StrategicRISK

THE KNOW EDGE

MANAGEMENT LIABILITY

In the aftermath of the global financial crisis, boards are being held to account as never before. The finger of blame is shifting to directors and officers. So this time, it really could be personal.

By Jessica Reid, *StrategicRISK* editor (Asia-Pacific)

ZURICH®

THE LEADER

Around the world there are hundreds of offences for which directors can be held personally liable – and on an almost monthly basis, new legislation comes into force that increases their exposure.

In this issue of *The Knowledge*, we wanted to get a deeper understanding of some of the key challenges of corporate management liability. We therefore sought the views of 75 risk managers from across Asia-Pacific in our *StrategicRISK* Advisory Panel.

Our survey found that fears about anti-corruption and anti-money laundering legislation, and about criminal and regulatory fines and penalties, continue to feature in the top worries keeping risk professionals – and their directors – awake at night. But a rising concern for many is the potential personal liability for directors in the wake of a cyber breach.

The risk is increasing too in the face of rising shareholder activism and a growing number of regions introducing new legislation around data protection and notification.

In fact, despite the swathe of regulation implemented since the global financial crisis, rule-makers show no sign of relaxing their approach. Many experts predict regulatory scrutiny will only intensify, particularly in Asia, where the idea of good corporate governance is a relatively recent concept. Whichever way you look at it, boards today are being held to account more than ever before. Many would argue that this can only be a positive development.

Email jessica.reid@nqsm.com

THE SURVEY

All is not lost as the hacking menace grows

The threat of a disastrous cyber breach – and of lawsuits against specific company directors – is all too real, say risk managers

Data loss is seen as the biggest emerging threat to directors' and officers' (D&O) liability, a Management Liability Survey of *StrategicRISK*'s Advisory Panel has found.

The panel singled out data loss as the D&O risk most likely to occur and to have the greatest impact financially. Close behind was 'breaching industry regulation', with 'employment practice claims' rounding out the top three (see scattergraph, right).

Some 77% of respondents also said that liability owing to a cyber breach was a bigger concern to their board than it was 24 months ago. This will come as no surprise to insurers, who are seeing a rise in client enquiries about management liability connected to cyber breaches.

"It's a huge threat," says Alex Morgan, Zurich commercial insurance chief underwriting officer, Japan, adding that a breach is now "a matter of when, not if".

"If [a cyber breach] happens and it becomes apparent to a potential litigant that [the company directors] didn't do anything to prepare, then there is scope for them to be sued individually and that's a critical part of D&O cover. What have you done firstly to mitigate it, and secondly to prepare yourself for how you respond to it, is where directors really are at risk."

Lendlease group head of risk and insurance and RIMS Australasia president Kevin Bates says most directors are alert to the evolving risks that cyber presents. "Directors are acutely aware of personal accountability and, therefore, exposure that does exist in areas which were previously deemed as 'emerging', such as cyber," he explains. "They're asking the correct questions and taking appropriate mitigation."

Bates says a key element of Lendlease's approach to cyber risk has been to focus on business resilience and disaster recovery.

"It's like drug testing in sports. You actually don't know what you're going to find, which means that the hackers – or the cheaters in sport, for example – will always be ahead of the testers, or indeed the programmers in this case."

In the event that something does happen, he says, the important question is: "Can we be back up and running quickly?"

PCCW head of risk management and compliance David Ralph agrees that resilience is key. He recommends risk managers treat cyber like any other risk to help their directors minimise personal liability. "Our job as a risk manager is obviously to provide them with adequate defence as well as good advice on how to stop things from happening," he says.

When it comes to their D&O policy, risk managers are most concerned about how any claims against directors and officers will be controlled and settled (56%). Almost as concerning (54%) is whether the policy will respond to claims in all jurisdictions.

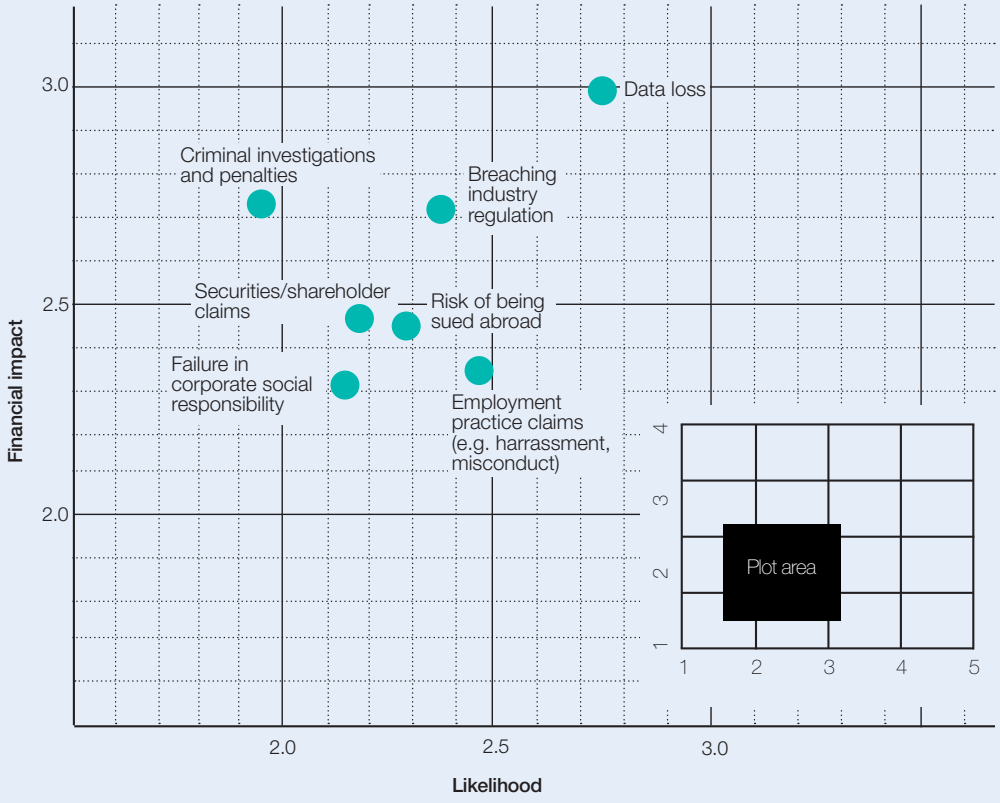
When asked about industry regulation breaches – the management liability risk ranked second – the panel's responses were mixed. The most frequent answers, in terms of which regulatory risk their company was most concerned about, were corruption and anti-money laundering. Many in Australia also cited new mandatory data loss legislation. "With technology constantly evolving, I am concerned with the raft of regulations which will have to come into play to govern this," one respondent said.

Another listed their company's top concerns as "breach of privacy and newly introduced mandatory reporting laws, corruption (especially with regards to supplier landscape and potential customers)" and "dealings with government entities in legislated areas".

IN THE LINE OF FIRE

HOW THE PANEL VIEWS POTENTIAL THREATS TO EXECUTIVES

DIRECTORS' AND OFFICERS' RISKS



METHODOLOGY

Respondents were asked to rate a series of risks to directors' and officers' liability, by likelihood and financial impact on a scale of 1-5 (1 being very low, 2 being low, 3 being medium, 4 being high and 5 being very high). This scattergraph plots the average score for both likelihood and financial impact.

