COMPUTER TERMINAL VELOCITY: APRA'S RESPONSE TO AN ACCELERATING RISK

GEOFF SUMMERHAYES
Executive Board Member
Australian Prudential Regulation Authority

Insurance Council of Australia Annual Forum
Sydney
7 March 2018

Good morning, and thank you for the invitation to speak here today.

This is the third successive year I have addressed the Insurance Council of Australia's Annual Forum, each time providing APRA's perspective on an emerging risk. In 2016, it was culture, an issue that's not gone away. Last year it was climate risk, which continues to grow in importance. This morning, I want to discuss the growing prudential threat to Australian financial institutions posed by cyber risk.

It's worth rhetorically asking whether cyber is really an *emerging* risk. It's hardly a new threat; every sensible home computer user, let alone major financial institution, has relied on virus protection software for decades. APRA created its Information Technology Risk team 16 years ago, and issued its first prudential guidance on information security in 2010. Yet in the past few years, cyber risk has raced quite dramatically up the list of concerns faced by businesses, governments and regulators, both here and overseas.

Some commentators dubbed 2017 "The Year of the Hack"[1], as the world became reluctantly acquainted with such malware and viruses as Crash Override, Triton, Not Petya and Wannacry. Locally, the Australian Cybercrime Online Reporting Network recorded 30 per cent more reports in the September quarter last year than it did in the first quarter of 2015 when it commenced operation. Internationally, a breach at US credit monitoring firm Equifax exposed the personal information of almost 150 million Americans[2] in what is often described as the worst corporate data breach to date. Global companies of the scale of Yahoo and Uber revealed they'd suffered major data breaches involving, in Yahoo's case, literally *billions* of user accounts[3]. The spectre of hacking also haunted the 2016 US election,

[1] http://www.huffingtonpost.com.au/entry/data-breach-hacks_us_5a3a7f56e4b025f99e13cdbe

[2] https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821

[3] https://www.wired.com/story/worst-hacks-2017/

and hasn't subsided since. No doubt many observers concluded that when not even the CIA is safe from hacking[4], the world is confronting a serious problem.

The Insurance Banana Skins report, produced by PwC and the Centre for the Study of Financial Innovation, starkly illustrates the change of thinking in the insurance industry. In the 2017 survey[5], which had more responses from Australian insurers than any other country, cyber risk came in number two, behind change management, as the issue of most concern. In the previous survey in 2015, cyber risk was fourth. But in 2013, it didn't even make the list – from afterthought to second biggest perceived risk in just five years. It may be more appropriate then to refer to cyber as an accelerating risk, rather than an emerging one.

For insurers, every risk is an opportunity, as the expansion of the cyber insurance market demonstrates, but the issues raised by underwriting such an inherently unpredictable threat are topics for another day. What I'd like to address today is APRA's view on the extent to which the defences of the entities we regulate, including insurers, are up to the task of keeping online adversaries at bay, as well as responding rapidly and effectively when – and I use that word intentionally – a breach is detected. Importantly, I will also outline what steps APRA is taking to strengthen the industry's cyber resilience, including announcing a new measure that will require all regulated entities to lift their cyber security capabilities.

An insidious threat

I need hardly tell you that any time your organisation's name or product is trending globally on social media sandwiched between a hashtag and the word "fail", you're having a bad day. So it was for the Australian Bureau of Statistics on the night of August 9, 2016, as the country's first online census crashed due to a distributed denial of service (or DDOS) attack. What's fascinating – and frightening – about the incident, as recounted by ABS boss David Kalisch a few months later, was the Bureau was expecting the attack and thought it was ready[6]. The ABS had identified the risk of a DDOS attack, believed that the impact of a successful attack would be extreme, and considered an attack to be likely. As the ABS has acknowledged, their preparations weren't sufficient. The key lesson, according to David Kalisch, was that you can't outsource risk; although their outsource partner was culpable in practice for the failure, the Bureau suffered tremendous reputational damage because it was ultimately responsible for ensuring a successful census process.

