—Reprinted from PIA Magazine, December 2022, with permission from PIA Management Services Inc.—

**JAMES J. VENEZIA, CPCU, CCIS**
President, Animal Genius Sage LLC

# THE CYBER ROAD

## THE PAST, PRESENT AND FUTURE OF INSURANCE PRODUCTS

Historically, insurance products have followed the road most traveled with a few detours. By tradition, insurance product development has been a slow methodical process. However, this changed with the introduction of cyber insurance; this insurance emerged and accelerated through the market after a bumpy start. It continues to evolve at a pace close to the discovery of vulnerabilities—at least in the context of insurance products.

Underwriting insurance coverage and provisioning loss control services have improved with knowledge, technology and education. Generally, the latter (loss control services) creates friction for policyholders as integration of such services remains an arm's-length interaction, and it is often viewed with suspicion and ill will. The ill will may appear to be an unfair statement, until it is viewed from the perspective of the insured, who anticipates recommendations and premium increases, which are perceived to be costly, yet add no value to the bottom line of the organization.

Cyber InsurTechs—an insurance product model in which a company leads with proprietary technology bundled with a cyber insurance product—changed the model and perception of loss control services. This shift in perception has changed the cyber insurance distribution model as well as the expectations of insureds.

While it is hard to say whether the effectiveness of the change can be attributed to market timing, a harmonization of well-educated technologists with proprietary technology and vision, or marketing/education, it's likely that a combination of each of these factors, in varying degrees, has played its part.

## Cyber insurance became unique

From the early to mid-2000s, cyber insurance evolved slowly—as did most insurance products. From the teen-2000s forward, the product, including its underwriting process and purchasing simplicity, gained a momentum of its own due to several factors coming together to bring awareness to cyberrisks (i.e., the fear of reputational and existential loss; and realization that cyber risk financing solutions were available). While these factors drew interest from businesses and their boards of directors, insurance companies that struggled for growth and innovation, ramped up development of the cyber insurance product line and prioritized it as a revenue stream.

As the market for cyber insurance accelerated, the competing forces of building market share, and profitably underwriting accounts, collided for traditional insurers. This was partly due to an unanticipated escalation of ransomware attacks, miscalculations of attack vectors, and immature underwriting standards in terms of requirements for cyber security protections and employee education.

It is interesting that lessons learned about cyberrisks, over the decades, were not contemplated, or forgone, in favor of other objectives. Cyberrisks are well documented in:

- The 1989 book *The Cuckoo's Egg*, by Cliff Stoff; and
- *The Lazarus Heist*, the theft of which happened in early February 2016. It is well documented in the BBC podcast of the same name.

It appears that these lessons were far removed from the trainings of insurance professionals and the insurance underwriting community. Except for certain niches, generally, underwriting is not filled with technical specialists in specific disciplines, such as cybersecurity or software engineering. This is changing, at least with respect to cyber insurance where industry education continues to gain traction in an attempt at keep pace with threat actors.

The collision of market share and profitability was a hard impact for many insurance companies that originally anticipated loss scenarios that would track in the manner of the 2013 Target data breach, during which personal data exfiltration—and not ransomware—would lead to cyber insurance losses. This miscalculation became especially costly as many insureds, small businesses, and large businesses, were unprepared to protect themselves against such attacks.

This lack of preparedness was financially compounded for insurers that were not underwriting to a comprehensive baseline of cyber security hygiene. In addition, the insurance marketing and sales community did not fully understand cyberrisks, which likely led to a high percentage of adverse selection; with higher-risk insureds purchasing cyber insurance coverage while moderate- to lower-risk insureds sat on the purchasing sideline. Ultimately, the sidelines emptied onto the field as ransomware made every organization a likely target as social engineering causes every employee to be part of the attack surface.

This awakening to ransomware risk occurred while underwriting was still a relatively simple, frictionless process. Coverage grants and policy language was generous, and (of course) premiums were attractive to buyers.

As insurance companies learned hard lessons about cyberrisk, the technologist entrepreneurs were considering a model in which insurance solves the cyber risk conundrum and creates a more effective and efficient partnership between parties. This group of thought leaders recognized

**Education opportunity**
Create cyber education initiatives in support of stronger public education about electronic device perils and best practices.

a disconnect between loss control, partnership, and insurance coverage, and capitalized on an opportunity for a synergistic model.

