Could cyber risk be the next Big Short?

Traditional managing and underwriting of cyber risks point to vulnerabilities for insurers and the world economy. These vulnerabilities call for a new risk management paradigm.

Chris Harner, FRM
Chris Beck

Milliman

In a pivotal scene from "The Big Short," investment bankers can hardly contain their laughter when Michael Burry tells them he wants to buy credit default swaps on mortgage bonds, which will pay off if the underlying bonds default. Incredulous about the proposal, one of the bankers tells Burry the swaps would only pay out if millions of Americans defaulted on their mortgages, which had never happened. The scene is central to the film because it illustrates how the key market players missed the big picture, one that eventually led to 2008's subprime mortgage meltdown and the triggering of the global financial crisis. "Here was a strange but true fact." writes Michael Lewis, author of The Big Short, "the closer you were to the market, the harder it was to perceive its folly ." From the underwriters, to the bankers, to the market-makers, to the rating agencies, many players close to the market[1] lacked a sufficient systemic picture to see the true risk.

Could the same situation be brewing for insurers when it comes to cyber risk? The parallels between the lead-up to the mortgage crisis and the rapid growth of the cyber insurance market are eerily similar.

The seeds of turmoil

At the core of the mortgage crisis was a belief that what had not happened could not happen, namely that housing prices across the board could suddenly plunge. This interplay between "group think" and "confirmation bias" drove market participants to relax mortgage underwriting standards as they moved down the credit curve into deep subprime. Borrowers and lenders alike made the false assumption that if borrowers got into trouble, they could refinance their homes. Underwriters, risk managers, and traders relied on standard backward-looking models that failed to anticipate the interconnectedness of low interest rates driving housing prices and subprime loans which then flowed into MBS, CDOs, and CDO-squared hedged by Credit Default Swaps. The production, warehousing, and hedging of subprime risk resulted in greater counterparty risk, liquidity risk, and leverage within the global banking system.

The standard risk paradigm failed to identify the triggers that would lead to a tipping point in the market. Low interest rates introduced herding behavior in the market, resulting in the rapid expansion of subprime lending. The feedback loop between rising home prices and loosening underwriting/subprime lending played a large role in the bubble growing to the size it did. When adjustable rate mortgages began to reset and interest rates started to rise, the buying frenzy shifted to sudden panic as the market came to realize that borrowers could neither afford nor refinance their homes.

Like the early 2000's demand for mortgage products, today's demand for insurance products that efficiently transfer cyber risk is high. Growth is spurred on by strong demand resulting from the increasing number of data breaches at high-profile companies, low loss ratios, and insurers' sense of FOMO (fear of missing out). Premiums have climbed tenfold from $350 million in 2007 to $3.5 billion in 2017. It is estimated that by 2020, the market will nearly triple again, to somewhere between $8 billion and $10 billion, according to Morgan Stanley.[2]

Similar to the "hunt for yield" to compensate for low fixed income returns in the 2000's, soft market conditions in the property and casualty industry have added fuel to cyber liability's appeal. Insurers, initially cautious about underwriting cyber, have entered the market in growing numbers. There are approximately 170 carriers underwriting cyber in the U.S., up from approximately 18 in 2007. Five insurers underwrite about half of total premiums.

What makes this competitive market different from others is the nature of cyber risk. Unlike traditional product lines, cyber liability is a new exposure that lacks the decades of loss experience and associated data of other lines. Untested in the courts and with changing laws, cyber policy provisions could also prove to have coverage implications insurers did not intend. This vulnerability could be particularly troubling

1 For a counterexample, one consulting firm did foretell the larger underlying risk behind the mortgage crisis. See Milliman's November 2006 article by Mike Schmitz and Kyle Mrotek, "What happens when credit risks come home to roost?" Retrieved on February 28, 2019, from **http://www.milliman.com/insight/Articles/What-happens-when-credit-risks-come-home-to-roost/**.

2 Ralph, Oliver, "Cyber attacks: The risk of pricing digital cover." The Financial Times, March 18, 2018.

in terms of non-affirmative or "silent cyber" exposure in traditional products like D&O, E&O, contingent business interruption (CBI), fraud, crime, property, malpractice, aviation, marine, and other traditional lines of business. In one way or another, coverage for cyber liability could be linked to just about any product line.

