Deep Science Publishing
https://doi.org/10.70593/978-81-988918-0-8_2

DeepScience
Open Access Books

Chapter 2: Cyber insurance and the escalating need for digital risk mitigation in business and personal life

2.1. Introduction to Cyber Insurance

When the internet was originally developed and conceived, neither its users nor its inventors had any concept of the enormity and consequence of sharing information and connecting through cyberspace. Businesses, individuals, and countries around the world are now dependent upon this vast network of invisible connections and information. While dependence has encouraged innovation and economic development, it has also created a fragile structure that is subject to disruption by a few determined, creative, and well-placed individuals. For these reasons, cyber businesses are beginning to consider various ways to properly protect themselves. Chief among these is through investing in Cyber Insurance (Attract Group, 2023; Luxoft, 2024; McKinsey & Company, 2024).

The term "cyber insurance" refers to insurance and risk mitigation products and services that are focused on digital and electronic risks. Originally, cyber insurance products were coverages for data breach liabilities. In the years since that first sale, coverage for data loss and data breach liability has become the primary product found in the market. Cyber insurance as defined has expanded to cover other forms of digital risk. These include, but are not limited to, network security liability, cyber extortion and business interruption, media liability, losses related to social engineering fraud, as well as non-digital business risks that are heightened or made worse by the company's reliance on technology and data. To date, focus has mostly been on insuring loss from breaches of a company's sensitive data, especially personally identifiable information of customers or employees, as insurance for this risk is available and is fairly easy to model (Mobilunity, 2024; Stratoflow, 2025).

2.1.1. Background and Significance

As virtually all aspects of modern life have grown increasingly interconnected, so too have the digital networks that underpin our most basic functions. Industries as diverse as healthcare, transportation, and manufacturing, once seen as unassailable bastions of industry-specific security, have become among the most vulnerable to attack. Property, infrastructure, and operational weaknesses are implicated in countless successful attacks, ranging from the routine and banal to the extreme and outsized. Yet even for companies that have expended great resources conducting risk assessments and technological audits to close perceived gaps, protective measures seldom succeed in insulating them against internal and external threats. Sensitive data is easily exfiltrated by insiders. Internal systems easily fall prey to negligent or malicious employees or contractors. Internet hackers easily exploit burgeoning practices like cloud service outsourcing, remote work, and frequent software updates to trigger disruptions in company operations and consumer-facing digital services.

Fig 2.1: Cyber Insurance and the Escalating Need for Digital Risk Mitigation

Despite the growing diversity and costs of attacks, nearly all companies, small and large, pursue similar risk mitigation strategies in response. At the foundation of corporate practice, there remains a desperate faith that investments in tools and personnel will pay

dividends when it comes time to rebuild. But the operational and economic realities imposed by a globalized environment slip this belief into wild fantasy.

2.2. The Evolution of Cyber Threats

Over the last thirty years, the incidence of data breaches has increased globally. The evolution of data breach risk and trends provides much needed insights for business investment decisions regarding cyber security initiatives. Specifically, analysis of key industry data breach disclosures lends support to the position that targeted business investments in both data protection and cyber insurance intending to mitigate and transfer risk, offers valuable company bottom line benefits. Prior to going further, it is important to explain in greater detail data risks and related breaches, and the unfortunate frequency of negative business impact of data breaches occurring globally. In the last 12 months, a significant percentage of organizations surveyed reported that they had experienced some kind of significant cybersecurity incident, most frequently: ransomware attack, another type of malware infection, web-based attack, the compromise of a third-party vendor or partner, data breach or data theft or loss, and business email compromise.

To the dismay of most businesses around the world, cyber threats and their impact on business is not a 'new phenomenon.' With the incredible advances made in electronic communication technology, access to data and the ability to electronically store and communicate information and assets around the world has put an individual's rights to life's essentials, such as privacy and to have one's property and monetary wealth secured from cyber criminals and hackers, into peril. Globally, the concept of data vulnerability and terrorist actions to financially benefit themselves from committing data theft, is not a new issue. Data breaches involving terrorist methods of deception such as wire fraud, money laundering, or employee theft are increasingly occurring all around the world as a result of faster data manipulation, storage, processing, and transmission capabilities associated with modern electronic technology.

