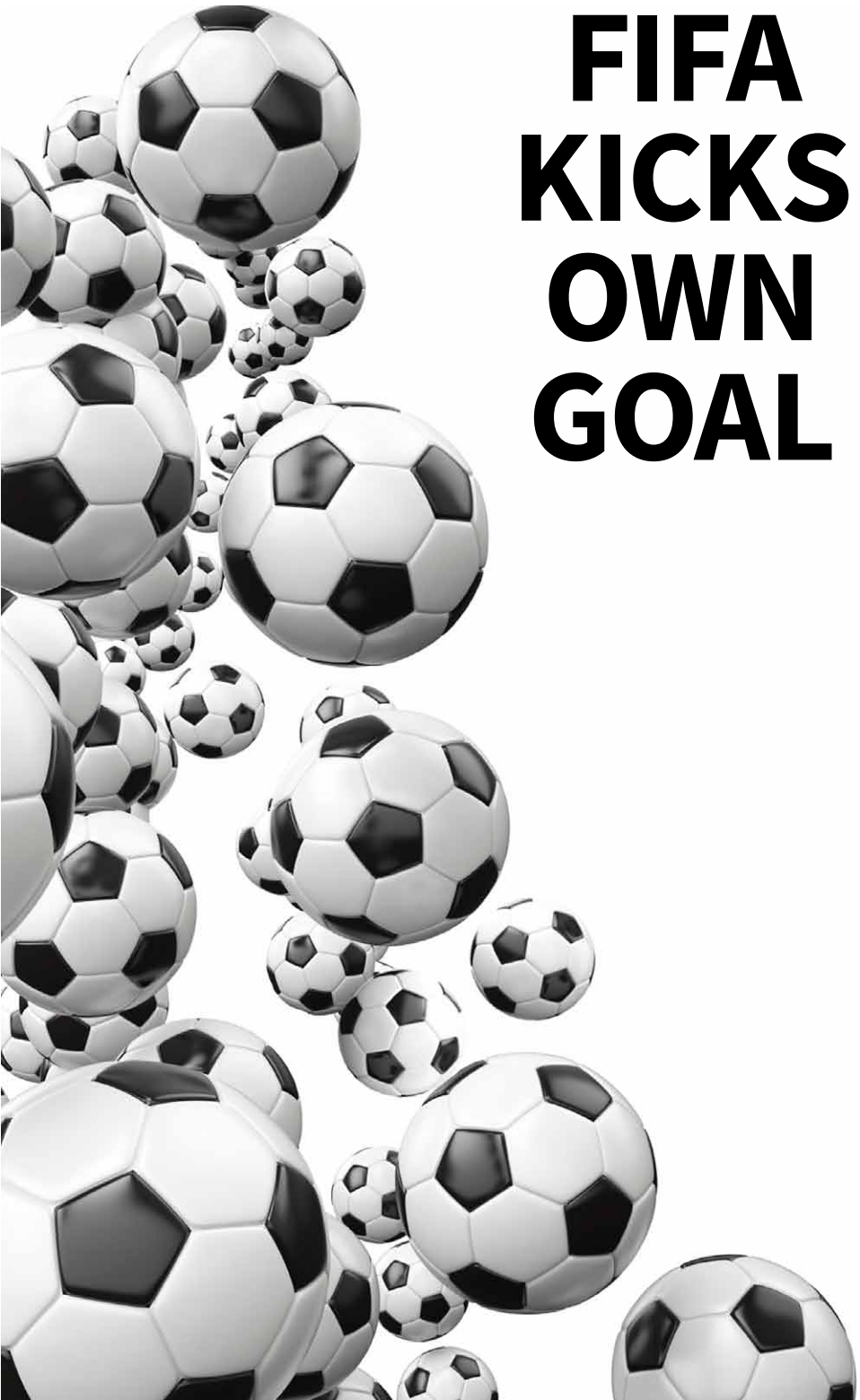
GRC PROFESSIONAL
GOVERNANCE • RISK • COMPLIANCE

JUNE 2015 | THE OFFICIAL MAGAZINE OF THE GRC INSTITUTE



FIFA KICKS OWN GOAL

MORE CLOUT FOR CCOS
CCO standing is on the up

DATA TROVES IN PERIL
Push to mandate reporting

RISK ROUNDTABLE
Experts speak their mind

ELEPHANTS AT LARGE
ERM in the public sector

CLIMATE CONFUSION
What future returns?

DESIGN ON CRIME
Spotlight on security

FINANCIAL CRIMES
ASIC talks tough on banks

GRC INSTITUTE
GOVERNANCE • RISK • COMPLIANCE

www.curasoftware.com

CURA

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

COVER STORY 12

FIFA red carded for corruption

In what has been dubbed the "World Cup of fraud", FIFA is starting to unravel as the FBI alleges "generations of bribery and corruption".

Contact us

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

GRC Institute

GRC Professional

Editor:
Mark Phillips
+61 2 8245 0704
Mark.Phillips@thegrcinstitute.org

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

FIFA blighted by bribery

News that the US Department of Justice had begun corruption and bribery investigations into FIFA would be no surprise to those who have been watching soccer's world governing body for some time. The surprising element is the sheer magnitude of the scandal.

As more and more details emerge, it appears money used to secure host status for numerous World Cups has then been directed to other affairs, including possible election of a national government. There is a long way to run on this story yet, but it currently looks as though FIFA has kicked the ultimate own goal.

In this edition of *GRC Professional* we also feature a story on the practice of risk management in the public sector. In it, we examine some of the factors unique to GRC professionals operating within government departments or agencies. This is a new focus for the GRC Institute. While we have always had members in the sector, we will be launching a new public sector discussion group as well as a one day pre-conference workshop dedicated to public sector GRC professionals.

Also, as the property market heats up in our region, so too do issues around the level of foreign investment and the amount of funds being moved in and out of countries and financial institutions. In this edition, we take some time examining concerns that property is not only being used as a means to launder money, but also what controls can be put in place to ensure organisations do not unwittingly become part of the money laundering pipeline.

Finally, I would like to take this opportunity to welcome on board our new editor Mark Phillips. Those who have been in the GRC profession for a number of years would remember that Mark did a stint with *Risk Management Magazine* before heading overseas for a number of years. He has now returned to Australia as our editor, and I am sure you will join me in wishing him every success in his new role.

Martin Tolar CCP, Managing Director, GRCI

As the property market heats up in our region, so too do issues around the level of foreign investment and the amount of funds being moved in and out of countries and financial institutions.

READER POLL

BYODs

THIS MONTH *GRC MAGAZINE* IS asking whether your firm has a strict policy on bring-your-own devices (BYODs) into the workplace.

If left unmanaged personal phones and tablets can open a Pandora's Box of risks for any organisation, particularly with regards loss of critical corporate information. How are you dealing with the issue?

- Does your organisation allow BYODs into the workplace?
- If so, does it have a solid BYOD policy document and insist employees sign it?
- Does your company continually update employees about emerging threats in mobile communications which, if unchecked, could compromise the data stored on BYODs?

Complete the survey here.

Results will be published in the July edition of GRC Professional.

LAST MONTH'S POLL

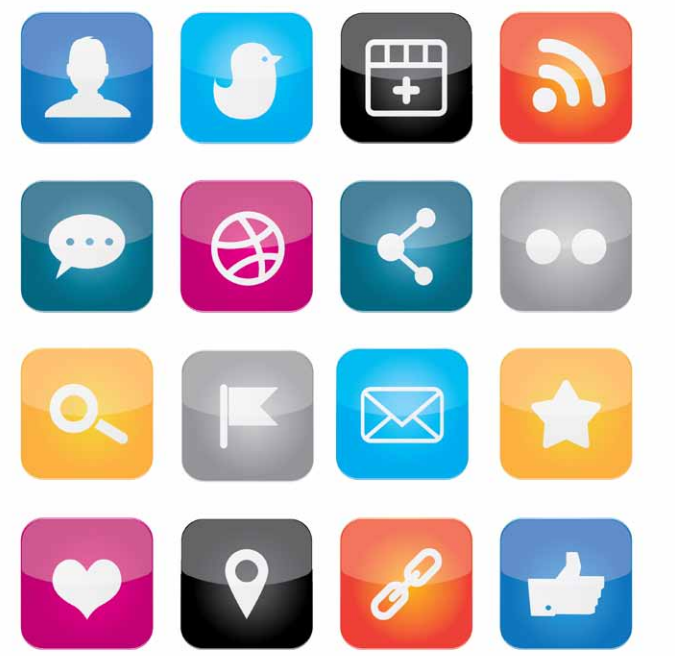
Social media

SOCIAL MEDIA HAS GIVEN NEW meaning to "the power of one", and because of it, all organisations are faced with either a new potential threat to their reputation or a great opportunity through which satisfied employees can become de facto ambassadors for their company.

Last month we asked whether your organisation uses social media proactively; whether the risk function monitors social media activity; if employees are educated on the risks; and whether there is a social media policy in place.

The results were mixed, with roughly half of respondents saying their firms do, in fact, keep close tabs on all aspects of the medium relevant to the organisation. On the downside, some professionals said a formal policy on its use does not exist, while the majority said education was "patchy". Most, however, believed their organisation was becoming more proactive in the use of social media.

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:

- SINKING INHERITANCES
- MILFORD SETTLES WITH FMA FOR NZ$1.5 MILLION
- SCHOOLS CAUGHT IN GET-RICH-QUICK SCHEME
- FIFA WHISTLEBLOWER ADMITS BRIBES IN WORLD CUP CHOICES

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

Banks face Catch-22 on AML

Delegates at the recent Association of Certified Anti-Money Laundering Specialists (ACAMS) European conference in London have slammed a lack of regulatory guidance with regards how banks are supposed to continue serving companies in high-risk countries.

While regulatorzs have been ramping up warnings on the wholesale consequences of de-risking, banks have been requesting clearer and more specific guidance on anti-money laundering (AML) and counter-terrorism financing (CTF).

"It is particularly worrying when the risks of non-compliance are so high," said HSBC head of financial intelligence unit for Europe, Danny Sanhye.

"There is a perception now from regulators of intolerance, that [AML] breaches are unacceptable, which has triggered a reaction from financial institutions, which is called de-risking. This is not a good thing, because we are not helping to fight money laundering."

Sanhye maintained that the withdrawal of banking services from certain sectors or regions would only create more avenues for criminal activity.

LexisNexis Risk Solutions AML global director, Chrisol Correia, agreed, warning: "In one way de-risking is seen as a means to eliminate the risks of AML compliance, but at the same time it may increase the risks of AML by driving it underground."

The UK's Financial Conduct Authority recently advised banks that in its view appropriate AML due diligence need not result in wholesale de-risking. However, even though banks have substantially increased spending on AML/CTF compliance, they are still struggling to cope with extensive know your customer (KYC) rules.