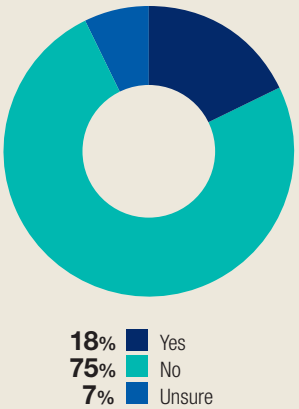
BIG NUMBERS

77%

The percentage of risk managers who say their board is more concerned today than it was two years ago about personal liability owing to a cyber breach.

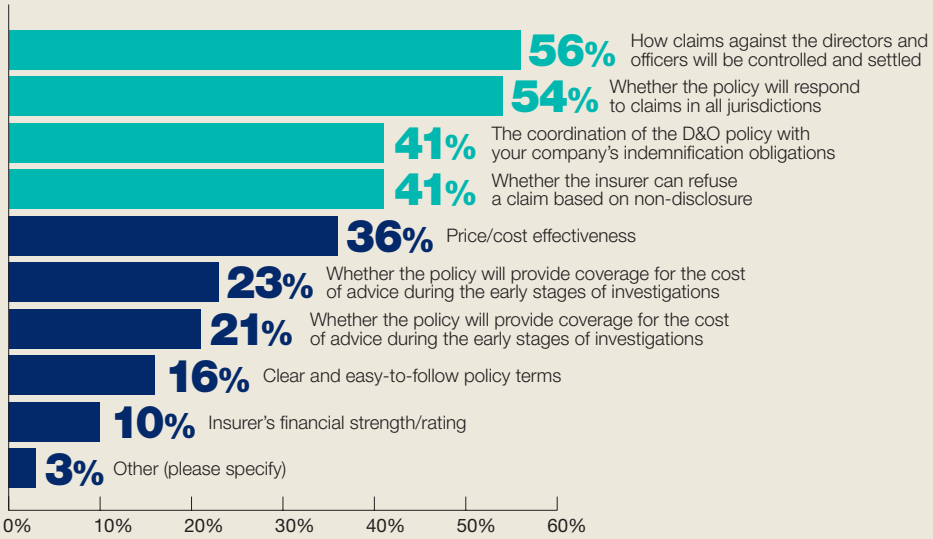
UNDER SCRUTINY

Has your company experienced a claim or investigation involving a director or officer in the past 24 months?



THEIR WORST FEARS

Thinking of your company's directors' and officers' insurance policy, what are your top three concerns?



Source: *StrategicRISK* Management Liability Survey

THE BIG QUESTION

Why more and more Asian shareholders are getting restless

An American cultural export, shareholder activism, could be one of the high-profile risks of 2017

If the power and influence of shareholder activism has so far passed you by, don't expect to remain in ignorance for long – it is picking up steam in Asia at a quite staggering rate.

Across Asia, the phenomenon inspired 77 campaigns in 2016, a 48% uptick compared to the previous year's 52, according to Activist Insight and Schulte Roth & Zabel LLP's annual *Activist Investing* report. It suggests Asia could be going the way of the US, which witnessed 450 campaigns in 2016.

Just ask Japanese electronics and energy giant Toshiba, which faces a damaging lawsuit in the wake of the accounting scandal that surfaced in April 2015. Four major trust banks – Mitsubishi UFJ Trust and Banking, the Master Trust Bank of Japan and units under Sumitomo Mitsui Trust Holdings and Mizuho Financial Group – are seeking compensation, running into billions of yen, after the book-padding issue hammered Toshiba's share price.

TWO OF A KIND

So, what exactly is shareholder activism? In a joint statement to *StrategicRISK*, Steven Balet, senior director, strategic communications, Perth, and Jason Frankl, senior managing director of the Forensic & Litigation practice at FTI Consulting, identified two distinct types: economic activism, and governance and/or social issue activism.

"Economic activism is frequently led by hedge funds and often calls on the company to make a change that the hedge fund believes will create value for the company in the shorter term," say Balet and Frankl.

"This type of activism may call for a company to sell itself, conduct stock buybacks, spin or sell an asset, or cut expenses and make other operational changes."

The second type of activism concentrates on governance and/or social issues. As the two men explain: "These campaigns are often led by individuals, pension funds or unions.

"Although these are two separate types of activism, they may, and often do, overlap. In fact, we have seen cases of pension funds partnering with hedge funds in activist campaigns at companies."

Jeremy Leibler, partner at law firm Arnold Bloch Leibler, says shareholder activism is not new: "However, in the last five to 10 years, it has become an established and recognised asset class, which is now starting to gain mainstream acceptance, particularly in the US.

TAKEN TO TASK

Case	Commenced	Description	Outcome/Status
Aristocrat	**2003**	Shareholders alleged that the company's financial accounts were incorrect due to the inclusion of certain revenue in circumstances not permitted by accounting standards, and that the company did not have reasonable grounds for statements made about its expected profitability.	The case settled in August 2008 after trial (but before judgment) for $136m plus $8.5m in costs.
Multiplex	**2006**	Shareholders alleged that the company did not properly disclose the full extent of significant cost increases and delays (or the risk of significant cost increases and delays) in the construction of Wembley Stadium, London.	The case settled in July 2010 (three months prior to trial) for $110m (including costs).
AWB	**2007**	The shareholders' claims were based on an alleged failure to disclose AWB's payment to an Iraqi entity in circumvention of UN Security Council resolutions and the making of allegedly misleading or deceptive statements in relation to the company's dealings in Iraq.	The case settled in February 2010 (three days into the trial) for $39.5m (including costs).
Centro	**2008**	Investors alleged that the Centro companies did not adequately disclose the full extent of their maturing debt obligations and the risk that they might not be able to refinance those debt obligations at forecast cost or at all.	The case settled in May 2012 (midway through the trial) for $200m (including costs).
National Australia Bank	**2010**	Shareholders alleged that the bank failed to disclose provisions for losses (or the need for such provisions) in respect of its exposure to more than $1bn of CDOs in the first half of 2008.	The case settled in November 2012 (weeks before trial) for $115m plus $12.5 million in costs.

CLASS ACTIONS

HOW THE NUMBERS STACK UP IN AUSTRALIA

- **467** class actions filed between 1992–2016
- **Class actions are increasing.** On average, 29.1 were filed each year from 2010–16, compared to 19.4 between 1992–2016.
- **The use of litigation funders has jumped.** No class actions were backed by funders between 1992-98; 49.5% were funder-backed in Federal Court between 2010-16.
- **Class actions with funders boast high settlement rates.** 92% compared to 48.9%.
- **Settlement times are rising.** Between 1992-2004, the time from commencement to settlement was 795 days; between 2004-16, it was 1,107.
- Between 1992-2016, 76% of funded class actions filed in Federal Court were brought on behalf of investors or shareholders.

* Statistics attributable to An Empirical Study of Australia's Class Action Regimes, Fourth Report: Facts and Figures on Twenty-Four Years of Class Actions in Australia by Professor Vince Morabito

"What's really fired things up is the willingness of institutions to team up with activist funds and activists to agitate for change in companies."

Jeremy Leibler
Partner, Arnold Bloch Leibler

"What's really fired things up is the willingness of institutions to team up with activist funds and activists to agitate for change in companies."

Josh Black, editor-in-chief of *Activist Insight*, says a number of factors lie behind shareholder activism's recent growth. "Investors have been expected to take a more proactive role in supervising corporate governance since the financial crisis," he says, "while in the US, regulations limiting the type of information companies can provide to major shareholders and mandating proxy voting have made the broader shareholder base more interventionist and friendly to shareholders who hold management to account."

Japan and Australia in particular have seen this rising tide – and in Balet and Frankl's view, other Asian countries should expect the same.

