2019

Back to the Future of Cyber Insurance

Tom Baker
University of Pennsylvania Carey Law School

Back to the Future of Cyber Insurance

Tom Baker

As any student of insurance history knows, it can be too soon to study an insurance market. A far more entrepreneurial business than outsiders realize, insurers regularly develop new products that don't work out. When one does work out, the mature product may not look much like the lightbulb that went off in the heads of the underwriters who invented it. So, if you study a new insurance product market too early, you'll get the wrong idea of what it's about.

When Leib Dodell described to me – at my dinner table in West Hartford over 20 years ago – the Safety 'Net product that Chubb was getting ready to launch, I knew immediately that I was in the presence of one of those crazy underwriters. Inside Leib's lightbulb, Safety 'Net was "internet liability insurance," which meant media liability insurance for the thousands of Main Street businesses that were becoming publishers by virtue of putting up a webpage.

Elsewhere in the universe at about the same time, Emily Freeman had a different lightbulb. Emily and her colleagues at Marsh developed Net Secure, the first "online insurance program," which meant business interruption insurance for "internet businesses" facing downtime from hacking, fraud, and viruses, with some liability and privacy loss protection as well.[*]

I caught up with Leib recently, by phone from his newest venture, Bar K, an emerging chain of dog park bars (yes, you read that correctly) that make productive use of distressed space inside city cores. I asked Leib to first imagine himself back at his Safety 'Net lightbulb moment and then to imagine himself immediately transported back to today: What surprises you about the cyber insurance market in 2019? What's the same today as back then?

Leib said that he was most surprised that the "first party" breach coverage turned out to be more significant for most people than the liability coverage. "That means Emily Freeman was right at the beginning, and I was wrong," he said. What is the same, he said, maybe even to a

surprising extent, is the uncertainty. The risks are still significantly unknown, the policies continue to evolve, and, as a result, pricing continues to involve lots of trial and error.

Leib's trip back to the future convinced me of two things. First, it's not too early to study the cyber insurance market. Leib may not have been right at the beginning, but he says that Emily Freeman was. That means there are twenty years of enough continuity that we ought to be able to make sense of what the cyber insurance market does and how it works. Second, there is at least one very big continuity that clearly deserves our attention: How have insurers managed for over twenty years to sell insurance against cyber risks that their underwriters don't (and can't) fully understand?

It's still early in my study, but I have a preliminary answer to that question that I've shared with Leib, as well as some cyber insurance professionals who haven't abandoned insurance in favor of urban development. They have encouraged me to share that answer with readers of the PLUS Journal. I encourage you to let me know where I'm right and where I'm wrong, because there is still plenty of time for me to get it right.

My answer comes in five and a half parts. The five are (1) providing valuable services beyond risk transfer, (2) contract design, (3) rapid iteration of pricing and forms, (4) limits management and reinsurance, and (5) claims disputing. The final half is public backstops and pools, which is a "half" because it hasn't yet gone beyond the talking phase.

Beyond risk transfer. Most notably to me, cyber insurers manage uncertainty by providing lots of easy-to-price loss prevention and loss mitigation services, so that the value proposition of a cyber policy includes "free" or low cost access to these high quality services, not just the risk transfer that typically motivates insurance purchase. These services often include risk assessments and intrusion testing, and they almost always include expert assistance in responding to privacy breaches, ransomware attacks, data destruction, and other cyber events. For many people, these services may be the most salient aspects of the coverage.

I include these services as *uncertainty management tools* for several reasons. First, the tools aim to reduce the frequency and severity of cyber losses, potentially reducing insurers' losses, especially the crucial area under the right tail of insurers' loss distribution. Second, to gain access to the post event services, policyholders must report those events to their insurers, allowing insurers to gather more and better data about loss events that they can use in contract design, pricing and underwriting. Finally, these services help insurers build demand for cyber insurance without exposing too much of their balance sheets to the underlying cyber risks.

Contract design. Insurers use contract design to manage cyber uncertainties in both cyber and non-cyber policies. In cyber policies, the key elements are narrowly defined coverage categories, typically with separate limits for each, and claims-made coverage for liability risks. The narrowly defined categories and limits interact with the rapid iteration of pricing and forms (which I'll describe next) to allow insurers to dip their toes in the water and only gradually go in deeper. The first party risks that provide the bulk of the protection have a relatively short tail, allowing insurers to get out of the water relatively quickly if they need to. The claims made coverage for the liability risks gives insurers some comfort that they can get out of the water quickly on the liability side, too.

In non-cyber policies, like traditional property, general liability, and errors and omissions policies, the most important cyber risk design element is the exclusion, to manage the "silent cyber" coverage under those policies and shift coverage to cyber policies. There is also an emerging trend, at least in the property insurance market, of a cyber coverage sublimit that, in effect, gives back part of the coverage for cyber risks that would otherwise be excluded, similar to the flood sublimits in commercial property programs.

