



# Growth in uncertain times

The need for dynamic risk management



In the 21st century there has not been a six-month period without a major crisis affecting several countries or industry sectors simultaneously. These crises have been varied and impossible to predict. To foster growth in these uncertain terms, dynamic risk management is vital.

Historically, corporate failings have been attributed to a lack of accountability, strategy and transparency. To overcome this it must be understood that dynamic risk management is not the responsibility of a single person or even department – it is the responsibility of everyone within the business, from the chief executive and the board, down to individual department heads and employees.

In these turbulent times, there are tougher expectations from regulators meaning corporates must demonstrate better discipline, responsibility and control. Failure to keep on top of, and comply with, existing and emerging regulation can jeopardise reputations and livelihoods.

In this publication we discuss perspectives and expectations of the board; about how you can mitigate and overcome challenges associated with reputational risk; how to improve governance, risk and compliance processes; how to define, establish and embed risk appetite; and how to foster the appropriate risk culture for success.

We will also look at how to effectively address risk throughout the supply chain; the threats associated with data leakage; and how emerging trends such as social media are changing the corporate landscape.

I hope you find this publication valuable in understanding the new playing field for risk management and that it provides insights to help you address the risks you face in your role and organisation.

Best regards,



**Craig Jackson**  
Risk Retreat Network Leader



# Contents

A view from the board	2
Reputational risk	4
Banking on governance, risk and compliance	5
The human side of risk: Protecting and creating value through culture	7
Making risk appetite practical	9
Building the road to the 2012 Olympic Games	10
Data leakage	13





THE  
HOLE  
IDEA  
WORLD  
GROW!  
Go global  
BUSY BUSY  
BUSY  
HTTP://  
Human  
Ideas

HELLO  
the  
www

Let's  
trade!  
APPS

85%  
online

Stock  
interconnected

DEAL



# A view from the board

Visibility and clarity of the risk function has never been more critical and challenging than it is today for members of the board. In the context of the turbulent global economy, companies now face risks that are more complex, interconnected and potentially devastating.

Risk in the financial services sector globally has contributed to large-scale bankruptcies, bank failures, government intervention and rapid consolidation. The repercussions have spread to the broader economy, as companies in nearly every industry have suffered from the effects of a global paralysis of credit markets, sharply reduced consumer demand and extremely volatile commodity, currency and stock markets.

In this environment, boards are mindful that courts can and will apply new standards, or interpret existing standards, to increase responsibility for risk management. And as a result, their expectations and perceptions around risk management processes and procedures have never been higher.

## Australian Stock Exchange guidelines

The continued principles-based, non-prescriptive approach to corporate governance by the Australian Stock Exchange (ASX) provides value, and balances the views of Australian corporates and stakeholders, however they do not eliminate risk and will not prevent future corporate collapses.

The ASX guidelines are part of a communication process designed to increase confidence in the capital markets without being too much of a regulatory burden. As a result it is absolutely critical that corporates move away from a reliance on box ticking and adopt a more dynamic risk management approach to suit their circumstances.

The general consensus among board members and senior executives is that the current environment calls for a continuous risk management journey. Despite the guidelines providing direction and allowing organisations flexibility in assessing governance, risk and compliance, companies should also consider other early warning systems (such as the development of lead risk indicators and the whistleblower services required under US law) to reduce risk of collapse and prevent significant surprises.

## Empowered regardless of reporting lines

Many organisations have difficulty in creating the correct reporting lines for the risk management function. The main reason for this is that risk management embraces most aspects of the organisation, such as strategy, finance, human resources, service delivery and public relations. In addition, the risk management function has close links to activities such as insurance, compliance, governance, internal audit and loss prevention. It is therefore understandable that the reporting lines for risk management are not immediately apparent.

Like all C-suite executives, the chief risk officer (CRO) has a difficult job. To be effective, he or she must have a prominent and meaningful voice in the C-suite and board level dialogue. Where they don't have this voice and are not involved in key decisions, significant gaps in risk control frameworks can appear.

From a board's perspective, regardless of the reporting line, the CRO's position and job description provides a seat at the table for important business decisions and empowers them to blow the whistle when needed.

In recent times, there has been an obvious shift in the reporting line of the CRO. Moves have been made to enhance the stature of the position, in some cases changing reporting lines so that the CRO reports directly to the CEO and in others enhancing risk reporting to the board or board committees.