2.2.1. Research design

Inasmuch as the major goal of this essay is not only to explore the cyber landscape growth in both its importance and its breadth but also to analyze the responses and solutions available to it, most of the information that underpins the text is presented in a descriptive and non-exhaustive way. The document adopts a qualitative research design to investigate the existent information, gathering relevant secondary data related to the dimensions under study. For this, a significant set of sources was consulted to enclose

key evidence to the analysis, having the Document itself as a source of information for the reader.

In particular, it uses legislation, regulatory guidelines, reports and guidance papers from trusted institutions, statements from key stakeholders and actors in the Cyber Insurance market, including Cyber Insurance Grids and Monitoring Scopes, Cyber Prevention Initiatives, Cyber Risk Modelling Builders, the Cyber Insurance market. It is also relevant to highlight that some specific topics were supplemented with primary data obtained through semi-structured interviews with specific experts in the area. Having described the methodology and main sources behind the gathering and construction of the key contents, we now proceed to the analysis The Cyber Insurance and the Escalating Need for Digital Risk Mitigation. The number of cyber threats is growing, as is the sophistication behind them. Layered Security is the best response to a landscape of several scenarios of exposure. Cyber Insurance provides a financial safeguard. Nevertheless, premiums must start reflecting risk levels adequately as these are detected and measured, and Cyber Insurers properly enclose their activities within the Layered Security structure. Only this way will they be able to protect their financial positions while decisively contributing to Digital Risk Mitigation within the Layered Security structure.

2.3. Understanding Cyber Risk

The term "cyber risk" typically refers to any risk arising from the failure of an organization's IT. However, it is understood differently in each country, as the regulatory approach regarding cyber incidents and insurance solutions vary significantly, reflecting varying degrees of market maturity. In general, only a few high-profile and high-impact incidents are published on, such as ransomware attacks against hospitals, sophisticated nation-state actions against critical infrastructure or the Cobalt Strike campaign against the cryptocurrency industry, both relying on vulnerabilities of supply chain management software. Encouraging protective investment using insurance can help mitigate the growing risk. However, insurance protects from a financial loss, not from the incident itself.

There are at least eight groups of cyber risks that can cause an incident resulting in losses for companies or third parties, as enumerated below. These are typically grouped further into pandemic and localized attack categories:

- Data Theft: Theft of sensitive data such as payment card details, social security numbers, trade secrets, or medical records.

- Service Disruption: Overwhelming service-targeting attacks such as denial-of-service attacks, which can cause insurable losses during service outages.

- Service Manipulation: Depending on the severity of the manipulation, it can also lead to serious insurable losses, such as a mix-up of medications.

- Governance Activity Subversion: Criminals logging in to take advantage of sensitive company governance processes such as merging with another company or appointing a new board member can cause serious losses.

- Supply Chain Manipulation: Exploiting software tools to inject malware and exercising control over connected third-party systems and stealing sensitive information from within a critical infrastructure can cause severe losses.

- Manipulating Company Perception: Gaining access to a company's online presence and posting critical information, which would mislead the public and damage its reputation.

- Security Control Switch: Ransomware or malware switching off security applications of connected machines.

