insights

FINANCIAL LINES

ZURICH®

YOUR 10 MINUTES WITH THE BOARD...

...what issues should you be raising?

Also in this issue:

'BRIC' country developments – what is the effect on insurance

Cyber attacks beyond identity theft

Speaking the right language on multinational cover

Contents

Welcome

Welcome to this edition of **Insights** on Financial Lines.

Have you recently been invited to present to the Board? We understand that those ten minutes are crucial. To ensure you make every minute count in this insight we will share with you some of the top issues to raise with your Board members and Senior Executives.

We also look at cyber crime. This very topical issue goes beyond identity theft and the risks can be much larger with the potential to bring down organizations' entire systems. With our expertise and know-how we can help you protect your business from this type of crime.

We have all experienced fall out from the economic turbulence over the past three years. For Financial Institutions the shake up has paved the way for expansion via mergers and acquisitions. The opportunities are great for business, but have you considered the potential opportunities for fraud? Our article on page 16 gives some recommendations for detecting fraud and possible preventative methods to consider.

Organizations are constantly looking for ways to improve investment income and business growth. For companies considering expansion into emerging markets we bring updates on Brazil, Russia, India, China and the Middle East.

We hope you enjoy this issue and, as always, your feedback would be most welcome.

Keith Thomas
Global Chief Underwriting Officer, Specialty Lines
Zurich General Insurance

Step carefully
through the employment liability minefield

Employment Practices Liability Insurance can protect companies when disgruntled employees make claims against them. But what actions can be taken to avoid or reduce the risk of issues arising in the first place?

Companies face a growing challenge from disruptive and potential costly actions taken against them by present and ex-employees who feel they may have been wronged or unfairly discriminated against at work. Legislation to protect employee rights is becoming more stringent and widespread around the world and knowledge of those rights is also increasing. Unsurprisingly, the frequency and severity of claims is rising.

Zurich estimates that approximately 75% of employment practices liability claims come from former employees and 20% from current employees who feel their rights have been violated. The remaining 5% are made by prospective employees. These figures emphasize how vulnerable companies can be if they don't have adequate policies and processes in place that are reviewed and updated regularly. Many companies see the benefits of taking out employment practices liability insurance (EPLI), which protects against financial risk from claims based on employment-related discrimination, harassment or wrongful actions, such as wrongful termination, unfair dismissal or non-compliance with data protection laws.

Employers are often keen to settle cases before they reach the court so the amount they pay out isn't always made public. Zurich estimates that around 98% of cases in the US are settled without being disclosed, but the evidence of recent statistics and case studies (see over page) shows the number of claims and value of settlements are generally heading in an upward trend.

What can go wrong?

Typical actions taken by employees, either individually or in class actions, include:

- **wrongful termination and unfair dismissal, including constructive dismissal**
- **discrimination and sexual harassment**
- **equal pay**
- **retaliation/whistle-blowing claims**
- **deprivation of career opportunity**
- **employment-related misrepresentation**
- **failure to employ or promote a person**
- **emotional distress and mental anguish.**

Legislation tightens

EPLI cover began in the litigious US but is now in global demand, often by multinational organizations that need to manage complex requirements in all the legal jurisdictions where they operate. Employee protection is a high priority in the European Union, with its anti-discrimination directives, Australia and many other Commonwealth countries. Even China enacted a law in 2008 that enables individuals for the first time to take action against their employer for discrimination.

Furthermore, the scope of who is punished is broadening. Zurich estimates that in nearly one third of cases, it is not only the employer who is named in a claim but also individuals, including directors, officials, supervisors and managers.

Twenty years ago, with email in its infancy and use of the internet fairly limited, few companies had or needed policies to protect themselves and their employees in the use of technology.

Trends encourage claims

The current economic climate is causing many companies to reduce headcount and employees who have been dismissed may be finding it difficult to find new jobs immediately. Ex-employees may decide that they were, in fact, unfairly dismissed and/or discriminated against when losing their jobs.

Class actions are increasing, too. Mass litigation often represents good revenue-earning opportunities for lawyers so we are seeing more cases go to court. Changing demographics, especially in an ageing population, increase the risk of age discrimination cases while a general increase in employee activism and trade union influence is also fuelling a rise in cases.

Companies that employ larger numbers of workers, such as in the retail sector, typically face claims more frequently but the higher-value payouts have focused on cases involving individuals, particularly in the financial services sector.

New threats

The spread of new technology is causing unwelcome exposure to possible actions from entirely new sources. Twenty years ago, with email in its infancy and use of the internet fairly limited, few companies had or needed policies to protect themselves and their employees in the use of technology. Today, with the burgeoning growth of Facebook, Twitter and other social networking channels, it is essential to try and prevent claims ranging from breaching company confidentiality to harassment, discrimination and defamation.

It's all about people

Ultimately, employment discrimination is down to people and how they behave. A company can have the best and most stringent controls, but could still face a claim. However, if a case does reach court or tribunal and the company can show it has adequate policies in place, it trains its employees on how to behave in the workplace and always investigates incidents that are reported, then the company will be in a much better position to successfully defend the case or minimize the financial exposure if compensation is awarded, than would be the case if the company lacked robust procedures.

Robert Hill, Partner and Head of Employment and Pensions at Barlow Lyde & Gilbert LLP in London, has seen these trends develop in the UK in recent years: *"Undoubtedly, in the current economic climate, employment-related claims are on the increase. This has been caused by a combination of large-scale redundancies, a difficult job market and a greater appreciation of employment rights. Whilst there is very little a company can do to avoid employment-related claims altogether, having robust policies and procedures in place and ensuring that all employees receive training on those policies and procedures will minimize the risk of claims. As and when issues do arise, it is imperative that the matter is fully investigated and action is taken where appropriate."*

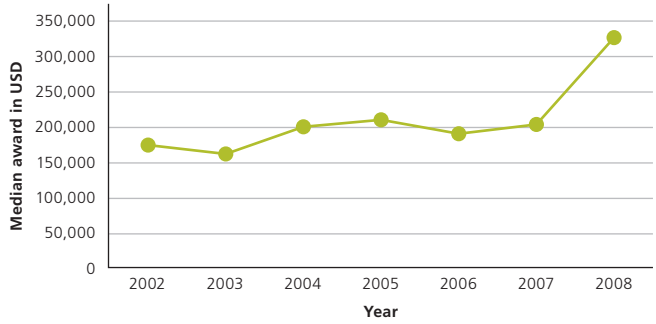
Take avoiding action

Reduce the risk of your employees taking action

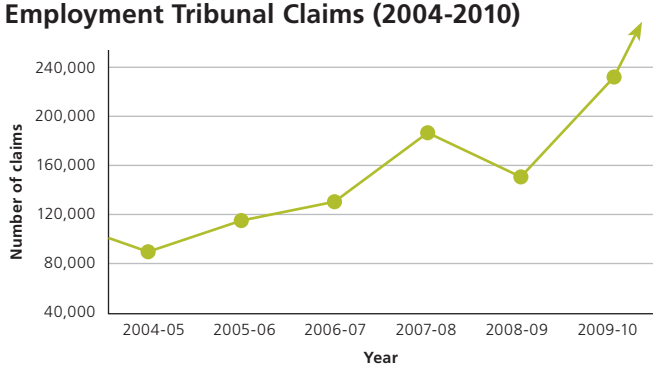
- Keep up with new and emerging legislation and trends, especially in new technology.
- Resolve internal complaints, especially if they involve potential class action allegations, before they turn into costly lawsuits.
- Set up a hotline for people who want to complain and encourage a culture of openness.
- Ensure diversity and anti-discrimination policies are enforced.
- Analyze employment data to remain up to date on key issues around hiring, termination, pay equity and promotions.
- Manage diversity initiatives consistently and compare your company statistics with the general labor market.
- Manage workforce reductions consistently.
- Ensure suitable equal employment and diversity training is available for employees and managers.