Many board members recognise that establishing a clear risk appetite is an important way to improve governance from the top, and will encourage CRO involvement in strategic decisions and throughout all business operations.

## Forward facing

The term "be prepared" is especially applicable to today's business environment, where organisations across all industries and locations are challenged by a volatile and unpredictable world. In addition to protecting internal resources, organisations must consider the security and well-being of their employees, partners, suppliers and customers, as well as the reliability of the partners in their supply chain.





The ability to anticipate and adjust to planned and unplanned forces and events – including market fluctuations – requires a proactive approach that takes into account all of a company's assets and vulnerabilities.

Not surprisingly, organisations are focusing on business resilience, which is the ability to rapidly adapt and respond to risks, as well as opportunities, in order to maintain continuous business operations, be a more trusted operator, and enable growth.

From a board's perspective, this business resilience is dependent upon risk management, scenario planning and information security. As a matter of best practice, at least one relevantly qualified, skilled and experienced risk management professional should be appointed. In fact, ensuring that the board's skill set is aligned to business operations to understand opportunities for growth and to identify and mitigate risks is vital for success.

A board must be comprised of directors who collectively have the skills, knowledge and experience to effectively govern and direct their organisation. The ideal skill set for a board will depend on the type, size, stage and strategic direction of the organisation as well as the nature of its business and the industries and sectors within which it operates.

It is important to note that each individual director is not expected to hold all professional and industry skills. Rather, these skills should be held collectively by the board as a whole. Boards also often assess whether they consider each identified skill to be 'essential', 'desirable' or 'purchasable' (meaning that the skill can be 'brought' or 'bought' into the board as and when required, for example, specialist human resource expertise or legal advice).

Once the board is established, regular board performance evaluations should address board skills and individual director attributes. The skill areas in this matrix should also be regularly reviewed to ensure that they remain aligned with the organisation's stage of development and strategic direction.

#### The outlook

While the primary board-level risk oversight role is typically allocated to a board committee or the CRO – the full board expects to also receive information about the company's risk management system and the most significant risks that the company faces. This can be accomplished through reports from the committee charged with risk management oversight or briefings provided by management and advisors to the committee.

The ability of the board to perform its oversight role effectively is dependent upon the relationship and the flow of information between the directors, senior management, and the risk management executives in the company.

If directors do not believe they are receiving sufficient information – including information regarding the external and internal risk environment, the specific material risk exposures affecting the company, how these risks are assessed and prioritised, risk response strategies, implementation of risk management procedures and infrastructure, and the strength and weaknesses of the overall system – they need to be proactive in asking for more.

The committee charged with risk oversight should have sessions in which they meet directly with the executives primarily responsible for risk management, just as an audit committee meets regularly with the company's internal and external auditors and liaises with senior management.

In addition, senior risk managers and senior executives should be comfortable in informing the board or relevant committee of extraordinary risk issues and developments that need the immediate attention of the board outside of the regular reporting procedures. As discussed above, the committee charged with risk oversight should also report on its discussions and findings to the full board on a periodic basis.



# Reputational risk

As risk management continues its evolution, reputational risk is emerging as a key issue for all organisations.

Often overlooked and underestimated, reputational risk has the potential to be one of the most harmful threats to a company today. One only needs to look at the recent trials and tribulations of companies such as Tiger Airways to see the impact that a regulatory issue can have on public perception and a company's revenue.

In an economy that is both global and volatile, intangible assets have become the essential wealth of many companies. In fact, intangible assets like reputation are often more important than the tangible products that a company produces and sells.

The entire organisation can be affected by a downturn in reputation and as such all of those within must play a part in managing reputational risk. This involves making sure that crisis management and crisis communication plans are in place, PR firms are engaged before an issue occurs, executives and spokespeople receive media training and that a business continuity plan is in place.

---

The entire organisation can be affected by a downturn in reputation and all of those within must play a part in managing reputational risk.