Correia reflected the view of many when he said the debate "doesn't seem to be resolvable".

ACAMS executive vice-president John Byrne conceded there doesn't seem to be an easy solution.

"In general, all of us want to see financial inclusion and help economies, but, on the other hand, financial institutions are pushed against the wall," he observed. "I don't get the sense that the regulators have been part of the conversation, but I think they have to be in order to try to solve this."

Terror risk rise for Western economies

Nine Western economies are now exposed to rising risk levels as a result of an increased terror threat, according to AON's Terrorism and Political Risk Map, compiled in partnership with The Risk Advisory Group.

The map shows that Australia, Canada, Belgium, Denmark, France, Germany, Norway, Ireland and Estonia are at higher risk. In addition to terrorism, top risks for business include a progressively uncertain and dangerous geopolitical environment, where the risk of armed conflict is growing amid changing and unstable regional balances of power.

"The data highlights that terrorism and geopolitical uncertainty are risks that businesses cannot ignore, and that they are as relevant to developed economies as to emerging markets," says The Risk Advisory Group head of intelligence and analysis, Henry Wilkinson.

"In a hyper-connected world, faraway problems can affect local threats and political violence can spread rapidly with little warning. However, a high level of risk doesn't automatically mean that these areas are closed for business. Companies can exploit the opportunities in any market with high quality intelligence and analysis, and a strategy to navigate and manage the risks."

The map shows a mixed picture, with a net reduction on country risk ratings worldwide, but with political violence and terrorism risks concentrating and intensifying around a smaller number of countries. The risk rating was reduced in 21 countries and increased in just 13.

The global picture is also one of marked polarity, with clusters of concentrated risk across South Asia, North Africa and the Middle East. Europe is at significantly greater risk from the rise of Islamic State.

Compliance candidates in demand in Singapore

Compliance professionals in Singapore are in continued demand, according to the Robert Walters "Global Salary Survey 2015".

The compliance recruitment market remained stable in 2014, with professionals experienced in anti-money laundering, advisory and financial crime especially sought after at management level.

A tightening of regulatory standards in the city state has also ensured that compliance remains high on companies' recruitment agendas, with firms taking a greater interest in eligible and capable domestic talent. The trend is expected to continue throughout the remainder of 2015.

However, because of the nature of the Singaporean sector – the need to liaise with key officials before advising a firm of regulatory change – there is an onus on local regulatory experience. A shortage in the area means employers are prepared to pay a premium to secure the right talent, with strong compliance candidates commanding an average increment of 20-30 per cent on a base salary.

The average per annum salary of a compliance analyst in Singapore is SG$50-90k, rising to SG$90-180k at management level.

War for talent heats up in APAC

Companies across the Asia Pacific (APAC) are finding it harder to recruit and retain qualified compliance professionals as would-be job applicants increasingly scrutinise organisations' ethical standards and their ability to proactively use technology to prevent and detect fraud, bribery and corruption.

According to new research from Ernst & Young (EY), eight out of 10 respondents would be unwilling to work for companies that they know, or suspect, to be involved in unethical practices.

For their part, companies say they are struggling with regulatory demands requiring them to look at increasing numbers of financial transactions and relationships in greater depth, especially given limited compliance resources.

The sentiment is particularly notable in Indonesia, Thailand and China, where governments have recently taken a much stronger anti-corruption stance. However, to date the results have been mixed.

Codes of conduct are still not being followed and whistleblower programs are either missing or underused. According to EY's "Asia Pacific Fraud Study 2015", the percentage of employees prepared to use their company's whistleblower hotline has dropped dramatically since 2013, down from 81 per cent to 53 per cent.

"Implementing a hotline is not enough," EY says. "Employees must feel confident that their reports will be dealt with in a transparent and confidential manner and they will be protected from retaliation.

It also found that joint venture partners, distributors, agents and vendors are a key risk to businesses in relation to ABAC compliance.

"Companies entering into a business relationship with a third party should conduct as much due diligence as they do with an acquisition," EY says. "Simply having ABAC policies and codes of conduct is not enough – the policies must also lead to behavioural change."

Employees in the region might be becoming more aware of the need to curtail corruption, but as EY notes:

"Compliance starts at the top. Leadership must engage proactively in compliance activities and demonstrate and communicate to employees a commitment to ethical behaviour."

Suggested starting points include translating codes of conduct into local languages during ABAC training. Further, global organisations need to be open to feedback from local offices on the challenges of dealing with changes to policies and procedures.

Qatar nominated to head IAACA

In a strange turn of events, despite FIFA being investigated for corruption, 2022 World Cup host Qatar has been nominated by 24 countries and world organisations to head the International Association of Anti-Corruption Authorities (IAACA).

China is currently president of the IAACA, with voting on Qatar's nomination to succeed it scheduled to take place at an IAACA general Assembly in St Petersburg on October 31.

In a formal statement, Qatar Attorney General and UN special advocate for stolen asset recovery, Dr Ali bi Fetai al-Marri, said: "Qatar has received a strong backing due to its efforts in combating corruption in all forms, whether locally or globally."

MORE CLOUT FOR COMPLIANCE OFFICERS

CCOs are gaining greater standing as key threats to enterprise security grow.

"Compliance functions are still spending a disproportionate amount of time collecting data, versus time spent adding strategic value to the business."

MODERN CORPORATE COMPLIANCE FUNCTIONS are gaining significantly more authority and stronger organisational support for compliance programs, according to a new study.

In its fifth year, the "In focus: Compliance Trends Survey" has revealed a tidal shift in the standing of compliance professionals, with 59 per cent of respondents reporting that the job of a chief compliance officer (CCO) is now a stand-alone position, compared to just 37 per cent in 2013. Some 57 per cent now report directly to either the CFO or board.

The study, conducted by Deloitte & Touche LLP, measured the responses of more than 360 compliance professionals from around the world representing more than a dozen industries including financial services, healthcare, and consumer and industrial products. While the data shows a clear trend toward a more empowered CCO with a higher position in the organisation, concerns and challenges related to broader recognition of the value of compliance persist. In addition, many companies' existing technology solutions continue to fall short of compliance needs.

CCO authority

Challenges remain in embedding compliance culture throughout the entire organisation and its extended enterprise. Results are also mixed on whether the enhanced authority and positioning of CCOs has enhanced the perceived value and level of support of the program throughout the entire organisation.

As with previous surveys, only a minority of respondents – 32 per cent in the 2015 study – believe the compliance program is recognised for driving business value throughout the company. With small staff numbers continuing to be the norm, support of the compliance program within the business is critical to the CCO as he or she tries to help build a strong, transparent, risk-intelligent enterprise, the study recognised.

On a related point, only 43 per cent said their corporations have designated compliance officers in subsidiaries, business units, or different geographic markets. Further, even among the minority that do, less than half (49 per cent) of business unit compliance officers report to the global CCO. Some 40 per cent report to local senior managers.

This gives rise to the key question of whether the entire compliance function has proper ability and authority to carry out its mission, regardless of a CCO's reporting relationship.

Risk assessment

Alarmingly, 30 per cent of respondents in the study revealed they still do not measure the effectiveness of compliance programs. Tom Rollauer, executive director Deloitte Center for Regulatory Strategies, Deloitte & Touche LLP, emphasises the importance of the risk assessment process.

"Risk assessment is at the centre of the effort to manage compliance risk," he maintains. "If you have a robust enterprise-wide risk assessment process, priorities will evolve out of that. CCOs should be setting compliance monitoring and testing priorities based on these risk assessments."

A potentially concerning trend carried over from the 2014 and prior surveys relates to oversight of third party relationships across the extended enterprise.

According to the study, third party compliance risks (see story opposite) continue to be the single biggest worry for compliance professionals, with proactive management of them being inconsistent. Some 42 per cent of respondents indicated that they always audit compliance with policies or regulations; 38 per cent always perform extensive background checks; and 32 per cent always require training or certification.

Big Data

Compliance teams have become increasingly interested in advanced predictive analytics that can aid in predicting future risks before they erupt into a →

catastrophe, or to assist with regulatory change management. Unfortunately, few tools can now perform such functions without major customisation.

"While Big Data and GRC tools may hold the key to effective risk assessment and control monitoring, many organisations are still waiting for the promise to be fulfilled," notes Deloitte enterprise compliance partner and national practice leader, Nicole Sandford. "New applications and increasing access to data are coming, and that will take compliance to the next level with predictive analytics."

"While Big Data and GRC tools may hold the key to effective risk assessment and control monitoring, many organisations are still waiting for the promise to be fulfilled."

A mere 32 per cent of survey respondents feel confident or very confident in their IT systems, down from 41 per cent in 2014. The report suggests this may trace back to the relatively small size of compliance departments, which forces them to depend on other departments or business units to supply the data CCOs need.

"In essence, compliance functions are still spending a disproportionate amount of time collecting data, versus time spent adding strategic value to the business through analysing and trending the data collected," Sandford says. •••

SUPPLY CHAINS A HAVEN FOR FRAUD

Despite risks, many companies still lack supply chain fraud prevention and detection programs.

MORE THAN ONE-QUARTER OF PROFESSIONALS (28.9 per cent) say their organisations experienced supply chain fraud, waste or abuse during the past 12 months, yet nearly as many (26.8 per cent) have no program currently in place to prevent and detect the risks, according to a new Deloitte Financial Advisory Services (DFAS) poll.

"When we ask executives overseeing supply chains why fraud risk management isn't more top of mind, we're consistently told that compliance resource constraints are to blame," says DFAS partner Larry Kivett.

"With reputational, litigation and regulatory repercussions hanging in the balance, companies can't afford to dismiss supply chain fraud prevention and detection. Schemes constantly evolve and come from every direction, making vigilance crucial."

Interestingly, employees (22.9 per cent) were the top identified source of supply chain fraud risk, compared to vendors (17.4 per cent), and other third parties (20.1 per cent), which included subcontractors and their vendors.

"Since every supply chain's unique risk profile stems from a mix of cultures, geographies, industries and subcontractors, developing an effective supply chain forensics program is often more art than science," adds DFAS principal Mark Pearson. "But, if you know where to look, red flags and other faint signals can help focus limited resources to drive supply chain transparency and efficiency while reducing fraud, waste and abuse risks."

Warning signs for supply chain fraud, waste and abuse can include:

- Bidding/procurement processes that are not robust or independent;
- Lack of sufficient clarity in third party invoice details;
- Poor or strained relationships with certain third parties;
- Infrequent or non-existent "right-to-audit" assessments of suppliers and licensees' practices;
- Little-to-no oversight into proper administration of agreements with third parties; and,
- Use of third party agreements that are sole-sourced without clear explanation or constructed as cost-plus agreements without clear definitions of cost and other relevant terms.