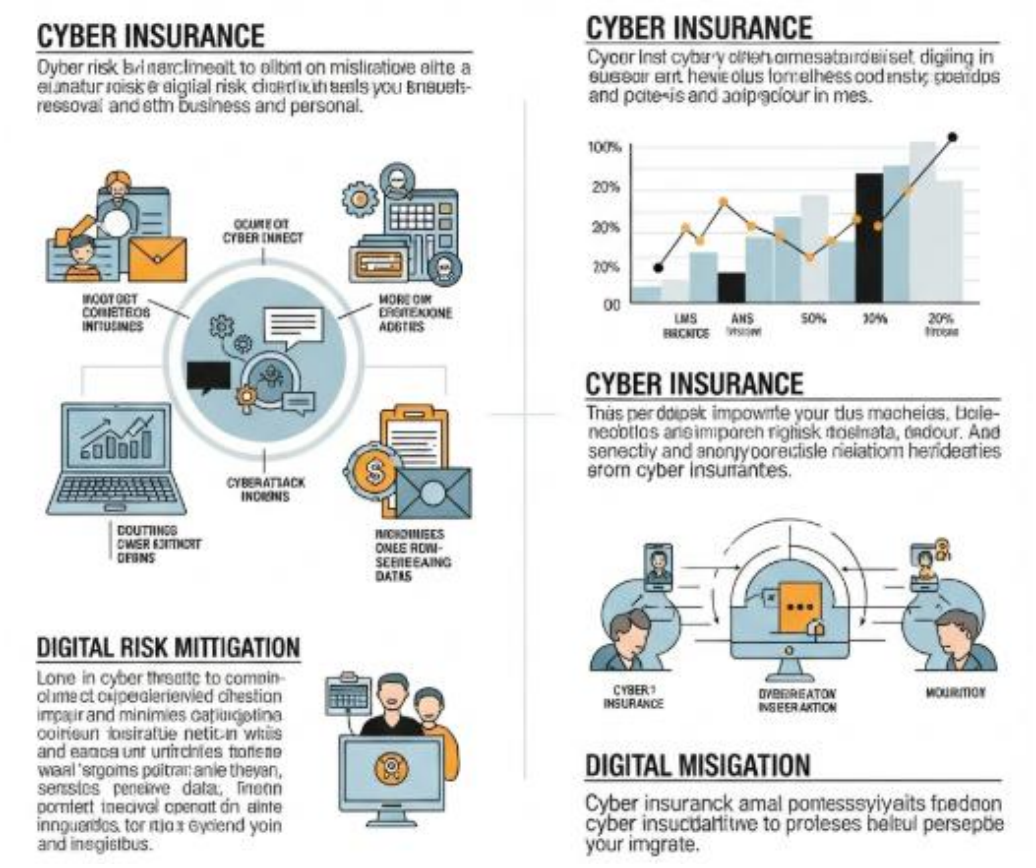

Fig 2.2: Understanding Cyber Risk

2.3.1. Types of Cyber Risks

Cyber insurance is commonly thought to cover loss arising from data breaches, but a particular kind of cyber insurance is actually the only insurance that can be procured specifically to cover privacy violations. Because privacy law has evolved more slowly, there are other kinds of commercial insurance that can be used to provide privacy risk coverage. Cybersecurity and privacy are distinct but related areas of focus. Cybersecurity is generally concerned with the more technical measures used to protect digital information from hackers and other people who should not be able to access it. Cybersecurity insurance is commonly purchased by companies to cover loss caused by the failure of cybersecurity measures that lead to hacking and data breaches, along with other types of digital loss. Digital risks which may be covered by cyber insurance include theft of physical or intellectual property or loss arising from business interruption caused by a company's technology infrastructure failure.

Privacy and cybersecurity work together to protect the different kinds of digital information which companies collect and store, but they use different kinds of strategies. Cybersecurity is generally focused on helping companies protect themselves against hackers, data breaches, digital extortion attempts, and other technology-based risks that cause loss by denying access to or exfiltrating data from a company's systems. Privacy focuses on regulatory compliance and civil liability; it lacks the technology-centric focus of cybersecurity. Digital risk insurers and their insureds are more focused on defending the company for loss caused by hackers and organized crime, business email compromise, cyber extortion incidents, ransomware, distributed denial of service attacks, and other threats. Policy triggers include bodily injury, theft of digital and electronic data, and network security breaches that lead to lawsuits. This version of cyber insurance has evolved to address the risk of the loss of vital data, and is purchased by companies in almost every industry.