Insurers, whose businesses rely on others outsourcing risk, may bristle at this notion, but cyber security presents a very different threat to most of the risks your industry deals with. Unlike a cyclone or flood, cyber attacks are difficult to predict or detect, can occur with great speed, leverage multiple vulnerabilities, can be executed from anywhere in the world, and are accompanied by a degree of malicious intent not present in a natural disaster.

---

[4] http://www.abc.net.au/news/2017-03-08/wikileaks-releases-thousands-of-documents-cia-revelation/8334366

[5] https://www.pwc.com/gx/en/industries/financial-services/insurance/insurance-banana-skins-2017.html

[6] http://www.abs.gov.au/websitedbs/d3310114.nsf/home/Australian%20Statistician%20-%20Speeches%20-%20Census%202016%20Lessons%20Learned

Regrettably, cyber crime is an expanding industry; it's lucrative, perpetrators enjoy low barriers to entry and face little to no prospect of prosecution[7]. Though governments and organisations are continually investing in their cyber security capabilities, criminals are also adapting and innovating their tradecraft to seek out new vulnerabilities and attack methods. In its 2017 Threat Report, the Australian Cyber Security Centre noted increasingly sophisticated techniques were being developed and deployed against well-protected networks[8]. Furthermore, several trends are expanding the potential weak spots for adversaries to exploit; in addition to the growing use of online services by customers to conduct transactions, entities are increasingly storing data outside their network perimeters and granting service providers access to their systems to perform business and technology processes.

Australian financial institutions are among the top global targets for cyber criminals. Australia is targeted due to its relative wealth and take-up of digital technologies[9], while financial institutions are attractive to criminals seeking money or personally identifiable information on customers – something insurers hold in spades. The most recent Insurance Banana Skins paper describes this sensitive customer data as "gold" on the black market[10]. Accenture's 2017 Cost of Cyber Crime Study[11] found the costs to Australian businesses were the second fastest growing behind Germany. Moreover, the study determined that the global industry segment with the highest annualised cost of cyber crime was yours – financial services. Backing this up, more than half the respondents to APRA's 2016 cybersecurity survey had experienced at least one breach in the previous 12 months that was sufficiently serious to warrant alerting executive management.

Taking all of this into account, APRA views cyber risk as an increasingly serious prudential threat to Australian financial institutions. To put it bluntly, it is easy to envisage a scenario in which a cyber breach could potentially damage an entity so badly that it is forced out of business. I should state that we consider the chances of such an outcome to be remote, especially for larger entities that invest millions of dollars each year in reinforcing their cyber capabilities. But it is no longer beyond the realms of possibility.

Reaction time

Despite this, APRA believes cyber security is generally well-handled by the entities we regulate. The prudential risk is less due to a lack of preparation by industry than the pervasive nature of the threat. Based on our cyber security surveys in 2015/2016 and again last year, as well as regular supervisory activities, it seems clear that cyber security is taken seriously, and entities are predominantly complying with the guidance provided by APRA in CPG 234. A report released last year by the Australian Strategic Policy Institute on cyber maturity in the Asia Pacific region placed Australia second overall, behind the United States.

---

[7] Cyber Maturity in the Asia Pacific Region 2017, Australian Strategic Policy Institute, p4

[8] 2017 Threat Report Australian Cyber Security Centre, p2

[9] Ibid, p46

[10] https://www.pwc.com/gx/en/industries/financial-services/insurance/insurance-banana-skins-2017.html p14

[11] https://www.accenture.com/au-en/insight-cost-of-cybercrime-2017

The launch in 2016 of Australia's first cyber security strategy, with a particular focus on greater cooperation between government and business, can only further strengthen the ability of financial institutions to identify and mitigate against cyber threats.

We have observed, however, several areas where improvement or increased vigilance by regulated entities is warranted, including some of the most elemental. As entities scramble to keep pace with the latest technological threats, APRA is concerned that basic cyber hygiene is sometimes being neglected. For example, a disciplined approach to maintaining the health of information assets is vital, including timely patching against known vulnerabilities and keeping systems current so they can be secured against new threats. Vigilance regarding access management (particularly privileged access – the 'keys to the kingdom') is also fundamental.