About two-thirds (65.3 per cent) of respondents reported their company conducts at least some due diligence on their third parties. Nearly half as many (29 per cent) evaluate third party supply chain fraud risks on an annual or more frequent basis.

"Don't fall into the 'it can't happen at my company' trap," Pearson warns. "Forces outside your company aren't always to blame. Employees often leverage transactions involving vendors and third parties to their own benefit via supply chain fraud, and when collusion is involved, detection and prevention is difficult."

Kivett believes vendors and other third parties have become accustomed to filling out surveys and engaging in discussions about their practices within supply chains.

"Individuals and groups that have nothing to hide work hard to clarify misunderstandings and improve relationships; those hiding illicit acts may not," he says. •••

"With reputational, litigation and regulatory repercussions hanging in the balance, companies can't afford to dismiss supply chain fraud prevention and detection."

FIFA RED CARDED FOR CORRUPTION

In what has been dubbed the "World Cup of fraud", FIFA is starting to unravel as the FBI alleges "generations of bribery and corruption". **Mark Phillips** reports.

"A can of worms has been opened and no-one knows for sure just how many are in there."

"I've been to Russia twice, invited by President Yeltsin. I've been to Poland with their president. In the 1990 World Cup in Italy I saw Pope John Paul II three times. When I go to Saudi Arabia, King Fahd welcomes me in splendid fashion. In Belgium I had a one-and-a-half hour meeting with King Albert. Do you think a head of state will spare that much time to just anyone? That's respect. That's the strength of FIFA. I can talk to any president, but they'll be talking to a president too on an equal basis. They've got their power, and I've got mine: the power of football, which is the greatest power there is."

– Former FIFA president João Havelange

Many profess to have been "shocked" by the 47-count indictment of senior past and present Fédération Internationale de Football Association (FIFA) officials for bribery and corruption, but soccer's worldwide governing body has been mired in murky goings-on for years.

Consider just a few past headlines:

"Bribery scandal batters Blatter and FIFA" – UK Guardian, 2002

"FIFA's dirty secrets" – BBC Panorama, 2010

"Money makes the world cup go round" – Bleacher Report, 2011

"FIFA has lost all credibility" – UK Financial Services Authority, 2011

While the US Department of Justice (DOJ) indictments suggest criminal activity extending over 21 years, and a parallel Swiss criminal investigation is looking into charges of money laundering involving the awarding of the 2018 and 2022 World Cups to Russia and Qatar, as far back as mid-2002 the world's press was reporting on serious non-compliance allegations made by FIFA whistleblower Michel Zen Ruffinen.

No effective enforcement was ever undertaken, and FIFA essentially continued in a regulatory, commercial and compliance vacuum until two of its key sponsors, Emirates and Sony, last year decided not to renew their contracts. Indeed, apart formal obligations under Swiss law, FIFA's only real accountability seems to have been to the multinational brands that sponsor it, few of which have ever expressed much interest in insisting on good governance.

And why would they? In 2014, more than a billion people worldwide watched Germany and Argentina battle for the World Cup. From a marketing perspective, the chance for such global exposure comes along only once every four years, and distractions like the absence of any worker rights or safety standards in building the 12 air-conditioned stadiums for the extravaganza in Qatar (which, with a team ranked 99th in the world, has never even qualified for a World Cup) are merely inconvenient truths that, almost certainly, will be forgotten when the first ball is kicked.

Sponsorship at risk

But maybe not. Although President Sepp Blatter has fallen on his sword "for the good of the game", there is a sudden disquiet among sponsors over the widespread moral outrage that is currently engulfing, and may yet consume, FIFA.

In Qatar – where 4000 guest workers are likely to die completing Cup infrastructure projects – the goose may be laying only a gold-plated egg, and one that is already cracking. According to UK-based intellectual property management firm Brand Finance, FIFA's toxicity is such that its sponsors stand to lose up to US$1 billion in value due to the reputational damage of being associated with FIFA.

"Without knowing how quickly FIFA is going to clean out the Augean stables, my recommendation to the major sponsors would be to move towards

the exit," Brand Finance chief executive David Haigh has said.

Even so, it still seems unlikely Qatar will lose the World Cup, despite it almost certainly having bribed to get it. But key sponsors like Coca-Cola, Adidas, Hyundai, McDonald's and Budweiser are justifiably anxious over the turn of events and how they may yet unravel. A can of worms has been opened and no-one knows for sure just how many are in there.

Unfortunately, sport and racketeering have long been bedfellows, but no entity entrusted with the oversight of any code has so blatantly or for so long snubbed pressure from governments, the media, public and regulatory watchdogs to implement reforms as FIFA. Unsurprisingly, questions have started to be asked as to whether punches have been pulled because the "FIF-dom" is too big to fail.

Still, nothing talks louder than money, and even though FIFA does not disclose how much it is actually paid by sponsors (it makes most of its money by selling television rights to the World Cup, with other revenue streams from hospitality rights, brand licensing, ticketing and investments) it is likely they contribute to nearly a third of its total revenues.

"Given their direct stake in FIFA's performance, reputation and standing, some sponsors have started to make uncharacteristic noises about the need for change."

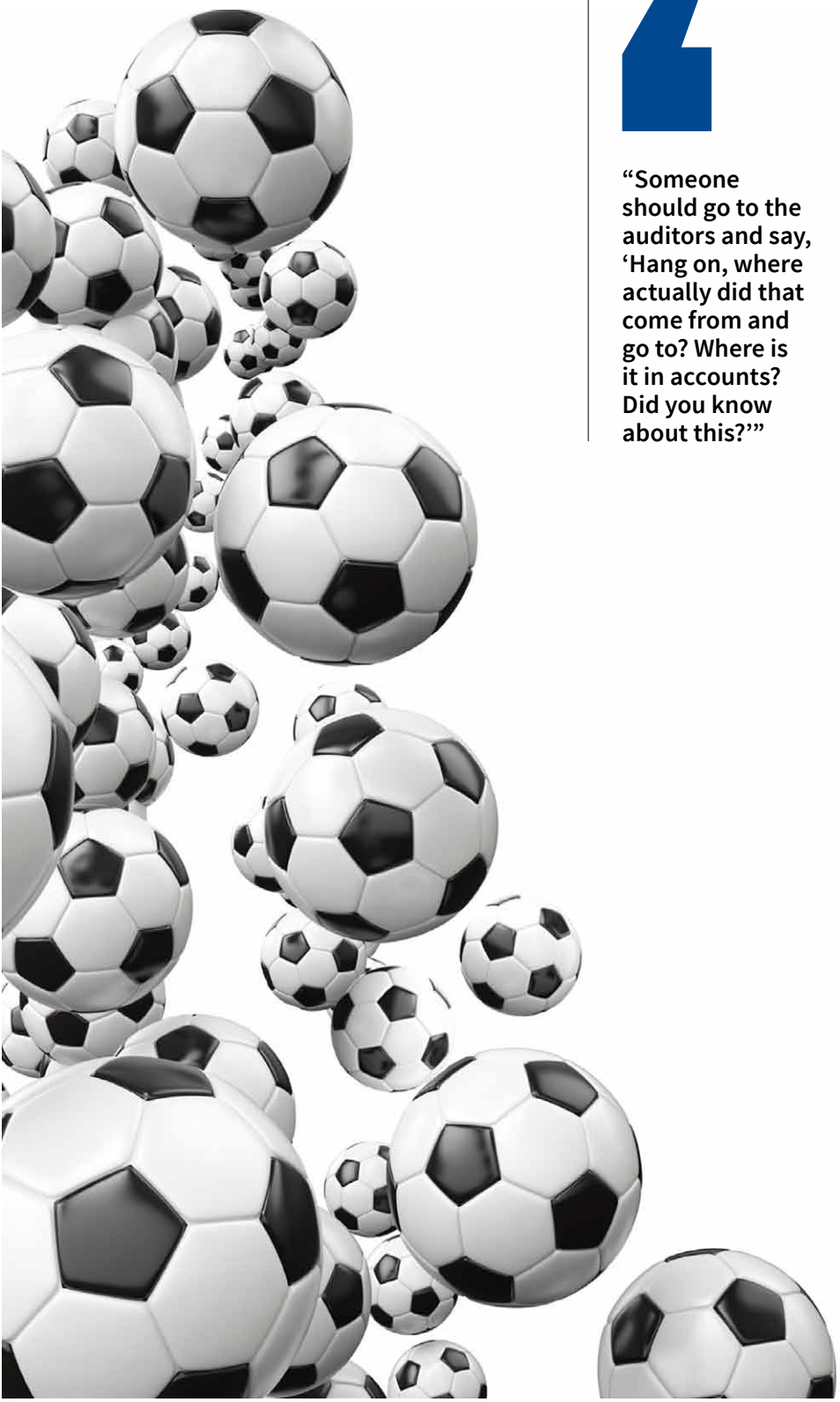
Given their direct stake in FIFA's performance, reputation and standing, some sponsors have started to make uncharacteristic (albeit still largely tepid) noises about the need for change. Visa has been the most forthright, threatening to pull its advertising unless FIFA immediately starts "rebuilding a culture with strong ethical practices".

Coca-Cola has welcomed the resignation of Blatter only days after he was elected to a fifth term as a "positive step for the good of sport, football and its fans".

Adidas, which has provided the official match ball for every World Cup since 1970, said "[the] news marks a step in the right direction on FIFA's path to establish and follow transparent compliance standards in everything they do."

Collateral damage

It is a small first step on what will likely be a very long path, and that assumes FIFA even intends to continue down it. Under its governing rules, the election of a new president and any fundamental reforms to FIFA statutes must be voted on by member associations and regional federations at the next FIFA Congress, which is scheduled for May 2016 in Mexico City.



"Someone should go to the auditors and say, 'Hang on, where actually did that come from and go to? Where is it in accounts? Did you know about this?'"

However, Blatter himself has conceded that this represents an unacceptable delay, and an Extraordinary Congress is expected to take place anytime from December of this year to March of next year.

For their part, FIFA's main sponsors will probably continue to show restraint until they know convictions are in and the extent of any crimes committed, and after that judge whether their own stakeholders consider the brand to be irrevocably toxoid.

Meanwhile, the fallout shows no sign of abatement. Activists in the US are targeting sponsors while Football Federation Australia (FFA), which rushed to the moral high ground when news of the scandal broke, has since come under fire.

When Blatter quit, it said in a statement: "The challenge is not just to change the top elected position, but the governance structure at all levels and the culture that underpins it. Australia will remain an active voice within the forums of FIFA and AFC [Asian Football Confederation] in promoting governance reform and a new era of transparency."