2.3.2. Impact of Cyber Incidents

Little more than a decade or so has passed since the first major cybersecurity incidents resulted in tangible damage for all of those involved and were covered widely in the press. Back then, the ramifications seemed narrow in scope, mostly affecting trusted systems and networks. Since then, rapid technological advancements have transformed economies and applied pressure to the very infrastructures that are meant to protect individuals, states, and corporations alike. Cyber incidents today are no longer targeted attacks intending to achieve a goal that is political or ideologically motivated. Instead, cyber incidents today are disruptive and damaging technical failures resulting from less-skilled cybercriminals operating in a world exposed to risk and capitalizing on soft targets. Today’s cybercriminals can execute such incidents at a massive scale. In fact,

increasing digitalization and even global events have driven some critical parts of the economy to a near-exclusive reliance on the same digital technologies that cybercriminals now use to execute their incidents. Indeed, partial or total failure of digital and critical systems for a few hours, days, weeks, or months can today endanger the existence of systems, sectors, parts of economies, and corporations. In short, the very aspects of modern developed societies that have contributed to the success of contemporary economics and politics have also unwittingly created a target-rich environment. Increasingly deliberate and disruptive cyber incidents risk causing near-systemic failure, for example, supply chains for specific products or corporate networks of specific sectors. Today's corporate cybersecurity decision-makers therefore need to acknowledge that their decisions may impact their companies, their industries, and society as a whole, with repercussions that enlarge the potential economic and political consequences of their company's failures.

2.4. The Role of Cyber Insurance

The primary purpose of cyber insurance is not to financially support organizations who suffer cyber incidents; rather it is to induce those organizations to take action to reduce the likelihood or severity of those incidents taking place. Effective cyber risk mitigation, including enterprise and vendor risk management, should be properly implemented to avoid the use of cyber insurance as a substitute for negligence prevention. Legal and regulatory measures would likely assign liability to companies for unwillingness to adopt best cybersecurity practices. Willingness to purchase cyber insurance on appropriate terms and conditions can be viewed as an indirect method to demonstrate adherence to the expected best practices in risk management. In effect, the existence of the cyber insurance market can induce companies to take those measures valued by insurers. Companies should be able to make informed choices to reduce risks in greater quantities or less costly amounts to a level acceptable to both insurers and the insured. Losses will not be paid if the insured did not follow through on a promise to take certain actions or made omissions regarding not implementing those actions.

Moreover, cyber insurance can have a key role with regards to company criminal enterprise risk because in the face of malicious action a policy might by primary effect pay to make investigators and lawyers whole again. However, it should be noted that cyber insurance policies do not necessarily have such a role in practice. A provider of cyber insurance should have the necessary expertise and resources, and in their absence, policyholders could be left without necessary help when they need it the most. Additionally, on-going investigations could also make it either impossible, or at least much more complicated, for the policyholder to take actions that duly comply with the contractual obligation to mitigate losses.

2.4.1. What is Cyber Insurance?

A decade ago, cyber insurance was an afterthought to many business continuity and disaster recovery plans. Fast-forward to today, and cyber insurance is required if a company wants to keep its doors open and business running in a cyber attack. Companies worldwide are diving head first into the world of cyber insurance, seeking coverage for any and all potential cyber events. They are looking for specifics on coverage offered by most major insurers, quantifying what is covered, what is not covered, various limiting factors, deductibles, costs of premiums, associated SLAs, and much more. Selecting the right cyber insurance is critical for an organization's growth and development, and with so many policies to choose from, making the right choice is critical. Cyber insurance is taking off like wildfire, with insurance companies aggressively underwriting and working with all types of businesses to assist in recovery from any kind of cyber incident that may occur. Cyber insurance has begun to reach into almost every possible facet of the cybersecurity world, covering critical infrastructure, organizations building a security foundation with program fundamentals, and more.

