GRC PROFESSIONAL
GOVERNANCE • RISK • COMPLIANCE

MAY 2015 | THE OFFICIAL MAGAZINE OF THE GRC INSTITUTE

RISK CULTURE

DOES YOUR RISK CULTURE STACK UP?

GRC INSTITUTE
GOVERNANCE • RISK • COMPLIANCE

www.curasoftware.com

GRC Solutions

Making Governance, Risk & Compliance More Effective & Efficient

- Supports multiple frameworks simultaneously for: **Enterprise Risk Management, Operational Risk Management, Project Management, Financial Controls Management**, and more.
- Built-in support for incident management, loss events and self-assessments.
- Comprehensive and flexible compliance capabilities.
- Email notifications and complete audit trails.
- Full audit support.
- Powerful executive dashboards, reporting and analysis capabilities.
- Configurable by business users to match your organisation's existing processes.
- Flexible installation options (on-site / hosted / software as a service).
- Deployed in more than 250 organisations worldwide, including:

BHP Billiton Bendigo Adelaide Bank Coca-Cola
Vodafone Woodside Energy Westfield

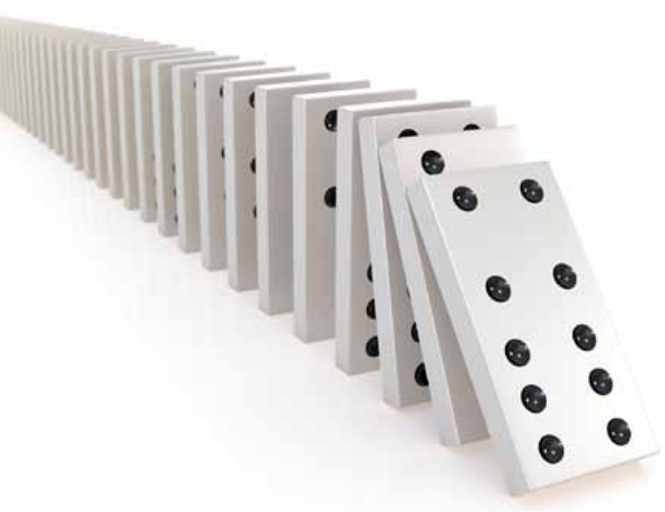
Contents

RISK CULTURE

9

Building Risk Culture

Companies around the world are spending huge sums of money improving their compliance systems and processes, but is it all in vain if the culture of the organisation remains toxic? How do you build and asses a risk management culture?



Contact us

GRC Professional is the official monthly publication of GRCI in Australia, New Zealand, Hong Kong & South-East Asia.

GRC Institute

Managing Director:
Martin Tolar
martin.tolar@thegrcinstitute.org

National Manager:
Naomi Burley
naomi.burley@thegrcinstitute.org

Ph: +61 2 9290 1788
Fax: +61 2 9262 3311
www.thegrcinstitute.org
GPO BOX 4117 Sydney
NSW 2001 Australia

GRC Professional

Editor:
Daniel Sheehan
+61 400 648 760
daniel.sheehan@thegrcinstitute.org

Advertising:
Naomi Burley
+61 2 9290 1788
naomi.burley@thegrcinstitute.org

GRC Conference line-up finalised

Welcome to the May edition of *GRC Professional* magazine. Since we last published *GRC Professional*, the team at the GRC Institute has finalised the line-up for our annual conference, to be held from 28-30 October in Melbourne. In addition, we have also finalised the program for our GRC Summit, to be held in Auckland on 10 June.

Both events promise to provide attendees with a panel of high-profile, engaging industry experts, who will speak on a range of diverse and insightful topics. For more information, see the inside back cover of this month's magazine.

Since our last edition, we have seen a number of interesting cases involving employees and how their use of social media has had a detrimental impact upon their employment prospects. We spend some time examining one high profile case in New Zealand, as well a recent spate of similar cases – some of which look to be heading to the courts. We explore this emerging area with a view to extracting some lessons for GRC professionals to manage the risks posed by the use of social media by employees.

In honour of Privacy Awareness week (3-9 May), held this month, we have a special report on privacy. In the report, we present an interview with Assistant Privacy Commissioner Angelene Falk, as well as exploring the topic of the cost of privacy breaches.

We also look at the growing demand for GRC Professionals in the financial services sector – an area that has seen, not only salary increases in some fields, but also the poaching of entire teams in bidding wars caused by shortages of skilled and qualified staff. While this represents great news for members seeking to increase their salary, we pose the question from an industry perspective: what does this mean for the stability of organisations, when attracting and securing suitably-trained risk and compliance professionals becomes difficult?

Finally, our cover story this month examines the ever-important but difficult-to-quantify topic of culture. Industry experts tell us how to build and assess an appropriate risk management culture.

This edition marks that last that will see Daniel Sheehan as the Editor of *GRC Professional* Magazine. I would like to take this opportunity to thank him for the contribution he has made in making this magazine one of the leading sources of information for GRC professionals. We wish him well in his future endeavors. From next month onwards, *GRC Professional* will be edited by Mark Phillips, a name that many of our longer standing members will recognize as the former editor of Risk Management Magazine. I am sure you will all make him feel welcome as he joins the GRC Institute team.

I hope you will find this month's edition as enjoyable and insightful to read as it was for us to compile.

Martin Tolar CCP, Managing Director, GRCI

We spend some time examining one high profile case in New Zealand, as well a recent spate of similar cases – some of which look to be heading to the courts.

READER POLL

Privacy Reform

IN THIS MONTH'S POLL, WE TURN our attention to social media. In the last 12 months, there have been a number incidents involving social media that have left corporations and individuals embarrassed. We want to know: how are you dealing with social media?

- Does your organisation use social media proactively?
- Does the risk function monitor social media activity within your organisation?
- Do you have a social media policy that has been reviewed by the risk function?
- Are staff educated on the risks of social media?

Complete the survey here.

The results will be published in the June edition of GRC Professional.

LAST MONTH'S POLL

Privacy Compliance

LAST MONTH, WE TOOK A LOOK at privacy compliance (see page 20 for our privacy special report this month). More than 70% of readers said the privacy reforms undertaken by the Privacy Commissioner have had an impact on how they manage customer data.

Some professionals are still struggling with privacy compliance, with more than 60% of readers saying privacy compliance is one of their biggest risk and compliance issues. Meanwhile, more than half of readers said that privacy reform had been a positive thing for business.

Thank you to all those readers who participated.

BEST FROM AROUND THE WEB

These were the stories being discussed at the GRC Institute this month:

SHED NO TEARS FOR SLOW DEMISE OF THE JOINT CEO-CHAIR ROLE

WHITE SUPREMACISTS STOLE MY IDENTITY TO SPEW HATRED ON THE TIMES OF ISRAEL

OBSERVATIONS ON THE FINANCIAL SYSTEM

WHEN NON-COMPLIANCE BECOMES A PUBLIC SAFETY MATTER

A HEDGE FUND BECOMES AN ACCIDENTAL HERO OF ANTI-CORRUPTION CAMPAIGNERS

BLUEPRINT OneWorld

ICSA Software International

Add extra protection against Malware threats

Blueprint BrowserProtect is the solution for advanced browser security

Contact us for a demonstration

+61 2 8096 8300 icsasoftware.com/bponeworld aunz@icsasoftware.com

Australian Government Launches White Collar Crime Taskforce

The Australian Government is establishing a new taskforce to fight serious, organised financial crime. According to the Government, this type of crime poses a genuine threat to national security and to the integrity of Australia's economy, financial markets, regulatory frameworks and tax revenue collection.

The Government will provide $127.6 million over four years for investigations and prosecutions that will address superannuation and investment fraud, identity crime and tax evasion.

The Serious Financial Crime Taskforce includes the Australian Taxation Office, Australian Crime Commission, Australian Federal Police, Attorney-General's Department, Australian Transaction Reports and Analysis Centre, Australian Securities and Investments Commission, Commonwealth Director of Public Prosecutions and Australian Customs and Border Protection Services.

The Taskforce is the continuation of Project Wickenby, which finishes in 2015.

Project Wickenby has so far raised over $2.1 billion in liabilities, as well as increased tax collections from improved compliance behaviour following interventions. To date, 76 individuals have been charged with serious offences and there have been 44 criminal convictions.

According to Treasurer, Joe Hockey, "The Serious Financial Crime Taskforce will have an unquantifiable positive benefit on the financial wellbeing of members of the community who, without the Taskforce, may be victims of financial crime. It will also help ensure all taxpayers pay their fair share of tax."

SFC emphasises proper disclosure of inside information

The Hong Kong Securities and Futures Commission (SFC) has highlighted the importance of the proper disclosure of inside information by listing applicants and listed companies.

Drawing on a number of examples identified in recent listed company announcements, the SFC has described some of the factors to be considered when determining whether information needs to be disclosed. This includes, among other considerations, the certainty and materiality of the information, as well as whether it diverges from market expectations. The SFC also advises companies to be careful when they repeat information, either included in their prospectuses or otherwise already announced.

The SFC has reminded entities of the obligation placed on sponsors to conduct reasonable due diligence to ascertain the accuracy of the information disclosed in listing documents. Additionally, the SFC makes it clear that, where the identities of a listing applicant's major customers are not included in the prospectus, then this information cannot be supplied at roadshows or in marketing materials. Listing applicants are also encouraged to ensure incentive schemes for initial public offerings are appropriate and easy to understand.

NSW ICAC bolstered

The NSW Government has confirmed it will legislate to confirm all past corruption findings by NSW ICAC remain valid, including the cases in the Eddie Obeid matter, after a High Court ruling put them in jeopardy.

The Government will also ask an independent panel of experts, chaired by the former Chief Justice of the High Court, the Hon Murray Gleeson AC QC, to review ICAC powers.

NSW Premier Mike Baird said the review of ICAC's powers would be delivered to the Government by July 10, "…so that a second Bill, if deemed necessary, can be introduced later this year."

Priorities for boards – balancing growth and ethical conduct

In a low growth world, businesses are under constant pressure to find new revenue streams. This is leading many to look to the emerging economies in Asia, Latin America and Africa, where a less developed business environment creates opportunities for growth. Yet this exposes the business to risks and can strain the risk function.

Advisory Firm, EY, has released a report looking at this issue. They say moving into new markets, and into rapid-growth markets, does bring additional risk. EY says good compliance programs do not inhibit growth, rather the opposite is true, and compliance enables business to move into growth areas, safely.