The FFA itself is now understood to be under FBI investigation for a controversial $500,000 payment that ended up in the pocket of disgraced former FIFA executive Jack Warner. Further, the Australian Federal Police is evaluating allegations of misappropriation of funds during Australia's $46 million bid for the World Cup, focusing on that $500,000 payment.

FIFA's auditor, KPMG in Switzerland, has also been dragged into the morass.

KPMG was not only responsible for auditing the umbrella organisation in Switzerland, but also member associations around the world that receive FIFA funding. Notably, it was auditor for the official Russia and Qatar organising committees whose successful bids to host the World Cup have been tainted by bribery allegations.

Some auditing analysts believe KPMG should have caught, and called out, the alleged illegal activities, particularly given FIFA's tarnished history.

In comments made to financial information website MarketWatch, Jerry Silk, a partner at law firm Bernstein Litowitz Berger and Grossman, who has sued global audit firms, said he was surprised KPMG would not have uncovered

evidence of the acts currently being investigated by the US DOJ.

Referring to an alleged US$10 million bribe payment at the centre of the US investigation, England Football Association chairman Greg Dyke also expressed concern, stating: "Someone should go to the auditors and say, 'Hang on, where actually did that come from and go to? Where is it in accounts? Did you know about this?'"

Being FIFA's statutory auditor, KPMG is bound by professional confidentiality and says it cannot comment on the matter.

Anti-money laundering experts remain unimpressed, arguing that root-and-branch reviews of past FIFA transactions are needed in order to demonstrate counter-money laundering compliance. Meanwhile, Barclays, Standard Chartered and HSBC are scrambling to review a number of transactions, totalling hundreds of thousands of dollars, after the trio were named in the US DOJ indictment.

Too little too late?

Through it all, Domenico Scala, independent chairman of FIFA's audit and compliance committee, is putting on a brave face.

"FIFA has worked hard to put in place governance reforms, but this must go further to implement deep-rooted structural change," he has declared. "A number of steps have previously been proposed but have been rejected by members. Today more than ever, FIFA is committed to ensuring that changes are implemented and upheld.

"Nothing will be off the table, including the structure and composition of the executive committee and the way in which members of the executive committee are elected. I expect this to be an important aspect of reform, as the structure of the executive committee and its members are at the core of the current issues that FIFA is facing.

"While FIFA operates in line with all applicable laws and international accounting standards, FIFA recognises that many have questioned the transparency by which FIFA operates. To address specific calls, FIFA will seek to publicise the compensation of the president and executive committee members and propose term limits.

"FIFA is fundamentally committed to change and determined to address the issues that continue to undermine FIFA and football more broadly. Now is the time to move forward. There is significant work to be done in order to regain the trust of the public and to fundamentally reform the way in which people see FIFA. These steps will ensure that the organisation cannot be used by those seeking to enrich themselves at the expense of the game."

"To address specific calls, FIFA will seek to publicise the compensation of the president and executive committee members and propose term limits."

Closed shop

Of course, many maintain that the time to move forward has long since passed. Blatter still insists he had no idea of any wrongdoing and that it was impossible for him to keep tabs on everyone within the organisation. Given he has been president since 1998 and an integral part of FIFA for over 40 years, it's hard to fathom how this rings true.

For all its committees, FIFA has essentially been a closed shop to the outside world. Once, when questioned on FIFA's ethics, Blatter replied: "I will not go into discussions with people that like to create problems." Little surprise, then, when a One World Trust Global Accountability Report scored FIFA with just 27 per cent in its transparency section, nor that even before the FBI investigation 84 per cent of the British public perceived it as being corrupt.

Scala is on the right track when he blames the structure of FIFA's executive committee and its members for many of FIFA's woes. As mentioned, FIFA is essentially an umbrella group of different football confederations from a host of geographic jurisdictions, each of which are responsible for their own internal governance.

Further, some have far more clout than others. Compounding the problem is that even though good corporate governance is premised on principles of transparency and responsibility, depending on their legal frameworks and business traditions, different countries can have very different ideas not only on how to achieve and manage it, but what it actually constitutes.

In addition, many of FIFA's associations around the world are in very poor countries, with money ostensibly meant for the development of football sometimes provided in cash, without appropriate oversight. It borders on patronage which, in turn, has grown the risk of a "look after us and we'll look after you" mentality.

Ironically, if and when a new approach to governance comes, it will need to appease not only millions of football followers around the world, but multinational sponsors that pour countless millions into FIFA's own existence.

"An organisation has little if not its reputation."

Words of warning

The FIFA scandal has destroyed the professional reputations of many and will almost certainly damage more. Here are five lessons to be learned.

- Allegations of corruption were nothing new long before the DOJ indictments, yet Blatter stonewalled and maintained they were groundless There needs to be a continuous focus on corporate culture and appropriate disclosure, and certainly no place for wilful ignorance in any organisation.
- Global organisations in particular must stay abreast of international trends in anti-corruption legislation. As the legal landscape changes and greater expectations around transparency develop, a new raft of risks emerges for organisations that fail to flag internal anomalies or audit discrepancies.
- Despite overt or subvert pressures to "toe the company line", risk and compliance professionals have a responsibility to all stakeholders to expose misconduct when it is detected, regardless of by whom it is perpetrated, and irrespective of potentially negative consequences.
- An organisation has little if not its reputation. The reputational damage wrought on FIFA has undoubtedly been immense, albeit thus far hard to quantify. However, international police agency Interpol no longer wants anything to do with it, having just suspended €20 million donated by FIFA in 2011 towards its "Integrity in Sport" program. Clearly, any issues with the potential to inflict brand damage need to be brought to the immediate attention of management and/or board of directors by those charged with providing assurance to stakeholders and governance officials.

FBI director James Comey perhaps best sums up the serious risks of not learning from FIFA's mistakes: "If you touch our shores with your corrupt enterprise, whether that is through meetings or through using our world-class financial system, you will be held accountable for that corruption." •••

FINANCIAL CRIMES

Edition Twelve June 2015

Security warning after Qld business hacked
Page 18

AUSTRAC warns on local property fraud
Page 19

Fraud drop "disappointing"
Page 20

ASIC sets sights on banking culture

The Australian Securities and Investments Commission (ASIC) is calling for tougher penalties on financial crimes with chairman Greg Medcraft telling a recent stockbroker conference in Sydney that they need to "inject so much fear that it stops people from breaking the law".

Medcraft's comments came hard-on-the-heels of preliminary findings from a study by Macquarie University into the risk culture of Australian banks which, among other things, reveal that bank executives are oblivious to cultural deficiencies and that more than half of banking staff believe remuneration plans encourage excessive risk taking.

Alarmingly, the Macquarie study has equated some banker personality traits with "Machiavellianism" and found that "avoidism" – where employees believe risk breaches will be ignored or excused – is endemic.

"People are sick of it," Medcraft declared. "When culture is rotten and inappropriate investments become worthless, it is not the wealthy who are being fleeced. Markets might recover but often people do not. The benchmark manipulation scandals all over the world, and problems locally in the financial advice sector, demonstrate this."

Over the past year, ANZ Banking Group, Commonwealth Bank of Australia, National Australia Bank, and Macquarie Group, among others, have been caught up in governance scandals. Medcraft dismissed any suggestion that they were just a few "bad apples".

The regulator is clearly worried that cumulatively, they may weaken the entire sector. As Medcraft himself acknowledged, public confidence in financial institutions is low.

He said a poor bank culture – such as one that is focused only on short-term gains and profit – drives poor conduct.

"When ASIC uncovers poor conduct and poor culture, it generally finds the issue spreads across the whole organisation," he said. "And that makes us look deeper."

Speaking before a Senates Estimates hearing in Canberra, Medcraft later said that it was up to the government to initiate a "broad review of penalties" to ensure there were appropriate civil penalties in place to deter misconduct among the country's banks, brokers, financial advisers, credit providers and other Australian financial services licence holders

He said it was up to the government to provide the regulator with the tools necessary to ensure "fear of penalties outweighs the temptation of greed".

Medcraft's comments followed a revelation by ASIC commissioner Greg Tanzer that the regulator is currently reviewing the incentive and staff promotion structures of three unnamed investment banks in Australia.

Medcraft said all financial institutions need to determine whether their remuneration and rewards facilitate inappropriate conduct. Further, he emphasised the importance of an environment wherein employees can express concerns without fear of retribution. •••

E-commerce fraud: best and worst countries

Online fraud is alive and well just about everywhere, but some places more so than others. In fact, according to a new study by fraud prevention software firm Forter, if you want to avoid fraud, it matters a great deal where your online provider is based.

Through analysis of more than one million e-commerce transactions over the course of 2014, Forter determined that Africa has an average fraud rate 10 times that of the world's average. It is followed by South America (three times the average) and Asia, which despite the huge number of consumers engaging in e-commerce in the region, is right on the average.

On a country-specific basis, Forter found that e-commerce fraud tends to poorer economies, but in particular those with accessible internet infrastructure. According to Forter business development vice-president, Noam Inbar, these are also countries where the chances of being pursued by law enforcement and being extradited are lower.

"Weak economic conditions drive more people to crime and decent internet infrastructure makes online fraud easier," Inbar says.

Indonesia lays claim to the dubious title of being the world's most fraudulent country, followed by Venezuela, Brazil, South Africa and Romania.

At the positive end of the spectrum, Scandinavian countries are the safest, holding down three of the top five slots, with Denmark being the least fraudulent country on Earth and Finland and Norway not far behind. New Zealand took second place with regards safety of online purchasing, with Switzerland ranked fifth.

Interestingly, the analysis revealed that fraud rates of transactions using Google's Android operating system were twice that of iOS, something Inbar attributes to the open nature of Android.

"That openness allows fraudsters to better study the system and find the weaknesses therein for access," she says.

The onus, she adds, is on everyone shopping online to regularly monitor their bank statements and credit ratings, and to always ensure use of strong passwords. •••

Security warning after Queensland business hacked

An international company based in Brisbane recently paid Bitcoin worth thousands of dollars to hackers after it was targeted by a ransom demand following the theft of sensitive data.

Queensland police refused to identify the company, but said that after paying the demand the hackers attempted to extort more money by threatening to launch an online attack against a child of one of its employees.

The company refused to cave in to the new demand and contacted the police, which said the hackers then "profiled a senior member of the organisation, identified their family and threatened to discredit members of his family through online attacks, particularly targeting a child".

"This is a very serious attack on an organisation and quite traumatic for the business, the victim and his family," Acting Assistant Commissioner, State Crime Command Brian Hay said.

"We are strongly urging businesses to ensure their computer systems are secure and protected from hackers, that they adopt a policy of not paying ransom demands and carefully consider the information posted on social media.

