# Cyber Risk In A New Era: Let's Not Be Quiet About Insurers' Exposure To Silent Cyber

**March 2, 2021**

## Key Takeaways

- Cyber attacks are on the rise, as are the financial losses that can follow in their wake.
- Yet the cyber insurance market is underdeveloped, and cyber cover is often tacked onto existing liability or property insurance policies that were not originally intended to cover cyber risk.
- In some cases, the policies do not explicitly include or exclude cyber cover, thereby exposing the insurers to the risk of "silent cyber", or losses to settle unexpected cyber-related claims.
- The development of stand-alone cyber insurance products would reduce this risk and clarify the scope of the cyber cover for policyholders.
- Insurers with sophisticated risk management frameworks and those that invest appropriately in cyber expertise are best placed to provide specific cyber insurance products and reap the benefits.

PRIMARY CREDIT ANALYST

**Manuel Adam**
Frankfurt
+ 49 693 399 9199
manuel.adam
@spglobal.com

SECONDARY CONTACTS

**Simon Ashworth**
London
+ 44 20 7176 7243
simon.ashworth
@spglobal.com

**Charles-Marie Delpuech**
London
+ 44 20 7176 7967
charles-marie.delpuech
@spglobal.com

**Johannes Bender**
Frankfurt
+ 49 693 399 9196
johannes.bender
@spglobal.com

**Robert J Greensted**
London
+ 44 20 7176 7095
robert.greensted
@spglobal.com

The pandemic year of 2020 saw a step change in the complexity and sophistication of cyber attacks and, therefore, in the nature of cyber risks. The financial consequences for the victims of such attacks are huge. According to the Hiscox Cyber Readiness Report 2020, the median cost of a cyber attack rose almost sixfold worldwide between 2019 and 2020. Yet only 26% of the firms sampled in Hiscox's report have a stand-alone cyber insurance policy. Most rely on generic insurance policies, or have no cyber insurance at all.

The cyber insurance market therefore has huge growth potential, but insurers lack the products to appropriately meet expected future demand. Cyber cover is often bundled into existing property or liability insurance policies, and in some cases, the policies do not explicitly include or exclude cyber cover at all. This gives rise to "silent cyber", or the risk to insurers of losses from cyber-related claims on policies that weren't intended to cover cyber risk. Even when the inclusion of cyber cover is explicit, a lack of transparency in both the policy's definition of cyber events and its terms and conditions creates uncertainty about the scope of the cover. The importance of transparency and clear wording in policies became evident last year, when some insurers suffered reputational damage after rejecting policyholders' business interruption claims amid the pandemic.

In S&P Global Ratings' view, the development of stand-alone cyber insurance products would reduce the problem by clarifying the scope of the cover. Such products would also be better suited to the complex and dynamic nature of cyber risk. Even better would be the development of a stand-alone cyber line of business managed via a cyber center of excellence. This would have many advantages for insurers, chief among them preventing cyber-related claims accumulating across many different lines of business, as well as the difficulties in handling such claims. It would also allow insurers to mitigate the risk of silent cyber, as well as take a centralized and coordinated approach to data collection and research, which is vital for accurately calculating risk-adequate premiums.

## Bundling Cyber Cover Into Traditional Policies Only Muddies The Waters

Existing insurance policies often include cyber risk on a nonaffirmative basis, in other words, they do not explicitly include or exclude cyber risk. This contrasts with affirmative policies that explicitly include cyber risk. Thanks to the development of more sophisticated analytical tools over the past two years, insurers are gradually moving away from nonaffirmative policies by using clear and transparent inclusions or exclusions, which we see as positive (see "Cyber Risk In A New Era: Insurers Can Be Part Of The Solution," published Sept. 2, 2020). We also observe a trend of insurance companies developing dedicated cyber teams and recruiting external cyber talent into the insurance industry.