"Companies worldwide are battling to survive and grow in what have continued to be highly adverse economic conditions. In this environment, growth and ethical business conduct can sometimes appear to be competing priorities," says David L Stulb, Global Leader Fraud Investigation & Dispute Services.

"Many mature economies are struggling, while some growth markets in Asia and South America are decelerating. As a result, management and boards are increasingly focusing their attention on "the next BRICs." Whether one is speaking of Indonesia, Nigeria, Mexico or Turkey, among others, the opportunities to secure new revenues in rapid-growth markets are significant. Part of evaluating these opportunities is to understand the associated risks. Many of these markets have historically been perceived as having high incidences of fraud, bribery and corruption."

"Organisations need to make concerted, risk-focused efforts that target areas of potential exposure, and management needs to lead by example. Record levels of fines, penalties and profit disgorgements secured by the US DoJ and SEC in the past year certainly raise the perceived and actual cost of non-compliance. Companies and their boards must weigh the upside and downside risks associated with varying degrees of compliance enforcement within their organisations.

The report asks how can boards and those tasked with compliance respond to these challenges?

- First, they must ensure effective lines of communication with a broad range of roles within the business. This will enable the board to question the information they are given
- Second, improvements can be made to focus compliance reporting to the board.
- Third, boards must make sure they are asking the right questions. These could include:
  - Does management at headquarter level understand local risks and have strategies been developed to deal with these specific risks?
  - Can management demonstrate the contemporaneous effectiveness of its anti-corruption compliance efforts to its stakeholders?
  - Does the company know how many third parties and agents represent it, particularly in dealing with those that could be considered "government officials?"
  - Is management making the best use of the latest forensic data analytics techniques to monitor compliance in real time?
  - Assuming that contracts with third parties normally contain audit rights, how many times has the company conducted an audit, principally to gain comfort around bribery and corruption risk?
  - Does the company have clear criteria to guide it with respect to how extensive pre- or post-acquisition anti-corruption due diligence should be, or whether to conduct it at all?

Growing beyond, therefore, requires a nuanced view of individual markets and cultural norms, balanced against the statutory language of a proliferating number of bribery and corruption laws.

EY says changes to a company's culture to mitigate the risks of fraud, bribery and corruption cannot be made overnight. Organisations need to make concerted, risk-focused efforts that target areas of potential exposure, and management needs to lead by example.

"Only then will companies be able to properly balance the priorities of growth and ethical business conduct, while seizing opportunities in these highly adverse economic conditions."

complianceWave

The New Standard for
Effective Compliance Communication

Access the world's largest multi-media library of crisp, engaging ethics and compliance communications.

Available in Multiple Languages

www.compliancewave.com/GRCI

RISK CULTURE

Companies around the world are spending huge sums of money improving their compliance systems and processes, but is it all in vain if the culture of the organisation remains toxic? How do you build and assess a risk management culture? Can culture really be changed? **Daniel Sheehan.**

Weaknesses in the risk management framework, as well as in decision-making processes and in assigning clear accountability for identifying and addressing behaviours not supportive of sound risk management, enable particular risks to take root and grow.

IT MAY HAVE BECOME ONE OF THE MOST over-used clichés in business text books, but Peter Drucker's famous euphuism, 'culture eats strategy for breakfast,' is as true today as it ever was. This notion is particularly true when it comes to risk and compliance, especially in light of repeated breaches that have occurred in financial institutions around the world.

The scale of misconduct in some financial institutions has been so widespread and severe that ongoing issues of culture are being raised by regulators. In particular, the Financial Stability Board, the International body that monitors and makes recommendations about the global financial system, has been a leading advocate for including issues of culture in prudential supervision. It was its December 2013 report, 'Guidance on Supervisory Interaction with Financial Institutions on Risk Culture,' that first kicked-off the debate around culture and supervision.

According to the report, outcomes-based supervision involves proactive assessment of the decisions of the financial institution, based on its strategic vision, business model and risk appetite framework; supervision is not only about ensuring compliance with the rules, but also with the spirit. "At the crux of this supervisory approach is an understanding by both the financial institution and the supervisor of the institution's risk culture."

Failures in risk culture are often considered a root cause of the Global Financial Crisis, as well as headline risk and compliance events (FX and LIBOR manipulation, sanctions and AML violations and financial advice issues in Australia). The Financial Stability Board says, a "financial institution's risk culture plays an important role in influencing the actions and decisions taken by individuals within the institution and in shaping the institution's attitude toward its stakeholders, including its supervisors. A risk culture that promotes prudent risk-taking, and discourages unrestrained profit maximisation without due regard to risks, supports an environment that is conducive to ensuring emerging risks that will have a material impact on a financial institution, and any risk-taking activities beyond the institution's risk appetite, are recognised, assessed, escalated and addressed in a timely manner.

"Weaknesses in the risk management framework, as well as in decision-making processes and in assigning clear accountability for identifying and addressing behaviours not supportive of sound risk management, enable particular risks to take root and grow."

Partly in response to the Financial Stability Board views, culture became a key part of the oversight responsibilities of the UK Conduct Authority, and in Australia with APRA. With the regulators making culture a priority, inevitably it has trickled down and become a hot topic amongst not only risk teams but boards and CEO's as well.

But it is not just the regulatory imperative driving firms to look closer at their culture. With many firms spending multiple millions on new compliance systems and staff, they want to be getting value for money. If the culture is not right, that money is likely to be wasted.

For risk and compliance staff, recognising that culture is important is the easy part; the hard part has been assessing what is an appropriate risk culture and implementing the necessary changes to change culture.

Paul Korte is a financial services risk and compliance expert who has worked in leadership roles in Australia and Asia and has grappled with cultural change at financial institutions. "We had some very public examples in the press recently of institutions overseas, and domestically, of what appears to →

be systemic risk and compliance cultural problems," Korte says. "Internationally, I am talking about FX and Libor rigging, and money laundering violations, and in Australia, we have serious issues around the quality of financial advice. These are all very public examples of culture failures."

Korte says there are lagging and leading indicators of risk culture that can provide a useful insight into the health of culture before a scandal or breach occurs. Leading indicators include things like reward and recognition policies and the corporate Code of Conduct. Lagging indicators include metrics such as incident identification, escalation and management practices.

Risk culture surveys have become a popular tool for risk professionals in recent years. Korte says they can be a valuable diagnostic tool. "In practice, a series of questions is sample distributed to the organisation. There is a usually a subset of questions for your management and the board, and other questions for line management and staff. Typically the surveys are segmented for different areas of the business and also the risk function. This enables you to see what the views and attitudes are in the different parts of the organisation."

You can then see the informal view and baseline it against the formal view, as displayed in corporate policy.

Korte says that risk culture surveys are helpful because they reveal the 'unsaid' in organisations. "You can then see the informal view and baseline it against the formal view, as displayed in corporate policy."

Risk culture surveys also immediately tell you if staff feel it is a safe environment to challenge and escalate. If the results of the risk culture surveys differ widely from what management is being told in the formal escalation channels, than you very likely have a culture problem.

What is a bad risk culture?

There is no easy answer to this question. "We have all heard the criticisms about sales culture and organisations having the wrong emphasis on achieving short-term objectives and targets," says Korte. But the reality about what is a negative risk culture is more nuanced.

"One of the important points to remember when talking about risk and compliance culture is to take a step back and think about what the objective really is here. The objective of a risk management framework is to get an organisation to operate within its risk appetite, or put another way, operating within the set limits of acceptable risk-taking.

"Appetite is central to the whole discussion. It is the setting of the risk appetite, the setting of the boundaries and the operationalising of the boundaries within an organisation that is ultimately going to influence expected behaviours – which, in the end, impacts the culture."

Korte says when he talks about operationalising the risk appetite, he is talking about cascading it down from the board and senior leadership to an operational level. "I actually like to talk about the risk appetite as being the risk budget, so it is in terminology that business people can understand, and readily relate to. To the extent that it is possible, you need to quantify and put that into dollars and you need to translate that and cascade it down the organisation through setting appropriate tolerances, limits and targets."

Once that is established, you then need to incentivise staff to operate within the organisation's risk appetite. "Culture is essentially a derivative of the behaviours within an organisation, so you are

looking at how you can change or influence behaviour," Korte says.

"The reward and recognition policies within an organisation are an important, but not the only lever that can help an organisation to operate within that risk appetite. However, clearly, reward and recognition is going impact behaviour, which then impacts risk culture."

However, there are other levers as well. Risk governance and leadership is a key one. "We of course know about tone from the top, but it is also about the important role line management play in f setting the right example," Korte says. "Are leaders in the organisation positive role models for their junior staff members?"

Other key factors include whether or not there is accountability and ownership around risk, not only from the Chief Risk Officer but also owning risk in the business. The first line needs to understand that risk is primarily their responsibility.

Korte says transparency is also a key factor in determining culture. How is information shared and how does it flow around the organisation?

Escalation and effective challenge are also interesting concepts, when it comes to risk culture. Korte says effective challenge is when employees and managers are able to openly and constructively communicate. The next step on from that is escalation, and escalation is a key consideration in any discussion around culture.

The reward and recognition policies within an organisation are an important, but not the only lever that can help an organisation to operate within that risk appetite.

"Escalation is in effect the speed at which bad news travels vertically within an organisation," says Korte.

"One of the most important channels is matrix management. Matrix management is about giving employees a safe path for information to move vertically – the ability of staff to go to another person, or manager, who is not necessarily their line manager."

Organisations also need to invest in learning and development to help build appreciation for the value of risk management. Case studies are very important to learn from mistakes, says Korte. "Organisations should focus on real life examples from within their own organisation or from other organisations to learn where they went wrong." Learning from your own or others' mistakes can often be the best training tool.

Sally Freeman is Partner in charge of KPMG's Risk Advisory practice and helps companies deal with culture transformation. "We see risk culture as being fundamental to a client having an effective risk management process. If you set a risk strategy and processes in place, but you haven't set the tone and the culture, then it will be sabotaged. We see risk culture as being very important to any organisation. It is about doing the right thing, rather than whatever it takes. "

Breaking it down

"Risk culture has been seen as something that is perhaps a little bit nebulous, but we have broken it down into a model," Freeman says. KPMG looks at

several factors when assessing risk culture. "We look at the strategy and direction of the entity and whether risk is being considered in that. We look at whether there is a short-term or long-term focus, a customer focus or a profit focus.

