ASIC
Australian Securities & Investments Commission

The role of the regulator in the cyber insurance market

A speech by John Price, Commissioner,
Australian Securities and Investments Commission

Cyber Insurance Forum (Sydney, Australia)
21 September 2017

CHECK AGAINST DELIVERY

Introduction

Thank you for inviting me to speak today.

Forums such as this one play a critical role in promoting discussions about building a more secure and resilient digital economy for Australia.

Cyber insurance

We have heard this morning how the cyber insurance market is evolving rapidly around the world. While it is still in its infancy in Australia, it is easy to see its potential as an incentive for businesses to better deal with cyber risks. Just as the process of obtaining home insurance can incentivise home owners to invest in alarm systems, smoke detectors, and better locks, the same could be true for companies seeking to obtain cyber insurance. Cyber insurance providers can potentially contribute to the management of cyber risk by promoting awareness, encouraging measurement and by providing incentives for risk reduction.

Over the last few years, the increasing incidence, complexity and reach of cyber attacks have captured headlines around the world. During this time, a lot has been said about the need to raise awareness of cyber security across the community, industry and government.

Cyber attacks can undermine businesses and destabilise markets, eroding investor trust and confidence in the financial system and the wider economy. Because of the dynamic nature of cyber threats, it is increasingly essential that companies understand their risk and resilience against cyber attacks and most importantly promote a good risk culture.

Never before has this issue been more important for:

- the boards of companies, who help set the strategy and risk appetite for their organisations, and
- the executive management of those companies, whose role is to design and implement the company's risk management framework, and ensure it operates within the risk appetite set by the board.

Together, executive management and boards help determine the culture of a company. In short, 'the way we do things around here'.

For ASIC it's important that companies have a good risk culture in this area because that helps foster investor and consumer confidence and also fair and efficient markets. In our view, putting a price on cyber risk gives companies a strong incentive to develop a better risk culture.

Of course, ASIC also has an important role in regulating the conduct and disclosure of people who provide and market insurance products (including cyber insurance). We focus on conduct of insurers and distributers through the lens of fair outcomes for consumers and investors, including:

- customers and investors being treated fairly
- insurance products performing in the way that customers and investors have been led to believe they will and delivering value for money, and
- financial services firms taking into account consumers' information imbalances.

We do that because of our mandate. We are tasked with making sure there is an appropriate standard of transparency and appropriate regard for consumers as set through the laws we administer.

ASIC's approach in promoting cyber resilience

Several years ago, ASIC highlighted cyber resilience as a key strategic risk for our regulated community. Unsurprisingly, our focus on cyber resilience has only continued to increase. Our forward-looking four year corporate plan identifies digital disruption and cyber resilience in financial markets and services as one of the key challenges we currently face as a regulator.

As part of our role, we have been proactive in:

- raising awareness of cyber risks across the financial services industry. We published our "***Cyber Resilience - health check***" report in 2015 to raise awareness about compliance obligations with respect to effective management of cyber risks

- collaborating with the private sector, government, and local and international regulators. For example, in 2016 we published a report that included a number of good cyber practices and questions for boards to consider, and most recently, we were a key collaborator in the ***"ASX100 cyber health check"*** published earlier this year
- assessing and measuring the maturity levels in cyber preparedness of individual organisations and industry.

Our goal is to encourage improvements to cyber resilience practices for those entities operating in Australia's financial markets, which will in turn lift the overall cyber resilience of the financial services ecosystem.

The data that we have collected through our cyber resilience self-assessments from organisations in the financial sector over the past 2 years suggests:

- clear recognition that cyber risks management is front of mind for these organisations, but there is still work to do this area
- there is clearly a gap in the level of maturity in cyber resilience preparedness between large entities that have access to specialist skills and resources and of Smaller Entities (SME), some of whom have only just started the journey. There is an opportunity for improvements across the entire sector but most of all in the SME space.

Cyber resilience and boards

ASIC expects that all boards are considering their firms' cyber resilience.

In particular we expect boards to understand what it takes to improve an organisation's overall cyber resilience so it can survive and recover from an attack as quickly as possible.

There are some steps that boards can take in this area.

Firstly, they can periodically assess cyber resilience, identify and prioritise the risks to their critical assets and services.

Secondly, they should understand their compliance obligations with respect to risk management and business continuity. We expect cyber risks to be a component of their enterprise risk management framework. To that end, seeking out tailored cyber insurance would clearly be one of several management strategies that could be pursued to help manage that risk. Importantly however, there needs to be a good understanding of coverage and limitations of any insurance cover. By no means is cyber insurance a substitute for good risk management in this area.

Finally, organisations should know how they would respond if an incident were to occur.

Data security is another area that deserves urgent focus. There have been streams of high profile companies that have suffered a data breach in recent times. Reputational damage and the prospect of costly lawsuits arising from these events should not be lost on anyone.

Raising cyber security awareness of an organisation's leadership has never been more important. The regulator can play a role here but there is also potential for the insurance industry to do so.

Conclusion

At ASIC, we are spending time with boards and senior management speaking about our expectations on cyber resilience. Insurers can provide an important market signal that also promotes cyber-resilience. In developing their products however we think it critical that insurers treat their customers fairly and develop and sell a range of products and services that are aligned with consumer needs and that deliver value for money.

We will continue to assess maturity of cyber resilience across the financial sector, and where we see challenges to business, we will work with government and industry more broadly to explore how best we can assist.

Thank you.