Claims on the increase

US claims – Median Compensatory Awards (2002-2008)



UK claims – Employment Tribunal Claims (2004-2010)



- **US Median Compensatory Award, 2008***
  USD330,000
- **UK Employment Tribunal Claims, 2010****
  235,000 claims

*Jury Verdict Research, 2009
**Employment Tribunal and EAT Statistics (UK), 2010

Class action succeeds over unfair redundancies
A French automotive component manufacturer had to pay EUR 4.3 million to compensate dismissed employees when it closed a factory in France and made 260 of its 450 employees redundant. The court agreed that the redundancies were due to economic hardship but ruled that this reason by itself did not justify the dismissals as the company did not sufficiently communicate possible alternative job opportunities to employees.

Workplace discrimination payout to 6,000 employees
A pharmaceutical company had to pay USD 175 million in a certified settlement class of 6,026 female sales employees who worked between 2002 and 2010. This was one of the largest ever workplace discrimination class actions.

Race case compensation for loss of future earnings
An Asian bank worker was awarded GBP 2.8 million in compensation by an employment tribunal after successfully claiming race discrimination against his employer, because he was targeted ahead of a similarly performing woman due to the color of his skin. More than half of his payout was to compensate him for future loss of earnings.

Sexual misconduct action
In Australia, a worker lodged a AUS 37 million sexual misconduct action against a well-known department store and its former chief executive officer. It was alleged that the Board knew the CEO was a workplace bully and serial sexual harasser and breached their duty of care to protect her. Following conciliation talks with the Australian Human Rights Commission, she was awarded AUS 850,000.

Christoph Leuzinger, Global Deputy Chief Underwriting Officer, Management Liability, Zurich General Insurance.

Robert Hill, Partner and Head of Employment and Pensions at Barlow Lyde & Gilbert LLP. Rob is a leading employment lawyer, with over 20 years' experience of handling all types of employment-related litigation in the UK, in particular Employment Tribunal claims for discrimination, whistleblowing and unfair dismissal.

Cyber attacks beyond identity theft

Over the past decade, cyber attacks have evolved faster than the speed at which most companies and organizations can build adequate defenses against them.

The exposures arising from cyber attacks have advanced at an equal pace. It should come as no surprise that cyber security is one of the top five risks to watch according to the Global Risks Report, 2011 issued by the World Economic Forum.

The financial impact associated with cyber attacks resulting in theft or disclosure of personally identifiable information is traditionally quantified by analyzing direct costs associated with breach response such as notification, credit monitoring, forensics, public relations consultation fees, and legal defense along with indirect costs such as loss of customer confidence and decreased stock price. Costs may also include fraudulent charges or other expenses to an individual that result from identity theft. Effective risk management can mitigate these costs; however, there are several additional exposures that have materialized that could prove to be more catastrophic in nature.

Data breach reports seem commonplace these days largely since legislation in the United States and European Union requires most organizations to disclose the loss of third party or employee personally identifiable information. While data breach and privacy laws are generally helpful, most are aimed at protecting the privacy of individuals and making them aware of instances in which their sensitive personally identifiable information has been compromised. As such, the general public may be less aware of different types of cyber attacks directed at businesses and government organizations that intend to:

- **take over industrial control systems**
- **damage physical machinery**
- **take control of networks that control critical infrastructure like traffic lights, power grids, water supplies, military networks, telecommunications, and financial systems**
- **steal valuable intellectual property like source code, business plans, designs, and information used in contract bids**
- **disable systems to create the perception of chaos.**

Such attacks have the potential to cause severe financial harm, bodily injury, property damage, and harm to credibility. Each one bears strikingly consistent characteristics in that they are perpetrated by highly organized, technically sophisticated, and well-funded groups.

Some recent examples of these attacks include:

Stuxnet (June 2009) – a worm took control of a global company's industrial control systems embedded in an Iranian nuclear facility. The virus caused centrifuges to spin out of control in the uranium enrichment facility causing physical damage to the hardware.

Night Dragon (November, 2009) – allegedly targeted global oil, gas and petrochemical companies, as well as individuals and executives in Kazahkstan, Taiwan, Greece and the US. The attacks extracted industrial intelligence from corporate network assets in the targeted enterprises, and are reported to have compromised a number of control system computers.

Anonymous (November/December, 2010) – a hacker collective known as 'Anonymous' allegedly launched Distributed Denial of Service attacks against a number of credit card companies, payment processors, and supporting vendors, it is claimed, in retaliation for their actions against the secret document disclosure website Wikileaks. The targeted companies suffered down time on their websites and some were unable to process online transactions for a short period of time.

Pentagon Attack (November, 2008) – a flash drive containing malicious code was allegedly inserted into a laptop at a US base in the Middle East. The code succeeded in uploading itself onto a network run by US central command. The code ran undetected on both classified and unclassified systems and intended to transfer data to outside servers.

Estonia Attack (May, 2007) – Distributed Denial of Service (DDoS) attacks disabled Estonian banking and government websites. At the time, 90% of all financial transactions were conducted over the internet, and 70% of the population of 1.3 million filed tax returns electronically. It is widely speculated that the primary goal of the DDoS was to damage the credibility of the Estonian government.

Impact

The potential impact of these events goes beyond the traditional response of providing notification, credit monitoring, public relations, and so on since the attacks are not focused on theft of personally identifiable information. Incident response to events like the ones outlined above may include:

- comprehensive forensics examination by a third-party organization
- repair or replacement of damaged property
- medical bills for physically injured parties
- lost time and allocation of manpower
- devaluation of intellectual property and trade secrets
- overhaul of network security programs
- overhaul of defense systems
- redesign/engineering of critical infrastructure
- personnel reclassification.

Catastrophic loss is estimated in many of the scenarios outlined above due to the systemic impact on a mass volume of individuals and property. Losses arising from such attacks could be quantified using not only financial impact, but potentially bodily injury and property damage as well.

The unknown elements

There are several elements associated with cyber attacks that cannot be easily quantified and as such, cause great alarm. For example, it might be easy to calculate the replacement cost of damaged property, but how would you quantify an economic loss if:

- a nation's power grid were disrupted or taken over for an extended period of time?
- a rogue nation state obtained real-time access to another country's military communications?
- a terrorist group obtained access to a nation's water supply?
- a competitor obtained access to intellectual property and trade secrets?

The answers to these questions are not easily quantifiable and therefore create additional concern. In the wake of several global, large-scale incidents, the US Pentagon recently declared cyber attacks to be acts of war and subject to traditional military response. While follow through remains to be seen, this declaration may help provide incentive for foreign countries suspected of state-sponsored attacks to curb their behavior and actively seek to do the same to rogue factions within those states.

An international issue

It is clear from the examples above that most developed nations share the same exposures when it comes to the risk of cyber attacks. Apart from the laws established in the US, many developed nations have already identified the exposure to individual data privacy and as a result, have enacted data protection laws. The UK Data Protection Act of 1998 (amended in 2003), for instance, was effected to control the permissible extent to which personal data can be compiled, collected and registered. Another example is the EU Data Protection Directive, which serves as a comprehensive, overarching law to protect the fundamental rights and freedoms of EU citizens, in particular their right to privacy with respect to the processing of personal data. Other jurisdictions with data protection laws include Austria, France, Germany, Ireland, Norway, Russia, United Arab Emirates, Japan, Korea (effective 9/30/11), Taiwan, Uruguay, Canada, Mexico, and Australia. The fact that these jurisdictions have passed such laws indicates a general awareness of the importance of protecting the privacy of individuals. However, many are also beginning to increase their efforts around securing highly valued intellectual property assets and critical infrastructure to mitigate the potential catastrophic loss from cyber attacks.