"We look at the responsiveness of an organisation: how will it change and react if some of these things go wrong? We investigate what has been done with people who do not comply with the ethics of the organisation.

"We also consider competency and how that is assessed. Have you got the right skill set? Do they understand how their behaviour influences others? Do they have clear accountability?"

Freeman says motivation is a big factor. "Motivation is a critical part of culture. Is there a focus with career advancement on the greater good of the organisation, or is it short-term focused? Are employees incentivised to do the right thing, or are they pushed to make profit?

Motivation is a critical part of culture.

Does employee remuneration look at prudent conduct, as well as sales? Does it reward company-wide outcomes, or just individual outcomes?"

Korte agrees, but says incentives and recognition is not just about money and remuneration. "There are different motivating factors for different people. It doesn't always relate to money and it varies in different cultures. At times, the reward may be other forms of approval, avoiding discord, or simply making sure you appear to be part of the group."

Warning Signs your culture is in trouble

- There is no communication of defined-risk appetites.
- They are too focused on profit and the short-term.
- Limited or under-investment in planning for the future.
- Risk management may be a silo within an organisation.
- There is a culture of saying 'that is just the way it is,' and there is not a culture of speaking out.
- A fear of bad news or criticism of errors
- Tolerating of smaller ethical breaches; boundaries being stretched.

Changing Culture

Freeman says culture cannot change overnight. "We certainly find that risk culture does need to be built over time. But it also needs to be inspired. That is where we look to the leadership. Setting the example for others to follow."

"The risk culture can't be changed, if it just a risk management function on the side. We need to know the CEO, the C-levels, the board are engaged and committed to the risk culture transformation and they are consistently delivering similar messages."

Freeman says it is the greatest success when an entity comes up with a true statement of the way they wish to conduct business, it aligns with their values and there is a consistent message throughout the organisation on how things are done.'

"This is the way we work and these are the values we have." •••

FINANCIAL CRIMES

Edition Eight May 2015

Money laundering
Page 14

Procurement Fraud
Page 16

Corruption risk
Page 18

Merrill fined for compliance breaches

The UK Financial Conduct Authority has fined Merrill Lynch US$20 million for compliance breaches. Merrill Lynch incorrectly reported 35,034,810 transactions and failed to report another 121,387 transactions between November 2007 and November 2014. It was the biggest fine ever imposed by the FCA for transaction-reporting failures.

Transaction reports in the UK securities market have to include details of the product traded, the firm that undertook the trade, the trade counterparty, the price, quantity and trading venue.

The FCA said Merrill Lynch failed, over several years, to correct problems with its transaction reports. The poor performance continued, despite substantial FCA guidance and a history of transaction-reporting non-compliance, including a "Private Warning" issued in 2002 and a fine of £150,000 ($225,000) in 2006.

The FCA said Wednesday's £13.2 million fine consisted of a penalty of £1.50 ($2.25) per line of incorrect or non-reported data. The regulator said it raised the penalty from £1.00 ($1.50) per line used in the three most recent transaction reporting cases to increase deterrence.

Georgina Philippou, FCA Acting Director of Enforcement and Market Oversight, said, "Proper transaction reporting really matters. Merrill Lynch International has failed to get this right again — despite a Private Warning,

a previous fine, and extensive FCA guidance and enforcement action in this area."

Merrill Lynch agreed to settle at an early stage of the investigation, and received a 30% reduction in the overall fine, the FCA said. •••

DB given record fine for rate rigging

Deutsche Bank has been given a $2.5 billion fine over the rate rigging scandal. The fine was imposed by US and British authorities, who also ordered them to fire seven employees for alleged benchmark interest rate rigging.

It was the biggest fine ever imposed by the FCA for transaction-reporting failures.

The UK's Financial Conduct Authority (FCA) said at least 29 Deutsche Bank employees, including managers, traders and submitters were part of the scam, based mainly in London, but also in Frankfurt, Tokyo and New York.

As part of the settlement, Deutsche Bank pleaded guilty to criminal wire fraud and the parent group entered into a deferred prosecution agreement to settle US wire fraud and anti-trust charges. US authorities said independent monitors would be installed. •••

RBA Governor criticises misconduct

Australia's Reserve Bank Governor, Glenn Stevens, has criticised the instances of misconduct in the Australian financial system. In a speech, Stevens said misconduct is still plaguing the financial system.

"This has loomed larger for longer in many jurisdictions than we would have thought likely, a few years ago. Investigations and prosecutions for alleged past misconduct are ongoing. It seems our own country has not been entirely immune from some of this.

Stevens says, "Root causes seem to include distorted incentives, coupled with an erosion of a culture that placed great store on acting in a trustworthy way."Stevens argues that finance depends on trust. "In fact, in the end, it can depend on little else. Where trust has been damaged, repair has to be made. Both industry and the official community are working hard to try to clarify expected standards of behaviour. Various codes of practice are being developed, calculation methodologies are being refined.

"In the end, though, you can't legislate for culture or character. Culture has to be nurtured, which is not a costless exercise. Character has to be developed and exemplified in behaviour. For all of us in the financial services and official sectors, this is a never-ending task."

Australian property key money laundering risk

The Financial Action Taskforce (FATF) has said that laundered money is being used to purchase Australian real estate and authorities need to do more. Daniel Sheehan.

The Australian property market has been one of the strongest performing property markets anywhere in the world over the last decade. Property prices in Sydney, Melbourne and, until recently, Perth have grown strongly, defying global trends and troubles in the financial system. But what role has laundered money, particularly from China, played a role in the property boom?

It is difficult to quantify exactly, but according to FATF, there are substantial flows from money laundering heading to Australian property, and Australia needs to tighten safeguards against money laundering in real estate. Much of the laundered money is suspected of coming from China.

Chinese nationals invested nearly $6 billion in Australian property in 2013, according to the Foreign Investment Review Board. Much of this investment involved funds sourced from legitimate business; however, there is a widespread suspicion that corrupt public officials in China are using Australia as a means of getting funds offshore. Recently, Australia ordered a Chinese owner of a $39 million dollar Sydney mansion to sell within 90 days, as the property was purchased illegally. Treasurer Joe Hockey has also said Australia would beef up its investigations into foreigners buying residential properties.

For its part, China is also pursuing Chinese nationals aggressively who have taken money abroad. "Operation Fox Hunt" is the Chinese Government's plan to chase suspects who have left the country to seek refuge abroad. China has had some success in forcing individuals to return home to face charges, mostly by applying pressure on business and family contacts who have remained in mainland China.

"Australia remains at significant risk of an inflow of illicit funds from persons in foreign countries who find Australia a suitable place to hold and invest funds, including in real estate," says the FATF, in its review of Australian AML/CTF procedures.

"Australia is seen as an attractive destination for foreign proceeds, particularly corruption-related proceeds flowing into real estate from the Asia-Pacific region. Outward proceeds flows are directed mainly to major financial hubs in Asia and the Middle East, with tax proceeds also flowing to European havens."

Australia is seen as an attractive destination for foreign proceeds, particularly corruption-related proceeds flowing into real estate from the Asia-Pacific region.

The FATF is calling on real estate agents and other non-bank staff involved in the property sector to take more responsibility to weed out money laundering.

"A lot of reliance is placed on the banking and financial sector as gatekeepers, due to the absence of AML/CTF regulation and requirements on key high-risk designated non-financial businesses and professions (DNFBPs), such as lawyers, accountants, real estate agents and trust and company service providers. As a result of these factors, the effectiveness of the preventive measures in the financial system as a whole, and DNFBPs, is hence called into question to some extent."

A lot of reliance is placed on the banking and financial sector as gatekeepers ...

Other Recommendations

Aside from property, FATF had a series of recommendations for Australian authorities to improve its AML/CTF regime. The prioritised recommended actions for Australia, are:

- Undertake a re-assessment of Australia's money laundering risks, and formalise the ongoing processes for re-assessing risks. Australia should also identify metrics and processes for monitoring and measuring success.
- The authorities should place more emphasis on pursuing money laundering investigations and prosecutions at the federal as well at the state/territory level. The authorities should increase efforts to address ML risks associated with:

  - predicate crimes other than drugs and tax, including foreign predicates;
  - the abuse of legal persons and arrangements and the real estate sector;
  - identity fraud; fraud; and
  - cash intensive activities.
- AUSTRAC should incorporate more (inherent) risk factors besides data analysis from filed reports into identifying and assessing the risk of reporting entities. AUSTRAC should consider opportunities to further utilise its formal enforcement powers to promote further compliance by reporting entities through judicious use of its enforcing authority.
- Australia should ensure financial institutions are actively supervised for implementation of DFAT lists, most likely through a legislative amendment to the statute identifying and authorising the agency responsible for supervision.
- Australia should implement a targeted approach in relation to preventing NPOs from TF abuse. As a first step, Australia needs to undertake a thorough review of the TF risks that NPOs are facing (beyond the issues already covered in the NRA) and the potential vulnerabilities of the sector to terrorist activities.
- Ensure that lawyers, accountants, real estate agents, precious stones dealers, and trust and company service providers understand their money laundering/ terrorist financing ML/TF risks, and are required to effectively implement AML/ CTF obligations and risk mitigating measures in line with the FATF Standards. Ensure that reporting entities implement as early as possible the obligations on enhanced customer due diligence (CDD), beneficial owners, and politically exposed persons introduced on 1 June 2014.
- Australia should assess the risks of TF posed by all forms of legal persons and arrangements. Australia should also take measures to ensure that beneficial ownership information for legal persons is collected and available. Trustees should be required to hold and maintain information on the constituent elements of a trust, including the settlor and beneficiary

Overall, FATF says that Australian authorities have a good understanding of most of Australia's main money laundering (ML) risks ...

Overall, FATF says that Australian authorities have a good understanding of most of Australia's main money laundering (ML) risks, but need to develop their understanding further in certain areas. They coordinate very well activities to address key aspects of the ML/terrorist financing (TF) risks but some key risks remain unaddressed, and an underlying concern remains that the authorities are addressing predicate crime rather than ML. •••

Whistle blower highlights scale of bribery and corruption in procurement

Sylvain Mansotte was reviewing procurement processes when he uncovered a major fraud. His experience as a whistle-blower in the case was the genesis for a new business idea that could help whistle-blowers in the future and cut down corporate fraud. Daniel Sheehan met with Sylvain.

Organisations around the world lose an estimated five percent of their annual revenues to fraud, according to a survey of Certified Fraud Examiners (CFEs). Applied to the estimated 2014 Gross World Product, this figure translates to a potential total fraud loss of more than $3.7 trillion.