While we see the move towards affirmative policies as beneficial, insurers have tended to bundle cyber cover into traditional property or liability insurance policies, basing the inclusion or exclusion clauses on the wording of the existing policies and making them difficult to interpret. In most cases, such add-on cover does not cover a comprehensive list of perils. This can lead to confusion over the contractual scope of the cover. Such situations can result in intense debates when it comes to claims, as in the case below of Mondelez International Inc. (Mondelez) and its claim on its insurance policy with Zurich Insurance Group (Zurich).

### The Devil Is In The Detail: Mondelez Versus Zurich

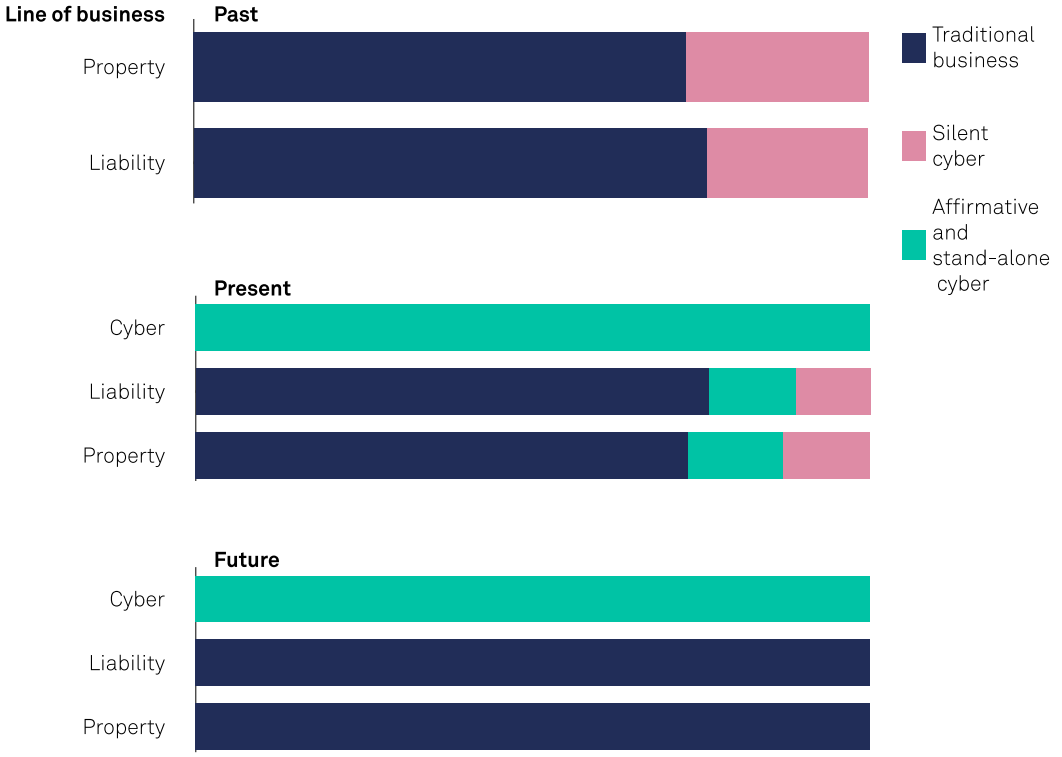
The ongoing legal dispute between Mondelez and Zurich highlights the risk of imprecise terms and conditions when cyber coverage is tacked onto existing insurance policies that weren't designed to cover this type of risk. Mondelez has an all-risk property insurance policy from Zurich that covers it for physical loss or damage to electronic data and software. Mondelez made a claim on this policy when it suffered from the global-scale ransomware attack "NotPetya" in June 2017. Zurich's position is that the policy language does not cover a "hostile or warlike action" such as NotPetya. Mondelez, in turn, alleges that Zurich has wrongfully denied a claim under the policy. The final decision in this lawsuit would be groundbreaking for the insurance industry, as it would set a precedent for other similar claims. However, such debates and lawsuits delay critical payouts and impede the sustainable development of a cyber insurance market.