"As more countries are changing their corporate governance rules to allow for greater shareholder engagement with companies, we expect more activism to follow," they say.

Black says relatively transparent markets are likely to see more activist activity in the coming years, especially where corporate scandals have tarnished management. He adds: "Singapore seems to be becoming a more active market, albeit partially led by local investors. We have also noted some activism in China, although controlling shareholders and government policy will likely limit this."

Leibler says that the nature of the activism may manifest itself differently in light of the cultural differences between the US and Asia, as it has in Australia: "American funds are more litigious and more aggressive, where in Australia much of the activism is taking place behind the scenes, and I'd expect to see that quieter, more subtle approach adopted in Asia."

DISAGREEMENT

Why might shareholders try to influence a corporation's behaviour? Chiefly, to unlock or enhance shareholder value by changing the firm's behaviour.

Most activism comes from shareholders disagreeing with the pace or direction of strategy. In some cases, there could be opposition to management; at other times, activists want to see a firm sold or think management is selling it too cheaply.

So, how should a company prepare for this as part of its risk mitigation strategy?

"By analysing its actions from an investor's perspective," say Balet and Frankl. "This is slightly different than analysing from the perspective of an activist.

"A company must communicate to the market in a way that highlights the thoughtfulness of the board's evaluation of the issues and the changes they have discussed and implemented.

"In the end, all activist campaigns are about whether change is needed at a company. In order to properly prevent or defeat activism, a company must have communicated the changes they have made."

Black agrees that perhaps the most critical thing a company can do is to communicate its strategy clearly and heed traditional shareholders' views.

"Boards should also question management decisions and ask themselves those questions that an activist is likely to ask," he says. "Several advisory firms will review the composition of boards to give the broader shareholder base's perspective."

Black adds that in an activist situation, independent directors are likely to have to justify their actions separately from management, so it helps to put some distance between the board and the CEO.

Leibler says companies must deal with any governance deficiencies that could be used as a point of leverage. "When boards look at themselves in the same way an activist might look at them, that means avoiding any inconsistencies between their public disclosures and other public statements, and developing and implementing sophisticated, meaningful shareholder engagement policies," he adds.

Should it garner enough high-profile victories, shareholder activism is set to snowball across Asia. Risk managers would be well advised to prepare for this.

THE NEXT TREND

Cyber defences not up to scratch? Maybe we'll see you in court

Increasingly, plaintiffs in the US are suing company directors for cyber breaches. They haven't yet gained a scalp, but boards and insurers worldwide worry it's only a matter of time before they do

Earlier this year, a listed Australian company took out a cyber insurance policy. No big deal, you might think: corporates are increasingly looking to insurers to transfer their cyber risk. What makes this purchase interesting is that previously, the business spurned such standalone cyber products. So, why the change of heart? A key reason was to cover individual directors' accountabilities and responsibilities, the company's risk manager told *StrategicRISK*.

It's a clear sign that boards are wising up to the possibility that they could be held personally liable for a cyber breach.

"The more that the public becomes aware of the dangers of how vulnerable data is and how sensitive data can be protected, companies will be running out of excuses for failing to protect that data, and eventually that liability will fall with the directors personally," says Aon Risk Solutions' financial services and professions group Asia director, Andrew Mahony.

Consider the US. To date, four cases have been brought against directors in relation to cyber hacks, with Target and Home Depot executives involved in recent cases. These were dismissed and settled out of court, but many think it is only a matter of time before a precedent is set, with the advent of regional legislation that requires companies to report data breaches. "We're keeping an eye on [the US] to see how cyber risk will materialise and change and how insurance policies will respond," Mahony says.

Alex Morgan, Zurich commercial insurance chief underwriting officer, says: "The minute that we have a finding which really articulates the plaintiff's complaint and how the plaintiff draws the connection between the breach and the directors' actions, I think that will be something of a watershed moment."

Client queries about how its directors' and officers' (D&O) insurance policy would respond to such an incident are rising, he adds. "Board members are realising that the financial impacts [of a cyber breach] are huge, and therefore they're worried they'll be potentially in trouble as part of their fiduciary obligations. The extension of that is, they know they've got to buy D&O – and if a cyber event does happen, they want to know if their D&O will cover it.

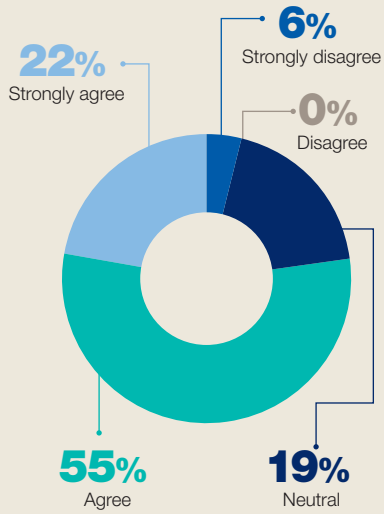
"Good policies won't have any specific exclusions. To the extent that an individual director is held personally liable for a loss [where the] underlying cause is a cyber breach, then it should be covered."

REWRITING THE RULES

In lines such as property and energy, many insurers have redrafted policies to exclude cyber events and thereby silo off the risk. Both Mahony and Morgan told *StrategicRISK* they did not expect a similar move in the D&O market. As Mahony says: "D&O policies are really quite unique in terms of the personal cover they give and provide. There's no clear merit in trying to distil out cyber risk or related claims."

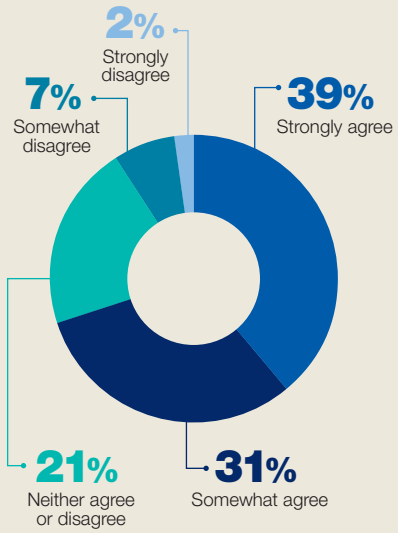
TIME TO THINK

To what extent do you agree with the following statement: "Our board and senior management is more concerned about liability owing to a cyber breach today than 24 months ago."



Source: *StrategicRISK* Advisory Panel Management Liability Survey February 2017

Do you agree or disagree with the following: "My company's board needs a better informed understanding of the underlying causes of insecurity in the country where I am based."



Source: Economist Intelligence Unit Survey, 2017

THE KEY CYBER QUESTIONS ALL BOARDS SHOULD ASK

By Bryce Boland, Asia-Pacific chief technology officer, FireEye

1. Who is in charge of cyber security? Ask your CEO who is responsible, because if it's not someone's job to get done, it probably won't get done. The owner should then be able to address the rest of the questions.

2. What are the biggest risks we face and the potential business impact of these risks? Weigh what the business thinks are the biggest risks against your own assessment, and ask them why. Their answer should demonstrate they have thoroughly thought this through.

3. What is our plan to address those risks? If the board is taking its role seriously, it will champion a plan to address the most serious risks to the business. Without this support, changes for the sake of security usually fail.

4. When incidents occur, what is the process and at what point are executives notified, and when is the board notified and how? Incidents must be escalated appropriately. The board should know at what stage incidents will be escalated to them and know what's expected of them. If there is a significant breach, understand what the lines of communication will be, if they're expected to speak with the media, and how they are generally expected to respond on security issues.