Much of this fraud is procurement fraud. According to PwC, procurement fraud is the second-most frequently reported form of economic crime, behind asset misappropriation. The PwC Global Economic Crime Survey 2014 showed 29 per cent of organisations had experienced procurement fraud, and it was most common at the vendor selection stage, followed by the bid process.

Fraudsec founder, Sylvain Mansotte, saw this type of fraud first-hand, when he was working at Leighton Contracting. Mansotte reported irregularities in the company's procurement records that led to unearthing of one of Australia's largest frauds.

When reviewing accommodation expenditure, Mansotte found a property, registered as an Australian business, had invoiced the construction firm $2 million in a single year. Mansotte found the property was linked to Leighton's Executive, Damian O'Carrigan. An investigation was subsequently launched and found O'Carrigan had been perpetrating fraud for more than a decade.

In 2000, O'Carrigan established a consultancy company, Acorn Cottage. O'Carrigan, as the Queensland finance manager, was able approve payments up to $5 million. He first billed Leighton Contractors $28,000 for consultancy services on 30 May 30 2000. Over the subsequent 12 years, he issued 308 invoices from Acorn Cottage to his employer, totalling more than $20.7 million.

The invoices, which O'Carrigan lodged fortnightly and sometimes weekly, ranged from $10,000 to $205,000 and he subsequently transferred the funds from an account registered to Acorn Cottage to a Commonwealth Bank account of his own.

While on the face of it, Mansotte should have been feted for his intervention, the reality was more complex. Like many whistle-blowers, he found the experience highly stressful. Mansotte was subsequently offered a new role in the risk and fraud department. "My job was to investigate and detect fraud and talk to whistle-blowers," he said.

> That is where FraudSec takes away the stress and delivers that message in a safe and secure way.

It was his own experience, and that of others, that led him to create Fraudsec. "If you think about my case at Leighton Contractors, they have over 400 projects going on at any time, so it is difficult to be across the detail of all of them. If you happen to see something illegal happening, you may want to report it and put a stop it, but if you say something, you want to be certain that no one is going to vilify or fire you.

"That is where FraudSec takes away the stress and delivers that message in a safe and secure way," Mansotte says.

Fraudsec is a cloud-based SaaS provider, assisting organisations to capture, track and manage fraud. Fraudsec allows anonymous messaging from the tipster to the organisation and two-way communication, whilst encrypting the data to maintain integrity.

Fraudsec claims that it puts the whistle-blower in the driving seat with real-time, anonymous two-way communication from any device. Whistle-blower reports fraud anonymously using a customised incident form available on all devices. Information submitted is encrypted using 256 Bit encryption, and the whistle-blower's IP address never leaks to the organisation. The organisation receives the incident form instantly and a two-way communication with the whistle-blower can then start.

Mansotte says whistle-blowers often know what is happening on the ground, but don't want to take the risk with, "a whistle-blower hotline or fill out a form on the intranet site that can be tracked by the company quite easily."

Mansotte says that the complete anonymity and the ability for two-way communication that can include not only text but →

files as well, are the key differences between his service and whistle-blowing hotlines.

"Enabling people from within the company to report anonymously is often one of the best ways to unearth it."

Mansotte says that fraud can be quite subtle; it does not have to be obvious. "Enabling people from within the company to report anonymously is often one of the best ways to unearth it."

"Fraud is only a focus, once you realise it is happening. Take the recent fraud in the IT department at CBA. Because that fraud occurred at CBA, all the major banks have launched internal reviews of their functions to make sure this type of fraud is not occurring in their business. But why wait for a problem to occur before empowering people?"

"You always think you are safe and your people are good and will do the right thing, but that just does not happen in real life."

Mansotte says the scary thing is that a lot of businesses will never know that fraud is even happening. "That is why enabling whistle-blowers to come forward is really important." •••

You always think you are safe and your people are good and will do the right thing, but that just does not happen in real life."

How procurement fraud occurs

- Failure to follow organisation's procurement policy and guidelines in awarding contracts to suppliers (e.g. bypassing thresholds by awarding contracts without a market tender process)
- Inappropriate or poor contracting, including inappropriate terms and conditions favourable to the supplier
- Collusion by an employee with an external vendor to defraud the employer (e.g. inflated contract prices, approving invoices for incomplete or substandard work). Employees may receive kick-backs, bribes or other incentives, or even be involved with the vendor in some capacity (e.g. as a consultant, director or shareholder)
- Establishment of a 'ghost' supplier or shell company to defraud through contracts, invoices and other payments
- Contract variations and increases to contract value made after contract commencement, and without market testing
- Inappropriate charges under cost-plus contracts, including cost/labour mischarging, defective parts and product substitution
- Falsification of documents, including fraudulent invoices.

Source: PwC

Companies underestimating corruption risk

Are multinational companies sleepwalking into compliance disasters?

A new survey has revealed that many companies, particularly those with operations in emerging markets, remain slow in changing their corporate approach towards corruption. The findings were contained in an annual survey of business attitudes to corruption, conducted by Control Risks, the global business risk consultancy.

The survey found a worrying disconnect between what the headquarters of large, multinational organisations believe about their anti-corruption programmes and the reality on the front line in higher-risk markets, such as China or Indonesia. The failure to reform internal practices is partly due to budgetary pressures on compliance teams, but many companies still underestimate the threat and the cost of getting it wrong. While they may have the right "tone from the top," the message often fails to reach those at the front line, who are then left to balance commercial targets with acting in a legal and ethical manner.

The message often fails to reach those at the front line, who are then left to balance commercial targets with acting in a legal and ethical manner.

In late February, Australian Federal Police (AFP) officers charged the directors of construction company, Lifese, with foreign bribery offences. Mamdouh and Ibrahim Elomar are accused of attempting to bribe Iraqi government officials to secure multi-million-dollar construction contracts in the country. While the case is only the second of its kind to reach Australian courts, the AFP has confirmed it is pursuing 14 active foreign bribery investigations.

"These charges serve as a reminder to companies that the AFP will investigate allegations of foreign bribery. Increased government funding has strengthened the AFP's ability to investigate suspect transactions and yet our survey shows only 39% of Australia/New Zealand companies were investing in additional resources to combat corruption," says Jason Rance, Managing Director Australia Pacific, Control Risks.

"An anti-corruption investigation against a company can threaten its very survival and impose significant cost, both financially, and to a company's reputation. More needs to be done by the companies to demonstrate compliance and protect themselves, their employees and shareholders. They need to look at practical measures, such as assessing corruption risk of a specific deal, potential partner or market entry strategy."

An anti-corruption investigation against a company can threaten its very survival and impose significant cost, both financially, and to a company's reputation.

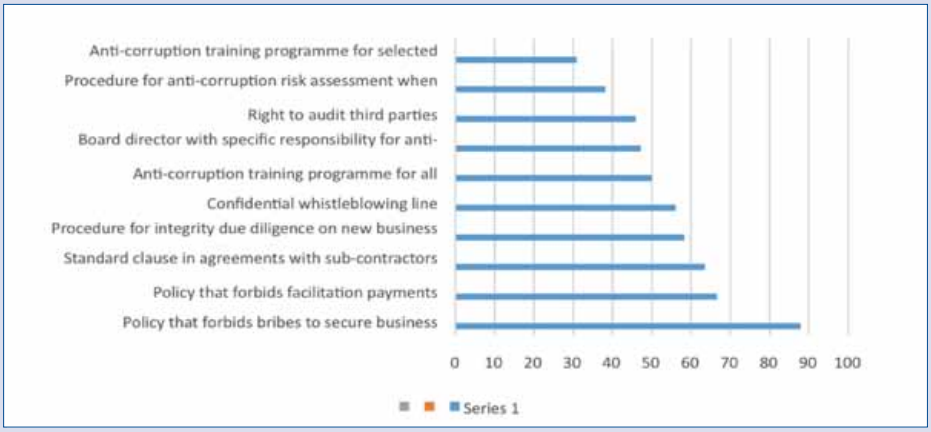
The global survey reveals there have been some improvements over the past 12 months, with 87.9% of companies having in place policies explicitly banning bribes to secure contracts. However, just under half still have no whistleblowing line, and a majority of the companies surveyed:

- Are ill-prepared to conduct anti-bribery investigations of employees
- Have no board-level responsibility for anti-corruption as an item on the risk agenda
- Are not providing anti-bribery and anti-corruption training programmes for those operating in high-risk functions, such as sales.

The survey reveals that among those companies surveyed:

- **47.5%** have board-level directors or compliance committees responsible for anti-corruption

Chart: how far companies had implemented the most important anti-corruption measures?



Source: Control Risks

- **46.4%** of companies in Australia and New Zealand carry out anti-corruption risk assessment procedures when entering new markets, compared with **38.2% globally**
- **64%** include a standard "no bribe" clause in sub-contractor contracts
- **58%** conducted integrity due diligence on potential new business partners
- **12.2 %** of Australian/New Zealand businesses feel that facilitation payments are essential to keep business going vs only 1.3% of businesses in the UK, but this figure rises to **27.5%** in India, **25.5%** in Mexico and **24.6%** in China
- **66%** ban "facilitation payments" to speed up government transactions – such as customs clearances
- **37.8%** would report a corrupt competitor to the police or to regulatory authorities.

In addition:

- **67.6%** do not believe they will have to conduct an anti-corruption investigation next year, in spite of the fact that 56.6% conducted one in 2013
- **44.7%** of respondents see no need for further investment in compliance.

"Governments across the world are demanding more of companies in the fight against corruption," says Jason Rance.

"This is true, even in markets where regulatory and law enforcement agencies are often under-resourced. Companies need to understand this change and take it seriously. Many companies now have the compliance processes in place, but this is only half the battle. Companies are getting better at talking the talk, but they need to walk the walk and introduce the real changes in culture and process." •••

What not to do

A large multinational in the media sector recognised the need to introduce a third party due diligence programme in order to ensure compliance with the "adequate procedures" required by the UK Bribery Act of 2010. Faced with over 2,000 agents and distributors in China alone, this was a daunting task, so the company decided that the completion and submission of self-disclosure forms would suffice as "due diligence." Questions included: "Have you ever paid a bribe to secure business?" and "Are any of your shareholders or directors public officials?" Unsurprisingly, nobody answered yes. Three years on, they have been the subject of a corruption probe in China relating to the activities of one of their agents.

