Quarterly Newsletter

Volume 14, Issue 4, May 2015

Government provision of catastrophe insurance: risk-informed premiums

John McAneney, Rade Musulin, Delphine McAneney, George Walker, Ryan Crompton and Roger Pielke Jr

This Issue

Sponsors

Aon Benfield

Australian Reinsurance Pool Corporation

Guy Carpenter

IAG Insurance

QBE

Suncorp Group

Swiss Re

Wesfarmers Insurance

In 2013 Risk Frontiers, together with colleagues from Aon Benfield and the University of Colorado, scrutinized a number of Government-sponsored insurance schemes (pools) in the US, Europe and New Zealand. Key differences between government and private sector insurance are summarised in Table 1. At the time the issue of government pools had high currency in Australia after large economic losses experienced in the Queensland and Victoria floods in 2011 and widespread criticism of insurers whose policy covers often excluded riverine flood. The latter situation has since turned around markedly with most insurers now offering flood cover, both flash (fluvial) and riverine, and with the expansion of the National Flood Information Database.

The study was funded by the National Climate Change Adaptation Research Facility and considered whether or not insurance had a useful role to play in encouraging adaptation to extreme weather in the face of a warming climate. For discussion of these themes the reader is referred to *Climate Change Adaptation and the Insurance System* which appeared in the June 2013 issue of Risk Frontiers Newsletter, or McAneney et al. (2014). Here we pose a different but related question: have government pools been successful in reducing risk?

The answer based on our review is no. Risk reduction per se has rarely been an explicit goal of Government pools, which have usually arisen in the face of perceived market failures of the private market, often following a significant natural disaster. In other words they were created to deal with crises in insurance availability after private insurers threatened to withdraw.

One of the means by which insurers might encourage risk-reducing behaviours is by charging property owners a premium that truly reflects risk. Private insurers in Australia are increasingly doing just this. In theory this should encourage local government to demand risk-informed land-use planning and resilient building practices.

But this was not the case for most of the pools examined in our study. In fact an ongoing contentious issue in the US has been the degree of political influence exerted to keep premiums low and to have policyholders in low- and high-risk areas charged similar rates. In the absence of adequate regulation, this lack of financial incentives for mitigation encourages development in high-risk areas.

Despite intentions to be the insurer of last resort, at least in the US, political intervention in setting premiums too low has sometimes seen government pools competing with the private sector and becoming the insurer of first resort. For example in 2008 after Hurricane Ike depleted the reserves of Texas Windstorm Insurance Association (TWIA), legislation was introduced requiring TWIA to stop pricing competitively and limit eligibility to property owners who had been declined insurance equivalent to basic TWIA cover by at least one private insurer. Premium pricing continued to be actuarially unsound, however, with the under capitalisation leaving the entity vulnerable to unmanageable losses. Calls for reform in the US may bring about some positive changes in

government-sponsored insurance pools, but there is debate as to the place of government-run entities in the disaster insurance market (Jaffe and Russell, 2006; Michel-Kerjan et al., 2014).

There is no a priori reason that pools could not encourage risk mitigation but we, like others before us, found little evidence of this. The National Flood Insurance Program (NFIP) and TWIA in the US proved exceptions to this 'rule'. A positive outcome of the NFIP is the high percentage of local authorities imposing floodplain management schemes based on the 100-year return period flood height; however, Burby (2001) questions the extent to which this has inhibited construction activity in flood-hazard prone areas or had much impact on federal disaster relief costs.

The TWIA has had a big effect on building standards, particularly for houses and other low-rise buildings. The program has been successful in enforcing mitigation measures by requiring that buildings meet appropriate weatherproofing specifications of the WPI-8 certification. A Texas Department of Insurance (TDI) windstorm inspector checks the building to ensure it complies with TWIA building specifications and, if the standards are met, a certificate is issued. Prospective buyers now have an expectation of TDI Certification when viewing any property.