5. What is the standard of care for cyber security in our industry? If your industry has cyber security regulations, you must ensure you are in compliance, but compliance is only a baseline. Many of the most devastating breaches strike fully compliant organisations.

6. How comprehensive is our cyber incident response plan and how often is it tested? Major breaches are often highly disruptive and create confusion. It's critical that the right stakeholders are identified in advance and have prepared. Who will be the external face? Is customer support prepared? Are communications and legal involved?

7. What resources are in place to assist during major security incidents? Look for legal support with cyber security expertise. Consider having your law firm engage forensic investigators directly so their work can be protected by attorney-client privilege, if that applies to your jurisdiction. Identify a crisis communications team with significant experience in this area.

Take, for example, the Australian company that purchased standalone cyber insurance recently. The concern was not that its D&O policy would not respond to a cyber-related claim. In part, the directors wanted to limit their personal liability by showing that they took the risk seriously.

Pierre Noel, chief security and privacy officer for Huawei and treasurer for the Pan-Asia Risk and Insurance Management Association, agrees that insurance plays a critical role in mitigating cyber risk as it relates to personal liability. He recommends a three-pronged approach: "One, educate the board so that they have a thorough understanding on the liabilities and implications. The 'I did not know' is not applicable any more (at least in most countries). Two, board directors have to ensure the organisation is deploying a proper cyber-security programme, with mechanisms commensurate to their assessment of the risks. Three, [an insurance] policy to cover board directors and a policy to cover cyber risks within the organisation, reflecting the efficiency of the cyber risk management."

Noel stresses that no organisation is immune to a cyber security incident. He adds: "As long as we can demonstrate that the board was concerned about cyber risks [and] paid real attention to the problem and its resolution, board members are, by and large, immune to personal liability issues."

David Ralph, PCCW head of risk management and compliance, concurs. He says: "Provided that we are putting in place adequate measures to identify such risks and taking reasonable and appropriate measures to mitigate them, then there's a reasonable argument that the directors and officers are going to be reasonably well protected against any personal liability."

But while directors recognise liability for a cyber breach as a corporate responsibility, he says many have not linked that back to their obligations as a board. "Over time, we'll see it developing out that way, especially if we do see start to see cases of it being brought specifically against directors in their failure to ensure that controls are in place to protect data." For the moment, we're seeing "executive officers falling on their swords, rather than directors being held accountable".

Many believe that this is bound to change. Indeed, regulators in Asia-Pacific are taking a tougher stance on data protection, says Zurich's Morgan.

"They're following the lead of their US and European counterparts and bringing in data protection regimes. People realise that this is an urgent threat and now you've got politicians responding," he says.

Australia's Senate recently introduced legislation that compels certain companies to notify customers and authorities of any data breach. And a firm could, in theory, be subject to a civil penalty for a breach of the country's Privacy Act, says Allens managing associate Valeska Bloch – if, for example, a board knew that there was a significant risk but failed to act in advance.

The Act states that directors must have "appropriate" oversight of cyber risks. But how do you define "appropriate"?

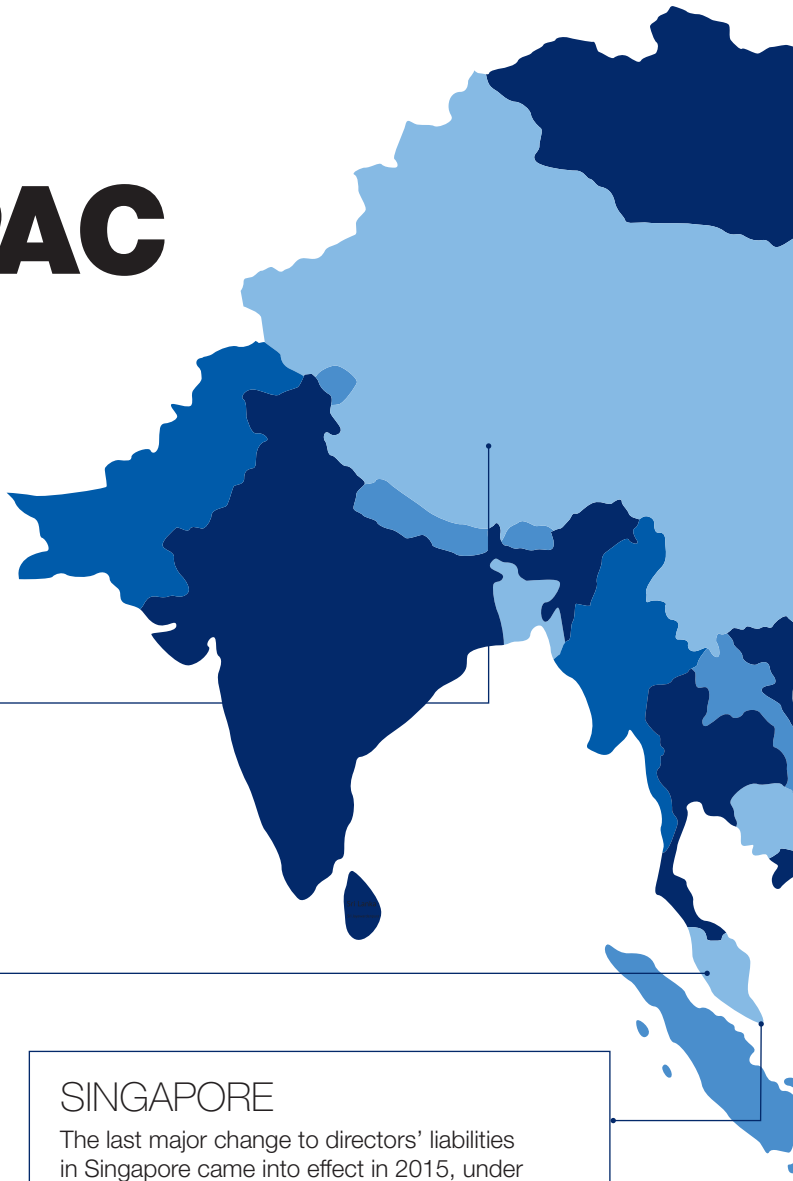
"The first thing is making sure that you are aware of what the risks actually are," says Bloch. "A central part of that is being aware of the systems that the business is reliant on, the data that they possess or control or have access to, and then understanding the different potential points of vulnerability." She says boards must ensure the company has a range of systems, processes and procedures in place to deal with those risks, and keep them updated.

It seems clear that directors will be held increasingly liable for a range of emerging risks, including cyber. It's only matter of time before one of them's on the hook.

THE WIDER PICTURE

The rough guide to APAC regulations

On a country-by-country basis, we look at the shifting rights and responsibilities of Asia-Pacific's directors and officers



CHINA

D&O insurance was introduced into China in 2002 by Ping An Insurance and Chubb Insurance. Uptake remains low, however, with only about 5% of Chinese listed companies in the country's A-share stock exchange having brought D&O insurance, according to reports.

But ongoing reforms to China's initial public offering (IPO) rules, coupled with the scandals of some Chinese companies listed in overseas stock exchanges, may see this change and uptake increase.

