ASIC
Australian Securities & Investments Commission

Building resilience: The challenge of cyber risk

A speech by Greg Medcraft, ASIC Chairman,
Australian Securities and Investments Commission

Australian Chamber of Commerce and Industry business reception event
(Melbourne, Australia)
15 December 2016

CHECK AGAINST DELIVERY

Introduction

I wanted to talk to you tonight about a critical issue in today's environment. A key risk that is increasingly on the minds of regulators, governments, and businesses. And one that is becoming more and more critical as technology evolves at an increasingly rapid pace. That issue is cyber risk.

Technology developments mean we are now able to make thousands of transactions in a second and send masses of data around the world instantly, but at the same time, this has increased the risks we are exposed to.

There has been significant growth in the number, sophistication and severity of global cyber attacks in the last few years. Cyber attacks are happening all the time.

Between July 2015 and June 2016, CERT (the national Computer Emergency Response Team, which sits within the Attorney-General's Department) responded to almost 15,000 cyber security incidents – 418 of which involved systems of national interest and critical infrastructure.

PricewaterhouseCoopers (PwC) also recently found that 65% of Australian organisations experienced cyber crime in the last 24 months.

So tonight, I'd like to touch on:

- ASIC's vision – and what we see as our five key challenges

- what is cyber resilience and why is it important
- what ASIC is doing in the area of promoting cyber resilience – and what is happening in the international sphere.

ASIC's vision and challenges

ASIC's vision

ASIC's vision is to allow markets to fund the economy, and in turn, economic growth. In doing so, contributing to the financial wellbeing of all Australians.

We do this by:

- promoting investor and consumer trust and confidence
- ensuring fair and efficient markets
- providing efficient registration services.

ASIC's long term challenges

How we achieve our vision in the future is influenced by the five key challenges we face. The challenges we face, and our strategy for responding to them, is set out in our four-year corporate plan, which we published in August. You can find it on our website, asic.gov.au.

The five key challenges we see in achieving our vision are:

- conduct risk and the balance between a free market-based system with investor and financial consumer protection
- digital disruption and cyber resilience in our financial services and markets
- structural change in our financial system through market-based financing which is driven by the growth in superannuation
- complexity in financial markets and products driven by innovation
- globalisation of financial markets, products and services.

This year, we have identified cyber resilience as a key priority, signalling increased regulatory scrutiny of this issue. Cyber resilience is now widely regarded as one of the most significant concerns for the financial services industry and the economy at large.

The cyber resilience of our regulated population is, therefore, a key focus for ASIC. Already, our cyber risk taskforce (for financial markets) is operating and proactively collaborating with industry, regulators and the Government.

What is cyber resilience and why is it important

Cyber resilience is the ability to prepare for, respond to and recover from a cyber attack.

There are a number of key ways a cyber attack might harm an organisation or a person, such as:

- integrity breaches – the manipulation of correct data
- confidentiality breaches – theft of personal information
- availability breaches – such as shutting down critical infrastructure and online services.

Cyber security is fundamentally important to all organisations that hold confidential information. Moreover, it is critical to maintaining trust between the organisation and its customers.

Industry research shows that over 60% of customers would stop using a company's products or services if a cyber-attack resulted in a known security breach. This would have a catastrophic impact on any business, even if the breach was temporary.

The dynamic nature of the cyber threat landscape means that a comprehensive and long-term commitment to cyber resilience must be embedded within organisations' culture.

Resilience is more than just preventing or responding to an attack – it also takes into account the ability to operate during, and to adapt and recover, from such an event. Customarily, organisations have focused on protection against cyber attacks. However, a resilience-based approach to cyber attacks is vital for organisations to better adapt to change, reduce exposure to risk, and learn from incidents when they occur.

There is simply no such thing as 100% cyber security. As well as being focused on preventing cyber attacks, organisations need also have strategies in how they respond to attacks when they occur, and how they recover from attacks.

What is ASIC doing?

So what is ASIC doing in this area?

The increasing incidence, complexity and reach of cyber-attacks can undermine businesses, destabilise fair, orderly and transparent markets and erode investor and financial consumer trust and confidence in the financial system.

We see that cyber attacks are a major risk for our regulated population. This risk is equally real for both large and small participants.

The Financial Stability Board (FSB) recently released a paper examining the financial stability implications of some recent financial technology (fintech) innovations that the market is seeing. The FSB gives the example of fintech giving new players, such as digital wallet providers, access to existing market infrastructure (e.g. payment systems).

The FSB notes that these new players could be organised very differently from traditional participants, and pose new operational risks. These new participants – with varying levels of robustness in their cyber resilience measures – increase the market infrastructure's susceptibility to cyber attack.

The FSB's example is one, of many, that highlights that the electronic linkages in the financial system mean the impact of a cyber attack can spread quickly – potentially affecting the integrity and efficiency of global markets and trust and confidence in the financial system.

