GFIA
GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

March 2018

GFIA Observations on Cybersecurity

Cyber risk is a global issue that continues to evolve as the world becomes increasingly connected and supply chain interdependencies become more prevalent. Further, Innovation such as emerging vehicle technologies, smart homes, and advancements in medical devices underscores the pervasiveness of cyber risks in our evolving society. International communities, both private and public, have a heightened awareness of the threats our governments and businesses face and continually place cyber awareness and resiliency efforts at the top of their list of concerns. The insurance industry is no different and places great importance on securing its own information systems. In addition, the property and casualty insurance community has a unique voice in this dialogue due to the cyber risk insurance products. We address both of these issues separately in more detail below.

Insurer Data Resiliency Efforts

GFIA recognizes that countries have different approaches and cultural viewpoints for addressing privacy and cybersecurity risks. However, to the extent possible international governments should harmonize baseline data security expectations that may be found in regulation, legislation or guidance documents. There should be coordination on an international level to avoid multiple inconsistent regulations for international businesses. Such harmonization will allow for efficient and cost effective regulation that protects consumers and industry, particularly for insurers that operate across multiple jurisdictions. GFIA has identified the following foundational principles that can be incorporated into government approaches that will promote harmonization while enabling the best outcomes and respecting international interests.

- **Flexible and Risk Based Approaches** — The cyber threat landscape and resiliency technologies are continually evolving, which means businesses must implement flexible information security policies that will allow them to adapt their system controls in a risk-based manner. As such, governmental entities that impose baseline data security requirements should ensure that they are technology neutral, flexible and allow businesses to implement them based on a business's individual risk profile. This approach will benefit consumers and businesses, because data security will not be tied to outdated best practices that the bad actors have already adjusted to.

- **Information Sharing** — The sharing of **threat data** is an important mitigation tool. A business's ability to share real-time threat data and potential mitigation tactics may prevent the spread of the same or similar cyber-attacks in a rapid manner. Even if a business is not a victim of the same attack immediately, there is an increased knowledge base that broadens a business's monitoring proficiency. Sharing should not be limited amongst private entities, but should also involve reciprocal sharing with the government. A government/private sharing arrangement should consider guidance on the level and type of sharing that should take place and whether the appropriate mechanism is a centralized collection mechanism or one that involves flexible input to agencies. Further, some countries may determine that information sharing should be mandatory while others propose that it is most successful if done on a voluntary basis with incentives such as liability protections and anonymity. Whichever approach a government takes the fundamental benefit of shared collective knowledge is beneficial.

  Likewise, a repository of **incident data** populated by individual companies from a broad representation of industry participants potentially allows entities to compare and assess their own approach to cybersecurity in a risk-based manner. There are a many issues that need to be considered when developing a repository, to include privacy, confidentiality, and liability issues, nevertheless it is a worthwhile exercise to consider the efficacy and viability of this resource.

  Regardless of whether the information sharing involves threat data or incident data the benefit goes beyond individuals and reaches insurers as well as, because the better risk aware a company is the better insured they are. However, it is important to note that there are certain commercial sensitivities related to sharing of cyber insurance data that we will reflect on later in this paper.

- **Public-Private Partnerships** — Preventing, or at least limiting, cyber intrusions and their impacts is a shared goal of the government and private sector. Therefore, public-private partnerships allow collaboration for leveraging the expertise of each party and can avoid unintended consequences of some regulatory requirements. A public-private partnership is not only important in collaborating ways to increase cyber resiliency efforts, but also in the aftermath of cyber-event when collaboration is needed to stop the spread of an intrusion.

Cyber Risk Insurance

Cyber risk insurance is commonly mentioned when discussing cyber resiliency efforts. The proliferation of cyber risk insurance will vary by country but it is a growing and evolving product line globally. Cyber risk insurance is sold as a stand-alone product or as part of a package policy. Cyber risk insurance offers customers many benefits. First and foremost, it is a valuable risk transfer mechanism, but it can also serve as a useful evaluation tool to accompany and assist in each individual business's risk calculations. For instance, cyber insurers may offer pre-event risk assessments and table-top exercise and employee training resources. Post-event the insurer may provide access to expert forensic, legal and public relation consultants. It is a product that continues to evolve and innovate to meet customer coverage and resource demands and needs.

We note, however, there are challenges to the growth of the cyber insurance market and have identified some of these below. Each challenge may not be present in every jurisdiction or be considered at the same priority level, but as markets emerge challenges follow, to include:

- **Aggregated Exposure Risks** — Arguably, aggregation of risks is one of the biggest challenges to the growth of the cyber risk insurance market. Aggregation concerns are reflected in a single insurer's potential concentration of insureds from one event, whether from a widespread attack on an industry segment or based on the nature of the risk such that a number of interconnected third-parties may all be impacted. Similarly, the cloud can present a unique accumulation of risk scenario. There is also the issue of the potential to impact multiple lines of business. The "non-affirmative risk" reflects aggregation risk concerns in terms of understanding where exposures may exist in traditional policies. For example, a traditional commercial property policy and a D&O policy may have coverage implications for a cyber-event depending on the policy language. At this time, it is hard to get a complete picture of all the "non-affirmative" risks. However, insurers are keenly aware of all of these aggregation exposure issues and the market is growing responsibly and determining the best course of action to address any uncertainties the risks present.