Rapid iteration of pricing and forms. One very important way for insurers to manage uncertainty is to pay close attention to the results under their current book of policies and then to regularly and rapidly update policy forms and prices based on that information. Leib says that's what he did at the beginning, and that's what I observe insurers doing today. All that updating can drive some people crazy, and it means that the results under old policy forms

become increasingly less relevant for future pricing. But that's a tradeoff that allows insurers to venture into the unknown. Rate and form regulation complicate that rapid iteration, so cyber policies typically are issued in the surplus lines market, which is largely exempt from that regulation.

Updating traditional policies, which are subject to that rate and form regulation, is more cumbersome. As a result, fine tuning the approach to the silent cyber coverage in a traditional policy will take longer than fine tuning a cyber policy. As a corollary, explicit grants of cyber cover will remain largely the province of cyber policies, at least for now, except perhaps in the large commercial market, where regulation is less intrusive because regulators expect that brokers and risk managers generally provide adequate protection for policyholders.

Limits management and reinsurance. For insurers, limits management and reinsurance are two different, but highly complementary strategies for managing uncertainty. Limits management is a complicated topic that perhaps can best be explained by identifying the key moving parts: the amount of the cover provided to any particular customer against any particular set of risks; the amount of cover provided to each customer segment against a set of risks; the amount of cover provided overall against a set of risks; and the relationship of all these things to the other risk and customer segments of the insurer. The most complicated parts include assessing the relative risks of different customer sectors and assessing the potential for aggregation (in other words, lots of claims all at the same time) within and across sectors. Reinsurance is a complementary strategy, because reinsurance contracts can be crafted to share or cap the insurer's exposure on a customer, customer segment, product segment, or company wide basis (and other ways as well).

Reinsurers need their own limits management strategy, too. They need to decide how much cover they're willing to provide to any particular insurer against any particular set of risks. They need to segment their insurer customers. And they need to track and manage their exposure, not only on an insurer by insurer, segment by segment, and product line by product line basis, but also according to their exposure to specific large policyholder companies (which

buy towers of insurance from multiple insurance companies), on both the liability and asset sides of their balance sheet.

Not surprisingly, reinsurers are highly focused on the uncertainties of cyber risks. They and their vendors are building tools to track and model cyber risks. They are engaging with technical experts to understand and assess cyber risk, especially from an aggregation perspective. And, so far at least, they are selling cyber reinsurance only on a quota share basis, meaning that they share a fixed percentage of the reinsured risk with the ceding insurer from the first dollar all the way up to the limit of the reinsurance contract. Reinsurers are not yet willing to sell cyber reinsurance on an excess of loss basis (a form of reinsurance in which the reinsurer pays all or a share of losses after the ceding insurer pays a certain amount) because they are not prepared to reinsure only the (more uncertain) right tail of the loss distribution.

Claims disputing. Almost nobody in the insurance industry likes to talk much about claims disputing. But claims disputing can be an important uncertainty management tool. Claims disputing provides the opportunity for a deeper dive into the circumstances of a big loss than would otherwise generally be the case, generating knowledge that has the potential to inform underwriting and contract design. Claims disputing also clarifies the meaning of insurance policies and, thus, the boundary of the risk transfer. This has been especially important for silent cyber, and the current litigation regarding war exclusions in cyber policies suggests that claim disputing will help define the boundaries of the risk transfer under cyber policies as well.

Public sector backstops and pools. The litigation over the application of the war exclusion points to my final category: public backstops and pools. The concern underlying the war exclusion litigation is that state-sponsored or state-encouraged cyber attacks differ from ordinary cyber attacks in at least two important ways.

First, ordinary cyber events are more like ordinary crime and negligence and, typically, are not intended to destroy the businesses affected. When the perpetrator acts with intention, the objective typically is theft or ransom. When the objective is theft, the perpetrator tries

hard not to disrupt the business; where the objective is ransom, the perpetrator needs to provide credible evidence that the disruption can be undone, or the business will not pay the ransom. By contrast, state sponsored or encouraged cyber attacks are more like terrorism: the objective is permanent destruction, greatly increasing the business interruption loss, the costs of rebuilding the system, and the data restoration loss.

Second, state sponsored or encouraged cyber attacks are more likely to be directed to cause maximum destruction, shutting down essential services, or replicating on a massive scale. This raises concerns about loss aggregation, which, as we learned from the impact of the terrorist attack of 9/11 on life and workers compensation insurers, can affect insurers in unforeseen ways.

These differences suggest that there may be a role for the public sector in arranging financial backstops or pools for at least some cyber risks. While it's too early to identify the precise justification for this kind of arrangement, candidates include the destructive impact of a massively aggregated loss on insurer capital, the fairness of using public funds for projects that benefit society as a whole, the social security provided by having a backstop in place, and the potential consideration that the insurance industry could be asked to provide to the government in return for these arrangements, such as cyber event data and cooperation in disseminating best practices.

---

[*] Edmundo Conchas, Web retailers clamor for 'hacker insurance,' Dallas Business Journal, September 24, 2000.