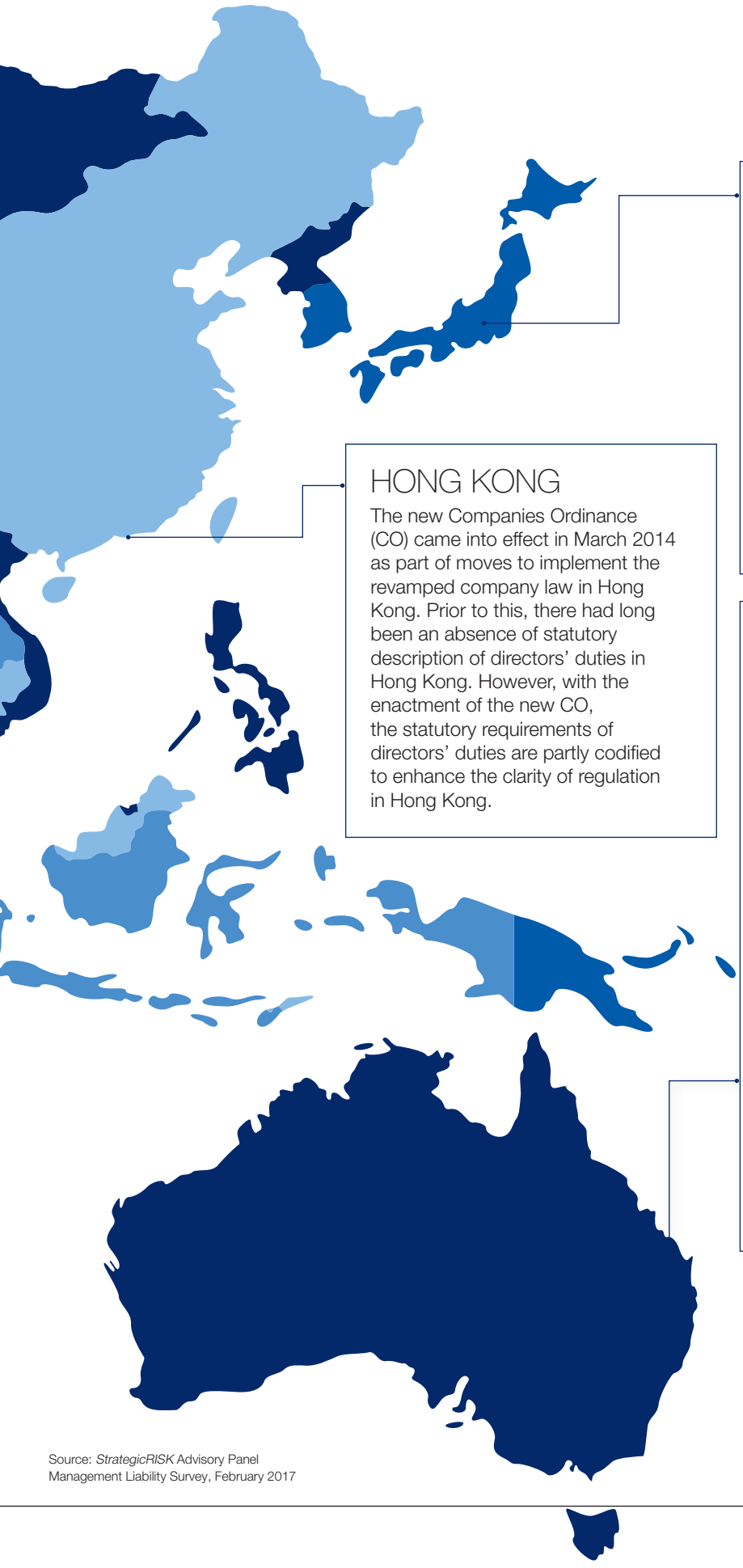
MALAYSIA

The introduction of the Companies Act 2016 marked a major milestone for corporate Malaysia. In line with international trends, the new Act, which came into force in January 2017, sets out a refined legal framework for the formation, operation and dissolution of companies. For directors, there is a general increase in the sanctions they will face for breaches. More serious infractions can result in a five-year imprisonment and 3 million renminbi ($435,000) fine, or both, if there is a criminal conviction. The Act also clarifies that a person is regarded as a director of a company if "the majority of directors of a corporation are accustomed to act in accordance with the person's instructions and directions". This would mean that any person who can instruct the company board on how it should act would be subject to the same duties and responsibilities as the directors.

SINGAPORE

The last major change to directors' liabilities in Singapore came into effect in 2015, under the Singapore Companies (Amendment) Act 2014. Among various legislative amendments, the definition of a director was widened and the maximum age limit removed. Two other key changes are:

- Directors' fiduciary duties were extended to cover the improper use of a director's position to gain an advantage for himself, for any other person or to cause detriment to the company (for which a director will be criminally liable).
- Companies are also now allowed to provide indemnity against liability incurred by their directors and officers to third parties. However, such indemnity cannot be provided for payment of fines in criminal proceedings, payment of penalties in respect of regulatory non-compliance, defending criminal proceedings where the officer is convicted, and defending civil proceedings brought by the company in which judgment is given against the officer.



JAPAN

In March 2016, Japan's National Tax Agency (NTA) announced a new tax treatment of premiums for directors' and officers' liability insurance. Typically, such premiums had been recognised in Japan as salary income. But under the new tax treatment, a company does not need to treat the amount of the insurance premium that covers shareholder derivative actions as a director's salary income, provided that the company bears the cost of the premium, pursuant to corporate approvals such as resolutions by a board of directors. It is reported that about 90% of listed Japanese companies had D&O insurance as of March 2015.

HONG KONG

The new Companies Ordinance (CO) came into effect in March 2014 as part of moves to implement the revamped company law in Hong Kong. Prior to this, there had long been an absence of statutory description of directors' duties in Hong Kong. However, with the enactment of the new CO, the statutory requirements of directors' duties are partly codified to enhance the clarity of regulation in Hong Kong.

AUSTRALIA

International law firm Clyde & Co has predicted a number of changes in Australia's directors and officers (D&O) market this year as more risks come into focus.

It predicts that soon, directors and officers could potentially be exposed to legal action for failing to properly account for the impact of climate change on their business.

In the words of lawyers Dean Carrigan and Yvonne Lam: "The relevance of climate change risks is heightened for D&O in industries such as insurance, energy and commodities, where the company's business model would be directly impacted by the increase in the frequency and severity of extreme weather events linked to climate change."

A second emerging risk that could play a role in the D&O market is cyber.

In February, the country introduced mandatory data breach legislation. Potentially, this could result in financial exposure and reputational damage to the company and its directors, who may incur personal liability as a result of any data breach.

Source: *StrategicRISK* Advisory Panel Management Liability Survey, February 2017

THE UNDERINSURANCE ISSUE

Telltale signs that your D&O cover is inadequate

Just how big an issue is D&O underinsurance, and should Asia-Pacific's directors and officers be worried about it? Game-changing legal cases may provide the answers very soon

Sometimes it feels like the problem of underinsurance is overstated. A cynic might even suggest that it's largely a ruse, cooked up by the insurance industry to scare corporates into buying more policies.

However, while it may be simplistic to suggest that the whole of the corporate landscape is affected, it does seem to be the case that in some areas more than others, underinsurance is an issue.

Take directors' and officers' (D&O) insurance – a contentious concept that has long been a standard product for large corporations. Without it, the argument goes, managers could not make major decisions without the threat of personal liability hanging over them.

But just how big an issue is D&O underinsurance?

"Historically, there's been a perception that the risk is low and therefore companies do not need to take out much cover," says Alex Morgan, chief underwriting officer, commercial insurance, Japan, Zurich.

"The average limit profile of Asia firms is significantly smaller than that of US or European firms. Particularly in countries like Japan, where historically, individual directors had to pay a portion of the premium as a fringe benefit. So they just didn't buy very big limits."

In Australia, says Morgan, people understand that there are big exposures, so the country doesn't have the same underinsurance issue as the rest of Asia.