"Organisations need to think about putting in place a strategy to counteract or respond to these types of incidents. But the one message that I cannot stress enough is to never comply with extortion demands and report these matters to us immediately."

In the Asia Pacific region, Australia is placed first for such attacks, and globally seventh.

According to Symantec security specialist Nick Savvides, attackers generally focus on wealthier countries, and as such Australia is a frequent target.

Symantec's "Internet Threat Report" has highlighted that of the cyberattacks on Australian organisations in 2014, 30 per cent impacted large organisations while 40 per cent took aim at SMEs. •••

Nine charged with fraud

The Independent Broad-based Anti-corruption Commission (IBAC) has laid more than 100 charges against nine people allegedly involved with procurement of infrastructure at Public Transport Victoria and the former Department of Transport. A company has also been charged.

IBAC's Operation Fitzroy examined circumstances around procurement between 2006 and 2013.

The alleged offences include conspiracy to cheat and defraud, obtaining financial advantage by deception, misconduct in public office, giving and receiving secret commissions and furnishing false information.

The nine have been summoned to appear in the Melbourne Magistrates' Court on July 6.

HK talks tough to banks

With fallout from the FIFA scandal (see story page 12) showing no signs of abating, Hong Kong's banking regulator has warned that it will sanction any institutions that fail to fully comply with anti-money laundering regulations.

In a formal statement, head of the Hong Kong Monetary Authority's anti-money laundering and financial crime risk division, Stewart McGlynn said: "Meeting anti-money laundering expectations, particularly around higher risk customers, remains a challenge for some banks. There should be no doubt on the part of the industry or the public that where they do not, we will take action."

The recent indictment by the US Department of Justice of FIFA officials referenced US$1.2 million being sent to an HSBC account in Hong Kong, most of which was later transferred via Standard Chartered Bank in New York to a Cayman Islands-based bank. •••

AUSTRAC warns on local property fraud

The ante has been upped to stop Australian property being a prime investment opportunity for money launderers

Following the April release of a report by the Paris-based Financial Action Task Force (FATF) which determined that Australian property is a haven for international money laundering, two top lawyers have been caught on video in conversation about how regional leaders appropriate funds from their own people and lodge them in Australian bank accounts.

According to a report in Fairfax media, an undercover "sting" caught a Papua New Guinea lawyer explaining how a "prestigious" law firm and Queen's Counsel issue inflated invoices to conceal the movements of corrupt money.

The footage, which was filmed by anti-corruption NGO Global Witness, exposes complacency among Australian politicians and enforcement agencies, as well as gaps in regulation. It follows news that corrupt Malaysian officials have teamed with Australian property developers to launder kickbacks through a student apartment complex in Melbourne.

The revelations coincide with the release of a new AUSTRAC report, which says criminals are being drawn to real estate in Australia as a means to launder illicit funds because it is possible to purchase in cash, offers reliable financial returns and ownership can be disguised.

It says methods of laundering money include mixing illicit funds with loan funds, manipulating property value, use of third parties to present as the official owner, purchasing properties to facilitate criminal activity, and generating rental income to seem legitimate.

According to AUSTRAC, criminals are also using professional facilitators such as lawyers to help them seem legitimate and to conduct transactions on their behalf. These include establishing trusts and other structures to hide identity, recovering fictitious debts and making payments through lawyers' trust accounts.

Key indicators include:

- multiple and unexplained funds transfers, especially from overseas;
- difficulty identifying the ultimate source of deposits; and
- moving funds to/from a law firm's trust account and to/from bank secrecy or high risk jurisdictions.

In its report, FATF singled out China as the main source of international money laundering in Australian real estate.

It said that while regulation of major money laundering and terrorism financing channels, such as banking, remittance and gaming, is largely effective, most designated non-financial businesses and professions (DNFBPs) are still not subject to AML/CTF requirements and have insufficient understanding of their risks. These include real estate agents and lawyers. •••

Buyer dodged investment laws

As warnings about loopholes which exempt real estate from onerous disclosure requirements escalate, Treasurer Joe Hockey has vowed to enforce new foreign investment laws.

The government recently announced penalties, such as hefty fines and prison terms of up to three years, for foreign investors illegally buying properties in Australia

The treasurer's announcement coincided with news that a Chinese businessman was the mystery buyer behind the purchase of one of Australia's most famous homes, Altona in Sydney's Point Piper, for $39 million.

The mansion was bought through a complex structure of shelf companies and holding trusts, including nominee arrangements that have been reported as stretching from Melbourne to the British Virgin Islands.

At the time of the purchase, the buyer, Wang Zhijun, did not have permanent Australian residency, which contravenes laws that prevent foreigners from buying established housing.

"Foreign investors who think they may have broken the rules should come to us before we come to them," Hockey has warned.

Buyers who come forward before November 30 2015 will be forced to sell properties, but will not face criminal prosecution.

According to Hockey, the Foreign Investment Review Board is currently investigating 195 cases of purchases by foreign investors, including 24 by those who voluntarily flagged their own possible breaches.

Know your customers

KYC rules don't just have to apply to financial institutions. Here are some questions businesses of all sizes should ask to help protect against money laundering.

Do you really know the customer? Were they referred by a reliable source or from an obscure or unknown origin? If a seemingly affluent new client suddenly arrives at your doorstep, alarm bells should ring.

Do you really understand a customer's proposed transaction and are you going to be comfortable executing it? Does the transaction make sense considering what you know about their business?

Is this the usual way transactions are done or are there some curious kinks in it? For example, why would a total stranger offer to invest a substantial sum in your business?

There is no such thing as a too lengthy paper trail. Are there any records you should be keeping to better protect yourself?

What tech tools might be relevant to your business in stopping any involvement with money laundering schemes?

What are the latest ploys being used against your types of business?

Fraud drop "disappointing"

Despite a decline in monetary losses and the number of victims, results from a concerted anti-fraud campaign have been less than expected.

Despite the number of high-profile data breaches in 2014 (see story page 22), fears about record losses were not realised – even though the US Federal Trade Commission reports that identity theft was the most-complained about category in 2014, accounting for 13 per cent of complaints.

Notwithstanding the high total, both the number of victims and fraud losses declined from 2013, according to Javelin Strategy & Research's just-released "2015 Identity Fraud Study". It shows that thieves stole US$16 billion from 12.7 million US consumers last year, down 11 per cent from US$18 billion the previous year. The number of victims also fell 3 per cent from 13.1 million.

Thieves stole US$16 billion from 12.7 million US consumers last year, down 11 per cent from US$18 billion the previous year.

However, Javelin director of fraud and security, Al Pascual, says that in light of a massive effort from regulators, businesses and financial institutions to curtail breach losses via swift replacement of impacted cards, more sophisticated monitoring, and alerts to notify consumers of suspicious activity, the lower figures do not suggest any turnaround in the fight against fraudsters.

He believes the coordinated efforts should have resulted in a bigger drop, pointing to the fact that there is still a victim about every two seconds in the US.

Overall, 5.2 per cent of Americans were victims of identity theft, credit card fraud, or similar issues

Overall, 5.2 per cent of Americans were victims of identity theft, credit card fraud, or similar issues last year, according to the Javelin study. The majority involved credit card fraud, with victims of data breaches three times as likely as the general population to be a fraud victim. In cases where a breach exposed social security numbers, victims became twice as susceptible to identity theft or fraud.

On a positive note, instances of new account fraud – where a criminal uses personal information to obtain new loans, credit cards and other accounts – did dramatically decline, down from US$3 billion to US$2 billion. According to Pascual, this kind of fraud now impacts just 0.29 per cent of consumers, the lowest Javelin has ever recorded.

Unfortunately, 13 per cent of victims do not notice the misuse for more than a year. •••

Hackers raise the cost of a coffee

Criminals have come up with a clever new way to steal money from back accounts, targeting Starbucks customers' coffee accounts as a side door.

The hackers are using the chain's mobile payment app to drain the stored value of gift cards, then using Starbucks' auto-reload function to obtain consumers' associated debit and credit card details.

The scheme is part of a new fraud trend wherein hackers are targeting third party firms that create alternative payment systems and attacking them, finding that they are often easier to breach than financial institutions. In the process, they are turning rewards programs, points and prepaid cards into cash.

The strategy has worked because many Starbucks customers link their credit or debit cards to gift cards that are loaded onto mobile payment apps. Once a criminal steals a Starbucks mobile or gift card login credential, stealing from associated cards is relatively easy.

CROSSHAIR ON CYBERSECURITY

With the troves of customer data retained in Australia described as "a honeypot for malicious actors", the push is on to legislate mandatory data breach reporting. **Mark Phillips** reports.

"We will consider incorporating cyber resilience in our surveillance programs, across our regulated population."

IT IS LIKELY 2014 WILL BE REMEMBERED for highly publicised mega cybersecurity breaches such as at Sony Pictures Entertainment and JP Morgan Chase, along with their cost. However, while these attacks stole the headlines, millions of other breaches took place around the world and, according to one estimate, resulted in the theft of over 1 billion records of personal identity.

According to PwC's "Global State of Information Security Survey 2015", 42.8 million cybersecurity incidents were detected and reported in 2014, a 48 per cent increase over 2013. That's the equivalent of 117,339 incoming attacks per day, every day.

On a compound annual growth rate, there has been an alarming 66 per cent year-over-year increase in attacks since 2009. But as PwC itself admits, the figures are far from definitive. Many organisations have strategic reasons for not reporting incidents, while others remain blind to the fact they have even been attacked.

The upshot, one cybersecurity firm has claimed, is that as many as 71 per cent of compromises are undetected, let alone reported.

Be this as it may, there has been a growing push in Australia to change the regulatory environment so that the reporting of incidents that are detected becomes mandatory. The Australian Privacy Principles, which came into force in March last year, saw the implementation of a voluntary data breach notification scheme.

As Angelene Falk, Assistant Commissioner regulation and strategy at the Office of the Australian Information Commissioner (OAIC), explained in the May 2015 issue of *GRC Professional*, an overriding objective is to create a culture where risk and compliance managers incorporate privacy issues as a key part of governance.

However, taking this one step further, in a recent address Australian Securities and Investment Commission (ASIC) chairman Greg Medcraft tellingly warned: "We will consider incorporating cyber resilience in our surveillance programs, across our regulated population."

ASIC believes organisations have customarily focused on protection against cyberattacks, and it is true that historically many senior executives and boards have been largely hands-off with regards to the risks posed by data breaches and cyberattacks. However, growing concern about potential damage to brand reputation, class action lawsuits and costly downtime has been a game-changer, much as was the case for financial risks following the Enron scandal.

Data protection is now fundamentally a business challenge in addition to being an IT challenge.

Cyber resilience

In response, ASIC now maintains that a resilience-based approach is vital for organisations to better adapt to change, reduce exposure to risk and learn from incidents.