1. Government insurance pools can raise funds post-event by issuing government bonds, levies on policies and/or assessments on insurers, or new taxes.
2. Private insurance systems must prefund all losses - it is not acceptable to have a loss and then try to collect funds to pay for it after an event.
3. Private insurance systems usually attract taxes on profits, which can mean that earnings on funds needed to pay claims from infrequent events are taxed away because they show up as income in years without extreme events. Government insurance systems are not bound by this constraint.
4. Private insurance systems operating in a competitive market increasingly set prices related to risk.
5. Government can use its sovereign power to compel one group of consumers to pay too much in order to provide a subsidy to another. In doing so, governments may dilute the incentives for mitigation by subsidising high risks from low risks or by raising revenue for losses from an unrelated source, such as a tax levy.
6. With financial backup or guarantees from the state, government pools can fall back on resources not available to the private sector.
7. Private insurers have polices with a term normally about 12 months duration.

Table 1: Attributes of government-sponsored catastrophe insurance pools vis-à-vis private sector insurance

It is possible that with political will and well-informed debate it may be possible to get the balance right and have voluntary and public providers of insurance working together to reduce risk and increase societal resilience in the face of future catastrophic events. The paradox, as Jaffee and Russell (2006) put it, is that any such well-designed public catastrophe insurance programme will end up looking much like "an equivalent competitive private market." There are no easy answers.

Bibliography:

Burby, R.J., 2001. Flood insurance and floodplain management: the US experience. *Environ. Hazards*, 3, 111-122.

Jaffee, D.M., Russell, T., 2006. Should Governments Provide Catastrophe Insurance? *Economists' Voice,* Berkley Electronic Press, 1-8. Available at: http://faculty.haas.berkeley.edu/jaffee/Papers/095BEPress06.pdf.

McAneney, J., Crompton, R., Musulin, R., Walker, G., McAneney, D., and Pielke R., Jr., 2014. Reflections on disaster loss trends, global climate change and insurance. Chapter 4, pp. 337-339. In *Applied Studies in Climate Adaptation* (Eds. Jean P. Palutikof et al.) John Wiley & Sons.

Michel-Kerjan, E.,Czajkowski, J. and Kunreuther, H., 2014. Could Flood Insurance be Privatised in the United States? A Primer. *The Geneva Papers on Risk and Insurance* doi: 10.1057/gpp.2014.27

From the Cyber-Risk Frontier

by Foster Langbein, Risk Frontiers

Internet events in the last few months – most notably the Sony hack and its fallout - have seen a turning point in the perception of cyber-risk. This is true not only at the private company level but we also now see major concern being expressed at the government level, with US President Obama devoting part of his State of the Union speech to addressing cyber threats.

The reason for the changing view is the marked escalation in the damage hackers were willing to inflict on a private company – Sony Pictures Entertainment (SPE). In marked contrast to large hacks earlier last year of Target and Home Depot and now the recent attack on Anthem Insurance, where personal information including credit card data was stolen for financial gain, the attack on SPE appears to be much more about public humiliation of the company. The hacking group, calling themselves the Guardians of Peace (GOP), first of all managed to exfiltrate more than 100 Terabytes of commercially sensitive data, including unreleased movies, finance details, confidential HR documents and entire archives of email including embarrassing negotiations with many Hollywood celebrities, dumping everything online, whereupon it was gleefully published by the world's press. The wiper malware embedded by the hackers then proceeded to erase the thousands of computers and servers that were switched on and attached to the company's network, leaving only a screen with a skeleton image and the words "Hacked by #GOP". SPE's CEO Michael Lynton likened it to stealing all your possessions and then burning your house to the ground. The attack plunged SPE into an almost pre-digital age of paper memos, temporary email accounts and BlackBerrys unearthed from the basement of the company's HQ. It took something like two months before the company was fully online again.