"They buy small limits [in Asia] and that's because they underestimate the level of exposure they've got, but we're potentially seeing a couple of game-changers floating around," he adds.

One, perhaps, is a civil lawsuit brought by the Securities and Futures Commission in Hong Kong against Citic in 2014. The allegation is that in 2008, Citic Pacific, as it was then called, failed to disclose at once that it had lost billions of dollars from a currency hedge gone wrong.

A ruling on the case, expected in the first quarter of 2017, could result in five company directors paying compensation of HK$1.9bn ($245m) to 4,500 investors.

"This one's a potential watershed, because you have got the regulator taking a much more proactive role in the prosecution," says Morgan. "You have got a suit that looks a lot like a class action … and it's got big quantums.

"The number is huge – $245m. If this judgment comes down against it [and] the directors are forced to pay, then that will show what we as insurers have been saying for a while: you really do have big exposures."

Morgan says risk managers and directors often underestimate the defence costs in such investigations.

BANDWIDTH PROBLEM

A survey by Allen & Overy and Willis Towers Watson ('Directors' liability, D&O: The changing face of personal exposure'), indicates that 27% of respondents have experienced a claim or investigation involving a director of their company. For public companies, the figure is 39%, but only 10% of private firms have encountered such claims, according to the study.

> "It seems to me that there are only so many concerns board members can realistically be expected to keep at the front of their minds at any one time."
>
> **Francis Kean**
> Executive director, FINEX Global

"There may be a bandwidth problem or attention span deficit issue here for directors," warns Francis Kean, executive director in Willis Towers Watson's FINEX Global team. "It seems to me that there are only so many concerns board members can realistically be expected to keep at the front of their minds at any one time."

For example, says Kean, areas such as corporate manslaughter, employment-related disputes and anti-trust claims tend not to feature prominently among directors' liabilities concerns. Nonetheless, they do pose a very real risk.

RIMS Australasia board member Eamonn Cunningham, formerly chief risk officer at Scentre Group, says the landscape for D&O liability is changing. These days much more is expected of officers, and directors in particular.

"This stems from the fact that the standard required from directors and officers has increased in the minds of those stakeholders that they owe a duty to," says Cunningham.

"Augmenting this increase in potential liability is the additional demands currently placed on directors and officers."

Furthermore, says Cunningham, there is always the risk that a programme written for one country may not precisely meet the risks – or, indeed, the regulatory requirements – of another.

"Having locally issued underlyers is usually a sensible approach in 'problem' countries. Care needs to be taken as to ensure that there is a complete understanding of regulatory requirements as the enterprise may face difficulties in getting claims paid," he adds.

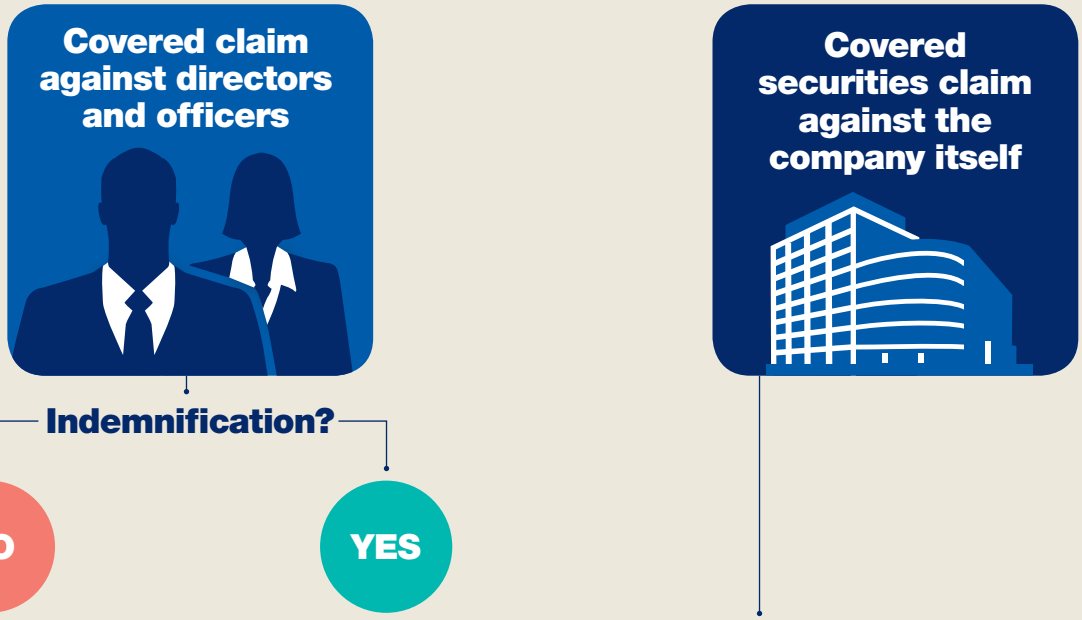
DEEPLY IMMERSED

So, how can the underinsurance issue in D&O cover be solved?

It is vital, says Cunningham, that the broad, deep enterprise knowledge expected of directors and officers comes from total immersion in the business.

PROTECT AND SURVIVE

THE STRUCTURE OF D&O INSURANCE



A QUESTION OF SCALE

Limits of cover will vary considerably based on the size of the company.

"This is particularly important for non-executive directors. Board chairs must lend a hand to facilitate this process. The best board decisions come from debates underpinned by an expansive, relevant knowledge base," he says.

"Reliance on an insurance programme can only come from a comprehensive understanding of the liabilities that could potentially arise."

Cunningham says external risk advisers can complement the efforts of board members and officers in mapping out risk scenarios' nature and loss potential.

> "If this judgment comes down against [Citic in Hong Kong and] the directors are forced to pay, then that will show what we as insurers have been saying for a while: you really do have big exposures."
>
> **Alex Morgan**
> Chief underwriting officer, commercial insurance, Japan, Zurich

Zurich's Morgan suggests that for companies to bridge the gap and make sure they do have the appropriate cover, existing policies need to be assessed regularly.

"Often the level of cover has not been discussed with the board," he adds. "It's a decision made by procurement or someone in risk management, rather than with the people that really require the protection.

"They should seek professional advice from brokers who do benchmarking and can look at limit adequacy."

THE SYSTEM

Who'd be a whistleblower?

Businesses should be pleased when staff report unlawful or unethical behaviour. So why are employees so often scared to come forward?

"Nothing is confidential," says a risk manager from a major global corporate, speaking to *StrategicRISK* about his company's whistleblower programme.

His admission brings into sharp focus the fears the many employees face when considering whether to report unethical or unlawful behaviour at their company.

Take Sally McDow as an example. The former senior compliance manager at Australia's Origin Energy alleges that the company has serious compliance failures at its gas and oilfields, a culture of leaks, spills and explosions, and a habit of intimidating anyone brave enough to speak out.

Her claim will be heard in the Federal Court, in the first ever case to test whistleblower protections in Australia.

Like many whistleblowers, McDow paints a distressing picture of her treatment. She claims management told staff she was being investigated and had "made stuff up". She further alleges that a recruiter told her she was unemployable in Brisbane as a "known" whistleblower, and that she should change her name or move country.

Sadly, it seems failures in company whistleblowing programmes are not uncommon. In a *StrategicRISK* survey of its Asia-Pacific Advisory Panel, 15% of respondents said their company's whistleblowing scheme was ineffective.

"More often than not, the identity will be revealed and shared among top management," one respondent said.