The cyber discussion has evolved from mandatory technologies involving firewalls, intrusion detection, endpoint protection, and other technology to mitigate risk to more of a business continuity discussion. Technology budgets are now including funds for cyber insurance policies spanning various requirements to enable some level of financial recovery associated with an event. Hackers are demanding larger ransom payouts to unlock systems, and companies are willing to pay these significantly increased ransom demands to avoid possible perspiration or complete loss of business data, vital functions, and customer satisfaction. Organizations are now compelled to partner with an insurance company to assist in risk reduction by helping build a well-planned response effort to a potential incident. All of these changes have shifted the cyber discussion on both sides of the transaction to financial implications and business ramifications.

Cyber insurance has truly become a business continuity topic, aiding organizations in responding to malicious events in the most efficient and effective manner possible. The insurance company can assist in the development of capabilities while also helping to facilitate the overall recovery once an event has occurred. Many companies now require some level of cyber insurance as a condition of operation as it relates to ongoing business requirements. Partnerships are being formed between insurance and cybersecurity companies to assist organizations.

2.4.2. How Cyber Insurance Works

Cyber insurance is designed to protect businesses from losses resulting from data breaches, hacking and other types of cybercrime. Cyber insurance helps reduce the

impact of online threats, as it can help indirectly improve the quality of a company's network security. Cyber insurance doesn't cover everything, however, and the coverage itself can be tricky to obtain, understand and navigate. Cyber insurance is often sponsored or underwritten by companies that offer other types of insurance, including coverage for property damage, general liability and business interruption. It can be purchased by a variety of businesses, including everything from large corporations to small businesses. Privacy liability coverage protects businesses from data breaches that result in the exposure of sensitive information, such as personal identification, protected health information, or payment card information. Regardless of the type of insurance, businesses may be subjected to policy exclusions. Cyber insurance also mitigates risks associated with working with third-party vendors, as assessments can be performed to manage any liability for breaches that impact the data of other organizations. A business looking to purchase a cyber liability insurance policy typically goes through an insurance broker who specializes in this type of insurance. The business fills out a detailed application that asks questions about the company, the sensitive data it handles, and the security measures it has in place; these measures may include firewalls, intrusion detection and prevention systems, business continuity planning and disaster recovery systems, and employee training. The insurer then assesses the application based on the risk profile it creates; the information a company provides can significantly impact its cyber risk profile and what it pays for insurance, as policyholders with strong cyber defense postures can reduce their premiums. The higher the risk, the higher the price — or the application may be denied altogether. The details of the coverage depend on the type of policy purchased.

2.5. Market Trends in Cyber Insurance

Insurers are still struggling to build a pool of insureds large enough to provide an effective spread of risk. And with the cyber insurance market seeing rapid growth, companies must carefully evaluate coverage options to ensure their choices both protect their companies and don't break the bank. The growth of the cyber insurance market is breathtaking. The global insurance market for purchasing cyber insurance is estimated to be worth at the end of 2020. This represents an astonishing increase over the gross premiums written for such insurance policies in 2019. Analysts expect that the total cyber insurance market will reach over in premium volume by the mid-2020s. Others have an even higher expectation with some investment banks claiming it will grow to by 2025.