The US government has, for the first time publicly, laid the blame for the attack on a foreign state actor –the Democratic People's Republic of Korea (DPRK), a claim vigorously denied by the North Korean regime, though they championed the attacks when they occurred due to the hackers demand that the movie "The Interview", a comedy poking fun at the regime, not be released in cinemas.

The attribution to the North Korean regime is however a somewhat contentious issue, with several high profile security researchers raising doubts about such a clear-cut assertion. Despite the seemingly straightforward narrative that the hack was made as retribution for making and releasing "The Interview", at one point threatening 9-11-like consequences and leaving the majority of picture theatres too scared to show the film on its opening date, the original demand email signifying the start of the hack on November 24th made no mention of the film at all. It appears as if it was only after links had been conjectured in the press about the film that demands targeting its release were made. Furthermore, once it seemed maximum entertainment-value had been squeezed from this demand, the GOP changed their mind and stated that it would be ok to release the movie after all.

Perhaps more telling is that analysis of the internals of the malware reveal lists of hard coded server paths and passwords revealing a deep knowledge of SPE's internal IT architecture – something that seems much more likely the result of privileged insider knowledge. The alternate narrative offered is that the hackers were associated with disgruntled ex-employees out for revenge. Revenge certainly seems a more likely motive given the design of the malware appeared to be aimed at maximum disruption whilst the release of the data into the public sphere rendered it valueless. And indeed there has been a long ongoing period of large staff layoffs since the 2012 announcement of a 3-year massive cost cutting restructure over all divisions of Sony, reducing their workforce by over 10,000 employees.

For now the attribution question has to be left unresolved. The FBI, with support from the National Security Agency's (NSA) North Korean SIGINT (signals intelligence), have said they have convincing evidence the hack originated from the elite cyber unit inside the DPRK known as Bureau 121. The Obama administration deemed this enough to impose further sanctions on North Korea. Frustratingly, the publicly revealed parts of this evidence seem fairly flimsy and, for now at least, full evidence such as complete logs will not be forthcoming. However, many are not prepared to take the FBI at its word after past grave intelligence failures such as the evidence for weapons of mass destruction in Iraq.

Moreover, in the sphere of cyber-attacks, attribution is hard – not only is the actual evidence gathering difficult, there being many techniques for anonymising or spoofing internet addresses and credentials, but the actual hacking groups themselves are not necessarily neatly defined national groups sitting in a single location. Often they are more amorphous groups spanning multiple countries united by some common cause – and often only loosely united at that - with infighting and splinter groups producing contradictory threats and attacks.

In practical terms, a much more important question is the how rather than the who. The hacking ploy used against Sony was a standard - almost mundanely so: a spear-phishing attack gained the credentials of at least one high level administrator which allowed the stealing of data and placement of the damaging malware throughout Sony's network. Even the wiper malware itself was known beforehand – it appears to be an improved version of Shamoon that had impacted the oil and gas sector in 2012, most notably the Saudi arm of Aramco. A year later in 2013 it was used against South Korean banks and TV stations and a month after that in a series of damaging cyber-attacks across South Korea where it was known as "DarkSeoul". So, despite SPE's security provider and the FBI largely absolving SPE of much responsibility for the attack, many independent observers have highlighted some pretty sloppy security practises and wondered how exactly it was not noticed that such a huge volume of data was leaving their network.

Although there is still more to play out in this story, SPE is forecasting a $35M loss over the next year, covering damage, investigation and repair of systems affected by the hack. This amount, Lynton claims, is easily

covered by the firm's cyber-insurance though some lawyers have suggested those covering the loss will be carefully scrutinizing the fine print on these contracts in light of Sony's lax approach to security. A further complication may well be whether the attack could be classified as cyber-terrorism, for which some cyber cover includes exclusions, and whether protection might fall under the Terrorism Risk Insurance Act (TRIA) only recently extended by Obama after it lapsed at the end of 2014.