Another remarked: "In Asian culture, employees are not keen to make such complaints for fear that they be 'marked' by colleagues as a 'bad person'."

To prevent whistleblowers from being victimised, protection needs to be guaranteed and a culture of transparency and accountability must be promoted. But how can a firm ensure its whistleblowing programme is effective, particularly when operating across multiple jurisdictions?

> "The key message is allowing employees to have a range of different channels by which they can provide information – and at the same time, having a culture that really supports speaking out."
>
> **Lauren Witherdin**
> KPMG Australia forensic service

Lauren Witherdin, a director in KPMG Australia's forensic service, says it's important to consider any whistleblower programme as part of a holistic fraud and corruption control strategy.

"The key message around a whistleblower programme that's effective is allowing employees to have a range of different channels by which they can provide information – and then, at the same time, having a culture within the organisation that really supports speaking out, and whereby there's trust that the senior management will respond appropriately and take matters seriously," she says.

GPT Group chief risk officer Diona Rae says there are inherent difficulties in evaluating the effectiveness of a whistleblowing programme.

"If [there is] no use of the programme, does that mean [it is] ineffective or just no issues? We have used our annual staff survey to ask questions around confidence in the service, willingness to use it, etc."

The results of the survey are yet to be published, but it's worth asking what might dissuade some employees from using a whistleblower hotline.

Rae says: "They need to have a level of trust in the whistleblower officer, the policy, and indeed the organisation. It comes down to whether they believe the organisation will follow the process."

Astro Overseas vice president, enterprise risk management, Patrick Abdullah agrees. He says "the risk that confidentiality of the whistleblower is not maintained, and the whistleblower being subject to harassment or victimisation" would dissuade someone from using the company's service.

One can only speculate whether, with the benefit of hindsight, McDow would have used Origin's whistleblowing programme.

PIECEMEAL APPROACH

Legal protection also varies greatly from country to country. According to a 2015 DLA Piper report, Japan and China are taking the lead in Asia-Pacific, with express legislative provisions outlawing detrimental treatment of workers who blow the whistle.

Hong Kong offers no statutory protection; Australia does, but at present only through a series of general laws.

"Australia's piecemeal and limited approach to whistleblowers to date is out of step with the approaches adopted in a number of our larger trading partners, including the protections afforded to whistleblowers in the United Kingdom, the USA, Japan and China," DLA Piper employment partner Brett Feltham says.

This could change, though, since the Federal Government announced in its 2016-17 budget the introduction of arrangements to better protect whistleblowers, and a series of parliamentary hearings set for the first half of this year.

THE RIGHT THING TO DO

WHISTLEBLOWER PROTECTION REGIMES

	US	UK	Germany	France	Netherlands*	Hong Kong	Japan	China	Australia*	South Africa	Canada
Overall protection rating	★★★	★★★	★★	★★	★★	★	★★★	★★★	★★	★★★	★★★
Express laws	Y	Y	N	N	N	N	Y	Y	Y	Y	Y
General dismissal laws	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Protection against retaliation	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
External reporting encouraged	Y	N	N	N	N	N	N	Y	Y	N	Y
Internal reporting encouraged	Y	Y	Y	N	N	N	N	N	Y	Y	Y
Consultation on whistleblowing procedures required	N	N	Y	Y	N	N	N	N	N	N	N
Board/management investigation of disclosures required	Y	N	N	N	N	N	Y	N	N	N	Y
Government/ regulatory incentives to disclose	Y	N	N	N	N	N	N	Y	N	N	N

Little or no protection ★ Some protection through general laws ★★ Express protection ★★★

* Jurisdictions where new whistleblowing laws have been proposed. Source: DLA Piper Whistleblowing Law Report 2015

When the legislation is inadequate, how can companies ensure the anonymity of their whistleblowing programme?

One approach is to contract out the service to a consultancy. KPMG said 80% of its whistleblower reports over the past 12 months had elected to be anonymous.

Challenges remain, however. A risk manager whose company uses KPMG's FairCall whistleblower service said: "If people know that the tip has come from a whistleblower, there will be an internal hunt to find out who it is. For that reason, I now won't tell management that the report came from FairCall, just that the issue came up in our regular auditing process."

An ineffective whistleblower programme should also trouble company directors and officers. Feltham says that even where a programme is legally compliant, it may still fail to bring up internal issues.

"A programme which is ineffective in this way may potentially expose a company to corporate disaster, whether through substantial financial loss, product associated flaws/risks and/or reputational damage which could have otherwise been avoided," he says. "If those situations arise, then directors may themselves be held accountable for those events."

Another challenge for corporates is adopting a consistent global approach that accommodates differences in legislation and culture. In China and the US, for example, legislation provides financial incentives or bounties to the whistleblower if their allegations hold water. Employees in China are also obliged – by law – to report any suspected criminal wrongdoings.

Similarly, a multi-jurisdictional footprint may introduce difficulties in terms of the response, both from a language and logistical perspective. "If you've got matters coming in from all around the world, you need to be able to very quickly and efficiently respond within 24 hours," KPMG's Witherdin says. "That may mean mobilising on-the-ground investigation and legal services pretty quickly."

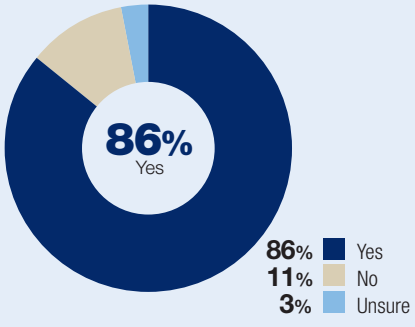
A perennial risk is that the hotline receives vexatious or frivolous reports.

"The important thing is to have the right triaging procedures in place to make sure that management time can be focused on the important and serious matters that are genuine," Witherdin says.

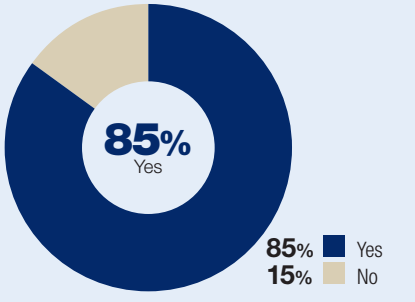
What is plain is that vast improvements need to be made across the board to improve whistleblower protections and corporate governance.

COME ON, BE HONEST

Do you have a whistleblower programme at your workplace?



In your opinion, is your whistleblower programme effective?



Source: StrategicRISK Advisory Panel Management Liability Survey February 2017

THE PEOPLE

TEN QUESTIONS EVERY COMPANY SHOULD ASK THEIR INSURANCE BROKER ABOUT DIRECTORS' AND OFFICERS' LIABILITY INSURANCE

Avryl Lattin,
Partner, Clyde & Co

1 What is an appropriate limit of D&O cover? The level of D&O cover your company requires will depend on a variety of factors, including: the ownership structure of the company (whether it is publicly listed or a private company); the size and complexity of the corporate group; the number of directors and officers you are looking to cover under the policy; and the location of your business operations.

2 Does the D&O policy include cover for shareholder class actions? For publicly listed companies, a D&O policy may be endorsed to include cover for the company for loss resulting from a securities claim brought by shareholders (Side C cover). If Side C cover is part of the aggregate limit under the policy, then it may be prudent for directors and officers to obtain additional cover for non-indemnifiable loss.

3 What is the period of cover under the D&O policy? The standard period of cover for a D&O policy in the Australian market is 12 months. A D&O policy will typically provide cover for claims made and notified during the policy period. Some policies provide cover for an extended discovery period.