Source: Control Risks, International Business Attitudes to Corruption

Quick Tips: Anti Corruption Framework

In short, companies need the following:

- Clear policies that are communicated effectively, both internally and externally. The message should be: "This company doesn't pay. There is no point in asking."
- Strategic leadership and "tone from the top," including a willingness to accept short term delays and commercial costs arising from refusal to pay larger, as well as smaller, bribes.
- Risk assessments that are concerned with attention-to-detail for high-risk areas, as well as broader country assessments. Companies need to ask how far specific business processes – especially the most time-sensitive ones – are exposed to demands for bribes.
- Training that includes practical strategies for resisting demands for small bribes if, as is often the case, these are part of trainees' everyday experiences. For example, a straight refusal – "this company doesn't pay" – may be sufficient. In other cases, the company or the individual may need to appeal to more senior officials. The recommended strategy needs to be relevant to the specific environment in which the trainees are working.
- To take responsibility for what third parties do on their behalf, and to act accordingly. Delegating the payment of small bribes to business intermediaries, such as customs brokers, is not the answer, as demonstrated by a series of FCPA enforcement cases.

Source: Control Risks, International Business Attitudes to Corruption

THE COST OF DATA BREACHERS

How costly is a data breach? A new report looks at the mounting cost of data breaches. **Daniel Sheehan**

The average total cost of a data breach for the companies is $3.5 million.

PRIVACY AND DATA PROTECTION HAVE shot to prominence in the risk and compliance profession in recent years. The much-publicised hacking attacks on Target, JP Morgan and Home Depot shocked consumers and business, with millions of personal details compromised.

The Target hack saw a CEO and Chief Information Officer forced to resign, and the firm estimated the breach cost them more than $150 million. The Target case was at the more extreme end of the data breach scale, but a recent report shows that the average cost of data breaches has been prohibitively high.

The IBM and Ponemon 'Cost of Data Breach Study: Global Study' found the average total cost of a data breach for the companies is $3.5 million. Or looking at it another way, the average cost paid for each lost or stolen record, containing sensitive and confidential information is $145.

The average cost of a data breach per Australian organisation is slightly less, but still $2.5 million, with the average breach involving 20,000 records in Australia.

Likelihood of breach

The likelihood that an organisation will have a data breach was also looked at in the report. Companies are far more likely to have a small data breach than a major breach. The research provides an analysis of the likelihood of one or more data breach occurrences in the next 24 months.

The chart on page 21 shows the probabilities of breach incidents involving a minimum of 10,000 to 100,000 compromised records. As can be seen, the likelihood of data breach steadily decreases as the size increases. While the likelihood of a data breach involving a minimum of 10,000 records is estimated at approximately 22 percent over a 24-month period, the chances of a data breach involving a 100,000 records is less than 1 percent.

Causes of data breaches differ between countries. Companies in the Middle East and in Germany were most likely to experience a malicious or criminal attack, followed by France and Japan. Companies in India were the most likely to experience a data breach caused by a system glitch or business process failure, and UK companies were more likely to have a breach caused by human error.

Malicious or criminal attacks are most often the cause of data breaches, globally. Forty-two percent of incidents involved a malicious or criminal attack, 30 percent concerned a negligent employee or contractor (human factor), and 29 percent involved system glitches that includes both IT and business process failures.

Malicious attacks are also more costly, when they do occur. Data breaches due to malicious or criminal attacks cost companies $159 per individual record compromised. This is significantly above the average of $145 per compromised record and the cost for breaches caused by system glitch and human factors ($126 and $117, respectively).

Responding to a Breach

The good news is that the damage can be limited, if you are prepared. A strong security framework results in the greatest decrease in the cost of data breach. Companies with a strong security framework at the time of the data breach reduced the average per record cost to $132 ($145–$14.14). Other factors that can mitigate the costs include having incident response planning and business continuity management plans in place and having a chief information officer with enterprise-wide responsibility.

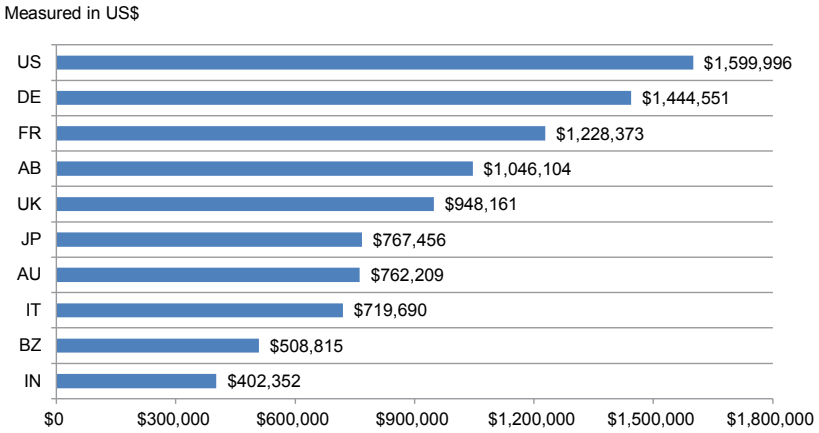
Advisory firm Deloitte says the results show that companies need to take their data and privacy responsibilities seriously.

"The way an organisation responds to a data breach has changed consumers' perception of privacy from one of simply trusting an organisation to keep data safe and secure, to one of being transparent, and letting the consumer know of any change in data use or a data breach," says Deloitte Partner, Tommy Viljoen.

"As individuals become more aware of how much personal data is captured through technology and

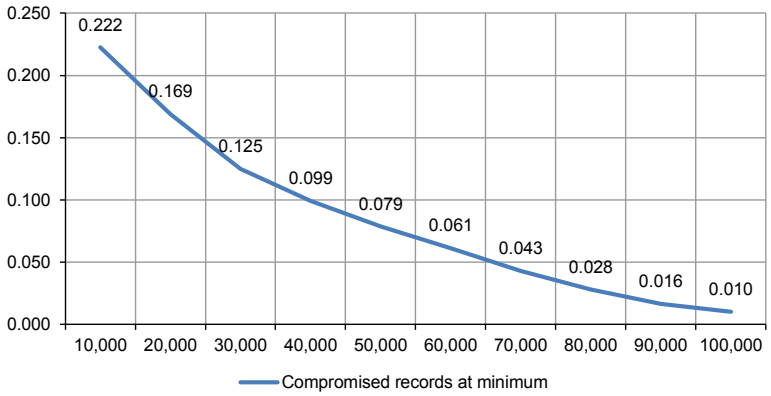
As individuals become more aware of how much personal data is captured through technology and connectivity, we are becoming increasingly sensitive as to how our information is being used and disclosed.

Figure 1: Average post data breach costs



Source: IBM and Ponemon 'Cost of Data Breach Study: Global Study'

Figure 2: Probability of a data breach involving a minimum of 10,000 to 100,000 records



Source: IBM and Ponemon 'Cost of Data Breach Study: Global Study'

connectivity, we are becoming increasingly sensitive as to how our information is being used and disclosed."

Gavin Cartwright, also from Deloitte, says culture is absolutely critical. "With great power comes great responsibility." He said: 'The Power' today comes from the volume of personal information being gleaned by organisations from users, both directly and indirectly. And 'The Responsibility' is an increased need and expectation from Australian consumers for transparency, security, ethical use and overall governance.

"It is critical that, as organisations derive benefit from personal information, the consumer is kept informed about the use and any changes to their data," Cartwright said. •••

OFFICE OF THE PRIVACY COMMISSIONER

Angelene Falk, Assistant Commissioner Regulation & Strategy

Australia's biggest ever privacy reform, the establishment of new Privacy Principles in March 2014, commenced just over 12-months ago. How has progress been in the first 12-months?

One of the key hallmarks has been engagement with business, the government and the community

PRIVACY COMPLIANCE IS OFTEN RANKED in the top 3 issues that risk and compliance professionals face. With the spread of technology, the globalisation of data and the threat over information security there is a number of privacy related risks facing business.

In Australia, professionals have also had to face law reform. It was in 2012, that the Federal Parliament passed a bill that changed the Privacy Act. From March 2014, there was one set of Privacy Principles, known as the Australian Privacy Principles. As part of these reforms, there is new credit reporting provisions and new enforcement powers for the Privacy Commissioner. The Privacy Reform process started in 2006, 18 years after the Privacy Act was first introduced in 1988. The bill includes changes to the Privacy Act recommended by Australian Law Reform Commission in 2008.

These new principles are called the Australian Privacy Principles (APPs) and are harmonised across government and business. They replaced the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs).

Under the changes, there is 13 new APPs, with the biggest changes being disclosure of personal information for direct marketing, and on cross-border disclosure of personal information.

GRC Professional spoke with Angelene Falk, Assistant Commissioner at the Privacy Commissioner about the progress made over the last 12-months.

We're just over twelve months into the privacy reforms in Australia. How are things progressing?

We spent 12 months preparing for and then implementing the law reform agenda. That has meant a big increase in the work coming into the Australian Information Commissioner's Office. One of the key hallmarks has been engagement with business, the government and the community. We have been working really closely with businesses. Business really does have diverse relationship with privacy. So, for example, the credit industry, direct marketers, the health sector, social media; they're all dealing with personal information and privacy issues, but all with

a slightly different perspective. Business engagement has really informed the guidance that we have developed for business.

Can you explain some of the guidance notes you have produced for business?

The OAIC produced guidelines to the Australian privacy principles, and guidelines on how to develop a privacy policy, how to conduct privacy impact assessments on business, how to secure personal information and deal with data breaches. All of those resources have, I think, provided a very good foundation for business to implement their reforms. Feedback from business is that it has been very helpful. Our approach has been to encourage voluntary compliance through the provision of guidance. That is really the basis of our regulatory approach. We want to help as much as possible. We want to make sure the guidance we produce takes account of business needs.

One of the key hallmarks has been engagement with business, the government and the community

Has the global business environment made things more difficult?

We're very much aware that personal information is moving around the world, and that each jurisdiction operates under a different framework. Whilst we need to be most cognisant of our local regulatory obligations, we want to ensure that what we're telling business is also something that will help them comply globally.

Are you satisfied with progress on compliance?

We know there is still room for improvement, which is why we want to emphasise the importance of privacy and governance structures. We want risk and compliance managers to have privacy issues as a key part of their 'business as usual' risk equation.