With loss ratios in the mid-30s, cyber liability has provided a strong financial incentive for insurers to participate in the market. But current profits are not a proxy for risk, especially if insurers find they have priced for individual losses rather than a catastrophic event. Like the subprime crisis feedback loop, underwriters and reinsurers are often lacking visibility and transparency regarding cyber risk. In particular, many reinsurers do not possess the "look-through" of the underlying policies within their treaties, just as holders of CDOs and CDO-squared could not "read the tape" of the underlying mortgages embedded within the cash flow waterfall. To date, it appears most underwriters have treated cyber as a risk, not as a peril. At this point, it is premature to tell if pricing has been accurate because large losses have primarily been confined to isolated situations or individual companies. It is often stated that a breach is a question of *when, not if*. If we think of cyber risk in terms of a loss distribution, breaches to date fall within the area under the curve composed of expected loss rather than the area of unexpected loss, or the tail. Indeed, our preliminary research confirms that most companies overestimate the initial loss and are able to cope with a cyber event—for now. This situation could all change. Suddenly.

The interconnectedness of risk: A dress rehearsal for the big event

In early July 2017, Ukrainian police stormed the offices of a local family-owned computer company in Kiev, whose accounting software was used throughout the country. But it was far too late to remedy the damage that the company had unwittingly done to dozens and dozens of private and public organizations near and far.

A week earlier, in a matter of a few hours, the now infamous NotPetya malware had infiltrated the company's computer networks and brought down the operations of four hospitals in Kiev; six power companies; two airports; more than 22 banks, ATMs, credit card payment systems in retailing and transport; and nearly every federal agency in the Ukraine. According to an account by Wired magazine, one Ukrainian government official estimated that 10% of the country's computers were wiped.[3]

But the damage was not confined to Ukraine's borders. Large and small companies around the world fell victim to the malware. Included among them was shipping-giant A.P. Moller Maersk, whose story perhaps best reveals the havoc that a cyberattack can wreak on even those far beyond the walls of a target company's offices.

Maersk's problems started soon after an administrator at the shipper's Odessa office downloaded accounting software from the Ukrainian software company. The accounting software unwittingly carried code developed by Russian military hackers that allowed them to remotely run computers with unpatched Windows software. So virulent was the rapidly moving malware that it was able to use the password information from unpatched computers to infect patched computers.[4]

Without a functioning computer network, shipping containers at Maersk's port subsidiary, APM Terminals, could not be processed or shipped. Cargo began to back up; the port terminal in Elizabeth, New Jersey – which processes as many as 3,000 trucks per day – was closed by the Port Authority after trucks couldn't get their cargo in or out.[5] Shipping customers, especially those distributing perishable goods or just-in-time components, had to find alternate means of shipping their products, often at premium prices. New bookings were halted. This was the case days after the cyberattack.

NotPetya demonstrates the interconnectedness of cyber risk: the malware cost Maersk upwards of $300 million; it cost Merck $670 million in 2017, including sales and manufacturing losses, as well as remediation expenses; and it cost FedEx's European subsidiary, TNT, $400 million in remediation and related expenses.[6] The U.S. government estimates the total cost of the attack to be around $10 billion.[7] Speaking at the World Economic Forum in Davos last year, Maersk's chairman noted the malware forced the company to reinstall "a complete infrastructure," including 4,000 new servers, 45,000 new PCs, and 2,500 applications over 10 days.[8]

Technology and globalization have connected companies and other organizations in ways only imagined 10 years ago when cyber insurance first came on the market. "The Internet of Things," artificial intelligence, and cloud technology – among other advances – are now used across every sector of the economy and point to a more and more cyber-dependent world.

3 Greenberg, Andy. "The Untold Story of NotPetya, The Most Devastating Cyberattack in History." Wired, August 22, 2018. p. 11.