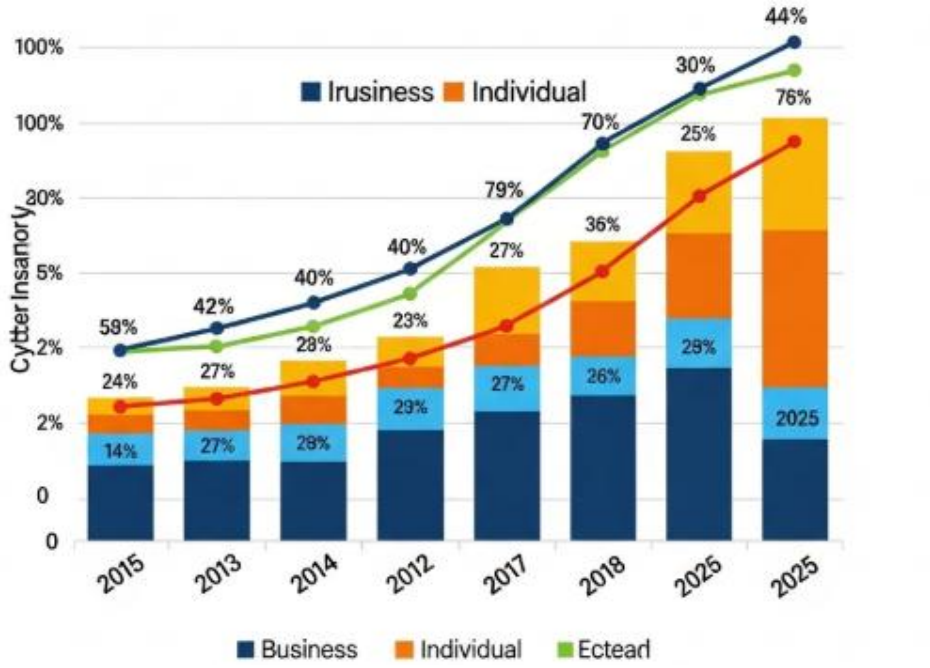

Fig : Cyber Insurance and the Escalating Need for Digital Risk Mitigation in Business and Personal Life

2.5.1. Growth of the Cyber Insurance Market

The cyber insurance market is basically a risk transfer mechanism for digital perils, like hacking, data theft, data loss due to natural disasters, DDoS, business interruption, consortium liability, etc. As the digital risk landscape expands dramatically and evolves to new scales, businesses and organizations are increasingly recognizing the necessity of transferring some risk through cyber insurance, not merely self-insuring coverage gaps. Cyber insurance transfers some of the real – and often severe – financial consequences of a cyber attack or a data breach in exchange for premium paid. Cyber insurance confirms the fact that failure to prevent a breach makes an organization liable for damages incurred from that incident.

The cyber insurance market is growing at a fast pace and is projected to reach more than USD 65 billion by 2027. There is continued debate about whether this level of market growth is sufficient to ensure affordable coverage for those that want or need it. The global cyber insurance market will increase from USD 9.2 billion in 2020 to USD 20.4 billion by 2025 at a CAGR of 17.5%. The increase is not just linked to the growing frequency and severity of ransom payments, but that it also reflects the growing pressure for organizations to close the security gaps and to comply with federal regulations.

Similar projections are also being provided by various other market research companies. Cyber insurance will be mandatory for businesses with more than USD 1 million in revenue by 2025. A separate study finds that governments on both sides of the Atlantic are considering requiring companies to hold cyber insurance in order to counter the risk that they pose for the economy and other enterprises linked to them.

2.5.2. Key Players in the Cyber Insurance Industry

For the purposes of this report, we will define the players in the insurance industry as those companies insuring cyber risks either as standalone cyber insurance, elements associated with more traditional offerings or as aggregate policies covering a number of risks within the insurance domain. Insurers selling such standalone products include the leading players in the cyber insurance arena. In addition, there are a growing number of smaller insurers selling standalone products that utilize third-party risk assessment and financial modeling services in order to underwrite cyber risks.

The companies competing in the cyber insurance industry are utilizing a variety of methods to compete for market share. A number of leading players are beginning to utilize third-party risk assessment and financial modeling services as part of an effort to provide more customized policies that hedge their own underwriting exposure. The leading financial modeling firms are being approached by insurers in the industry covering various parts of the cyber risk landscape. The offerings of some of these firms have been modeled specifically to cover a specific peril, such as ransomware attacks.