Our complaints statistics show there is room for improvement. Since the new laws commenced, we have had an increase in complaints made by

individuals, if you compare that to the previous 12 months. So, from March 2014 to March 2015, we had over 4,000 privacy complaints. So, that was a 43% increase over the same time for the previous year.

With everyone having 12 months now to bed down their processes, we have started to roll out a program of assessing compliance with the reforms. The Privacy Commissioner has looked at specific issues, particularly privacy policies. The whole rationale behind having a privacy policy is so individuals can exercise choice and control over how their personal information is being managed by business. Transparency is key. It's the way in which a business communicates and earns trust when it comes to the handling of people's personal information.

Recently, we released the results of our assessment of the online privacy policies of 20 Australian and international organisations– mainly across the business sector, but also some government websites.

While we found some very good examples of privacy policies, we found room for improvement. That is particularly true in terms of readability. A privacy policy should be a communication tool, not a risk management or legal tool. We found many of the policies were still too long, with the longest being 18,000 words. We would like business to make this information available in a simpler and more accessible way.

We are also encouraging cultural change by ensuring privacy is being imbedded through systems and processes in a 'daily' way.

Do you have a model for businesses to follow when producing a privacy policy?

There are certain things that have to be included. If it's a very simple business model, then it might be possible to convey that information succinctly. But even when there is greater complexity, we encourage businesses to take a layered approach to conveying messages. Start with the simple messages; if people then need more-detailed information, provide links to it.

What is driving the Privacy Commissioner's interest in culture?

key part of privacy compliance is having both leadership and by-in from-the-top to ensure privacy is a key part of the business. *Australian Privacy Principle One* does require all businesses to have processes, procedures and systems in place to make sure they can comply with the privacy principles. Key to guaranteeing that happens is to ensure you've got the resources, the leadership and also the accountability. It is not only about implementing those processes and procedures, it is about reviewing them and maintaining them over time.

What have been the enforcement priorities?

As part of the reforms, the Commissioner was given some new regulatory powers, and it was important we outlined how those powers would be exercised. We released a regulatory action policy that gives the Commissioner's approach to exercising his powers. We're encouraging voluntary compliance, we're issuing guidance and we're working with business to provide information and advice. As mentioned, we are also encouraging cultural change by ensuring privacy is being imbedded through systems and processes in a 'daily' way. But there are options, if other regulatory actions are required. Those options include enforceable undertakings, making a determination in a federal court, or in serious cases, we could seek a civil penalty through the Federal Court.

We have implemented a voluntary data breach notification scheme. Where a data breach has occurred through business, they can voluntarily report that to us, and we can provide advice and guidance on how they can deal with that data breach. When that has occurred, and the businesses has shown they are dealing with it appropriately, and they're taking remedial action to make sure the issue

is not repeated, then it may be that no further regulatory action is required.

However, if that's not the case, or if a serious breach comes to our attention through the media, then it's more likely the Commissioner might look at an investigation on his own. Included in the kind of things we consider before taking action is the number of individuals affected by the issue and the seriousness of the breach (e.g. does it relate to financial or health information?). We also look at what benefit would arise from further regulatory action.

In matters where the Commissioner has conducted investigations on his own initiative, a number were as a result of business not properly securing personal information. For Instance, the Pound Round matter is a case where a medical centre had medical reports kept in a garden shed at the back of an abandoned property, and the reports were found flying around at the back of that property. So, clearly, no proper steps were taken to secure sensitive health information.

How can a company avoid a data breach?

There's the obvious things like physical and information security. But it's really about having that holistic approach. What we sometimes see is where a lot of small things going wrong results in a big breach occurring – for example, where a small change to a technology solution inadvertently results in the information becoming accessible on the internet. It's about making sure the controls are in place, wherever personal information is being dealt with. Appropriate checks and balances must always occur.

Personal information is a business asset; as such, it needs to be protected and valued like any other business asset. The businesses that recognise that are more likely to put in place systems to manage and protect it. Unfortunately, the most common wake-up call to take privacy seriously is a big data breach. The $162 million loss from Target's 2013 data breach is a case in point, and it is worth remembering that this data breach also cost the CEO and the chief information officer their jobs. The cost of a data breach is much less when a business has in place a plan to deal with data breaches. So it comes back to those privacy governance structures – making sure there are the systems and processes in place.

The cost of a data breach is much less when a business has in place a plan to deal with data breaches.

An example in Australia is the investigation that the Commissioner opened into the Department of Immigration and Border Protection. The Department published a sensitive report online and within that report was embedded data that disclosed the personal information of around 10,000 asylum seekers. In that case, there was a failure of systems and processes. So, whilst the actual trigger for the disclosure may have been human error, in reality, it was the result of a failure of process.

What is the Privacy Commissioner's role in metadata initiatives?

A committee hearing process was held to review data retention laws, and the Privacy Commissioner appeared at that inquiry, as did representatives from the telecommunications industry. That legislation has now gone through. Telecommunication providers now have a period of time to develop implementation plans.

Telecommunication providers now have a period of time to develop implementation plans.

The OAIC has received some additional funding in this year's budget to make sure we can give the scheme the kind of privacy oversight that's required. Telecommunication providers already have an obligation to keep personal information secure. The fact that additional data sets are required, and that those data sets now need to be kept for a longer period of time, means that there should be increased oversight. •••

Beyond Risk

The risks that businesses and government face each day are constantly changing, and consistently complex. With a strengthened risk management strategy and framework in place, you can create a competitive edge.

With a sharp insight into the ever-changing risk landscape, KPMG will work with you to develop a strategy that does more than keep your business compliant and protected. By embedding an understanding of risk into the core of your organisation, you can be confident that the decisions you make and the conscious risks you take lead to fundamentally better results.

Ready to turn risk into an advantage? Talk to KPMG.

kpmg.com.au

KPMG

EMPLOYEE RIGHTS IN A SOCIAL MEDIA AGE

A recent case highlights dangers of social media and threatens to change the face of privacy laws in New Zealand. **Simon Lapthorne**

It is a confluence of all the modern points of public interest in employment: employee privacy and Facebook; damage to reputation; a significant sum of money; and a sense of scandal.

THE RECENT HUMAN RIGHTS REVIEW Tribunal (HRRT) decision in the case of Hammond v Credit Union Baywide has been the source of significant interest, not only for compliance professionals, lawyers and other relevant professional communities, but also for the New Zealand public.

It is easy to see why. It is a confluence of all the modern points of public interest in employment: employee privacy and Facebook; damage to reputation; a significant sum of money; and a sense of scandal.

The facts of the case are that Ms Hammond was employed as a mortgage broker with Credit Union Baywide (Baywide), located in the Hawke's Bay. Following her resignation, and while on gardening leave during her notice period, Ms Hammond held a private dinner party for a friend of hers, a Baywide employee who also had resigned. The party was attended by ten close personal friends, five of whom were current employees of Baywide.

Ms Hammond and her friend had become disillusioned with Baywide, particularly in relation to the circumstances of their departures. As an outlet for these frustrations, Ms Hammond baked a cake for her guests adorned with the words "NZCU F*** YOU" and the word "C***" along the side. The font used was that of Baywide's new branding.

The HRRT decision goes to some length to contextualise the cake, commenting that its reception was positive, being met with laughter, and even going as far to note that the cake was "delicious". Wanting to spread the "topical and hilarious" cake, Ms Hammond posted a photo of it on her Facebook page.

The privacy setting on Ms Hammond's Facebook page meant that only those accepted by her as "friends" had access to the photograph. At the time, there were approximately 150 such friends who could now see the cake.

Shortly after the party, the executive team at Baywide became aware of Ms Hammond's cake and the picture of it posted on her Facebook page. However, because of the privacy settings, they could not view the photograph. To get around this, Baywide's HR Manager, Ms Alexandra, required a junior employee to access Ms Hammond's Facebook page, against her will. Baywide then took a screenshot of the cake.

Outraged by the cake, Baywide telephoned at least four HR agencies in the Hawke's Bay area to "warn" them against employing Ms Hammond and the agencies were sent a copy of the screenshot. The CEO of Baywide also emailed staff about the cake, saying to them:

"I'm sure you'll agree that we do not want people at Baywide who behave in this manner, or do not align with our values or our organisational culture."

Ms Hammond had by then secured a new job at a company called Finance Point, with whom Baywide did business. Baywide called FinancePoint, informed them about the cake and told them that if they did not terminate Ms Hammond's employment, Baywide would cease supplying them with business. FinancePoint refused and that is exactly what

I'm sure you'll agree that we do not want people at Baywide who behave in this manner, or do not align with our values or our organisational culture.

How private is a written conversation initiated over the internet with 200 "friends", who can pass the information on to a limitless audience?

Baywide did. Feeling responsible, Ms Hammond resigned from her new job after only three weeks.

The legal issues

The HRRT stated in its judgment that, while this was the first occasion in which it had been required to consider the operation of the Privacy Act 1993 (Act) in the context of social media, particularly Facebook, application of the information privacy principles in the Act was a straightforward exercise. It further considered that it was deciding a privacy case with employment law implications – rather than the other way around.

The key issues were:

(a) whether the collection of the screenshot by Baywide was for a "lawful purpose", including the need to protect its commercial reputation and to address potential misconduct by an employee.

(b) whether there was a breach of Principle 11 of the Act, which prevents an agency holding personal information from disseminating that information other than in exceptional circumstances.

Findings

The HRRT did not support Baywide's claim in regards to the first issue, finding that commercial considerations and potential misconduct related to the employment relationship were not within the purview of the Act granting its jurisdiction.

In terms of the second issue, Baywide conceded that it had breached Principle 11 by:

(a) contacting recruitment agents; and

(b) emailing staff about Ms Hammond's resignation.

However, Baywide denied it had breached Principle 11 by contacting FinancePoint and argued that FinancePoint had already seen the cake, prior to being sent a copy of a photo of it.

The HRRT did not accept this argument, and found the exceptions in Principle 11 do not include circumstances where the information disclosed is already known to the recipient. Instead, the HRRT considered that the focus of Principle 11 is on the disclosure itself, not on what may or may not already be known by the recipient.

Remedies

The HRRT was scathing about Baywide's active intent to damage Ms Hammond's reputation and her ability to find new work. The HRRT accepted that Ms Hammond was humiliated, and suffered considerable stress and anxiety as a result of Baywide's actions. It ignored Ms Hammond's contributory conduct, and her duty of fidelity to Baywide when loading the photograph to her Facebook page.