In what is considered the first of its kind in Europe, Germany recently opened a Cyber Defense center to protect its critical infrastructure including electricity and water supply. In a public statement consistent with the ideology of the US and other developed nations, German Chancellor Angela Merkel declared cyberwarfare "as dangerous as conventional war."

The North Atlantic Treaty Organization (NATO) has for some time considered cyber attacks among the greatest security threats to the developed world. Over three years ago, the organization announced the opening of a Cooperative Cyber Defense Centre of Excellence in Tallinn in the wake of the cyber attack that disrupted Estonian government and banking websites. More recently, the Estonian government incorporated a volunteer force named the ‘Cyber Defense League’ into its military structure.

Austria is in the process of building a cyber defense structure that will include 1,600 soldiers as well as several secret service departments while the Netherlands has allocated part of its armed forces budget to cyber warfare-related activities in 2011. The UK government has also allocated a substantial amount of funds to improve cyber security. Equally as concerned, France and China are increasing their efforts to fortify their nations' infrastructure to defend against cyber attacks.

Given the actions of these developed nations, it is resoundingly clear that cyber attacks are perceived as a legitimate threat to critical infrastructure and intellectual property on a worldwide scale.

Effective risk management techniques and risk transfer:

- Designate a senior executive with enterprise responsibility for management of information security.
- Use firewall technology at all points of presence and utilize formal firewall configuration standards.
- Utilize intrusion detection and prevention systems (network and host based) and update signatures and anomalies on a frequent basis.
- Deploy anti-virus software on all systems. Software should also detect and remove other forms of malicious software.
- Use commercial grade technology to encrypt data in transit and while at rest on the network.
- Prepare, implement and test a formal incident response plan.
- Prepare, implement and test a formal business continuity and disaster recovery plan.
- Analyze how to best transfer quantifiable risk and defend your organization from catastrophic exposures.
- Take steps to determine what risks are insurable and which must be self-insured. Are there policies in the commercial insurance market that would respond if an intangible asset depreciated as a result of a cyber attack?

Tim Stapleton
Assistant Vice President, Professional Liability
Product Manager, Zurich North America

Sources:

Examples of Attacks

http://blogs.mcafee.com/corporate/cto/global-energy-industry-hit-in-night-dragon-attackshttp://online.wsj.com/article_email/SB10001424052702304259304576373391101828876-lMyQjAxMTAxMDEwNTExNDUyWj.html
http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=1
http://www.computerworld.com/s/article/9200541/MasterCard_SecureCode_service_impacted_in_attacks_over_WikiLeaks
http://articles.cnn.com/2010-08-25/tech/pentagon.cyberattack_1_military-networks-cyberdefense-military-computers?_s=PM:TECH

An International Issue

http://www.theregister.co.uk/2011/06/16/germany_cyber_defence_to_defend_infrastructure/print.html
http://www.theaustralian.com.au/australian-it/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826

Your **10 minutes** with the Board **starts now...**

Top five topics to raise with your company directors and officers
If you are looking for insights into what key topics to raise and discuss with your board of directors and corporate officers, here are our recommendations:

1 The impact global anti-bribery statutes will have on D&O liability

Some countries have recently passed, and begun to enforce, anti-bribery and anti-corruption laws. Two such high-profile laws are the UK Bribery Act 2010 (which took effect on 1 July 2011) and the US Foreign Corrupt Practices Act (FCPA).

It is clear that the global enforcement of anti-bribery statutes has, and will continue to have, a dramatic impact on the liabilities of directors and officers (D&Os) of both local and global companies in more ways than one. Global companies might be subject to dual liability under anti-bribery statutes in their home country and abroad. In addition, for companies encountering foreign judicial systems caution must be used. What may be legal in one jurisdiction may be illegal in another, which can be confusing. For example, Ying 'Natalie' Zhang points out, "unfortunately, differences in the fundamental notions on which the US and China base their laws can confound American business people."[1]
It is paramount for D&Os to be aware of their global responsibilities and liabilities. It is no longer enough just to know what is legal in your home country.

How large is the exposure?
The top ten largest settlements under the FCPA between 2008 and the present, totalled USD 2.8bn,[2] with three very high-profile settlements amounting to between USD 185m and USD 800m. Recently there was a finding of liability in excess of USD 9m for violation of the Canadian anti-bribery laws. So when considering potential exposures, the sky really is the limit.

It is indeed in the best interest of companies and their D&Os to ensure adequate and effective anti-bribery compliance procedures are in place to help limit exposure. But of course, having written procedures and ensuring compliance with those procedures is two quite different things. Therefore companies and their D&Os must ensure there is proper training around these policies, a clear understanding in the company that anti-bribery procedures will be strictly enforced, dissemination of the policies and procedures to local subsidiaries and joint ventures, and of course, good internal audit.

What impact does this have for D&O insurance?
The D&O insurance marketplace is taking a cautious, 'wait and see' approach to the new exposures, but is anticipating significant increases in investigations (defense costs) and fines. The market is already seeing an increase in defense cost expenses as a result of the government scrutiny. We are also seeing an extension of coverage for certain insurable fines assessed against the D&Os as a result of bribery allegations. This coverage is usually sub-limited and largely applicable to non-indemnifiable loss only.

To find out more about the liabilities of D&Os in connection with the anti-bribery statutes of the UK, the US and China, view a three-part webcast series exploring these issues: www.zurich.com/globalfinanciallines/home/

[1] 'Complying With Chinese Anti-Bribery Law' 2006, Ying 'Natalie' Zhang
[2] FCPA Blog, June 2011

2 Do we have a truly global D&O insurance program?

If you are a global company with multiple subsidiaries domiciled in various countries around the world, or even a mid-sized company with a couple of subsidiaries domiciled outside of your home country, the short answer is likely to be 'probably not'. It is simply no longer tenable to argue that a global company with multiple subsidiaries domiciled in various countries around the world can rely upon one D&O insurance policy to legally and efficiently cover its global exposures. In order to ensure D&Os are covered for their liabilities around the world, local D&O insurance contracts must be issued in every jurisdiction where insurance law requires they be issued by a licensed insurer.

Directors and officers must understand that all D&O insurance policies carry a limitation (ie. exclusion) to pay loss only where such D&O policy is legally allowed to pay. This language can usually be found in the policy's definition of loss or in public policy. A carrier that does not (or cannot) issue local wordings in territories where such policies are required, instead simply stating it will 'endeavor' to pay the loss, is simply not providing a truly global program. D&Os would be running a serious risk that their claims may not actually be covered. D&Os need to have access to a global D&O insurance program where local policies are issued where required.

There is no shortcut from the requirements of a D&O insurance program. Therefore, it is essential to ensure you choose an insurer who understands the issues of international D&O programs, has the appropriate licenses and can issue the D&O contracts in the 'restricted territories' which are required, has the global claims network to manage the program and has the experience in servicing such programs.

3 D&O litigation trends – are the frequency and severity of claims increasing?

The number of D&O claims is on the rise globally. Recent reports indicate that many of these claims are governmental investigations, which means a significant increase in defense costs from historic numbers.

- A report by Aon cited 307 non-US D&O claims (15 of which were brought against subsidiaries of international parent companies) between January 2007 and December 2008.[3]
- An increase in D&O liability has been highlighted in more country-specific data released by Nera Economic Consulting, specifically within Australia, Japan, US, Brazil and Germany.
- NERA Economic Consulting has also reported an increase in securities class actions in Australia. The report states that securities class action filings in Australia set a new record in 2009, breaking the previous record set in 2008. The report goes on to state that a key factor in the recent increase in securities class action filings has been litigation funding companies. These companies act like an investor in the litigation providing up-front money to the plaintiff to fund the litigation. The litigation funding firms have clearly fuelled the increase in litigation in Australia, which is why directors and officers of UK PLCs should be concerned. It appears litigation funding companies now have their sights on the UK.

