ASIC
Australian Securities & Investments Commission

Challenges for our capital markets

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

Deloitte Australia (Melbourne, Australia)
24 September 2015

CHECK AGAINST DELIVERY

Introduction

Thank you for the opportunity to speak here today.

Today I really wanted to cover four key topics of great relevance to our markets. These are:

- global regulatory trends and how they will impact Australia
- culture as a key driver of conduct
- cyber resilience
- the importance of informed markets.

By covering these topics today I am not suggesting that audit committee members, CFOs or CROs necessarily have primary responsibility for how they are handled within firms. What I do think, however, is that these are critical issues and that it is important for you to reflect on these issues and what they might mean for you and your firms in future. They are certainly the types of issues that 'keep me awake at night'.

But before I begin I wanted to alert you to ASIC's Corporate Plan for 2015–16 through to 2018–19. This is a key document setting out our vision, what our strategic priorities are, where we see future challenges and risks, and what we intend to do about it. What I will say today has been written against that context.

Global regulatory trends

A key opportunity presented by globalisation is allowing the free flow of capital across world markets. Australian companies increasingly rely on global markets to raise capital.

In the March quarter of 2015, 45% of Australian-listed equities were held by foreign investors. Over the past decade, the proportion of non-financial corporate debt issued offshore has risen strongly, to 75% as at June 2015. The total level of Australian investment abroad reached $2.1 trillion in the March quarter of 2015, split almost equally between equity and debt investments. This represents a 23% increase from the level a year before.

An important driver of these developments has been greater cross-border activity, competition and integration. Offshore global providers are increasing opportunities for the Australian market, targeting important areas like over-the-counter markets, futures trading, and clearing and settlement.

At the same time, increased globalisation and cross-border developments can mean greater fragmentation across businesses, services and transactions, potentially compromising market integrity and the outcomes for investors and consumers.

Challenges include:

- slow and uneven implementation of international regulatory standards, which could lead to inconsistent or lower standards in some jurisdictions – it might also add complexity for Australian market participants accessing international markets
- risks to Australian investors from emerging market issuers – entities listed in Australia that have substantial assets or management offshore in emerging markets
- increased trading options for investors through dark pools, alternative exchanges and international trading facilities, which may result in regulatory arbitrage and risks to investors.

Over the medium term, these long-term challenges raised by globalisation will continue to hold our attention. We want to meet these challenges by:

- influencing international policy and actively participating in international cooperation and standard setting
- pursuing bilateral and multilateral arrangements with our counterparts to reduce regulatory burdens for cross-border activity and build capacity
- where appropriate, taking cross-border enforcement or other regulatory action
- analysing intelligence on innovative businesses, services and transactions in global markets.

Culture as a key driver of conduct

Much has been said in recent times about issues of the culture of people and companies in our financial system. So let me pose a question – does ASIC have any role with regards to the culture of participants in our financial system? I would say it does.

First, the law itself (through the Commonwealth Criminal Code) recognises the concept of ‘corporate culture’ in regulatory compliance. As a law enforcement agency it should be no surprise that we take an interest in it.

Second, from a regulator's perspective, ASIC is concerned about culture because, together with financial incentives, it can be a key driver of conduct within the financial system. Given that there often is a strong connection between poor culture and poor conduct, we consider poor culture to be a key risk area with respect to our role as a conduct regulator.

Finally, I would make the simple point that culture and good governance can make a difference from a commercial perspective. Research has shown that businesses with a strong culture tend to have sustained high performance over the longer term. Further, a good culture should remove the need for a lot of internally generated red tape that often seems to plague large organisations. My position is pretty simple: good culture should not mean mountains of red tape and armies of compliance staff. If your staff accept and really believe in doing the right thing by your customers, the need for a lot of internally driven rules falls away.

So what are some of the things that ASIC looks for when thinking about these issues? Let me mention three things:

- communication – expected conduct and behaviours need to be clearly articulated
- challenge – existing practices need to be challenged and employees should be encouraged to escalate potential practices or behaviours of concern
- complacency – boards should not become complacent and managing conduct risk should be an ongoing process that is continually reviewed, enforced and validated.

And, for the all-important question, what is ASIC planning to do in this area? A key thing is that more than ever we are intending to build concerns around culture into our existing risk-based surveillance reviews. We want to share information with boards and management when ASIC's surveillance suggests they want to do the right thing but there may be cultural problems within their firm that they are not aware of.

But, of course, where we see bad conduct – whether caused by problems with culture or otherwise – we are ready, willing and able to enforce the law.