Looking at the facts as a whole, the HRRT found that an appropriate sum to adequately compensate Ms Hammond for the severe humiliation, severe loss of dignity and severe injury to feelings inflicted was $98,000. It also made orders relating to loss of earnings, loss of a benefit and legal costs – totalling $168,000 in damages. Prior to that, the previous highest award had been $40,000.

In view of the extraordinary circumstances of the case, the HRRT also made orders restraining Baywide from continuing or repeating any such breaches, and requiring it to send each recruitment agent a retraction along with a copy of the HRRT's decision, asking them to delete the screenshot.

Implications – Privacy

Clearly, the case has significant implications for privacy law in New Zealand. It indicates that privacy breaches will be taken seriously, but it also creates confusion as to when and how. This is because there have been previous comments in cases that appear contradictory. For example in the case of Hook v Stream Group, the Employment Court stated:

"How private is a written conversation initiated over the internet with 200 "friends", who can pass the information on to a limitless audience?" "Facebook posts have a permanence and potential audience that casual conversations around the water cooler at work or an after-hours social gathering do not."

Hammond, on the other hand, seems to imply a reasonable expectation of privacy with regard to comments made on Facebook – although the HRRT attempted to distance its decision from being about Facebook directly. It does seem that these two decisions reflect a far wider tension between public and private, with people's lives being publicised (mostly by them) in an unprecedented way, and we predict this will increasingly be a point of contention in law and compliance.

Damages

The case sets a very high benchmark for damages, and might signal to an aggrieved employee that there is a more lucrative avenue for recourse than following the traditional route of the Employment

Relations Authority. The award of $168,000 in damages by the HRRT was promptly followed by another award of damages by the HRRT of $45,000 in a racial discrimination case.

In contrast with compensation awarded in the Employment Relations Authority – which averages in the range of $5,000-$10,000 in regards to hurt and humiliation (which made up $98,000 of the award in Hammond) – awards are substantially higher in the HRRT.

Obviously, this relates in part to differences in the cases and the fact that Ms Hammond waited nearly two years for her award. There are also additional stages before an individual can attain any success in the HRRT – for privacy complaints for example, the Privacy Commissioner has to undertake a full investigation in the first instance.

The difference in levels of awards does, however, pose an interesting question as to whether a new path is emerging for aggrieved employees.

The relationship between employer and employee

There are also features of this case of significance to the employer/employee relationship.

The case reinforces a David and Goliath dynamic in the employer/employee relationship in most circumstances, but provides in particular that enforcement of discipline is limited to the confines of current employment.

Ms Hammond's conduct was ignored by the HRRT in determining damages and the clear implication is that Baywide overreacted to the cake in an extreme way.

The case raises interesting questions: did Baywide feel Ms Hammond's actions were subordinate? Was there a personal element – media reports suggested Ms Alexandra, the HR Manager, was let go shortly after – or was it a difference in humour, the language perhaps? One cannot imagine such a reaction to a cake proclaiming "NZCU sucks".

The case reinforces a David and Goliath dynamic in the employer/employee relationship in most circumstances, but provides in particular that enforcement of discipline is limited to the confine of current employment. There is an air of personal reprimand to making the CEO retract his comments to staff and recruiters, as the HRRT did. It serves as a clear reminder that employers need to deal with issues discretely and manage any personal or moral outrage at all times.

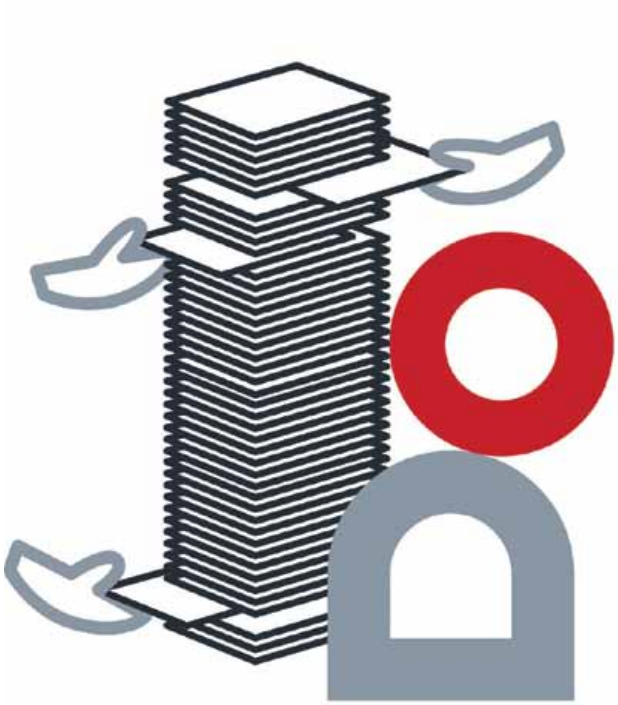
The Hammond case has created quite the buzz, and with good reason, as the implications are extensive. It will be interesting to keep track of these as they permeate cases to follow. •••

BoardPad

Worried about your board documents being leaked?

BoardPad safeguards and controls distribution

Your problem...



Our solution!

Contact us today for a demonstration

ICSA Boardroom Apps,
Level 33, 264 George Street, Sydney
+61 2 8096 8300 info@boardpad.com boardpad.com

A software company of the Institute of Chartered Secretaries and Administrators

Securely delivering digital papers across many devices

SOCIAL MEDIA – IS IT WORTH THE RISK?

Social media continues to plague institutions and its employees. Do your staff know the risks? **Daniel Sheehan**

The case is a stark reminder that employee social media use can be a risk for organisations.

Australian broadcaster SBS has become embroiled in a complex and potentially legal dispute after firing one of its employees for his social media use. Journalist Scott McIntyre is suing the broadcaster for discrimination, after it dismissed him for expressing controversial views about ANZAC Day on Twitter.

The case has been lodged with the Fair Work Commission, claiming SBS breached its policies and did not follow due process when it sacked the soccer reporter. The case is a stark reminder that employee social media use can be a risk for organisations. If employees are permitted to use social media, their use should be governed by a strict code of conduct to ward off potential legal challenges and reduce the chance of being exposed to reputational risk.

The legal case will be an interesting test case for organisations and social media. In the case, McIntyre was sacked after tweeting on ANZAC Day that, "'brave' ANZACs in Egypt, Palestine and Japan," were involved in, "summary execution, widespread rape and theft."

Other tweets said, "Not forgetting that the largest single-day terrorist attacks in history were committed by this nation & their allies in Hiroshima & Nagasaki," and, "the cultification of an imperialist invasion of a foreign nation that Australia had no quarrel with is against all ideals of modern society."

Communications Minister, Malcolm Turnbull, said the tweets were, "despicable."

Law firm, Maurice Blackburn, said the case was not about whether McIntyre's views were correct, but whether they represented a political opinion for which he should not have been sacked.

"The Fair Work Act protects employees from adverse action by their employer (including sacking), if they express political opinion," Maurice Blackburn said, in a statement.

"It is alleged SBS took action without a proper investigation and consideration of all relevant issues.

"It will be contended that Mr McIntyre had an unblemished work record and, if a proper process had been followed, he would still be employed in his chosen career."

McIntyre is not the only person to fall foul of bosses for social media use. There have been numerous recent cases of a similar nature. The management of social media risk does not stop at a review of social media controlled by the organisation, but must also include external, publicly-available information and commentary relating to organisations across social media. That includes employees using social media for their own personal use.

Social media has become a key reputational risk issue for many organisations. Yet as these cases highlight, many organisations and their employees do not truly understand those risks. •••

Quick Tips: Managing social media

KPMG's social media risk tips:

- Have processes in place to identify emerging or current social media risks facing the organisation, including lack of governance framework, and a formal review of current external-facing social media assets operated by the organisation;
- Ensure policies and procedures are put in place in order to appropriately manage ongoing social media risk;
- Understand the various impacts that social media can have on the organisation, not just from a brand and reputation perspective, but broader risk categories;
- Consider creating an enterprise-wide 'social media steering committee' that contains various areas of the business, including risk, legal and HR – to consider the various risk controls and concerns from social media; and
- Ensure the procedure for social media risk management has been considered as part of the ERM framework – perhaps including it in the annual Internal Audit plan.

SKILL SHORTAGES DRIVE DEMAND FOR RISK AND COMPLIANCE STAFF

The shortage is really being driven by demands from the regulators. There are a large number of regulatory change projects currently underway.

Is there a skill shortage of adequately-qualified risk and compliance staff? **Daniel Sheehan**

NEW REGULATIONS AND HEIGHTENED regulatory oversight are driving a surge in hiring of risk and compliance staff in financial services institutions and other highly-regulated industries. Those with backgrounds in anti-money laundering and commercially-savvy compliance managers are particularly sought after.

Harriet Tommany-Hall is a risk and compliance expert at executive search firm, Heath and Ford. She says there is a real shortage in qualified AML and financial crime staff. With FATCA compliance, new CDD rules from AUSTRAC and increased focus on sanctions compliance, AML departments of banks are some of the most overworked areas in risk and compliance.

The lack of qualified staff is making compliance in these areas more difficult and exposing their organisations and the financial system to greater risk.

Tommany-Hall also said there is demand for first-line risk managers, particularly those not from an audit background. Another area in demand is commercial, business-facing compliance managers.

"The shortage is really being driven by demands from the regulators. There are a large number of regulatory change projects currently underway."

"In insurance and wealth management, APRA's CPS220 is a big driver in the risk space that surrounds the independence of risk within insurance entities. CPS220 demands a clear reporting line for risk management, thus ensuring risk does not report through a CFO or a General Counsel. Risk needs a clear reporting line into the board."

This has meant a lot re-structuring and hiring in insurance. "CPS220 is now in force, but companies are still re-structuring and re-organising. Some of the bigger players are doing that more successfully, while some of the smaller and mid-sized players are having more difficulty. APRA is not going to leave them alone – this is a big focus for APRA – so it is the hiring and re-structuring work that has to be done."

The regulatory breaches in financial advice are driving hiring trends at the banks.

"On the wealth management side, something that has been a big focus in the last year is financial advice," Tommany-Hall says. "ASIC's enforceable undertakings and other regulatory actions are driving hiring in the wealth management area of the big banks. ASIC is really putting a lot of pressure on companies to ramp up their advice compliance function."

Ironically, by focusing scarce qualified risk and compliance staff on regulatory change and not 'business as usual' risk work, regulators may be actually increasing, not decreasing, risks within organisations.