- In a separate report, NERA Economic Consulting discusses its findings about securities litigation in Japan. Total damages from misstatements in Japanese securities litigation cases rose to a record 45.9 billion yen in 2009 from 9.9 billion yen in 2008. NERA goes on to state that the "45.9 billion in 2009 is larger than the aggregate amount of securities litigation damages determined by court decisions in Japan for the entire previous decade."[5]

In the US there has been an increase in lawsuits against D&Os brought in state courts. For example, derivative actions, claims alleging breaches of fiduciary duty, claims arising out of mergers, acquisitions, and pension trustee / Early Retirement Income Security Act (ERISA) claims.

Brazil is a new concern. There has been a significant increase in governmental investigations brought against D&Os of Brazilian companies. We have particularly noticed an increase in investigations by the CVM (which is Brazil's Securities and Exchange Commission). Although generally the costs of these investigations are not on par with damage amounts in the US, they can still be substantial for an individual D&O. If that is not bad enough, Brazil requires a locally admitted D&O policy to be issued in order for coverage to take place.

The last country to highlight is Germany. German D&Os have always suffered from a significant number of claims brought by supervisory board members against the management board – the so-called Insured v Insured claim. German law makes it a legal duty for the supervisory board to bring such actions if they believe any member of the management board to have breached his/her duties to the company or the shareholders.

In summary, we are seeing an increase in D&O cases around the world as compared to historic numbers, for various reasons such as:

(1) local regulators becoming more vigilant in enforcing their laws and collecting fines and penalties;

(2) shareholder activism;

(3) extra-territorial reach of regulators making D&Os subject to more government actions outside of their home country; and

(4) new and more stringent requirements being placed on D&Os.

4 Why do we need D&O insurance?

A company and its D&Os must ask the most basic question 'Why do we purchase D&O insurance?' This may sound like a simple question with a simple answer – to protect the company's D&Os. However, it is slightly more complicated.

You would also have to question why the D&O policy contains coverage for costs of investigations into the affairs of the company, public relations fees, pre-claim investigation costs (which in many cases would be paid for by the company as a cost of doing business) and, oddly, costs incurred by the company in determining whether a derivative claim should be brought against the very D&Os for whom the policy has been purchased. Obviously the more non-D&O related losses are covered under the D&O policy, the quicker the limit of liability of the policy can be eroded or exhausted.

Some companies view the D&O policy as asset/balance sheet protection for the company itself, along with the D&Os, therefore the D&O policy would include coverage for the individual D&Os but also company reimbursement coverage and entity securities claim cover. This is a very different approach, which may open up and exhaust the D&O limits of liability for entity losses, rather than just loss of the D&Os.

Whichever your approach, the purpose of this quick article is to simply raise the issue and pose the question: ***'Why do you purchase D&O insurance?'*** The answer is a personal one for each company and its D&Os. It is the insurers, job to produce a product (a D&O insurance contract) that is tailored for each insured no matter what their answer is to the aforementioned question.

[3] 'Update on D&O Claims Outside the United States.' Aon, 2009

[4] Advisen Topical Report: European D&O Insurance Market to Benefit from Governance and Legal Reforms, 2011

[5] NERA Economic Consulting, 'Trends 2010 – Year End Update: Securities Class Action Filings Accelerate in Second Half of 2010.

5 Are all D&O insurers alike?

Today, there are over 50 insurers worldwide selling D&O insurance. This provides for a very competitive marketplace. It is important for D&Os to examine what they want from their insurer. Is price the only decision factor?

Directors and officers should look for an insurer who has:

(1) established itself as a leader in the D&O marketplace through its long-term presence in the market, product innovation, thought leadership and insights;

(2) a proven global footprint, and is able to meet the requirements of today's D&Os to provide valid insurance products on a global basis;

(3) strong global claims capabilities to manage the increasingly complex liabilities and claims of D&Os today;

(4) stable financial strength;

(5) an experienced underwriting team to provide top-level service.

In summary, it is important for an insurer to understand the strategy of a company in purchasing its D&O policy and then provide the best coverage possible to meet this strategy. It is equally important for the D&Os to understand what is being covered in their D&O policy. In short, ensure you read your D&O policy.

Paul Schiavone
Global Chief Underwriting Officer for Management Liability and Financial Institutions
Zurich General Insurance

Exposing fraud

in a post-merger financial world

Detecting fraud is difficult enough, but even more challenging for organizations following expansion through mergers and acquisitions. The recent upheaval in the financial services sector creates risks but also presents opportunities to thwart the fraudsters.

The massive shake-up in the financial services sector over the last few years has had a dual effect on expanded organizations. It has increased exposure to potential fraud perpetrated by employees while enabling them to expose dark practices that may have otherwise continued undetected.

Acquisition upheaval

Whenever there is a restructuring there could be an increased risk of fraud. Auditing practices have to adjust, processes must migrate and detection teams must combine across the merged organizations. This can create gaps in efficiencies as well as difficulties and delays in gathering data that could identify irregular activity. Multiple mergers often occur in quick succession, and when layered on top of each other can create an almost continuous process of re-organization.

Standards and guidelines that need to be applied post-merger can be hard to bed down, especially across international boundaries where different regulatory and legislative regimes are in place. These can make it challenging to impose new processes and policies designed to prevent fraud without breaking the law, for example on the use of CCTV, or rules on monitoring email and internet usage by employees.

A question of trust

Cultural resistance to new processes can be another stumbling block that increases the likelihood of fraud being committed if employees are resistant to changes in their work practices. The workforce has to have confidence and trust in the new regime designed to reduce fraud.

The bond of trust with customers can also come under pressure. It is not uncommon for managers to have continuous relationships with customers stretching back many years and even decades. This can lead customers to entrust managers with their assets and to make investment decisions on their behalf, while at the same time accepting lower standards of reporting on their investments. Such situations have an increased potential for fraud as well as non-compliance with internal or regulatory procedures that could lead to fraud that is hard to detect. Rotating staff is the obvious answer, but this has to be balanced with the negative impact it may have on customer satisfaction and loyalty.

Reliance on insurance

Fraud insurance transfers the risk of unexpected losses but it can make organizations complacent about taking steps internally to reduce these risks. There is also the question of the quality of service and cover the insurer provides. For example, an insurer may not indemnify a loss if it cannot prove a fraud has been committed. Finding proof that an employee has enriched themselves can be difficult and it may take time to gather the necessary evidence.

It is important that organizations are transparent with their insurance partner to avoid mis-matches in expectations on disclosure, loss prevention management activities and fraud prevention standards. The impetus for organizations to do this is that the cost of their premiums may be lower and their insurance cover will be of better quality if they demonstrate a good history of pro-active loss prevention management.

Inevitably, fraud will occur, but the efficiency of controls and measures to combat wrongdoing determines both the frequency at which it will occur and the likelihood that it will be discovered. Sometimes a simple change in what through the years have become routine checks and controls is enough to improve the likelihood of discovery.

Fraud prevention measures

- Audit branch networks regularly, including surprise visits.
- Find the most appropriate reporting structure – for example, auditors should report to other audit teams rather than senior executives, who may not be impartial if problems are revealed.
- Introduce remote controls and IT tools to monitor deviations from standard practice.
- Segregate duties so no single person carries out an entire process themselves – for example, granting and approving a loan application.
- Rotate employees to avoid complacency and bad practice creeping in.
- Set thresholds in authorizing funding so approval from senior managers is required if above a certain maximum limit.