4 Ibid., p. 12, p. 7.

5 Ibid., p. 12.

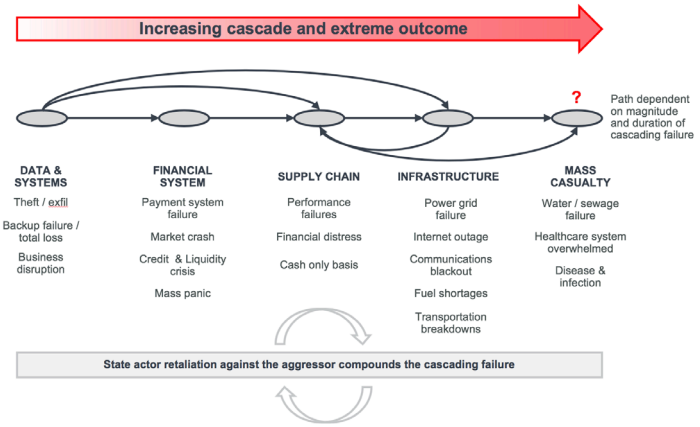
6 Nash, Kim S., Sara Castellanos, Adam Janofsky. "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs." The Wall Street Journal, June 27, 2018. Retrieved on February 28, 2019 from **https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906**.

7 Ibid., p. 10, 11.

8 Chirgwin, Richard. "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation blitz." The Register, January 25, 2018. Retrieved on February 28, 2019 from **https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/**.

Over the years, managing this cyber risk has moved from that of lost laptops to profit-driven hackers and state actors with the resources and technical sophistication to cripple their adversaries. Globally, governments are now devoting civilian and military resources to offensive and defensive cyber capabilities. A rush to gain exposure to cyber by [re]insurers, increasingly networked devices, the role of state actors, and globalization have created a highly interconnected cyber landscape, all setting the stage for a systemic event.

FIGURE 1: THE INTERCONNECTEDNESS OF CYBER RISK



Yet companies today have trouble keeping up with updates and security patches, as the NotPetya attack poignantly demonstrates. Cyber security and hygiene requires a heavy investment by companies, many of which are unclear how to quantify this risk appropriately. And even with the proper cybersecurity investment, companies often struggle with knowing where their cyber dollars will have the greatest impact. Should funding be put toward patching, upgrading encryption and detection capabilities, or boosting monitoring? With a myriad of threat scenarios, quantifying and allocating funds appropriately requires a reevaluation of the evolution of cyber risks.

The need for a new risk paradigm

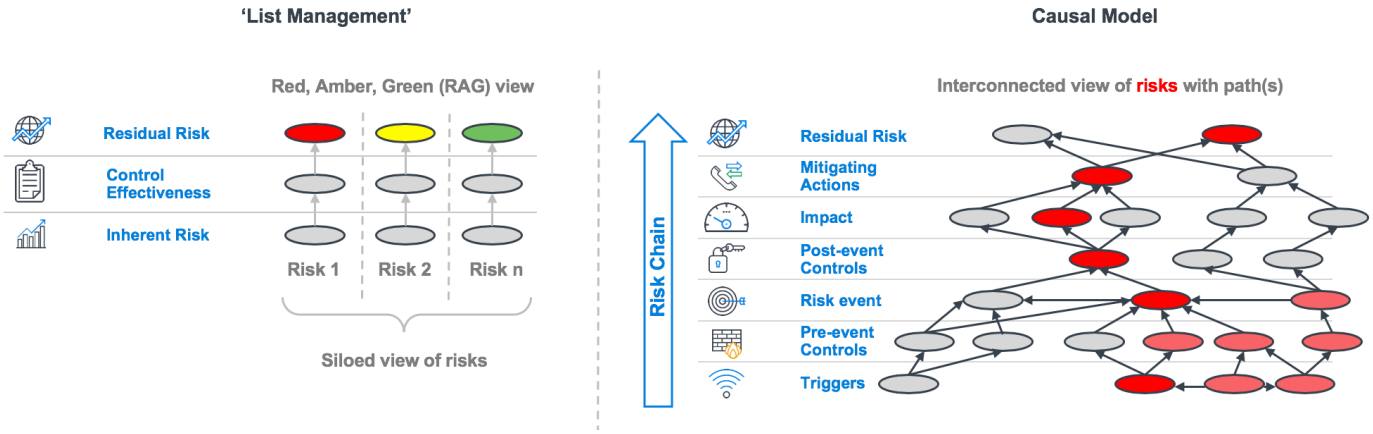
As the market matures, insurers appear to struggle with how best to assess cyber risk, in particular the "silent cyber" risk embedded in their policies. The industry appears stuck in the old risk paradigm, also known as a "list management" approach. With "list management," a taxonomy of risks and controls are evaluated by some form of scoring, and then an estimated likelihood and impact may be assigned, along with perhaps a heat map as the output as can be seen in Figure 2. Gauging cyber risk has followed the predictable pattern of other operational risks, including: 1) conducting qualitative checklist or formulaic assessments resulting in red/amber/green (RAG) outcomes; 2) utilizing classic scenario analysis; or 3) some simple forms of quantification leveraging classic frequency/severity or CAT methodologies.