The industry is already beginning to see major pricing volatility, with a number of the bigger players in the market reporting increased losses in the cyber insurance space, driven both by increasing costs for claims and exits from the space by major reinsurers. With claims costs increasing, the pressure is on insurers to increase policy pricing, while at the same time, smaller insurance providers are entering the space and choosing to undercut the pricing of existing insurers and take on a far larger proportion of the risk share.

2.6. Conclusion

Organizations examine their security budgets and how much is too much. One way to supercharge the cyber insurance program is to offset risks through actual security controls in every critical area outlined in this work. Properly scrutinizing and defending an organization will lower the likelihood of filing claims or making insensitive requests for business disruption and data breach. If an organization wants to generalize, insurance coverage could offset properly classified costs based on the critical areas discussed in

previous sections. A focus on the critical five areas of Governance, Information Technology, Operational Technology, Cyber Threat Intelligence, and Risk Management is more accurate for selecting and classifying risk for cyber insurance purposes than just a policy on cloud security. The five areas are a guideline. Some organizations may gravitate toward one key area. The insurance underwriter areas should be able to glean useful information specific to their organization's needs to maximize a productive partnership. I explored the potential of a partnership between an organization and a cyber insurer in honestly reviewing their concerns. Organizations can gain loss control services to redirect a claim due to business interruption or data breach issues. In this new paradigm, organizations may be more inclined to share sensitive claims data with a trustworthy cyber insurance provider. Insurers will benefit from having a wealth of data at their fingertips to use predictive modeling and actively offer layers of support to prevent the claim from taking place. With a closer relationship, organizations will benefit from more customized programs and will use them as true advisors. An organization's interest in consummating the relationship for mutual benefit will be key.

2.6.1. Emerging Trends

Cyber risk, and without a doubt the digital risk burden, are continuously growing in sophistication toward businesses of all types and sizes. And while companies' management teams and cyber professionals attempt to defend their organizations against cyberattacks and other risk events, there may be no company that is next in line for becoming a victim of a high-profile cyber attack, such as ransomware. Nevertheless, luckily for businesses, shareholders, and C-suites, the cyber insurance market appears to have turned a corner, balancing the equation through new underwriting choices and improved risk models that provide companies with a level of risk as well as a potential safety net.

Their evolving risk and solutions condition is forcing companies to recognize how to access silos with their partners in the cyber insurance market that may lie beyond property and casualty insurance. Those buried silos are being unearthed by direct brokers who specialize in tech and cyber coverages as well as the reinsurance markets, which write the insurance, leaving original insurance company reserves and models subject to periodic pressures during loss cycles.

The goal of this chapter has been to provide a realistic view of the current broken state of balance in the cyber risk and insurance markets and to offer company executives factual tools and content to utilize when trying to determine what cyber insurance is and is not, to realize that cyber insurance is critical to consider and incorporate into their overall risk programs, and to offer clients simplified value as they look to discuss their specific areas of need, structure, and capacity with their insurance brokers. We have

made a conscious effort to simultaneously provide a detailed program review and a general overview in order to address both new and seasoned buyers.

References

McKinsey & Company. (2024). Tech-driven insurers: How to thrive in 2030. McKinsey & Company. Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/tech-driven-insurers-how-to-thrive-in-2030 mckinsey.com

Attract Group. (2023). Digital Transformation in Insurance Industry: Unlocking the Potential. Attract Group. Retrieved from https://attractgroup.com/blog/digital-transformation-in-insurance-industry/ attractgroup.com

Stratoflow. (2025). AI Enhanced Claims Processing. Stratoflow. Retrieved from https://stratoflow.com/insurance-industry-trends/ stratoflow.com

Luxoft. (2024). Automation and virtualization power efficiency. DXC Luxoft. Retrieved from https://www.luxoft.com/blog/top-10-insurance-technology-trends-2024 luxoft.com

Mobilunity. (2024). How Predictive Analytics and ML Are Reshaping the Insurance Landscape. Mobilunity. Retrieved from https://mobilunity.com/blog/technology-trends-in-insurance-industry