Challenging times: potential fraud case studies

False credit

A corporate client manager credited funds on the account of a client against cheques provided by the client, but before they were actually converted into money. The cheques were eventually left unpaid, creating a EUR 21 million hole in the branch's accounts.

Too much trust

A branch manager gained the unconditional trust of clients, allowing her to dispose of clients' funds as she saw fit, which resulted in millions of Euros of investment losses. The manager then dipped into other clients' funds to cover the losses and created false statements, so the problem went unnoticed for several years. The difference between the artificial statements and the official ones was estimated to be around EUR 32 million.

No segregation of duties

A bank employee granted mortgage and personal loans in breach of the bank's internal regulations that caused an estimated loss of EUR 15 million. This was possible because they could grant and approve loan applications. The fraud was exposed when 18 loan applications were made from a single client with insufficient supporting documentation.

Giuseppe Donadoni
Senior Underwriter, Financial Lines,
Zurich Global Corporate Switzerland

Directors & officers insurance for banks in the Middle East –

an increase in demand

The impact of the global recession on the Middle East's banking sector, together with tougher regulations and an impetus to attract inward foreign investment, have combined to trigger increased demand for Directors & Officers cover.

The number of notifications of D&O claims in the Middle East's banking sector is rising rapidly and Zurich estimates it approximately doubles every two to three years.

Traditionally, banks in the Middle East have focused on bankers blanket bond coverage (BBB) for protection against first-party loss. This protects the bank against loss of money due to employee infidelity or clients acting dishonestly. Directors & Officers (D&O) insurance represents a new dimension by providing protection against third-party loss in the face of greater regulatory scrutiny, more stringent rules and tougher fines to back up wrongdoing. Demand for D&O cover is a response to the region's changing risk management landscape.

Personal protection

D&O insurance protects the personal assets of managers and their families from liability arising from a wrongful act committed in their managerial capacity. The policy can also safeguard the bank's assets if the claim relates to equities or bonds issued to raise capital. As well as external third parties, we are seeing a steady rise in claims from employees against directors and officers, particularly for dismissal following changes in employment terms due to the economic crisis.

The number of notifications of D&O claims in the Middle East's banking sector is rising rapidly and Zurich estimates it approximately doubles every two to three years. The type of D&O products for the Middle East market are similar to other countries but to be effective they need to include local content to comply with specific regulatory requirements in individual countries in the region. Some countries in the region are considering imposing a compulsory D&O insurance for all listed companies.

Responding to the global meltdown

The popularity of D&O insurance stems from the fallout following the global financial crisis, which impacted Middle East banks differently from the US and Europe. They escaped the worst of the devastating impact of toxic sub-prime mortgage debt and their balance sheets were generally not as over-leveraged. However, many lacked strong corporate governance infrastructures and suffered from poor lending policies, for example making loans with less scrutiny than would be required in the UK and US. So when greater liquidity was needed, a number of Middle East banks went bankrupt due to loan defaults and undetected fraud committed by customers that had gone undetected.

The Middle East is transforming its financial services sector with greater regulatory control to build its reputation and attract increasing volumes of foreign investment.

Regulatory change

As a consequence, the Middle East is transforming its financial services sector with greater regulatory control to build its reputation, protect bank assets from fraudulent attacks and attract increasing volumes of foreign investment. Financial services authorities set up in each country in the region provide a stronger regulatory backbone with more rules and disclosure requirements, greater transparency and better lending controls.

The effect has been to increase the risks faced by directors and officers who may find themselves personally liable if rules are breached. Officials now have added responsibility to implement risk management processes or face the prospect of fines and penalties. Greater diligence and accountability is called for. Banks listed on stock exchanges face the greatest scrutiny, although non-listed organizations are also encouraged to invest in greater governance – they, too, have suppliers and joint venture partners who could claim for wrongful acts, for example, on building and infrastructure projects that don't go according to plan.

Protecting human capital

The drive towards greater transparency and more regulation is essential for the Middle East to maintain the inward flow of human capital that helps the economy develop underpinned by a strong banking sector. Executives who have developed, their careers in countries where D&O cover is commonplace expect this protective shield in case they are exposed to claims. It is a therefore a good way to enhance the view that the Middle East economy is good for international investors and that, if things do go wrong, there is recourse through the courts and a legal system that has more clout than in the past.

With Gross Domestic Product across the Middle East expected to continue rising at rates as high as 5-10% per year in some countries, international investors are keen to take advantage of new business opportunities. The increase in demand for D&O insurance goes hand in hand with that positive development.

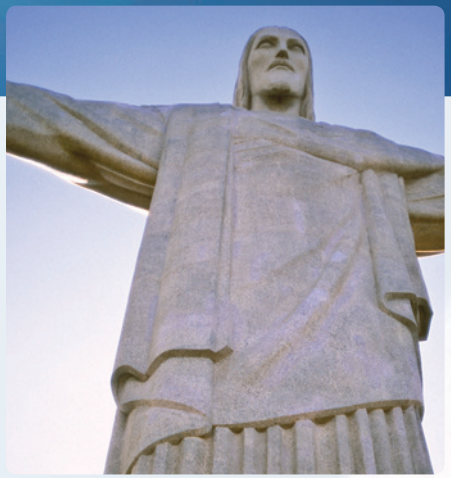
Dominik Bark, Head of Management Liability and Financial Institutions, Middle East & Africa
Zurich Insurance

COUNTRY DEVELOPMENTS –
BRAZIL, RUSSIA, INDIA & CHINA (BRIC)

what is the effect on insurance?

China is now the world's second-largest economy with a Gross Domestic Product (GDP) of approximately USD5.87 trillion. Russia is the largest global producer of many commodities. Brazil and India are in the news almost daily with reports of exponential growth.

With economic development comes increased regulation and fiscal supervision. In this article we take a look at recent changes to the laws in Brazil, Russia, India and China (BRIC) that may impact purchasers of financial lines insurance.



Brazil

The explosive growth Brazil has experienced is in part a result of the maturing of the country's capital markets where laws protecting minority shareholders' rights, for example, have garnered confidence. Investors are also freer to choose where to put their money; with pension funds (which hold assets of around USD 342 billion) they have been allowed to place money with alternative-investment firms since 2009. The country's growth looks set to continue with massive planned infrastructure projects, in part in preparation for the 2014 FIFA World Cup and 2016 Olympics, requiring USD 50billion of investments, many of which will be private.

Local hedge funds managed around USD 243 billion in assets at the end of 2010, up by 23% from 2009, according to the Brazilian Financial and Capital Markets Association, and private-equity firms oversee USD 36 billion. There has also been a significant appreciation in the real.

In 2010, the biggest-ever equity offering took place in Brazil, where Petrobras, the Brazilian state oil company raised USD 70 million. 11 Brazilian companies conducted Initial Public Offerings (IPOs) in 2010 raising US 6.4 billion. Despite rising inflation, Brazil expects about 30 IPOs in 2011 fuelled by GDP growth rate, the consumer and retail sectors, and government major infrastructure plans. Although the forecast is far below Brazil's IPO peak in 2007, more and more large companies are going public and the capital market is becoming more liquid and deeper.

This heating up of the capital market has had a direct impact on the insurance industry. Although Public Offering of Securities Insurance (POSI) is still a very new product in Brazil (it was first launched in 2007) the interest over this product has increased, in part due to the increased investigation powers over traded companies of the Brazilian Securities Exchange Commission (CVM).

In 2010 CVM regulations toughened transparency duties of listed companies towards investors and the CVM. One such rule established that publicly traded companies must disclose to the market information about any indemnification agreement or Directors & Officers insurance policies they may have entered into. It appears that the amounts sought by the CVM to settle an investigation under 'termos de compromisso' have increased since details about the level of insurance cover purchased by companies has become known to the CVM.