- **Lack of Data/Risk Modeling** — Modeling efforts are underway, but cyber risk is hard to quantify because it is a moving target that is always changing and evolving. It is also a new risk with intangible consequences that are hard to quantify and often times it is hard to identify whether the bad actor is a nation state or criminally motivated bad actor, which present different risk profiles and coverage challenges. Further, bad actors are not always the source of a cyber-failure. Cyber risk can include accidental events with no malicious intent such as system or software failures and employee mistakes.

  As with any emerging market, there will be a period of time within which there is a lack of historical data; however, insurers are making large investments to grow their data banks and this is where a tension arises as to how much information insurers are willing to divulge/share from a competitive perspective. One potential solution that insurers and general business entities are exploring globally is an incident data repository that would include information about a cyber-event that individual business entities from a multitude of industries would report regarding their own recent cyber-event. Details on how the repositories will advance, if at all, remain to be seen, but it is one example of a government and industry working together for a potential solution. Data Breach notification obligations also present an opportunity to develop important data points as we saw with the development of the U.S. insurance market and are expected to see in the European Union with the adoption of the General Data Protection Regulation and NIS Directive.

  Similarly, there must be a strong trust bond between the insurer and insured to enhance the data obtained from individual insureds. The underwriter must be able to access all of the client's data and IT processes in order to analyze the risk or settle the claim. Access to this information can be considered as sensitive by the customer. It is therefore essential that the client trust the insurer in order to optimize the underwriting experience.

- **Lack of Cyber Risk Awareness** — While the demand for cyber insurance will ebb and flow as media reports of high profile breaches emerge, ultimately the decision to buy insurance will rest on a business's risk calculations. Businesses do not always appreciate their cyber risk exposure for a variety of reasons (i.e. industry category, type/amount of data stored, size of the business, etc.) and do not anticipate they are a potential target or have a high risk of loss. Therefore, these entities are not going to see the need for a risk transfer tool like insurance or will factor in that their money will be better spent elsewhere possibly

on strengthening their cyber risk posture. A lack of risk awareness is a challenge that is broader than the impact on insurance take-up rates and is one that governments have identified as a universal concern. While government sometimes suggests that insurers can bridge this awareness gap through the underwriting process, this is not necessarily an issue that insurers can and should fix.

- **Lack of Cyber Expertise** — Underwriters are not cybersecurity experts, so some insurers will bring experts in-house or consult with external expert consultants. The lack of cyber expertise in the workforce sometimes creates a challenge of a limited pool of experts for insurers to tap into.

  However, this is another challenge that is broader than the insurance industry and countries are tackling this issue with increased educational opportunities whether it is providing educational grants or supporting programs to include cyber as a core element of the education system beginning at a primary school level. The insurance industry can help meet this challenge by supporting such public policy initiatives.

- **Consumer Education** — A critical component of a new and emerging insurance market is consumer education. Cyber risks should be considered a peril and coverage for the cyber peril can be addressed, in whole or part, in a dedicated stand-alone policy or embedded in a multi-peril policy that may include cyber as one of the many causes of loss. Consumers need to work with their insurer and broker to perform a gap analysis and understand where traditional policies may be insufficient and where a stand-alone policy or buy-back exclusions will help.

  Also, as with any emerging market insurance policies and terminology will initially differ among insurers and harmonization/standardization will occur organically as the product evolves and the product becomes more available. As such, we caution policymakers to avoid forcing standardization before the market is ready, which could impede market development and competition. Further, standardization/harmonization at this point could curb innovation which would result in products that are not well-matched to the needs of the market. For instance, individual businesses have unique and potentially dynamic cyber risk profiles, or cyber-footprints the nature of which will dictate different protections. Therefore, standardization will not best serve the development of insurance products that could be tailored to provide the best insurance protection for these individual risks profiles or cyber-footprints. Additionally, while alignment in terminology of risks may be beneficial to help companies and consumers better understand cyber insurance, it is occurring organically, where appropriate, in the market today. As this organic evolution continues, we are reminded that this is another reason that education and the broker relationship are critical to help consumers compare and contrast policies and find the best coverage for their needs.

- **Government Backstop** — Cyber events caused by acts of terror are already included in some terrorism risk insurance pools or are being considered for inclusion. However, broadly speaking a government backstop dedicated to catastrophic cyber events that are or are not an act of terrorism is premature at this point. GFIA members note that it is important to give the market time to evolve before considering a government backstop.

The challenges above are identified to increase awareness of the current market limitations, but to also emphasize that the insurance community is exploring ways to innovate and overcome these challenges and that with time the market will evolve organically. Where appropriate the government and private industry may find ways to work together to overcome the challenges, but we recommend caution in moving forward with any type of regulatory mandate that would stifle innovation and growth. For instance, the French GIP ACYMA is an example of a partnership between the government and the private sector to address cyber insurance issues and the United States and United Kingdom there are joint public private efforts to explore methods of sharing cyber-incident data. As noted above, cyber insurance is a valuable tool for a number of reasons and as such GFIA is excited about the continued responsible growth of this market globally.

GFIA contacts:
Steve Simchak, GFIA Cyber Risks working group Chair (ssimchak@aiadc.org)
GFIA secretariat (secretariat@gfiainsurance.org)

About GFIA
The Global Federation of Insurance Associations (GFIA), established in October 2012, represents through its 40 member associations the interests of insurers and reinsurers in 61 countries. These companies account for 87% of total insurance premiums worldwide, amounting to more than $4 trillion. GFIA is incorporated in Switzerland and its secretariat is based in Brussels.