The direct damage to systems is, however, surely only a very small part of loss sustained at SPE. The business interruption resulting from the extensive downtime, liability for the exposure of personal information for which SPE is already defendant in a growing number of lawsuits and the reputational damage from the exposed personal communications would appear to be of much greater consequence. The revelations of confidential emails aired in the press in the most embarrassing way has led to SPE's Co-Chairman Amy Pascal stepping down from her post.

The aftermath of the attack has seen major growth in the demand for cyber insurance. The particulars of the hack also mean we are likely to see an evolution of the security policy requirements for cover as well as a tightening of what exactly is covered. Expect to also see more regulatory compliance requirements in the cyber arena. President Obama has just signed into law an executive order promoting the sharing of cyber-security data in the private sphere and the creation of an agency - the Cyber Threat Intelligence Information Center (CTIIC) - to manage the process. The hope is that all of this will lead to a concomitant improvement in companies' security practices. It should certainly prove to be a boon for cyber security consultancies and incident response teams. The Sony hack has indeed been a game-changer.

Andrew Gissing

In March, we were excited to welcome Andrew Gissing back to the Risk Frontiers team. Andrew is an emergency management expert and a former student of Risk Frontiers where he completed his Master's thesis, focusing on the estimation of commercial flood damage. Since leaving in 2002, Andrew has performed various senior executive roles in the emergency management and social services sectors, including that of the Deputy Chief Officer of the Victoria State Emergency Service (VICSES).

Throughout this time Andrew has been responsible for significant achievements such as:

* Development of the new Emergency Management and Communications Division at VICSES, which is responsible for emergency planning, emergency risk management, community education, assurance, media and corporate communications;
* Enhancement and implementation of community emergency risk management and flood emergency planning arrangements in Victoria;
* Completion of state level emergency plans for flood, storm, earthquake, tsunami and pandemic in both Victoria and New South Wales;
* Design and implementation of new community engagement programs such as the successful Business FloodSafe program; and
* Development and leadership of Enterprise Risk Management and Business Continuity frameworks for the NSW Department of Family and Community Services.

Andrew is an experienced crisis leader having held senior state-wide leadership roles during some of Australia's most recent natural disasters such as the 'Pasha Bulka' Storm (2007), Black Saturday Bushfires (2009), and the Victorian Floods (2010/11). He has also been a member of the Australian Emergency Management Assistance Team.

Andrew is passionate about risk management and his main interests lie in enhancing the capability of organisations and communities to manage risk and ultimately enhance their resilience. Andrew is known for his strategic leadership, and in the provision and implementation of end to end management solutions, including cultural change.

At Risk Frontiers, Andrew will lead our engagement with the public sector and grow our range of service offerings to include Enterprise Risk Management, Business Continuity and Crisis Management. Andrew can be contacted at andrew.gissing@mq.edu.au.

Thomas Loridan

Originally from Cannes in the south of France, Thomas left the French Riviera at the age of 20 to study applied mathematics (and drink wine) in Bordeaux. He later moved to the UK to follow the University of Reading's MSc course in "weather, climate and modelling", before getting his first job in Barcelona as a research support engineer in the Earth Science department of the Barcelona Super Computing Center (BSC).

Missing the weather in London, one year later Thomas decided to head back to the UK and begin a PhD in boundary layer meteorology under the supervision of Prof Sue Grimmond at King's College London. His PhD focused on the modelling of urban heat and momentum fluxes in weather and climate models using simplified urban canyons to represent the urban landscape.

On graduation Thomas joined the catastrophe modelling company RMS and participated in the development of their latest Japan Typhoon model. His principal task was to model the evolution of typhoon wind fields as they transition from fully tropical systems to extra tropical storms at higher latitudes. Thomas is now very excited to start a new chapter with Risk Frontiers and keep on studying tropical cyclones and their specificities in different regions of the world. Thomas can be contacted at thomas.loridan@mq.edu.au.