As entities increasingly seek out external expertise to buttress their cyber security resources or address capability gaps, APRA has noted that assurance over service providers' cyber security capabilities varies widely in comprehensiveness. Any weaknesses in a contracted third party's cyber security practices can effectively become a beachhead for an attacker to penetrate an entity. Addressing this is especially important amid mounting evidence that cyber criminals are targeting trusted third parties, especially service providers, to gain access to a range of primary targets. In a recent example of this, several Australian government websites, including the Victorian Parliament and the Queensland Civil and Administrative Tribunal, were compromised when a browser plug-in made by a third party became infected with malware[12].

The findings of APRA's cyber security surveys can be found on our website[13], so I don't want to run through everything here. But one finding I do want to emphasise is the need for an enhanced industry focus on responding once an incident has occurred. APRA recommends all entities adopt an 'assumed breach' posture; in other words, you should presume that, at some point, your organisation will experience a significant cyber security incident. Our view is that the maturity of regulated entities' ability to respond to and recover from cyber security incidents varies considerably, although it seems to be improving. In our 2015 cyber security survey, 56 per cent of respondents had tested their ability to respond to and recover from cyber security incidents during the previous year – meaning almost half hadn't. In our survey 12 months later, the proportion that had tested their incident response plans rose to 78 per cent, although we surveyed a slightly different group of respondents, so direct comparison is difficult. And while 90 per cent of respondents to last year's survey had formalised response plans for plausible cyber security scenarios, these plans were often untested and lacked integration with business continuity and disaster recovery plans. The finding aligns with a report by the Australian Securities and Investments Commission (ASIC) into the cyber resilience of Australia's financial markets released in November last year[14]. ASIC found that a third of the organisations it surveyed didn't have cyber incident response plans in place.

---

[12] http://www.abc.net.au/news/science/2018-02-12/hackers-use-australian-govt-websites-to-mine-cryptocurrency/9421906

[13] http://www.apra.gov.au/Insight/Pages/Insight-Issue4-2017.HTML#article2

[14] Cyber resilience of firms in Australia's financial markets, Australian Securities and Investments Commission, 2017

This is a concern for APRA. Just as it's often said that it's not the crime but the cover-up that gets you, the lack of a tested and effective response to a cyber security breach can be a bigger risk for entities than the related incident. The introduction just weeks ago of the new Notifiable Data Breach scheme increases the reputational risks of a data breach by forcing entities to promptly notify affected customers and the Australian Information Commissioner[15]. Social media further intensifies the potential reputational risks of cyber incidents by amplifying customers' ability to identify and call out what they perceive to be unacceptable practices. Keeping quiet and hoping no-one notices is not an option.

Returning to the case of US credit monitoring firm, Equifax, many reports have described the clumsy way the company handled the public disclosure and response in the aftermath as being more damaging than the actual incident[16]. The standalone website the company set up for victims contained vulnerabilities, and its design encouraged the creation of imposter sites and aggressive phishing attempts. Then the official Equifax Twitter account amazingly tweeted the same fake link, not once, but four times. Making the situation worse, it emerged the hackers penetrated Equifax's systems through a known vulnerability for which a security patch was available. As sloppy as that may be, Equifax is not alone in that regard. Participants at a Financial Stability Board workshop on cyber security last October stated that 90 per cent of threats could be mitigated by basic cyber security hygiene[17].

Faster, higher, stronger

To assist industry remain resilient to the growing cyber threat, I can announce today that APRA is releasing for consultation our first prudential standard on information security. The new cross-industry prudential standard CPS 234 builds on the guidance APRA released in 2010 and backs it with the force of law. This decision should be seen as an indication of just how seriously APRA views the issue of cyber security.

Proposed CPS 234 complements the requirements laid out in CPS 220, APRA's cross-industry prudential standard on risk management. The new standard will reinforce that boards have ultimate responsibility for their entity's information security, requiring it to be sufficient to enable, under all reasonable circumstances, the entity to meet its obligations. In order to do this, regulated entities will be expected to maintain sufficient information security capability to deal with changing vulnerabilities and threats, and continually test this for effectiveness. The standard will also require regulated entities to be able to detect and respond to information security incidents in a timely manner. In line with APRA's Business Continuity Plan standard, regulated entities will be expected to notify APRA within 24 hours of experiencing a material information security incident.