Early on, the offerings of the cyber InsurTechs appeared suspect to many insurance professionals who relied on a traditional insurance model to underwrite, loss control and issue insurance products. A portion of the insurance community questioned the wisdom of offering protective technology services in conjunction with an insurance policy. In addition, several InsurTechs used multiple insurers to address a policyholder's insurance needs. Important questions were raised by some insurance agents and brokers, which included the following:

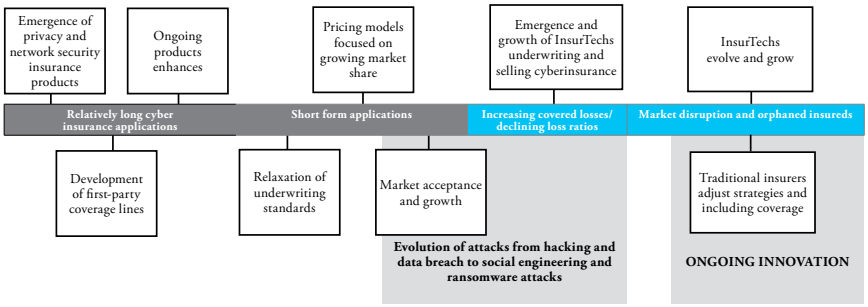
- Could this create a conflict of interest if a technology platform failure led to a lag in loss control and a subsequent claim event?
- What about the quota share insurance arrangements—which were uncommon for many traditional admitted insurance lines (those lines primarily sold by the insurance agent and brokerage community)—was this the right way to structure coverage for the long run?
- Would the claims handling services be satisfactory? Early rumors caused many to envision a lone individual taking the initial call and fumbling to toggle it to a disbursed team of cyber claim professionals.

It is safe to say that these concerns quickly subsided as cyber InsurTechs proved their value to the insurance and business communities. These products became favored as a formidable partnership, which addressed a potentially grave uncertainty; this was especially true for small- and middle-market businesses. The type of partnership created by the cyber InsurTech model was lacking in the traditional insurance product model where portals could not match actionable information inclusive of cyber security expertise that was a phone call away. The model quickly became and continues to evolve as an attractive alternative to traditional insurance.

## The new age of insurance

Let us consider the growth of the cyber InsurTech model as part of the new age of insurance, in which the insurance model continues a trend toward integrating technology advances and advantages into a traditionally human-led relationship; from underwriting and claim handling, to risk scoring/benchmarking, preemptive loss/threat intelligence, and parametric claim triggers. The table below provides a sequence of events in the development of cyber InsurTechs and a sense of the evolving cyber insurance environment.

### How we got to today




As the cyber insurance market continues to evolve, an important consideration for insurance professionals having the cyber insurance conversation is framing the unique aspects of, not only, different cyber insurance policies, but also unique cyber insurance underwriting, product delivery, services, and product life-cycle models. One way to think about the conversation is as follows.

**Traditional insurance company perception:** To understand the success of the cyber InsurTech model it is helpful to look at the traditional insurance model and insureds' perceptions.

Traditional business insurance tends to be viewed as something you buy and set aside for that moment you hope never comes—a claim that ultimately tests your expectations of the policy. Unfortunately, cyber insurance products offered by the traditional insurance community quickly fell into this category.

Typically, the model leaves risk management to the insured, the brokerage team and (maybe) an outside consulting group. Portals for information are a nice touch, although most go unexplored and unused.

In this model, a cyberpolicy is accepted or declined based upon an application, without a meeting with the insured or collaborative conversation about cyberhygiene and actions that might allow for re-underwriting the coverage. This model tends to shut the door on often loyal clients who feel abandoned in the face of significant risks.

Alternately, traditional cyber insurance may have some potential advantages.

- Historically, traditional insurers have written most cyber insurance exposures, this includes providing (real, not silent) coverage on a variety

of policy forms, including property insurance via electronic vandalism endorsements and specific cyber insurance endorsements; directors & officers insurance specific to fiduciary duties and governance; crime insurance specific to employee dishonesty and insider cyberthreats, as well as social engineering.

- Traditional insurers have handled claims within the structural coverage areas addressed by cyber insurance, including regulatory claims and government actions on directors & officers insurance; property and business interruption claims; kidnap and extortion claims; personal injury and media liability claims; and crime claims, including employee dishonesty; as well as weather-related claims that require significant and coordinated claim handling across a large geographic area.

The above experience gives the traditional insurance platform a good deal of direct and indirect intelligence and skill as it relates to cyberrisk and related claim handling, for some insureds this is a critical value.

## Cyber InsurTechs

To differentiate between the initial construction of the cyber InsurTech model and the evolution of the model, cyber InsurTechs will be described as versions, specifically, version 1.0 and 2.0, followed by a look at further evolution (version 3.0).

**Cyber InsurTech version 1.0:** Version 1.0 created an insurance model of collaborative partnership. From a technical perspective, the partnership allows an insured to manage cyberrisk and events from a loss identification, loss control and loss indemnification perspective aided by technology along with supportive cyber security technicians.

Early on, the model lacked some of the best-in-class insurance coverage language provided by the traditional insurance companies. This is an important consideration as the coverage tiers and limits are not indicative of coverage quality and depth. More recently, InsurTechs have improved their policy forms, and in many cases matched the quality of the traditional insurance company coverage language.

The model combines proprietary technology platforms, designed for underwriting and quoting, as well as policy issuance and real-time risk management services from identification through remediation. Frequently, insureds receive targeted alert messages with information related to necessary corrective actions.