4 Who is covered as an "Insured Person" under the D&O policy? A list of persons covered by the D&O policy will usually be set out in the definition of "Insured Person". You should ensure that all persons intended to be covered by your policy are captured by the definition. Policies typically cover directors and officers, shadow directors and employees of the company involved in senior management. Policies may also include cover for a range of other persons such as retired directors and officers, prospective directors and persons serving on management committees.

5 What "Claims" are covered under the D&O policy? "Claims" covered under D&O policies will generally include any written demand, civil proceeding, criminal proceeding and formal administrative or regulatory proceeding, and appeals from such proceedings. Usually, the claim must allege a wrongful act committed by the director or officer, acting in that capacity. Companies in certain industries may want to consider including cover for regulatory investigations (which may not always result in formal proceedings but which can be very expensive nonetheless).

6 What "Loss" is covered by a D&O policy? The D&O policy will insure a director or officer for various specific types of loss. Cover for reasonable legal costs associated with defending a claim is usually included but such costs may not always be advanced immediately. Some D&O policies are tailored to include cover for additional expenses such as public relations expenses, bail bond expenses and reputation protection expenses. Sub-limits often apply to these categories of expenses.

Generally, a D&O policy will not include cover for criminal fines or penalties, taxes or government duties, any multiplied portion of damages awarded or uninsurable matters.

7 What are the "Exclusions" under the D&O policy? It is very important to understand the exclusions that apply to your D&O policy and to ensure that the type of claims that may arise in respect of your business will be covered.

Standard exclusions include claims arising from an act, omission or dispute which occurred prior to the policy period which a director or officer knew, or ought reasonably to know was likely to give rise to a claim. Claims arising from deliberate acts of fraud or dishonesty are also commonly excluded.

8 How does the D&O policy apply to each director and officer? It is critical to understand how the policy works in respect of each individual director and officer. For example, if one director fails to disclose information which is relevant to the insurer deciding whether or not to issue the policy, will this result in cover being reduced or even denied for all Insured Persons? A number of D&O policies include "severability and non-imputation" clauses that ensure innocent directors and officers still have the benefit of the policy in such circumstances.

9 Do we need any specific extensions to our D&O Policy? You should carefully consider the potential risks your organisation and board face and discuss the type of tailored D&O policy you may require. Various extensions are available to cover specific types of liability such as prospectus liability, tax liability and breaches of privacy. You may also look for an extension to cover regulatory risks particular to your industry, such as occupational health and safety investigations.

10 Do we need a standalone defence costs policy? In certain Australian states, third parties may assert a statutory charge over insurance monies. At present, an insurer is not prevented from paying defence costs to a director or officer as a result of a statutory charge. But this issue has been decided differently in New Zealand and is yet to be considered by the High Court of Australia. A supplementary defence costs policy may prove to be a worthwhile addition to your D&O program and will also provide additional cover for legal costs incurred by directors and officers in the event that the D&O cover is exhausted as a result of a large liability.

EXPERT VIEW

BY **ALEX MORGAN**, CHIEF UNDERWRITING OFFICER, COMMERCIAL INSURANCE, JAPAN, ZURICH

THE CHANGING FACE OF MANAGEMENT LIABILITY

An increasingly litigious environment, a crackdown of global regulators and a broadening scope of risks and exposures. It's easy to see why some people argue that we're heading into a perfect storm when it comes to directors' and officers' (D&O) liability.

While no one can predict exactly how or where the changing exposures will come from, it's safe to say that the spotlight will continue to shine brighter on directors for perceived failings in corporate governance.

But first let's look at the two main drivers that will continue to underpin D&O claims. First, things that have material adverse impact on the share price, such as an earnings surprise or downgrade, or even an insolvency event. That is, when people lose money from investing in a business, they will often look to sue.

The second key driver of D&O claims is regulatory investigations. Regulators took a kicking in the aftermath of the financial crisis, but they've found their voice and they've got teeth.

From royal commissions to other public enquiries, and a growing body of heavy-handed regulators such as the Environmental Protection Agency, the Securities and Exchange Commission, the Financial Conduct Authority, and the Australian Securities and Investments Commission, there are an increasing number of players looking to show their worth and keep directors on the hook.

What all this means is that the exposures that are borne by company directors and officers in the future could look vastly different from how they look at the moment.

Gone are the days when a board could simply rely on their chief financial officer to tell them that their accounts made sense and wipe their hands of responsibility. In the wake of the global financial crisis, board members now have a proactive responsibility to have a basic understanding of, and be asking appropriate questions about, their company's financials.

It is likely only a matter of time before the same will be said for cyber, environmental and technology-related risks.

While no one is suggesting that board directors of the future will need to be cyber experts, they will need to ask the right questions to ensure their company puts in place the appropriate technology, people and processes to ensure the business is protected from the risk.

Environmental liability is another area that we expect to see more from in relation to D&O claims. There are many recent and well-publicised cases where public outcry over companies harming people or the environment has led to political pressure to hold individuals to account.

> "In the wake of the global financial crisis, board members have a proactive responsibility to have a basic understanding of, and be asking appropriate questions about, their company's financials. It is likely only a matter of time before the same will be said for cyber, environmental and technology-related risks."
>
> **Alex Morgan**
> Chief underwriting officer, commercial insurance, Japan, Zurich

Another major driver of D&O claims in the future will be related to technological change, which will leave many companies behind. When this happens and they begin to struggle financially, this is where you often see companies exposed to behavioral issues – the very kind that can be the linchpin of a D&O case.

Take Blackberry as an example. Only a few years ago, it was one of the dominant players in the mobile phone industry. Today its market share is zero.

These things happen so quickly – a company's flying high, it's raising money, it's spending money and then the market fails and it's gone. Or a company's been there for 100 years and then all of a sudden, disruptive technology makes it obsolete. That means the company no longer has the same value and how the board manages that delicate transition and communicates their plans to stakeholders will be critical in their good standing with shareholders.

While it is clear that the exposures to directors and officers will change to some degree, what will stay consistent is the basic premise that if you are going to sit on a board, you need individual protection.

As a purchaser of insurance, directors need to make sure that the insurer that they've chosen, and the coverage that they buy, maximises the protection that they've got available as an individual.

Of course, there are certain things that no board can control or change. But what it can control is keeping the market informed of the risks that the company is facing and the strategies that it is implementing in the face of those challenges in an attempt to future-proof the business.

Now, more than ever, clear and consistent communication and transparent corporate oversight will be put to the test.

ZURICH®

NOW YOU CAN KEEP AN EYE ON YOUR RISKS FROM ONE PLACE.

Protecting the business you love is easier when you have a clear view of what might affect it. My Zurich is an online portal that gives you 24/7 access to real-time claims data, the status of your policies and wordings, including benchmarking for risk engineering data, in a transparent way.

FIND OUT MORE AT
zurich.com/my-zurich

ZURICH INSURANCE.
FOR THOSE WHO TRULY LOVE THEIR BUSINESS.

ZURICH®

This is a general description of insurance products and services and does not represent or alter any insurance policy. Such products and services may be made available to qualified customers through appropriately registered companies of the Zurich Insurance Group in the Asia Pacific region, including: in each of Hong Kong, Singapore and Japan; Zurich Insurance Company Ltd (a company incorporated in Switzerland) which is registered in each of these territories; for corporate life solutions in Hong Kong, Zurich Life Insurance Company Ltd; in Malaysia, Zurich Insurance Malaysia Berhad; in China, Zurich General Insurance company (China) Limited; and in Australia, Zurich Australian Insurance Limited ABN 13 000 296 640.