Cyber resilience

Any conversation about cyber resilience needs to start with the broader trend of 'digital disruption' to existing business models. For example, global investment in financial technology (fintech) ventures tripled to US$12.2 billion in 2014, from US$4 billion in 2013. This is a fantastic growth story. But this innovation provides both opportunities and risks. New digital strategies continue to challenge traditional business models, disrupting financial services and markets, and changing how they interact with investors and consumers across a range of platforms and devices.

Technological change has also increased the risks of cyber attacks. The number, sophistication and complexity of cyber attacks have increased markedly in recent years and are expected to accelerate in the future. In 2013, cyber attacks affected five million

Australians at an estimated cost of AU$1.06 billion. The estimated annual cost of cyber attacks to the global economy is more than US$400 billion.

The increasing incidence, complexity and reach of cyber attacks can undermine businesses and destabilise our markets, eroding investor and consumer trust and confidence in the financial system and the wider economy.

In response to the long-term challenge of digital disruption to business models and channels, we will highlight the importance of cyber resilience in the coming year to promote trust and confidence in the financial system and market integrity.

Cyber threats are increasingly diverse and sometimes unforeseeable. With the evolution of technology and global interconnectedness, this risk is constantly changing. Cyber attacks are considered a systemic risk to the financial system – especially attacks on essential or critical services, like banking and payments services or financial market infrastructure.

It is not possible for businesses or individuals to protect themselves against every cyber threat. However, we encourage firms and markets to improve their cyber resilience, particularly where exposure to a cyber attack may impact on individuals or market integrity.

So what is ASIC doing about this? We will focus on:

- promoting cyber resilience
- identifying potential cyber attacks in our markets through real-time market monitoring
- ensuring compliance with licensing obligations, including the need for adequate technological resources and risk management arrangements, and disclosure obligations
- coordinating and engaging with other Government departments to identify cyber risks and cyber resilience.

I want to be very clear, however. ASIC can provide guidance and encouragement – and we have even, in some cases, provided some tools based on international standards (such as the US National Institute of Standards and Technology (NIST) standard) against which people can assess their cyber resilience – but the question of what is the right level of cyber resilience for any company or licensee depends very much on who you are and what you do. In many cases, regulators other than ASIC will also have an interest. What we want to do is try to raise awareness and provide guidance about an issue that is not just a regulatory matter but something that goes to the heart of running your business.

Informed markets

Compliance with continuous disclosure provisions goes to the heart of ASIC's priority of promoting fair and efficient markets, and this issue remains a central focus for ASIC and our ongoing market surveillance work.

The integrity and efficiency of our financial markets depends on all investors having access to market-sensitive information about listed entities at the same time. Failure to properly disclose information can lead to regulatory issues and undermine confidence in a company. Leakage of information prior to market announcements can lead to continuous disclosure problems, insider trading and an undermining of investor confidence. It can also pose threats to the outcome of corporate transactions. Analysts briefings and market soundings prior to a major corporate transaction are particular areas that require care.

A key idea that I'd like you all to think about is that good continuous disclosure compliance comes down to preparation and organisation.

Often when continuous disclosure is discussed in Australia, an image of management caught by surprise and paralysed by a difficult disclosure decision arises. This tends to create the impression that continuous disclosure is something that is done in an hour or so, and that it is done solely by a few key members of management. However, this is not the case.

I'd like to stress that many people within an organisation have a role to play in ensuring that continuous disclosure obligations are met.

When problems arise it is frequently because the right frameworks to comply with continuous disclosure were not in place, rather than the directors simply making an incorrect decision under pressure.

A number of recent continuous disclosure and insider trading cases demonstrate the importance of robust internal controls, and indicate that more proactive, preventative work could have been done in these cases to manage the process risks associated with continuous disclosure obligations.

At a practical level, some of the steps an entity can take to minimise risk in this area include the following:

- having delegations in place for who has authority to speak on behalf of the entity – whether in response to an ASX 'price query' or 'aware' letter, or when they become aware of information that needs to be released to the market
- having a written rapid-response plan and making sure all board members, their advisers and senior staff are fully appraised of its contents. This plan and the systems that fall within it need to be subject to periodic review and stress testing to ensure effectiveness
- having a plan for when an entity will consider a trading halt is appropriate and having a template 'Request for trading halt' letter ready for use at all times
- making it a practice to prepare a draft announcement where there is prior notice of an event that may likely require an announcement to be made
- monitoring the market and the information it is trading on. The entity should monitor significant media outlets, including any relevant social media, for leaks or rumours that may require correction.

Remember, if an entity is not turning its mind to its obligations on a day-to-day basis, then it may not be able to adequately and accurately respond to the market, which could give rise to potential liability both for the company and the directors personally.