Insurers are making progress on developing specific cyber insurance policies with clear terms and conditions, and are starting to build stand-alone cyber business lines that can handle the challenges associated with underwriting this type of cover. However, they still have some way to go to meet policyholders' needs (see chart 1). At the very least, their progress needs to keep pace with the evolution of cyber risk. On the other hand, aggressive expansion into the cyber insurance

market without effective risk controls could also be detrimental to our assessment of insurance companies' balance sheets. In our rating framework, we not only assess the insurer's current state of play, but also the journey it may take to build up a sustainable cyber line of business. Should an insurer expand aggressively in the cyber market without proper management of cyber risks and effective risk controls, it could change our view of the insurer's risk exposure, capital and earnings, or governance scores.

Chart 1

**The Evolution Of Cyber Insurance: An Illustrative Example**




Relative values are purely illustrative. Source: S&P Global Ratings.


## Insurers' Divergent Approaches Create A Fragmented Market

We see a strong correlation between the sophistication of insurers' risk management and their approach to managing cyber risk. Generally speaking, reinsurers are pioneers in the assessment of cyber risk thanks to their sophisticated enterprise risk management frameworks and investments in expertise. For primary insurers, on the other hand, we still see a great disparity between those taking the risk of silent cyber seriously in their underwriting strategies, and those with less ambitious strategies. Some insurers have already screened all their policies and have explicitly included or excluded cyber risk in all of them. We view this favorably from an overall risk management perspective. However, some primary insurers have refrained from explicitly including or excluding cyber risk as they see a low risk of cyber attacks affecting their own portfolios. This exposes them to the risk of silent cyber.

Insurers that are most keen to establish themselves as cyber insurance providers and those that

have sophisticated risk management frameworks have started to offer cyber insurance either as a stand-alone product or as a separate component of traditional policies. However, the mix of different approaches makes for a fragmented cyber market. Although more choice is generally a good thing, heterogeneity is less helpful in this case because it is hard for prospective policyholders to compare the respective elements of the different types of cover.

## A Stand-Alone Cyber Business Line Reduces The Risk Of Silent Cyber

We see five key benefits of having a separate cyber insurance line of business (see chart 2). First of all, it can give insurers greater control of the risk of claims accumulating within their cyber insurance portfolio. Such accumulation risk can expose an insurer to high financial losses in the event of a severe cyber event, such as a cloud outage or a global ransomware attack. Handling claims is difficult and inefficient when insurers have bundled cyber components into many different insurance products. Developing a stand-alone cyber business line would also allow insurers to take a more centralized and coordinated approach to data collection and research. This is crucial, as a short data history and the highly dynamic nature of cyber risks complicate the calculation of risk-adequate premiums. Furthermore, a stand-alone line of business for cyber insurance would pave the way for management to devote more attention to cyber.

Emerging cyber risks in lines of business that had previously been unconcerned with such risks could shake up risk management considerations and premium calculations. Silent cyber risk is particularly important in this context, as, unbeknownst to the insurer, it adds additional risk to the initial risk exposure. In such a case, the fair insurance premium is likely to be higher than the existing amount, leading to a disadvantageous risk return for the insurance company. A centralized system of managing business-wide cyber risks would help improve the risk-return profiles of insurers underwriting cyber insurance. Such a system would also assist insurers in strategically buying reinsurance cover and building loss reserves, as it would simplify the calculation of the underlying risk and thereby increase transparency for the reinsurance company.

The way insurers handle a cyber insurance claim diverges materially from their handling of a property or liability claim. A centralized system would allow an insurance company to apply the appropriate claim prevention measures consistently, as well as to implement efficient claim-handling practices and data recovery in the event of a claim. This is important because there is a strong correlation between the cost of a claim and the speed of resolution and data recovery. Handling a claim on a stand-alone cyber insurance product is far more efficient than handling such a claim on several existing insurance policies, and in the worst-case scenario, claims on products from many different insurance companies. This situation would make systematic claim handling, fast resolution, and data recovery almost impossible, in our view.