The regulator interprets "cyber resilience" as an organisation's ability to prepare and respond to a cyberattack in a way that will allow it to continue during, or quickly adapt and recover from, an attack.

This, it says, is vital to supporting investor and financial consumer trust and confidence and ensuring markets are fair, orderly and transparent.

"The electronic linkages within the financial system mean the impact of a cyberattack can spread quickly – potentially affecting the integrity

"It is essential to constantly monitor the threat environment, understand who poses a threat, what their motivations are and the methods they prefer."

and efficiency of global markets and trust and confidence in the financial system," Medcraft says.

"[They] are a major risk for ASIC's regulated population and that means cyber resilience is an area of ASIC focus."

This represents a significant "upping of the ante", in that previously cyber incidents were thought to be mainly the domain of the Privacy Commissioner.

Data protection

On the international front, the Singapore Personal Data Protection Act has already established stringent standards for the collection, use and disclosure of personal data. Organisations that fail to comply are subject to penalties of up to SG$1 million. As well as suggesting that organisations have cyber insurance and be able to produce a comprehensive inventory of all security incidents and breaches, SEC guidance requires that businesses implement risk assessment processes and more effectively assess vendor risks and due diligence.

Meanwhile, the EU General Data Protection Regulation is likely to be beefed up this year with the addition of new requirements for breach notification to individuals and that organisations handling personal data conduct risk assessments and audits. Fines for compromised businesses may also be increased.

In Australia, Medcraft is currently encouraging businesses, "particularly where their exposure to a cyberattack may have a significant impact on financial consumers and investors or market integrity, to consider using the United States' NIST [National Institute of Standards and Technology] Cybersecurity Framework to manage their cyber risks or stocktake their risk management practices".

But as mentioned, ASIC is also making noises about a more hard-nosed approach, and there is certainly no shortage of parties who believe mandatory data breach notification provisions is essential.

Data breaches

Indeed, according to the latest Unisys Security Index, the top two concerns for Australians are data security-related: 52 per cent are concerned about unauthorised access to or misuse of their personal information; 51 per cent about other people obtaining or using their credit/debit card details.

Early in 2015 security company Kaspersky Lab revealed that over the past two years more than US$1.2 billion had been stolen by hackers

from a number of banks and financial institutions across 30 countries, including Australia. At the time of the report, the Australian Federal Police said it had not received a referral relating to the matter from the banking sector.

Enforceable change

Basically, proponents of enforceable change have argued that as businesses should already have policies and procedures in place to ensure the information they hold is protected from data breach attacks – including notification where there is risk of serious harm to affected individuals – why not make it mandatory? This, they maintain, would ensure personal information is protected by all, rather than just by a few.

It might also encourage businesses to become more proactive in protecting both their brand and customers from the growing wave of cybercrime – which, according to Interpol president Mireille Ballestrazzia, is largely perpetrated by organised criminal gangs and costs more than cocaine, heroin and marijuana trafficking combined – through adoption of improved data handling practices and new security initiatives.

It is certainly true that because the threat to high-value enterprise information is ever-changing, it is essential to constantly monitor the threat environment, understand who poses a threat, what their motivations are and the methods they prefer.

Incidents involving Target, Sony and JP Morgan have left no doubt as to just how significantly a cybersecurity breach can impact a company's bottom line. Forensic investigation and remediation costs related to a breach (even an unsuccessful one) can be extensive, not to mention costs related to lawsuits from customers, suppliers and shareholders and others related to day-to-day business disruption.

But these aren't the ones that now keep the management of public companies up at night: the most serious threat to the bottom line is reputational damage and loss of customer loyalty. It can take months, if not years, to recover from such a loss of confidence.

Indeed, lost business is potentially the most severe financial consequence for an organisation, and growing consumer awareness of identity theft and escalating concern about the security of their personal data following a breach has only served to exacerbate that.

As has been widely reported, earlier this year the parliamentary committee tasked with investigating the Federal Government's data retention bill put its support behind introduction of a mandatory data breach notification scheme. It is also something that has long been championed by Privacy Commissioner Timothy Pilgrim, who has been particularly critical of telcos and internet service providers when it comes to securing user data.

The Australian Information Industry Association, Australian Law Reform Commission, Law Institute of Victoria and Financial Systems Inquiry, among others, have also backed the proposal.

Pilgrim has warned that as things currently stand, the troves of customer data retained in Australia are "a honeypot for malicious actors". Telstra has echoed the view – itself having leaked 734,000 customer details in 2011 and close to another 16,000 in 2013.

Regardless, it has surprised many that the Federal Government has acted so quickly by stating that it will "introduce a mandatory data breach notification scheme by the end of 2015". It will apply to all Australian companies subject to the Privacy Act, not just telecommunications providers.

The proposal represents a significant new compliance obligation and will certainly increase the overall cost to companies of handling data security incidents, particularly given the concurrence of new metadata protection laws.

An obligation for companies to bring data breach issues to the attention of regulators and their clients will likely be a boon for the embryonic cyber risk insurance market. Because entities will no longer have the option of dealing with the issues in private, they will have to weigh up their increased exposure to reputational risks and associated costs.

However, the overseas experience has shown that insurance alone is no panacea to dealing with data breach attacks. Fundamental to the NIST Cybersecurity Framework cited by ASIC is the importance of a strong governance program which, in turn, needs to be driven by the board of directors.

This means that stakeholders scrutinising whatever losses a company incurs – and particularly anything not covered by insurance – will inevitably look at the steps the entity itself took to manage the risk of attack which, in turn, will in no small way include the role of its directors.

The writing is on the wall, and as of now all Australian companies need to start revisiting their cyber resilience plans.

"The proposal represents a significant new compliance obligation and will certainly increase the overall cost to companies of handling data security incidents."

Six key questions

In the US, where companies are already subject to a mandatory data breach reporting regime, law firm DLA Piper partner **Jim Halpert** has prepared the following brief guide to appropriate duty of care.

1. Do you have an incident response plan in place, and have you tested it? Incident response planning and testing is part of the NIST Cybersecurity Framework. Moreover, studies by the Ponemon Institute have shown that implementing an incident response plan for cyber incidents and conducting table-top exercises to gauge how your organisation acts on that plan are key countermeasures to reduce the costs flowing from a data breach
2. Are you conducting periodic cybersecurity risk reviews? Cybersecurity risk is sufficiently serious that companies often need to conduct outside assessments to meet duties of care and to pass third party cybersecurity audits required by customers. However, in the US unprivileged cybersecurity reviews conducted by accounting firms or security consultants can be used against the organisation in plaintiff's class actions or regulator enforcement actions.
3. Are you managing supply chain risk? Addressing vendor and supply chain risk is an important part of cyber risk management. One part of this effort involves managing vendor agreements to require, among other things, providing notice of suspected (not just actual) breaches, requiring third party security audits and obtaining adequate indemnification. A related test for purchasers and suppliers is tracking agreements that need updating when open for renewal and mapping notification obligations in the event of a breach. It can also be important to obtain third party security audits further down the supply chain of component suppliers.
4. How do you respond to a breach? When a breach occurs, it is critical to respond efficiently and strategically, conduct a thorough investigation and, wherever possible, provide notice at one time that is sufficiently specific to meet regulator requirements and provide credit monitoring or other protection to customers where warranted. In the case of a payment card breach, it is important to upload affected card numbers through a merchant's payment card processor so that the numbers are flagged for fraud monitoring to avoid potential card fraud.
5. Does your insurance adequately cover data breach risk? Insurance is a key part of risk management and can offer significant protection for monetary costs incurred from data breaches. Finding the right coverage for your organisation's risk posture is important.
6. Are you addressing cybersecurity risk in M&A transactions? Over the past decade, M&A transactions have resulted in some costly security liabilities. Cybersecurity risk has grown so important that it merits particular attention in the due diligence process. Further, cybersecurity risk must be addressed during post-merger integration. Legacy systems are often vulnerable to attack and it is important, where possible, to implement post-merger security solutions reflecting best practices.

Cyber Snapshot

A just-released study by the US-headquartered Risk Management Society has found:

- Only 51% of its membership purchases stand-alone cyber insurance policies.
- 58% carry less than US$20 million in cyber coverage.
- 49% of those with under US$20 million in coverage are paying over US$100,000 in premiums.
- 74% of those without cyber coverage are considering procuring it in the next 12-24 months.
- The top three first party cyber exposures are reputational harm (79%); business interruption (78%); data breach response and notification (73%).
- The number-one reported third party cyber exposure is disclosure of personal information (88%).
- 73% believe governments should regulate/legislate data and cyber privacy issues, with 58% believing they should also regulate legal liability, fines and penalties.
- The vast majority believe governments should not regulate loss of business, reputational issues, or business interruption.

•••

"The most serious threat to the bottom line is reputational damage and loss of customer loyalty."

THE INERCONNECTEDNESS OF RISK

At a recent KPMG and the GRC Institute roundtable, senior risk professionals debated the key issues in operational risk. **Daniel Sheehan** reports.

"There is a danger that the risk function can cloak itself in jargon, but the more it does that, the more difficulty everyone in the business has with it."

"In an insurance firm, in a sense everyone is a risk manager."

IN A GLOBALISED AND DIGITAL ECONOMY, risks travel rapidly. That makes operational risk more challenging and more important. But how can organisations respond to the challenge?

Colin Gomm, vice president risk and HSEC governance at BHP Billiton, told a roundtable in Melbourne last month that in today's world the entire business needs to take responsibility for risk. BHP's approach is to build risk into the fabric of the organisation, he said.

"The central risk function at BHP is two-and-a-half people," Gomm revealed. "That means there is not a lot of risk work completed in the centre of the organisation. There is, however, a lot undertaken in the operating areas of the business.

"It is built into all functional activity. Our expectation is that people will be looking beyond their immediate function and seeing the risks on the horizon that could have an impact. Risk should be built into the activities of the business, as much as it is in the operational risk program."

He continued: "All the work that everybody does is managing risk. It is not a specialisation different from what you do, it *is* what you do. There is a danger that the risk function can cloak itself in jargon, but the more it does that, the more difficulty everyone in the business has with it. The less you own and the more you give away, the stronger the risk function will be."

Chief risk officer at AIA Jarrod Sawers agreed. "In an insurance firm, in a sense everyone is a risk manager," he emphasised.

Sawers said expectation from the CEO is very important, and that the organisation has changed its corporate culture around risk.

"In the past, the chief risk officer, the chief compliance officer and internal audit would all present on risk and give reports on the key risks to the business,' he noted.

"Now, while these functions still report, every member of the executive at the table also presents their own risk profile and is challenged by the whole group. This helps cut through some of the jargon and silo thinking. When people have to front up and do that, it drives them to understand their risk profile."