These approaches are not suitable for quantifying cyber risk – due to the lack of historical experience and rapidly changing threats – nor are they sufficient for aggregating silent cyber. These approaches fail to identify the *nonlinear relationships* among multiple risks and how they are interconnected or multiplicative. They miss the potential for one risk to magnify the impact of another, masking a potential tipping point. In a "list management" framework, every time a risk is added to the list, capital is potentially constrained further because every risk implies the need for incremental capital, while ignoring the upside of the opportunity of taking that risk. It is a challenge that many companies struggle with as they have tried to aggregate risk and assess tail risk in order to find an accurate measurement of capital needs.

The "list management" problem is especially challenging with cyber risk due to its complexity, velocity, and novelty. Consequently, cyber requires a new paradigm for quantifying and aggregating this risk: the causal model approach (see Figure 2). The approach begins with creating a cognitive map that represents the complexity and interconnectedness of cyber risk as an effective tool for capturing an insurer's risk ecosystem. Like an environmental ecosystem that maps out a species' predators and prey, its sources of water and food, its migration patterns, and other influencers, a cognitive map representing cyber can bring in different risk vectors: stakeholders' different views of cyber risk; the multiple triggers that could, when interwoven, precipitate a crisis; the responsiveness of controls; and potential impacts of risk as it flows through the organization. Using proven techniques from the social sciences and complexity science, this information can be organized into a "minimally complex" system that provides a more realistic but understandable reflection of an insurer's risk and can better help quantify and justify the cyber risk spend.

This approach moves managers away from the trap of "list management," which limits a decision-maker's view of risk to rows and columns. Taking a minimally complex view that highlights causality, managers can see how risk is manifested and flows through the organization. Hard-to-quantify triggers like the reaction of investors or policyholders to a crisis can be modeled; the interconnections between multiple triggers can then be mapped to show how events may align against an insurer. This causal mapping can then alert the insurer to a tipping point. Looking back at the NotPetya attack, for example, a causal model could have helped Maersk understand which combination of triggers would lead to its inability to load and unload ships at its ports around the world. In other words, the risk management paradigm shifts from oversight to insight.

FIGURE 2: "LIST MANAGEMENT" VERSUS CAUSAL MODEL



The causal approach also allows risk managers to move past normalcy bias inherent in discrete scenario analysis and develop a plausible and fluid story of what may happen. They can go beyond the "frequency and severity" world that typically limits their focus to a fixed probability of loss that shows the pathways of how, when, and what triggers drive risk.

At the end of "The Big Short," after being proven correct, Michael Burry begins to eye the economy of water as the next troubled market. While there are parallels between the economics of water and the housing market, cyber may be the even greater risk: even access to clean water can be affected by a cyber attack. Every level of our financial infrastructure, our ability to communicate, and our access to energy are all linked and exposed to cyber. Cyber attacks have the ability to cripple our infrastructure, and the need to understand and manage this risk is vital. Seeing the whole picture in cyber could help avoid a systemic event beyond what we can currently conceive.

Milliman

Milliman is among the world's largest providers of actuarial and related products and services. The firm has consulting practices in life insurance and financial services, property & casualty insurance, healthcare, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

milliman.com

CONTACT

Chris Harner
chris.harner@milliman.com

Chris Beck
chris.beck@milliman.com