Chart 2

**Key Benefits Of Cyber As A Stand-Alone Line Of Business**

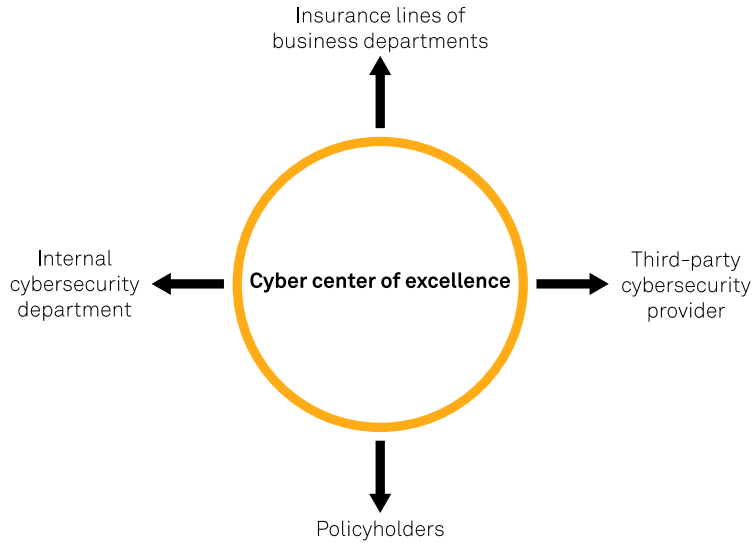

Source: S&P Global Ratings.


## A Cyber Center Of Excellence Can Streamline Insurers' Approach

A cyber center of excellence can help insurers shift cyber risk to one central line of business and capture all the advantages of a centralized approach. Such a center operates across all business lines and connects the different stakeholders working within them (see chart 3). It therefore provides insights and support with risk modeling to business lines. Such support could include identifying emerging cyber risks in property and casualty insurance, for example. The center can also coordinate services for policyholders, helping to reduce the cost per cyber-related claim. Moreover, it can bundle together in-house IT expertise and work closely with the insurer's internal cyber security department and its third-party cyber security provider to protect the insurer itself from any operational or reputational damage from a cyber attack. In our view, implementing a cyber center of excellence should assist insurers in shifting their focus from offering cyber products to offering cyber solutions, not only insurance cover, but also comprehensive assistance services. Such a center could help to improve insurers' assessments of accumulation risk through scenario-based tools, and offer employee and customer training, cyber-crime prevention services, claims and incident management, as well as data recovery.

Chart 3

**The Time Has Come For A Cyber Center Of Excellence**




Source: S&P Global Ratings.


## Cyber Has The Potential To Drive Industry Growth

One broad issue for the development and take-up of stand-alone cyber insurance cover is that policyholders feel they already have some cyber cover within their existing insurance policies. This makes it difficult for brokers and agents to sell stand-alone cyber cover, and could seem to strengthen the rationale for insurers to embed such cover in existing policies. However, even when the cyber cover is explicitly included in the policy terms and conditions, the situation is still risky. In our view, a severe cyber event that affects several lines of business at once could pose a systemic threat to insurers if it necessitates a fire sale of assets to cover losses, or results in severe reputational damage for the industry or limited capacity to cover traditional insured risks.

A comprehensive cyber strategy would give insurers the opportunity to restructure their businesses and expand their existing cyber risk definitions to make inclusions and exclusions more evident and comprehensible for policyholders. Policyholders should also find this helpful for increasing the efficiency and transparency of their own risk management decisions. Despite the challenges, we believe that insurers have the flexibility to cautiously expand their cyber insurance, as long as they can support the growth in demand at a reasonable cost. This would benefit policyholders and enable insurers to differentiate themselves from competitors. Cyber insurance has the potential become a growth driver for the industry and boost its reputation at the same time.

## Related Research

- Cyber Risk In A New Era: Remedy First, Prevent Second, Sept. 17, 2020
- Cyber Risk In A New Era: Insurers Can Be Part Of The Solution, Sept. 2, 2020

- Cyber Risk In A New Era: Disruptions And Distractions Increase Challenges For U.S. Public Finance Issuers, Oct. 19, 2020

This report does not constitute a rating action.