions-unreliable-in-isolation-due-to-deepfakes-by-2026

Granato, A., & Polacek, A. (2019). The Growth and Challenges of Cyber Insurance. Retrieved from https://www.chicagofed.org/publications/chicago-fed-letter/2019/426. https://doi.org/10.21033/cfl-2019-426

International Association of Insurance Supervisors. (2023). Global Insurance Market Report (GIMAR) 2023. International Association of Insurance Supervisors.

McDonald Hopkins. (2024).. Data privacy and cybersecurity. Retrieved from https://www.mcdonaldhopkins.com/services/Data-privacy-and-cybersecurity

Mott, G., Turner, S., Nurse, J. R. C., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. Computers & Security, 128, 103162. https://doi.org/10.1016/j.cose.2023.103162

Munich Re. (2024a). Auto cyber insurance. Retrieved from https://www.munichre.com/hsb/en/press-and-publications/press-releases/2024/2024-03-26-auto-cyber-insurance.html#

Munich Re. (2024b). Home Cyber Protection. HSB. Retrieved April 19, 2024, from https://www.munichre.com/hsb/en/products/personal-lines-insurers/home-cyber-protection.html#

National Association of Insurance Commissioners (NAIC). (2022). Cyber supplement report 2022 for data year 2021. Retrieved from https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf

Ramachandran, A. (2025). Multi-Agent AI in Insurance Underwriting Leveraging CrewAI, Claude 3.7, and OpenAI o3 for Enhanced Decision-Making and Operational Efficiency.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk? Journal of Cybersecurity, 5(1), tyz002. https://doi.org/10.1093/cybsec/tyz002

Ryan, P., Fokker, J., Healy, S., & Amann, A. (2022). Dynamics of targeted ransomware negotiation. IEEE Access, 10, 32836-32844.

Wrede, D., Stegen, T., & Graf von der Schulenburg, J.-M. (2020). Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. Geneva Papers on Risk & Insurance, 45(4), 657-689. https://doi.org/https://doi.org/10.1057/s41288-020-00183-6

Review

This article was accepted under the ***constructive peer review*** option. For futher details, see the descriptions at:

http://mumabusinessreview.org/peer-review-options/

Authors

Dalton Crabtree is the Specialty Claim Director at HSB. He is currently enrolled in the Doctor of Business Administration program at the University of South Florida. He is also a consultant supporting family businesses through enterprise transition. He received his Master of Science in Insurance Management from Boston University and his undergraduate degree in Finance from Saginaw Valley State University where he is also an adjunct professor in the Carmona College of Business.