There is also a disconnect between the →

skills needed to implement many of the regulatory change programs, and the skills the business needs on an ongoing basis. Once organisations build their new compliance programs to comply with heightened regulatory expectations, they will then need to find a way to sustain them over time efficiently. That is why risk and compliance needs to show real value to the business, beyond regulatory engagement.

"The most common failing we see in candidates are compliance professionals who are quite driven by the rule book. The main thing we see time and time again is a failure in their commercial interaction and being commercial with the business," Tommany-Hall says.

"There is a real difference in what the regulator says and what the commercial reality is. A key point to remember is that it is the business that pays the salary, not the regulator. Companies are needing and demanding more than black-letter-law-style compliance professionals."

The shortage is not driving salaries significantly higher, yet. "In terms of salaries, a year or so ago there was a definite dip. For example, a lot of the big banks were struggling to get sign-off for salaries over $150,000. So $150,000 was becoming quite a senior hire. More recently, it has stabilised, but we are still not seeing those really high salaries of three or four years ago."

There is a real difference in what the regulator says and what the commercial reality is. A key point to remember is that it is the business that pays the salary, not the regulator. Companies are needing and demanding more than black-letter-law-style compliance professionals.

Tommany-Hall also said the good news is that organisations are increasing their awareness of the importance of the risk function and that has been another factor in hiring and salary trends. That can only be a good thing for the long-term health of the profession, particularly if you happen to be in the job market. •••

RSA ARCHER GRC DEALS YOU THE WINNING HAND

RSA is proud to announce that we have been positioned by Gartner as a leader in four Magic Quadrants related to GRC. The Leader designation was given to RSA based on demonstrated ability to execute and completeness of vision.

See what the analysts say in the online reports:

- IT Vendor Risk Management
- Business Continuity Management Planning Software
- Operational Risk Management
- IT Risk Management

Visit RSA Archer | RSA APJ Twitter | RSA APJ Facebook | Contact Us

RSA

IN BRIEF

Global banks fined nearly $6 billion

Six global banks were fined nearly $6 billion in May as part of another settlement in a global probe into the $5 trillion-a-day market.

Citigroup, JPMorgan, Barclays, UBS and Royal Bank of Scotland were accused by U.S. and UK regulators of cheating clients to boost their own profits using invitation-only chat rooms and coded language to coordinate their trades. Bank of America Corp was also fined but avoided a guilty finding.

"The penalty all these banks will now pay is fitting, considering the long-running and egregious nature of their anticompetitive conduct," said U.S. Attorney General Loretta Lynch.

In total, authorities in the United States and Europe have fined seven banks over $10 billion for failing to stop traders from trying to manipulate foreign exchange rates, which are used daily by millions of people from trillion-dollar investment houses to tourists buying foreign currencies on vacation.

ASIC warns on property bubble

ASIC chairman Greg Medcraft has warned of a property bubble in Australia. It is the first time that ASIC has issued such a direct warning over Australian property prices.

"History shows that people don't know when they are in a bubble until it's over," Medcraft told the AFR.

Medcraft said is "quite worried" about Sydney and Melbourne prices, saying that with the current house price to average income ratio at an all-time high and rates at an all time low, risk was rising for buyers.

He said that while rates are at historic lows, they won't stay there and he cautioned borrowers who are taking on too much debt which they won't be able to afford once rates start to rise again.

NAB appoints professor to look at customer complaints

The Sydney Morning Herald has reported that National Australia Bank will provide aggrieved customers with access to a highly-respected law professor to shepherd their complaints through the bank. The paper also reported that NAB paid $14.5 million over the past five years to more than 750 customers who got bad advice from its wealth division. Dimity Kingsford Smith, from the University of NSW, has been named as NAB's "independent customer advocate".

BHP caught in FCPA probe

The Securities and Exchange Commission (SEC) has charged BHP Billiton with violating the Foreign Corrupt Practices Act (FCPA) when it sponsored the attendance of foreign government officials at the Summer Olympics.

BHP Billiton agreed to pay a $25 million penalty to settle the SEC's charges.

An SEC investigation found that BHP Billiton failed to devise and maintain sufficient internal controls over its global hospitality program connected to the company's sponsorship of the 2008 Summer Olympic Games in Beijing.

BHP Billiton invited 176 government officials and employees of state-owned enterprises to attend the Games at the company's expense, and ultimately paid for 60 such guests as well as some spouses and others who attended along with them. Sponsored guests were primarily from countries in Africa and Asia, and they enjoyed three- and four-day hospitality packages that included event tickets, luxury hotel accommodations, and sightseeing excursions valued at $12,000 to $16,000 per package.

"BHP Billiton footed the bill for foreign government officials to attend the Olympics while they were in a position to help the company with its business or regulatory endeavors," said Andrew Ceresney, Director of the SEC's Division of Enforcement. "BHP Billiton recognised that inviting government officials to the Olympics created a heightened risk of violating anti-corruption laws, yet the company failed to implement sufficient internal controls to address that heightened risk.

Largest fine in AUSTRAC's history

AUSTRAC has issued a record fine to one of the world's largest remittance network providers for systemic contraventions of Australia's anti-money laundering and counter-terrorism financing (AML/CTF) laws.

MoneyGram Payment Systems paid a $336,600 infringement notice for providing money remittance services through unregistered remittance businesses. This follows a fine to MoneyGram of $122,400 in January 2015 for the same type of contraventions, bringing the total to almost half a million dollars.

Both infringement notices arose from an AUSTRAC compliance assessment in 2014.

THANK YOU TO OUR MEMBERS

You've been generous in your support of the GRC Institute

Thanks to your continued membership and participation in our activities, we've had a busy year and have, we hope, returned the benefits to you ten-fold.

- This year has seen the completion of the project to take the Compliance Standard from an Australian Standard to an International Standard, which was an initiative sponsored, driven and steered by the GRC Institute for the benefit of our members and to ensure we place them ahead of the game.
- Increasing the production of our magazine, GRC Professional, from quarterly to monthly, making the content more timely and relevant and by changing to electronic format, allowing members to collate and utilise the magazine in more practical ways.
- Through our strategic international partnerships with other similarly focused associations we have been able to build the recognition of the GRC Institute qualifications internationally, supporting those members who have put in the time and effort to become qualified and develop themselves professionally.
- The GRC Institute has also passed its own audit as a Registered Training Organisation, ensuring the continued delivery of our unique courses as nationally and internationally recognised qualifications.

We would now like to invite you to renew your membership for the coming year and help us build on our continued successes, to keep the benefits coming back to our members and support you in your career goals.

You should have already received an invitation to renew via email and in the post is a letter to you to assist you with renewing as well. Options for renewal will depend on the type of membership you currently hold, so have a look at the instructions we send you and please let us know if you have any questions or would just like to action this with one of our staff members.

Accredited members should especially make sure they follow up on their membership renewal as the currency of your accreditation is dependent on maintaining membership and your CPD.

Once again, thank you so much for your continued commitment to both the GRC Institute and your career. We hope that we can continue to support you in the coming years but the only way we can ensure we remain relevant is to listen to you - so let us know if there are activities, resources or courses you think we should be delivering!

GRCI SUMMIT SERIES
NEW ZEALAND

The GRC2015 Summit Series moves to New Zealand in June. **The GRC2015 Summit Series** are leading international events for governance, risk and compliance (GRC) professionals, with Auckland event on June 10 designed specifically for New Zealand practitioners. The event gives delegates the opportunity to hear and learn from experts in the GRC field, including senior practitioners and regulators from New Zealand.

The full day program will give you the tools to keep improving your compliance and risk programs and end with a networking function.

SPEAKERS AND TOPICS

Opening Address & GRC Awards Presentation
Hon Paul Goldsmith, *Minister for Commerce and Consumer Affairs*

How to evaluate an effective risk culture
Celia Pankhurst, *Manager of Supervision, Financial Markets Authority*

Liam Jones, Outreach & Engagement Manager, *National Cyber Policy Office*

Turning conduct to your advantage: Marketing Strategies
Rajesh Megchiani, *Director, KPMG*

The integration of GRC Frameworks with Internal Audit to improve Business Continuity
Helen Marsden, *Chief Risk Manager, Unison Networks*

Risk Management on a Shoestring
Sarah Litltejohn, *Group Risk Manager, New Zealand Post*

The Great New Zealand Bake-Off. NZCU Baywide v Hammond. How to make sure social media risks don't cost you the big bickies
Simon Lapthorne, *Senior Associate Simpson Grierson*
Sarah Auvaa, *Head of Group Compliance, Spark*

Managing a changing regulatory environment
Sue Brown, *DLA Piper*

Employing risk management to achieve strategic business objectives
Nigel Toms, *Corporate Risk Manager, Watercare*

Update on New Zealand's Workplace Safety reforms
Bryce Fleury, *Manager Sector Engagement, Worksafe New Zealand Limited*

2015 GRC

CONFERENCE

28–30 OCT 2015 • MELBOURNE
CROWN CONFERENCE CENTRE

CHANGE CATALYST

CONFIRMED SPEAKERS

General David Morrison AO
Chief of the Australian Army

Paul Jevtovic
CEO, AUSTRAC

Michael Rasmussen
The GRC Pundit

Matina Jewell
Former UN Peacekeeper and a driver for policy change at the United Nations

Dr. Bronwyn Evans
Chief Executive Officer, Standards Australia

Sharon Zealey
Chief Ethics & Compliance Officer
Coca Cola Company

GRC INSTITUTE
GOVERNANCE • RISK • COMPLIANCE

Ten Integrated Modules

Choose one, or more. You decide.

Corporate Governance

Align your activities to achieve your strategic and operational objectives

Health & Safety

Provide employees with a safe and healthy working environment to help meet your legal OHS obligations

Risk Management

Identify, assess, control and manage potential impacts to your organisation

Environmental Management

Minimise your environmental liabilities and maximise your resources to help reduce your environmental impact

Compliance

Meet your regulatory and internal obligations to help achieve legal compliance

Audit Management

Develop, conduct and manage audits to evaluate current performance to achieve compliance

Business Continuity

Scope, plan and prepare for potential disasters or business interruptions

Claims Management

Manage workers compensation claims with advanced claims and case management processes

Incident Management

Log and manage incidents through to resolution to help prevent recurrence

Risk Analytics

Turn data into information to provide a real-time view of organisational performance

Try it today: www.riskcloud.net/tryit

riskcloud.net™
Risk Management on the Cloud

powered by riskware.com.au
Enterprise Risk Intelligence Software
Be Risk Aware