Sawers maintained that a key building block of the risk framework is stress testing. "We have approximately 12 stress scenarios that are [semi] realistic. For example, we may look at what would happen in the event of war in Indonesia.

"We insure approximately three million working Australians, so a stress test would look at what that event would do to the financial or job markets. They're questions we look into and hopefully find that we are not connected to that risk, but if we are, we ask ourselves what we should be doing to minimise exposure."

CNP Brands business manager Shaun McGrath said his firm's risk framework also needs to consider global issues, albeit from a slightly different perspective.

"We have to consider what is going on around the world in terms of the best practice standards being developed," he said. "We must be aware of risk and safety trends.

"While we must comply with Australian consumer law, what we really have to ensure is that the product is safe. It doesn't matter what the law says: every product we put into the marketplace must be safe. We can learn a lot from lessons overseas."

One of the big global risks facing all companies is cybercrime and data security (also see story page 22). According to Sawers, cyber risk is less about technology and more about behaviours.

"This is the real key," he said. "There is a huge amount of attacks from Russia and elsewhere but simple behaviours can stop many of them."

For example, Sawers talked about the importance of staff not making mistakes like opening up rogue emails, which can often open the door to cyberattacks.

Gomm added that executive behavioural training on data security is crucial.

"Most information is held at the most senior levels of an organisation, so you really need to focus on making sure executives know what is going on. They can be highly vulnerable."

Conduct risk

KPMG partner Sally Freeman said one of the biggest risks to emerge in recent years, particularly in financial services, has been conduct risk. She asked the panel how professionals were managing the challenge.

Sawers said employees need to understand the corporate culture of the organisation. "The question employees need to ask themselves is what do we stand for as an organisation? And is a behaviour in line with what we stand for? Having these corporate values gives you control."

Gomm also reflected on BHP's bribery and corruption breaches related to entertainment at the Beijing Olympics. He said it has been a learning experience for the organisation.

"We have learned a lot through our dealings with the US Government and the Foreign Corrupt Practices Act," he said.

"The challenge is to give people the confidence that if they raise a suspicion, it will not blow back on them."

"The challenge we faced was dealing with something that happened a long time ago. The first reaction to the investigation was that we had to be totally transparent and view it as an opportunity to learn. During the process of the investigation, we have been able to build what the US Department of Justice now considers a world class compliance program. We freely admit that this was not the case at the time of the breaches.

"A large part of an anti-bribery framework is giving people the confidence to raise concerns safely through a whistleblowing hotline, or something of that nature. The challenge is to give people the confidence that if they raise a suspicion, it will not blow back on them."

Risk appetite

Establishing a risk appetite statement is central to any risk management framework, Sawers said, something which AIA has had in place since 2010.

"We review it at least once a year and every time we are considering major changes to our business strategy. When we look at our corporate strategy we always ask whether it fits with our appetite for risk.

"Risk appetite is a very broad term, but it really just outlines the risks we want to take. We look at strategic opportunities over the next three-to-five years and decide if they will be within the risk appetite statement. If they are not, but we still want to pursue them, we have to review our risk appetite." •••

ELEPHANTS IN THE PUBLIC SECTOR

Risk management can be challenging at the best of times, but as **Marcus Turner** explains, the public sector faces a raft of frequently conflicting issues that need to be overcome.

"Risk management principles are elegantly simple, but implementation of effective practices can be vexed."

THERE IS ONE UNASSAILABLE TRUTH IN enterprise risk management (ERM).

You may have a well-qualified, experienced CRO, or at least a dedicated one. You may have engaged a well-credentialed consulting firm to develop your risk framework. But no matter how well crafted, no matter how well tailored that bespoke framework is against theory and AS/NZS ISO31000:2009, aligning it with corporate identity is critical. If not, it will become disconnected from the business.

At the heart of the alignment of risk management and its ability to support corporate objectives is the need to have an adequately defined risk appetite. Many organisations approach this in concert with establishing risk metrics.

However, regardless of whether you are in the public or private sector, there are significant challenges around how metrics are established and expressed. This is particularly the case where executive teams or boards do not properly understand how risk appetite can drive, or distract from, key objectives.

In the public sector, there is an additional layer of challenge around ERM that can become the elephant in the room. In fact, there are probably two publicly owned elephants; cultural identity and the "P" word – politics. We will deal with these in a moment.

Risk management principles are elegantly simple, but implementation of effective practices can be vexed. Again, the public sector has added complexity, arising from its raison dêtre. It has an underlying imperative to achieve business objectives and along the way provide value to "owners". In other words: to be economically viable and turn a profit.

Despite community expectations that public funds will be spent with efficacy, expectations within the sector can be different. It is a dilemma that has been stated and restated since the establishment of government.

In a contribution to *Forbes* magazine, professor of economics John Harvey stated: "The problem in a nutshell is that not everything that is profitable is of social value and not everything of social value is profitable."

And therein lays the kernel of one of our elephants. The public sector is not predicated on making a profit, nor does the business of government constitute a commercial enterprise.

People who work within that construct generally have a strong belief that they are there to contribute to a higher goal of serving the community, and often risk management is discussed in terms of achieving business objectives. I have heard from a cross-section of state and federal public constituents that risk management is a private sector construct about achieving profits. While this isn't a pervasive view, it is voiced sufficiently to be a concern.

The focus is different, the motivators differ and the outcomes differ – making a profit for the few and meeting community expectations of the many. However, the challenge exists for the risk management profession and managers alike.

How do we acknowledge the different environment and still be able to use risk management as an integral and vital part of governance, without it being simply a compliance exercise that provides little value?

Governments at state and federal level have over the past few years introduced instruments to promote better practice in risk management. The challenge is to ensure the "legislative requirement" can be met through ensuring appropriate risk management culture and capability within public sector agencies.

This cultural tapestry is not limited to the level of seniority of staff charged with "managing" the risk function, but it certainly includes seniority. I was fortunate in my time as a CRO within govern-

ment agencies, as those organisations placed the role in quite senior levels with fairly direct reporting lines to agency heads.

However, it was not the case with many of my colleagues. The end result was that risk management often languished, with the role poorly defined or understood. As a consequence, there was often inadequate investment in risk management infrastructure – people and systems.

Investment in risk management expertise to support the organisation in achieving its objectives is often an infinitesimally small slice of the overall budget. It might be a useful exercise to consider how many staff are dedicated to risk management. What is the proportion of the total budget? What is the investment in staff, training and supporting systems?

The upshot can be perpetuation of the view: "risk management does not offer value to what I am trying to achieve for the greater good". Its value and potential is never realised and the whole adventure becomes a check-box exercise against a prescriptive list. Do I have a risk management policy? Check! Do I have a risk management framework? Check! Is there someone whose position has overall responsibility for risk? Check! Do I have a risk register? Check! The list goes on.

The divide between truly effective risk management practice and the bare minimum required to satisfy central agency reporting requirements undermines the process. Staff responsible for risk assessments approach them with a minimum of training and with a view that risk management is simply a road block to what they really need to do. As a result, they just do the minimum to get it off their backs, which undermines integrity.

This leads to our second, not-so-tame elephant – a beast that is often the cause of frenetic activity and creates dilemmas of its own. Let me illustrate using a hypothetical example:

"We have defined our risk appetite and established risk metrics around a range of consequences and so forth. We have undertaken a risk assessment and finessed it so that it's well supported by logic, reason and the benefit of past experience. We now have the secretary's approval and yet the minister's office announced over the weekend to the media that we will be doing something completely different, starting Monday."

There are numerous instances where the best laid plans of agencies – no matter how carefully constructed and planned – can turn on the heartbeat of a press release. While this can serve as a stark example

"The problem in a nutshell is that not everything that is profitable is of social value and not everything of social value is profitable."

of differences in the application of risk assessment processes and tolerances, it generally points to different and sometimes divergent objectives.

The challenge for managers and risk management professionals is how to best integrate this phenomenon into the way we administer agencies, so as to enable an agency to respond to change. In comparison, large private sector organisations seldom need to deal with the abrupt and precipitous change in direction that is the common, albeit unsettling fare, of political "participation" in public sector administration (for the purposes of this article, political risk is considered with a capital "P", being the nature of exposure resulting from rapid changes to government policy).

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

"Investment in risk management expertise to support the organisation in achieving its objectives is often an infinitesimally small slice of the overall budget."

These elephants can cause egregious inefficiency as agencies struggle to respond to rapid and imposed changes, while simultaneously trying to manage a corporate culture where solid work seems to be undermined by political whim. "Change fatigue" can be as debilitating as the changes themselves, but attempting to tame these elephants is a first priority.

Many entities will look to a strategic risk associated with management agility and the ability to respond to change. The treatments tend to associate with clear planning processes, experienced public sector management, responsive and professionally competent analytics, good relationships with the respective minister's office, and so on. Similarly, cultural issues on risk management will lean towards ticking boxes and having efficient and effective reporting systems.

The key to managing these elephants is to attract and support a competent "risk leader". An effective CRO should be able to ensure both a technically robust and appropriate risk management system and support implementation of the governance platform. The challenge is trying to balance investment in risk management professionals and the cost required to attract those skills away from more lucrative private sector opportunities.

Attracting high-calibre candidates and supporting them will promote governance through aspects such as: providing expertise and advice; drive and leadership; capability building through executive professional development; and line management training. Most importantly, they will be able to capture the reasoning behind decisions and therefore more clearly align accountability and responsibility.

The upshot will be that the agency is able to respond more quickly and the relationship with the minister's office is supported. However, while rapid, unexpected changes may be reduced, they cannot be completely avoided. Even so, the agency will be able to interact with defensible risk assessments to more effectively inform ministerial thinking.

In much the same way as a CRO seeks to be a trusted advisor within the agency, the agency will cement a reputation as a trusted source of robust advice. •••

Marcus Turner is director risk and governance at HTM Group.

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

INVESTORS AT RISK AS CLIMATE CHANGES

A new study has shed light on the little understood impact of climate change on investment returns.

The Earth has entered a new period of extinction, a study by three US universities has concluded. According to the report, vertebrates are disappearing at a rate 114 times faster than normal.

– Science Advances Journal

FINANCIAL SERVICES FIRM MERCER HAS warned that the risks now posed by climate change are such that investors have no choice other than to factor them into projected returns.

According to Mercer, which has just released new research on the subject, investors can manage the risks most effectively by looking "under the hood" of their portfolios and factoring climate change into their risk modelling which, it claims, will require a "significant behavioural shift" for most.

The report, titled "Investing in a time of climate change", estimates the potential impact of climate change on returns for portfolios, asset classes and industry sectors between 2015 and 2050, based on four climate change scenarios and four climate risk factors.