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 our financial markets. However, we recognise that overall cyber resilience may only be as strong as the weakest link. We recognise the practical limitations in the role we can play to lift cyber resilience in individual organisations.

So our approach is to work with our stakeholders to ensure there is awareness of their obligations, awareness of the evolving cyber threat landscape.

ASIC has published two key reports in this area.

Cyber Resilience Health Check

In March 2015, we published a Cyber Resilience Health Check to help our regulated population to improve their cyber resilience.

In this report, we noted that the obligations on company directors and officers to discharge their duties with care and diligence extend to cyber security. However, many boards are still leaving it to their technology leaders to manage this threat.

In the report we outline some questions to help organisations consider their cyber resilience. The prompts highlight issues to consider as part of general governance practices, and the specific ways to identify, protect against, detect, respond to, and recover from, cyber risks.

This report also highlights the US National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity as a potentially useful cyber resilience resource for our regulated population.

Cyber Resilience Assessment Report

And then in March 2016, we also released a Cyber Resilience Assessment report into ASX and Chi-X.

This report covers a wide range of related topics including questions all boards should consider asking to ensure they are appropriately positioned.

Examples include:

- Are cyber risks an integral part of the organisation's risk management framework?

- How often is the cyber resilience program reviewed at the board level?
- Does the board need further expertise to understand the risk?
- What needs to occur in the event of a breach?

Asking these questions will engage the board in a richer dialogue about cyber resilience, and may contrast their organisation's approach relative to leading cyber security practices in the financial industry.

These practices cover a number of critical areas, including the need for:

- *strategy and governance* – board engagement on cyber risk strategy and execution while maintaining a highly responsive approach to new threats or elevated threats against an agreed risk appetite
- *collaboration and information sharing* – actively engaging with industry peers, government agencies and law enforcement to constantly scan for changes in the threat landscape
- *cyber awareness and training* – ensuring that employees and contractors are kept informed about this issue, to enable them to be an effective line of defence against cyber attacks, such as social engineering
- *proactive measures and controls* – implementing the Australian Signals Directorate's (ASD) 'top four' strategies to mitigate targeted cyber intrusions. These measures protect against a high percentage of cyber intrusions, and are reviewed annually by the ASD.[1]

Since the publication of this last report we have met with a number of stakeholders we had previously surveyed on the issue and discussed the progress they had made in meeting their cyber resilience goals. We are also broadening the scope of stakeholders we survey and providing feedback to them on better practices and trends we are seeing across the industry.

In time, we plan to extend the analysis undertaken in this report beyond financial markets to other important segments of our regulated population.

International coordination and cooperation

Like other aspects of the regulation of securities markets, mitigating the risks posed by cyber threats cannot be confined by national borders.

In the international sphere, IOSCO – the International Organization of Securities Commissions – is very much alive to the need to employ technology-related tools to improve enforcement capability. And also to encourage an international approach to promoting cyber-resilience.

[1] The current ASD 'Top 4 Mitigation Strategies' are 1. Application Whitelisting; 2. Patch Applications; 3. Patch Operating System; and 4. Minimise Administrative Privileges. The Cyber Security Operations Centre in ASD has stated that at least 85% of the cyber intrusions it responds to would be mitigated had agencies implemented these Top 4 strategies.

There are two aspects of this that I want to highlight.

The first is modernising IOSCO's Multilateral Memorandum of Understanding, or the MMOU.

When I was Board Chair of IOSCO, I championed an initiative to enhance the MMOU. The MMOU is the key document that securities regulators rely on to share information across borders to respond to cross-jurisdictional misconduct. The main way that the MMOU is being enhanced is to expressly provide for regulators to obtain and share internet service provider records and telephone records. We see these changes to the MMOU as critical to ensuring that regulators share the right sort of information that will really help to achieve successful enforcement outcomes.

The second is to highlight guidance released by the Committee on Payments and Market Infrastructures(CPMI) of IOSCO on cyber resilience for financial market infrastructures. This guidance is significant. It's the first internationally agreed piece of guidance on cyber security in the financial industry.

This guidance supports industry's ongoing efforts to pre-empt cyber attacks, respond rapidly and effectively, and achieve faster and safer recovery if the cyber attacks succeed.

Another goal is to ensure that these efforts to build resilience are similar from one country to another.

Conclusion

In conclusion, I want to say that the potential of cyber attacks on critical Australian infrastructure is unlikely to taper off.

We encourage all businesses to be aware of the cyber risks they face and take action to improve cyber resilience. The financial sector already collaborates in sharing cyber intelligence, but we also have an opportunity to invest in improved facilitation of this, so all business can benefit from sharing intelligence and approaches to improving their cyber resilience.

And as I've outlined, ASIC plays a key role in continuing to build trust and confidence in our financial markets.