Since 2007 there has been a loosening of market regulations in Brazil when the Brazilian government implemented new rules to update and restructure its laws governing the reinsurance sector (Complementary Law 126/07) and eliminated the previously existing state monopoly on the reinsurance trade. The goal of these reforms was to open the local markets to increased competition and improve the availability of insurance coverage and lower insurance costs in Brazil.

The reforms make it more difficult to implement global insurance programs that are effective, as insurers may no longer be able to utilize globally accepted prudent risk management strategies to meet the greater insurance capacity requirements that will prove critical to the development of the Brazilian economy. Reducing foreign insurance capacity for handling large commercial risks in Brazil will drive up prices as it will be become more difficult and expensive for Brazilian insurers to access foreign reinsurers.

Russia

Of the four BRIC countries, Russia has arguably suffered most in the recent global financial turmoil, with Brazil, India and China remaining the most sought-after and talked-about investment jurisdictions in the world. One significant change that has taken place recently, which is designed to help Russia compete with the other BRIC members, is the overhaul of its anti-bribery and corruption laws.

Russia is currently ranked no. 154 on the Transparency International Corruption Perception Index. Of the BRIC countries, India is closest to Russia in the index, but is still a significant 67 places higher (number one being the country with least bribery and corruption).

On 4 May 2011, Russian President Dmitry Medvedev signed into law a measure that significantly increases fines for bribery in Russia and now specifically applies to bribery of foreign government officials. The new federal law is entitled 'Federal Law dated May 4, 2011 No. 97-FZ On inclusion of changes to the Criminal Code of Russian Federation and to the Code of Administrative Offences in Connection with the Improvement of Government Administration in the Area of Fighting Corruption'. Russia has also signed up to the Organization of Economic Co-operation & Development (OECD) anti-bribery convention.

The new legislation prohibits commercial bribery and both receiving and offering corrupt payments to foreign government officials, and therefore the new law appears to resemble the UK Bribery Act and has greater reach than the US Foreign Corrupt Practices Act (FCPA).

With respect to commercial bribery, the new law changes art. 46 of the Russian Criminal Code and imposes the maximum fine for bribery at the amount of 100 times the amount of the bribe (not to exceed 500 million rubles – approximately USD 17.8 million).

Prior to the amendment, the maximum monetary fine for acceptance or offering of a bribe was significantly smaller: 500,000 to 1 million rubles. The monetary fines for commercial grease payments ('podkup' in Russian) were even lower: the offeror could face a maximum fine of only 300,000 rubles or an amount equaling salary/other income for the previous two-year period, and the acceptor could face a maximum fine of only 1 million rubles or an amount equaling salary/other income for a five-year period.

It is hoped that the new laws will significantly reduce the level of bribery and corruption that can have a great impact on companies doing business in Russia. As with the Bribery Act in the UK, the impact of the new legislation will only be felt to the extent that prosecutions are pursued and sentences passed.

There is no indication in Russian legislation that it would not apply to overseas companies doing business in Russia. In other words, if an overseas listed company or its constituents engage in commercial or foreign government official bribery in Russia, the offenders would be subject to fines and potential incarceration in Russia and therefore executives should be interested to know the extent of cover they are afforded by their insurance policies.

India

Currently there are 34 international banks operating in India which, as on March 31, 2010, in aggregate, held around 10.52% of the total assets of all scheduled commercial banks (including credit equivalent of the off-balance sheet assets).

In January 2011 the Reserve Bank of India (RBI), India's Central Bank, published a discussion paper regarding the regulation of foreign banks in India, specifically in relation to the form any presence must take. Until now, international banks have established branches in India which does not entail establishing distinct legal entities in India. However, the proposals appear to envisage eliminating this as an option. The new regime would require each bank to set up a wholly owned subsidiary if the RBI considers the bank to be 'systemically important'.

It is envisaged that any changes to the regulation of foreign banks in India will be accompanied by new rules regarding corporate governance. In particular, it is likely that the changes will include

Until now, international banks have established branches in India which does not entail establishing distinct legal entities in India.

requirements that the members of the board of directors of a subsidiary of a foreign bank should satisfy certain criteria including:

- 50% of the directors should be Indian nationals resident in India
- at least 50% of the directors should be non-executive directors
- at least 33% of the directors should be independent from the management; and
- Directors must satisfy the RBI's 'fit and proper' persons test.

Such changes will bring significant differences to the way that the parent bank manages its operations in India and may impact upon the risk profile of the business that is conducted in India by the bank.

The deadline for submitting comments to the RBI was March 2011 but formal proposals have not been published at the time of writing.

China

Reforms in China touch on all of the areas where the other BRIC countries are making changes.

On 1 July 2010, the Provisions on the Administration of Reinsurance Business 2010, issued by the China Insurance Regulatory Commission (CIRC), became effective. These changed and strengthened some of the existing rules concerning reinsurance and indicated a move towards opening up the reinsurance market in China.

Offshore reinsurance restrictions were abolished. Up until 1 July 2010, insurers were required to offer at least 50 per cent of a risk to at least two domestic reinsurers in China before looking to overseas reinsurers. This severely restricted overseas reinsurers from participating to any great extent in China's reinsurance market. With the abolition of this requirement, it is anticipated to have a beneficial impact on insurance rates.

Perhaps most significant is the desire to encourage even greater overseas investment and in doing so China has recognized the need to improve its record on bribery and corruption. Executives' duties are under particular focus. In 2010 the Supreme People's Procuratorate and the Ministry of Public Security jointly published a notice regarding the thresholds for imposing criminal liability on the directors/managers of non-state owned enterprises due to commercial bribes. Although it has long been the case in China that directors and senior managers may be held personally liable for violating relevant requirements under the criminal law, such as giving or receiving money or valuable gifts for the purpose of seeking or offering improper benefits, the jointly published notice makes it clear that enforcement of these obligations is now high on the agenda.

The investment opportunities and potential for economic growth in the BRIC countries continues largely unabated. With the developments there have been in the last ten years there is inevitably greater regulation and also risk for overseas investors and their executives. Insurance provision locally and internationally has evolved to keep pace with the risks involved and has developed new structures to ensure compliance with local laws where the size of the risk requires the capacity of the international insurances to be involved.

Martin Butterworth, Partner
Davies Arnold Cooper LLP

Graham Ludlam, Senior Associate
Davies Arnold Cooper LLP

Hermes Marangos, Partner,
Head of International
Davies Arnold Cooper LLP

Katia Puras, Solicitor and
Brazilian Lawyer
Davies Arnold Cooper LLP

REFORMS IN Pension Trustee Liability

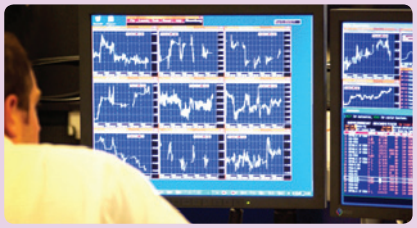
Trustees and administrators of occupational pension funds are responsible for running the funds for the benefit of beneficiaries. They must act in accordance with the trust deed and scheme rules, without being influenced by business interests. If trustees fail in fulfilling this duty, they could face fines by regulators, and be held personally liable. The sponsoring company of the pension fund could also be held liable in litigation.

Occupational pension funds are business as usual in some countries, for example US and UK. Companies domiciled within these countries should already be fully aware that charges could be made against their pension fiduciaries; therefore the use of insurance protection is already widespread. As Europe and other regions see a pace in pension reforms, systems may alter, leading to a stronger emphasis on occupational and private pension plans. This trend could lead to an increase in responsibility of pension trustees within these countries.