Different scenarios

The four scenarios represent a rise in global temperature above pre-industrial era levels of 2°C, 3°C and two 4°C scenarios (with different levels of potential physical impacts). Mercer collaborated with 16 investment partners, collectively responsible for more than US$1.5 trillion, to produce the report.

"We recognise that markets do not always price in change – they are notoriously poor at anticipating incremental structural change and long-term downside risk until it is upon us," says principal and head of Mercer's responsible investment team, Alex Bernhardt.

"The report identifies the 'what?' the 'so what?', and the 'now what?' in terms of the impact of climate change on investment returns, enabling investors to build resilience into their portfolios under an uncertain future."

Industry impact

A key finding of the report is that the biggest risk will be at industry level.

For example, depending on the climate scenario which plays out, average annual returns from the coal sub-sector could fall by anywhere between 18-74 per cent over the next 35 years, with effects being more pronounced over the coming decade (eroding between 26-138 per cent of average annual returns).

Conversely, the renewables sub-sector could see average annual returns increase by between 6-54 per cent over a 35 year time horizon (or between 4-97 per cent over a 10-year period).

Asset-class return impacts will be material, but vary widely by the climate change scenario. Growth assets, for example, are more sensitive to climate risks than defensive assets.

A 2°C scenario could see return benefits for emerging market equities, infrastructure, real estate, timber and agriculture. However, a 4°C scenario would have a negative impact on all these sectors except real estate, where risks could be mitigated through geographic risk assessments undertaken at the portfolio level.

"[Either way] we believe it's a significant investment risk that investors should be aware of and able to act upon in close collaboration with investment managers," says Mercer global CIO for mainstream assets, Russell Clark.

Notably, a 2°C scenario does not have negative return implications for long-term diversified investors at a total portfolio level to 2050, and is expected to better protect long-term returns beyond this timeframe.

"Climate change forces investors in the 21st Century to reconsider our understanding of economic and investment risk," notes State Super Financial Services CIO Damian Graham.

Allianz Climate Solutions GmbH managing director Kartest Loffler adds: "While global warming is a fact, we face great uncertainty around policy measures and the financial impacts in the nearer term are little understood."

Australia in strife

Meanwhile, civil engineers from the University of New South Wales have also released a new study into climate change, concluding that rising temperatures mean Australia is likely to face more severe storms like the ones that rocked New South Wales and Queensland earlier this year.

Their study states that the risk of flash flooding is also on the rise alongside temperatures, as warmer climates that lead to heavy downpours could see flooding as a major future risk for many parts of the country. •••

A DESIGN ON CRIME

In today's business world, proactive and integrated security practices are crucial, but who is responsible for them?

"Common threats such as theft, vandalism, fraud or workplace violence can have serious impacts on staff retention, organisational credibility and reputation."

UNDER RELEVANT WORKPLACE HEALTH and safety laws (WHS), every employer has a duty of care for the wellbeing of its employees. WHS legislation includes a model WHS Act, regulations, codes of practice and a national compliance and enforcement policy.

In larger companies, security precautions fall under the domain of a chief security officer (CSO), often working in close liaison with a chief risk officer (CRO). Measures can include fingerprint scans, hand geometry, retina or iris scans and facial, voice, handwriting or signature recognition, with intrusion detection bolstered by closed circuit television (CCTV) and, in some facilities, motion detectors, magnetic door contacts, duress alarms, and vibration and sonic detection.

However, many small- to medium-size enterprises (SMEs) have little need for such state-of-the-art technology, nor can they justify its cost. But that doesn't mean they can ignore due diligence. Even if there is a dedicated role within the organisation to oversee external security, the buck will still likely stop with senior management if something goes wrong.

Common threats such as theft, vandalism, fraud or workplace violence can have serious impacts on staff retention, organisational credibility and reputation and consequently a significant financial impact, whether it is in legal and recruitment costs, increasing security operational costs or even loss of revenue.

Fortunately, there are measures all organisations – regardless of size or budget – can incorporate to better protect the workplace.

Given that the security risks for any building are dependent on tenant mix, location and many other factors, identifying potential risks and developing appropriate responses is the key to an effective plan.

Vulnerability assessment

Undertaking a security review and audit will provide an immediate snapshot and health check on current security practices and determine security requirements and gaps. Typically, it will incorporate an assessment of items such as security system performance, obsolescence, appropriateness of measures in place to manage risks, the effectiveness and efficiency of incumbent maintenance regimes and associated staffing level needs.

The results of the review and audit should also incorporate an assessment of both capital and whole-of-life costs. By understanding the cost of managing risk, organisations can then effectively plan for future security costs and assess the return on investment of existing or proposed measures.

Security and design

The idea that the proper design and effective use of the physical environment can lead to a reduction in the incidence and fear of crime is at the heart of a concept known as CPTED (Crime Prevention through Environmental Design).

Although not a new concept, CPTED has made a strong comeback in the security arena in recent years. Indeed, there are some who maintain that building or renovating any facility without utilising CPTED concepts borders on negligence if safety is a significant concern.

With regard to the bottom line, there is no question that by enhancing a building's functionality, the integration of security can significantly reduce the overall capital cost of purchasing technology or overt physical barriers. Operating costs can also be minimised by reducing staffing levels. And should the security risk for a facility or its occupants change significantly during its life, robust planning will provide better scope for savings in applying retrospective treatment.

Basically, CPTED assumes that there are two types of users of space in the built environment – "normal" or those users who have legitimate purpose and intent, and "abnormal" users who do not act according to laws, policies and social norms. CPTED, founded on tenets such as lighting design, clear sightlines, landscaping for visibility and natural access control, helps to make the normal user feel at ease and welcome, while making the abnormal user apprehensive about engaging in inappropriate behaviour.

Cost-effective "smarts"

Once the audit process is complete and the most likely threats to the organisation identified. there are some basic CPTED principles all managers can put in place without necessarily consulting security specialists.

The key is to remember that criminals usually commit crimes in "comfortable" environments and that their comfort is heightened by isolation and concealment, where few witnesses exist and the chance of being identified is minimal. Sometimes, very simple changes to an area can create an environment that is uninviting for perpetrators.

For example, surveillance can be improved by creating clear and unobstructed sight lines in activity areas, reducing hiding places and creating the perception of witnesses. Access control can be increased by emphasising primary entry points and minimising secondary outlets.

Clearly mark transition zones that indicate movement from public, to semi-private, to private space. Put unsafe activities in safe spots, where surveillance is high and access is limited. Similarly, put safe activities in unsafe areas. This will increase the perception of safety in these areas and help to establish territorial behaviour.

There will always be situations where technology is necessarily the first option, but there are also many cases when a smorgasbord of CPTED strategies can be integrated into the design of a facility to create a natural security environment, either eliminating the need for cameras around the perimeter of a building or, at the least, reducing their number.

"You must be able to say 'this is what makes sense for us to do, and this is why it makes sense for us to do it'.

Ensuring that parking areas and walkways have ample lighting if they are used at night is one obvious precaution, as is low shrubbery so as to diminish the risk of surprise encounters. Ornamental yet hostile vegetation underneath accessible windows is another low-cost but effective defence strategy against breaking and entering.

Selling the solution

Regardless of whether an organisation is based in a low-crime suburban neighbourhood or high density inner-city locale, managers need to understand what it is they are trying protect and why.

Whether it consists of basic CPTED initiatives or high-outlay technology-driven surveillance and access control, or a combination of both, any security solution needs to be aligned with the company's mission, goals and objectives. Only by taking a proactive role in developing suitably tailored site-wide security solutions will those tasked with managing security be able to make the business case to the CFO or CEO and secure the funding they need.

In other words, you must be able to say "this is what makes sense for us to do, and this is why it makes sense for us to do it". •••

GRC PROFESSIONAL
GOVERNANCE • RISK • COMPLIANCE

GRC INSTITUTE AWARDS 2015

CONGRATULATIONS TO OUR WINNERS of the New Zealand regional awards for "Compliance Professional of the Year" – Kane Patena of Meredith Connell – and "Risk Management Team of the Year" – Sarah Butler and Hock Choo of Westpac New Zealand. Their success in the awards is testament to their hard work, creative thinking and passion.

Over the years of the awards, it has become apparent how reticent members are to put themselves forward for recognition or to even realise when they have made significant impacts on GRC outcomes for their organisations.

When reading GRCI's mission is to be the preeminent body for compliance and risk management professionals across the Asia Pacific, you may think, so what (and right now, you may be wondering what has this to do with the award winners)? Well, the "so what" factor is that as a professional association, we're here for *you*. The courses we have built and run are here for *you*. The events, seminars and publications we produce are for *you*. And the awards are for *you* – because you, our members, don't sing your praises nearly often or loudly enough.

The GRCI Awards have a very strict and unique set of criteria set by our Awards Panel – made up of your peers – that reflects the values associated with those who embrace the challenge of embedding a culture of compliance, risk, ethics and governance into their organisations. There are seven overall categories:

- Lifetime Member Award
- Honorary Fellow Award
- Compliance Professional and/or Team of the Year
- Risk Management Professional and/or Team of the Year
- Brian Sharpe Memorial GRC Institute Essay Competition Award
- GRC Institute CCP Graduate of the Year*
- David Squire Memorial GRC Institute Associate Graduate of the Year*

** Can only be nominated by course assessors*

Of these categories, it was agreed in 2013 to restructure the primary awards, the Compliance Professional or Team of the Year and the Risk Management Professional or Team of the Year, to provide opportunities in each of the regions we service for the talent and hard work of our members to be recognised within their own market. The winners of each of the regional awards then go on to qualify for consideration for the overall winner for that year in their category.

The two awards are given only to an individual and/or a compliance or risk management team for their significant contribution and commitment to innovation, tangible change or development of enhanced systems in their workplace. They can also recognise the implementation and/or integration into business systems of compliance or risk management outcomes in practice, within the compliance or risk management community, or work organisation.

Being able to demonstrate recognition by stakeholders and/or industry as achieving excellence in practice will be viewed favourably by the judging panel. The contribution should be overt and measurable, and winners should be justly proud of their achievements.

The other five awards do not have regional equivalents and are nominated only in the end-of-year awards, to be presented each year at the Gala Dinner.

We invite all members to, where appropriate, consider nominating themselves, their team or a colleague. The calibre of nominees and winners in recent years has demonstrated our membership's high level of experience and expertise, and the inclusion of you or your team in this elite group is certainly something to aspire to. •••

"We invite all members to, where appropriate, consider nominating themselves, their team or a colleague."

To nominate for any of the remaining regional awards or one of the other categories contact GRCI national manager Naomi Burley (naomi.burley@thegrcinstitute.org) for the necessary forms and to discuss relevant criteria.

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

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