Despite APRA's broad satisfaction with industry's approach to cyber security to date, there is absolutely no room for complacency. We expect all entities will need to lift their efforts to comply with the new standard. Once the standard is in place, APRA will start assessing compliance through our normal supervisory processes, and will consider requesting formal independent audits of compliance in due course. Internally, we are also strengthening our

---

[15] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

[16] https://www.wired.com/story/equifax-breach-response/

[17] http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices / p5

supervisors' abilities in this area by broadening their knowledge of cyber risk. In this way, our frontline supervisors will be better equipped to engage with you, assess your cyber preparedness, and give guidance on any areas that warrant improvement.

A discussion paper outlining CPS 234 in greater detail is now available on the APRA website. A 12 week consultation period has commenced, with submissions open until June 7th. APRA is aiming to finalise the new standard in November, with a view to the being effective from 1 July next year.

Rise of the machines

By reinforcing the prudential framework around information security, APRA's objective is for our regulated entities to be a hard target for cyber adversaries to hit, however often they take aim. If the nature of the weapons or tactics cyber criminals deploy against us change – and they will – then so too must the strategies and tools regulators recommend industry use to repel them. It's a view shared by the global regulatory community. The International Association of Insurance Supervisors (IAIS), of which APRA is a member, has begun developing guidelines for members on how they should conduct supervision of insurers' preparedness to tackle the risk of cyber attacks. Further, APRA supports efforts to introduce greater harmonisation between global and domestic cyber regulations. Given the interconnected nature of the threat, and the irrelevance of international borders to cyber criminals, greater co-operation and information sharing among regulators on cyber is more essential than for any other prudential risk.

One area of cyber security that APRA and its international peers are watching closely is algorithm risk. The rise of the Internet of Things and advanced data analytics have seen an explosion in the use of algorithms across the business world, including the financial sector. I know that insurers are highly attuned to the opportunities that artificial intelligence and machine-learning present for fine-tuning and innovation in risk assessment, underwriting, loss prevention and customer engagement. But algorithm use also brings risks that are not yet fully understood by industry or regulators. It is – if you like – an emerging risk within an accelerating risk.

By removing human oversight from important decision-making processes, and instead relying on machine-to-machine interactions, governance and transparency become inherently difficult. With their design unknown to most employees, and their working largely invisible to both entities and their customers, any flaws in an algorithm's functioning or conclusions may not be easily identified and addressed. These risks increase with the use of machine self-learning techniques, which impart greater predictive power to algorithms but make them significantly more complex. This opaqueness is already being targeted by cyber criminals seeking to corrupt either the algorithm or data used to train it, in order to manipulate its conclusions. Analysis released by Deloitte last year concluded that traditional risk management mechanisms designed for managing conventional risks were insufficient to properly govern algorithm risk[18].

[18] Managing algorithmic risks; Safeguarding the use of complex algorithms and machine learning, Deloitte LLP, 2017 p2

A test of stamina

Australia is the number one target of malicious software in the Asia Pacific region[19]. As of today, no APRA-regulated entity has suffered a significant loss due to a cyber incident but that's not for want of trying by cyber criminals. Their relative lack of success to date is a tribute to the thoroughness of risk management and cyber security across Australia's financial sector. Many institutions overseas have not been so fortunate. APRA can only hope such incidents act as a regular jolt to the circuit board of Australian institutions, reminding them that a significant cyber incident on an APRA-regulated entity is probably inevitable.

If that frank statement alarms you, it should. A sense of urgency is paramount given the scale of the threat and the speed with which it's evolving as the digital world expands. APRA's new information security prudential standard, CPS 234, is designed to assist; by complying with its provisions, regulated entities will be better prepared to safeguard the security of the data they hold and money they manage on behalf of their customers. Adopting an assumed breach mentality will create a sharper focus on incident detection and response capabilities and planning. This accelerating risk requires a rapid response, but also recognition that your stamina will be sorely tested. The challenge requires ongoing vigilance, improvement, investment and oversight because, though this race has no finish line, it's not a contest you can afford to lose.

[19] Australia's Cyber Security Strategy First Annual Update, April 2017 p10