Currently, pensioners in most European countries rely on the state for their retirement income. In France for example, the state-run pension system, known as Pillar I, accounts for as much as 75% of a retirees' income. However, significant demographic changes in most European countries (including an ageing population and low birth rates) will have deteriorating effects on state finances. Rising concerns about the future value of pensions, due to significant stock market losses during the most recent economic crisis, have led to pension reforms across Europe in the recent years.

Demographic changes

- **Demographic changes create a demand for supplementary pension plans in addition to those provided by the state to generate sufficient retirement income.**
- Presently, 19% of the population of the Organization for Economic Co-operation & Development (OECD) countries are aged 60 or older. It is estimated that this age group will represent 26% of the population by 2020.
- **According to the French statistics bureau (INSEE), by 2060 1 in 3 inhabitants in France will be aged 60 or older, however the most progressive increase of this age group will be in 2035, mainly due to the aging of the so-called 'baby-boomer' generation.**
- In emerging countries, not only the life expectancy increases, but also there is a noticeable growth in the working population. At the same time, the social systems have changed in these countries. Previously, it was not uncommon that younger family members took care of the elderly, where as now the older population find themselves on their own when they reach the retirement age. These changes can lead a higher demand for insurance and pension products.
- **Furthermore, in France and many other countries, the gap between the number of contributors to the pensions and pensioners has tightened considerably. The OECD has found that while in 1975, 13 million contributed to pensions and 4.1 million received pensions, in 2008 17.6 million paid into the pensions and 12.2 million received retirement payments.**



Pensions in the public eye

The economic crisis has had a significant impact on the performance of the stock market, which in turn has impacted the performance of pension investments. In the UK, many pension funds did not reach the required funding level and were forced to wind up with insufficient assets to secure their liability. This created much negative publicity and strong political pressure to increase pension legislation and regulation. As a result pension regulators have become stricter and focus on the performance of trustees has been enhanced.

The need for reform

The aim of any reform is to decrease the pension burden on the state and shift responsibility to households to save through an occupational system where participants and employers pay into or through voluntary individual pension plans.

At present, occupational systems prevail in mainly English speaking countries, which is why we see the markets for pension fund investments predominantly in the United States and the United Kingdom. In addition, pension funds do already play a crucial in some other countries such as in Norway, Iceland and in the Netherlands.

Occupational pension funds are often run by trustees or fiduciaries, which are susceptible to be held personally liable in case of failing to manage the pension funds adequately.

Claims made against trustees are often based on the following allegations:

- Breach of trust or breach of fiduciary duties imposed by regulation.
- Wrongful omissions.
- Misstatements.
- Mismanagement.
- Negligence or errors in the administration of a plan.
- Conflict of interest between the plan and business.
- Improper advice or disclosure.

An increasing number of claims occur against fiduciaries of defined contribution plans who allow participants to invest in the company's stock. The risk of investing all or most of their pension funds in company stocks becomes apparent when the

company faces financial difficulties or even bankruptcy: the beneficiaries may lose all or a considerable share of their retirement savings. Typical allegations are that fiduciaries misrepresented the risk of investing in company stocks, or that the fiduciaries of the plan have allowed to invest in company stock although the company went through financial difficulties.

Remember

- Always provide the participants with a variety of options for investment – diversification is the key.
- If investment in company stock is an option:
  - ensure that participants are aware of the risks – especially when the company faces the risk of significant stock drops.
  - limit the possibility of investments in company stocks (investment caps).

With regards to defined benefit plans, many claims arise out of the alleged under funding of plans; that is, allegations that fund investments of the contributions of the plan participants did not match the benefits due. Many companies saw the funding levels of their plans decrease during the economic crisis of 2008/2009 as a significant share of investments were made during in the securities markets.

Another type of claim is the allegation of improper plan amendments or errors/ omissions in the transfer or closing of a plan. Claims often occur when the level of promised benefits change after amendments have been made to the plan document due to the merger of plans after an acquisition.

Claims example

In this case, the insured's pension scheme was in the processing of being closed, to which a run-off policy had been purchased. The insured was notified by the pension provider (to which the scheme had been transferred to), that they had received a request from a deferred member, that on turning 65 he now sought the benefits due under his pension. The pension provider however, had no details of this member, although the member was in receipt of a certificate from the trustees confirming his entitlement to a pension. From investigation, it was concluded that due to changes in computer systems and from a move to paperless files, the records were misplaced. It was deemed that liability would be attached to the trustees and therefore, according to the policy, the Insurer would meet the cost of the annuity with the provider.

Remember

- Don't put all your eggs in one basket – again diversification of investments is key
- When there is an amendment to a plan, communicate accurately and promptly.

Unlike an extension to a Directors and Officers policy, which can be subject to potential conflicts of interest between the directors of the sponsoring company and the pension trustees, a policy written based on the needs of trustees, known as pension trustee liability or fiduciary liability insurance, can specifically provide personal liability covers to companies' pension plan trustees for claims brought by beneficiaries, regulatory authorities or other parties and to sponsoring company reimbursement.

Many companies saw the funding levels of their plans decrease during the economic crisis of 2008/2009...

Maryam Kashani
Underwriter Financial Lines
Zurich Global Corporate France

Making sure that crime doesn't pay

Commercial crime is a massive global problem and one that can often remain undiscovered for years. Statistics are hard to come by, especially as it is often a loss that companies do not wish to be publicized.

According to the Association of Certified Fraud Examiners, the figures are extraordinary: survey participants from 106 countries estimated that the typical organization loses 5% of its annual revenue to fraud*. Applied to the estimated 2009 Gross World Product, this figure translates to a potential global fraud loss of more than USD 2.9 trillion. Nearly a quarter of the frauds involved losses of at least USD 1 million.

What's going on? Ways to spot crime within your business

Commercial crime takes many different forms. It may arise internally through employee fraud or theft, or externally with criminal gangs and cyber thieves. Past experience shows that there is an increase in criminal activity during an economic downturn, and companies should be extra vigilant about the possibility of employee fraud, especially where redundancies, cost savings, and salary freezes are being implemented.

There are some classic risk indicators that companies should be aware of, though clearly caution should be exercised before considering whether fraud is taking place:

- Employees over-stressed, working late, reluctant to take holidays.
- Employees with unexplained wealth or living beyond apparent means.
- Increase in customer or supplier complaints.
- Subsidiary results 'too good to be true'.
- Close relationship between individual employee and contractors/suppliers.

Beating the criminals

Overseas offices

Commercial crime often takes place well away from the head office, often in small subsidiaries and overseas offices, where the local manager may have considerable power, legally and/or culturally. There is also the potential problem of using ex-patriots from head office as managers where they do not fully understand how the local business works, or the local language and culture. It is, therefore, important not to forget about remote subsidiaries when it comes to internal auditing, as well as ensuring compliance with the corporate policies, especially in relation to approvals and authorities.

Successful divisions

Another area that requires careful attention is where part of the business, a subsidiary or a division, is doing extraordinarily well, to the point where senior management or the board of directors decide simply to let them carry on and often will ignore warning signs from internal auditors.

An example of this, which involved the collusion of senior management at a subsidiary of a major listed business, saw the alleged theft of in excess of USD 25 million over more than five years, which was overlooked by internal audit, partly because the subsidiary had been expanding and was extremely profitable.

Staff

Segregation of duties is an absolute necessity but it doesn't always happen. 'One person approves, another person executes' should be the rule, but all too often there are situations where individuals have been able to approve and execute on their own.

Often, it is about simple prevention measures. For example, in the case of the employee in a finance department who obtained the pass codes for online banking for all his colleagues, which had been left in an unlocked desk drawer. He personally only had access to the system for small payments, but because he had the pass codes for others, no approvals were required, and over several years he stole around USD 5m. Thorough reference checks for potential employees who will have responsibility for stock and/or money can reveal issues.