A unique aspect of the underwriting process is the willingness to create a real-time underwriting and pre-binding partnership with an insured, offering personal loss control meetings and collaboration to address potential cyber risk concerns. This model differs from most traditional insurance experiences in which the underwriting door is shut, and the insured is left to address complicated cyber risk exposures independently.

Pre-binding meetings are handled in way to give the impression of a helping hand, as opposed to the arm's-length relationship that has characterized the traditional insurance model of pure application-based cyber underwriting.

The proactive relationship building leads to strength of partnership and willing collaboration, which may be the most significant difference between the cyber InsurTech model and traditional insurance model. Brokers who have participated in real-time underwriting and pre-binding meetings come to appreciate the partnership aspects of the interaction. This refreshing experience may be the key defining attribute of the cyber InsurTech model.

Partnership aside, it is difficult to judge whether the proprietary technology of the cyber InsurTech model provides an advantage to insureds in terms of claim avoidance. However, loss data provided from at least one cyber InsurTech indicates that the loss experience has been favorable relative to the traditional insurance company model; it is important to note several factors may account for this and more time is necessary for a complete assessment.

**Supply-chain risks**

Unidentified cyber supply-chain risk will lead to potential bottlenecks for businesses. This is a particular concern for small- and middle-market businesses that do not have the resources to audit vendors and enforce cyber insurance coverage requirements. These organizations will benefit from InsurTech innovations that offer attack-surface scans and robust supply-chain underwriting tools that include the ability to identify concerns specific to technology and nontechnology vendors, subcontractors and consultants. Facilitating this type of risk management will generate conversations and could help reduce cyber contingent/dependent business income risk and supply-chain interruptions.

While strong collaboration is a clear advantage of this model, it may be constrained by the lack of internal data and breadth of claim-handling experience brought by the traditional insurance company's cyber insurance delivery method.

Another point of interest is the fact that a couple of InsurTechs use multiple insurance companies on a quota-share basis to provide coverage. It has been expressed that this is a hedge against aggregation risk, although there may be other reasons, including a lack of individual insurer confidence in the model or in supporting the model.

The cyber InsurTech model has pushed the envelope on commercial insurance innovation and relationship building. Version 1.0 has set a standard that agents and brokers need to understand and include in a cyber insurance marketing strategy.

**Cyber InsurTech version 2.0:** While maintaining the characteristics of the previous version, this one adds another element to the model, proprietary end-point software designed to mitigate losses by reducing the insured's attack surface, limiting cyber event damages, and providing resiliency in the face of a loss through immutable back-ups.

When this model was introduced, it changed the cyber insurance paradigm. Now cyber security protection is no longer a limiting factor in attaining cyber insurance (at least to the extent an industry is within the underwriting appetite of the cyber InsurTech 2.0), as the cyber security protections are part of the cyber insurance offering.

This model allows an insured to hand off cybersecurity concerns to the InsurTech partner, attaining a relatively respectable level of cyber protections along with a quality cyber insurance policy.

**Awareness initiatives**
Cyber threat intelligence and awareness initiatives can be incorporated into other community alert systems to better inform the public about emerging risk and real-time vulnerabilities.

While this model has clear advantages to organizations with non-existent or immature cyber security frameworks, organizations with more mature cyber security frameworks and technology teams (internal or external) can be resistant to add another layer of software on their computers.

This model does require a detailed understanding of the insurance policy form. Failure to set up the proprietary end-point software on a computer will result in coverage limitations at the time of a loss.

**Cyber InsurTech version 3.0: What's next?** While it is difficult to predict the future, the cyber InsurTech model is likely to unleash a wave of innovation and interest in the insurance industry. An overlooked benefit of cyber insurance and the cyber InsurTech model may be the fact that it has made insurance interesting to technologists and students of the technology arts; this alone will raise the bar in insurance innovation at a rate the industry has not seen and that some may find uncomfortable.

The future is here with additional cyber insurance products based on parametric coverage triggers as well as those covering cryptocurrency emerging and developing.

## Conclusion

The future of cyber insurance will be transformative as traditional insurance companies, InsurTechs, cyber security technology providers, and governments seek more favorable protective measures to address economic and existential risks posed by cyberevents.

An insurance future with a synergistic integration of individuals who have specialized skill sets will continue to increase the momentum. These individuals who choose to showcase their talents to the insurance industry will continue to evolve the model led by unique technologies, real-time partnerships, and novel collaborations. The model will develop shared intelligence and become a leading force in cyber and economic security, as well as a key factor defining resiliency in the face of otherwise catastrophic exposures.

The components of such a model already exist, the key constraint is attracting talent and crafting a sustainable educational system to address the industry's unique needs.

*Venezia has more than 37 years of experience managing risk from start up to exit. His strength is working with visionaries in all walks of life through thoughtful, collaborative dialog to provide perspective and clarity with respect to managing existing and emerging risk. Reach him by email at venezia_jj@comcast.net. For more information, visit www.linkedin.com/in/jjvenezia/.*