Whistle-blowing

Lots of companies will have whistle-blowing policies but they need to convince their workforce that these are meaningful. Allegations have to be properly investigated for the policy to be effective. And there must be no negative outcome for a whistle blower whose allegations are established to be unfounded when the whistle blower acted without malicious intent.

Companies need to be vigilant, and it is vital to check out potential suppliers and customers to ensure that they are who they say they are. It is all too easy to establish fake websites, premises, phone lines and so on.

External fraud – customers and suppliers

As far as external threats are concerned, one area that is a concern is where individuals/companies purport to represent genuine suppliers or customers, and defraud the company. Companies need to be vigilant, and it is vital to check out potential suppliers and customers to ensure that they are who they say they are. It is all too easy to establish fake websites, premises, phone lines and so on. A change in bank account details for a supplier should always be carefully checked.

In one case, thieves stole the identity of businesses with excellent credit ratings. They then placed an order for a large number of mobile phones, which ended up in Africa and racked up a large amount of airtime costs.

Investigating the crime

Communication

Crimes obviously need to be investigated either internally or by the police, to ensure that companies know and understand exactly what has occurred.

The decision to reveal to employees and externally is difficult. Employees, suppliers and customers may have heard rumors and if a company has been cheated in a fraud it may want to show the market, as well as employees, that it won't be tolerated. Because of the potential risk to reputation, it is important to have a crisis management plan in place which includes a media response plan.

Recovery

It is vital to think about protecting recovery rights as soon as the crime is uncovered. One issue is whether to notify the police, because with their involvement there is the potential to lose control over the investigation and, more importantly, lose control over the recovery action.

Identifying where the money has gone can be difficult. Many companies will automatically turn to lawyers and/or auditors, but this can involve huge costs. Companies should ensure that they obtain a basic cost benefit analysis before progressing with recovery action. In one recent case, a company that was looking to recover from an employee who stole several million pounds incurred legal, investigation and forensic fees of more than GBP 700,000.

The message is that just because you have had a loss, it doesn't mean that you can't recover some of it. But think carefully before engaging lawyers and auditors.

While commercial crime is a sensitive issue, it does not mean that it should be ignored or covered up. Discovering commercial crime is often simply a matter of luck, but there is still much that corporates can do to deter criminal activity. And where a crime has been committed, there are measures that can be taken to mitigate the risk and perhaps recover some of the loss.

Christoph Leuzinger
Global Deputy Chief Underwriter,
Management Liability,
Zurich General Insurance

Matthew Thomas
Senior Adjuster
Charles Taylor Adjusting

*Report to the Nations on Occupational Fraud and Abuse, 2010 (http://www.acfe.com/rttn/2010-rttn.asp)

Speaking the **right language** on **multinational cover**

A multinational insurance program is an effective way to manage a portfolio of cover across multiple countries.

Get it right and you save time and reduce uncertainty. Get it wrong and it could cost you dearly, both in potential fines and exposure to risk if your insurance is found to be invalid.

In India and Japan, cash before cover rules mean that cover can only be provided after premiums have been paid in full. In Mexico you cannot backdate policies, while in Malaysia you should remember to calculate limits of liability in the local currency. If your policy includes operations in the United Arab Emirates then payment calculations in US dollars are permissible. Multinational programs offer the convenience of pulling together insurance under centralized control with uniform policies for every country where subsidiaries operate or have exposure to risks. This brings greater certainty and transparency but requires detailed understanding of a myriad of local regulations.

The price of making mistakes can be hefty fines issued by ever more vigilant authorities.

It's a steep learning curve but with the right planning an international program can run smoothly, allowing our customers to know they have global cover which they can rely on.

Growth in multinational programs

International programs for property and casualty cover are usually well understood and embedded in more established processes when it comes to renewing and extending cover. For financial lines, however, this approach is less well-established in certain countries and potentially subject to additional requirements, – for example, regarding money laundering, extra documentation and financial statements – together with a lack of a local standard wording in many countries and local legislation issues.

Zurich currently runs more than 700 financial lines programs and has issued over 5,000 policies in more than 180 countries. Zurich has seen steady annual growth rates in financial lines insurance: from 80 programs in 2007, to over 700 in 2011, particularly for directors and officers Liability, professional liability and employment practices liability. The globalization of business and broad choice of insurance products now available heightens the need to run an effective multinational program.

Good communication is key

Clear, consistent and timely communication with a customer's subsidiaries is essential. Even basic administrative errors can delay matters. Standardizing processes is therefore an important step towards reducing error rates, especially if policies are likely to change during the year.

By their nature, financial lines products often involve sensitive, personal information so it is equally important that only authorized people can access the documentation. This shouldn't, however, be a barrier to prevent the efficient flow of information in both directions.

Time to act

Ensuring premiums are paid on time can be more challenging than it sounds. Payment terms may be 30, 45 or 60 days to comply with local regulations. If policies are issued in local currency then attention must be paid to the prevailing exchange rate.

Small details are important – for example, using a 24-hour clock to avoid confusion. Not all polices start and end at midnight, as you might expect. In the US and Canada, for example, it is usually at one minute past midnight, while in Japan, Australia and Mexico the usual start point is 16.00.

Show me the money

A growing trend in international insurance is premium payment restrictions, particularly cash before cover (CBC), and whether or not cover can be backdated to the inception date once payment has been made. In India, for example, CBC rules are very strict. More countries are now implementing this rule eg. China.

A number of countries impose additional minimum premium requirements above those required by your insurer. These may be for local regulatory reasons or to protect local brokerage activities.

By their nature, financial lines products often involve sensitive, personal information so it is equally important that only authorized people can access the documentation.

Help is at hand

Your insurer should be able to provide you with regular advice and guidance based on years of experience. Ensure you choose an insurer with an international network of offices and local experts who understand local issues and policies. Running effective multinational programs relies on a combination of efficient channels of communication; clear understanding of local insurance rules and flexibility to act quickly when changes have to be made. You should receive regular contact from your insurer during the whole process.

Plan your multinational program

- Ensure local contacts are aware that an international program is in place.
- Keep abreast of changes in local conditions, policy restrictions and limits on cover.
- Ensure minimum premium requirements are adhered to in every country.
- Ensure premium payments are kept up to date and made on time.
- Ensure local contact details are accurate and up to date so your insurer knows who to reach as, this can save lengthy delays.
- Make sure you understand cash before cover requirements and whether backdating cover is permissible.
- At renewal, always check if any changes are needed – for example, contact details, premium limits or the currency used.
- Ensure any additional documentation for particular countries is prepared – for example to meet money laundering regulations.

The cost of getting it wrong

Argentine regulator fines broker for breaking local rules

An Argentine broker sold an individual buyer life insurance policies underwritten by two insurers who were not admitted or licensed in the country. The Ministry of Economy and Public Finances of Argentina fined the insurance buyer eight times the value of the premiums paid and the broker 15 times the premium value.

Swiss court voids policy from foreign insurer

Switzerland's Federal Office of Private Insurance declared that a professional indemnity policy taken with a foreign, non-admitted insurer was not acceptable and was therefore void. The broker who attempted to purchase the insurance appealed the decision but the ruling was upheld. The government agency subsequently refused to admit the broker into Switzerland's central federal register of insurance brokers.

Karen Wakefield, Senior Underwriting Service Specialist, Zurich Global Corporate UK

International Programs Central Hub – **email: fl_hub@zurich.com**

For more information on Zurich's financial lines, products and services, visit: www.zurich.com/globalfinanciallines

www.zurich.com

133668A01 (12/11) ZCA

ZURICH®