In direct contrast to the slow process of building up trust, a reputation can be ruined overnight. Reputational risks can come from any direction and in many forms:

- ▶ **Economic** – a sudden shift in consumers' taste can make a company look out of touch and unresponsive
- ▶ **Operational** – poor operational management can lead to inefficiencies that impact on the customer
- ▶ **Occupational health and safety** – unsafe practices can be damaging to health and impact on the safety of the work environment and the end product
- ▶ **Unfair employment practices** – discrepancies between the company's published values and the reality of the work place
- ▶ **Governance** – lapses in governance standards or ethics can be difficult to get back on track
- ▶ **Unfair competition practices** – behaviour that is inconsistent with the company's values and policies
- ▶ **Human error** – an involuntary or unintended breach of policy or service failure can lead to threat of litigation
- ▶ **Voluntary** – an intentional breach of security can have a disastrous repercussions

The situations listed above illustrate that reputation can be affected by a wide range of circumstances. The associated damage can often be directly linked back to the way in which an incident is managed. Organisations must have the

capacity to respond and proactively manage such situations, clearly communicating a problem rather than hoping it will pass by unnoticed.

In order to manage reputational risk and respond effectively to incidents, corporates should:

- ▶ Be proactive in communicating bad news. Waiting for another source to break the news creates an opportunity for messages to become skewed and important information to be omitted in favour of creating a more sensational story
- ▶ Be specific about the issue. Provide detailed information around the circumstance, the actions taken and the measures that will be implemented going forward in order to reduce any short or long term damage to reputation
- ▶ Demonstrate that you understand the concern of stakeholders and the impact of the issue on them and consider your approach to providing compensation

Reputations can be saved or destroyed in a matter of hours as a consequence of how a situation is dealt with in the public eye and inside the organisation. A company's reputation is invaluable and no matter how good the end product, once a reputation is damaged it can take years to restore. Planning for the worst ensures that whatever you come up against a clear, confident and fast response can be taken to ensure you achieve the best outcome possible.



# Banking on governance, risk and compliance

For years, companies have invested heavily in governance, risk management and compliance (GRC), increasing the size, magnitude and reach of their GRC functions and activities.



Now, in the aftermath of the most severe economic crisis in a generation, companies are acutely conscious of the need to demonstrate sound risk management. They believe that their reputations, customer loyalty and even their credit rating and access to capital depend on it.

As the trend towards increasing expenditure in GRC continues, many companies fail to grasp that their GRC investment, unless properly focused, is potentially being poured into a black hole and will not deliver the value investors and other key stakeholders demand.

## Why is spending on the increase?

Fear is one of the major driving forces behind the accelerated investment in governance, risk and compliance (GRC). Today, companies are operating in a more volatile risk environment. They face increased demands for more timely and insightful information from stakeholders who will not tolerate risk management failure.

For companies, public perception can have a dramatic affect on the business. It is not just high-risk industries such as banking and oil and gas that have seen their reputation and market capitalisation damaged by controversy in recent years. Consumer goods companies, food, automobile and even toy manufacturers have all felt investors' wrath. Scandals, wrong-doings and risk management failures all conspire to make companies nervous and even more likely to spend on

GRC. Being seen to invest in risk management is one way of communicating to stakeholders that their businesses are safe and reliable investments.

Companies are fearful too of rating agency judgments on their risk management, which can influence availability and cost of capital. As a result, they hike up their spend on risk management as a perceived safety net against failure.

Not only are companies afraid of risk management lapses, they are increasingly dependent on GRC to deliver "effective" risk management across their businesses. Their spending is indicative of this growing dependency. Interestingly, however, this spending and dependency is not matched by the value that business leaders think they currently get from GRC with many still wanting to further enhance their GRC function.

## How to get value from your GRC investment

Effective risk management isn't about spending more but rather about getting greater value from what is spent.

Companies would not ordinarily part with billions of dollars without the expectation of a healthy return. That is why risk expenditure needs to be treated as a strategic investment or business enabler – much like spending on a plant or equipment. It has to be capable of protecting and delivering value by way of improved business performance and an acceptable return on investment (ROI).





Although companies recognise the need to get more value from their GRC capabilities, and despite matching that impetus with spending, there is overwhelming uncertainty about how to design and implement the most appropriate GRC functions for their specific circumstances.

An effective GRC capability provides value by giving organisations the confidence to take on risk, rather than avoid it.

This capability helps with the identification of risk boundaries and tolerances and, above all, enables ongoing assessment of a company's strategic initiatives, such as capital programs, M&A and integration. It cuts costs by eliminating overlaps and redundancy in risk coverage and focuses management attention on the high – rather than low-priority risk areas. While the theory sounds good, what does it take for companies to build and deliver an effective GRC capability?

Successful organisations begin by identifying the sources of existing GRC expenditure. They measure and assess where risk management spend is currently targeted and pinpoint uncoordinated, overly complex or overlapping activities. Spend from low-value risk management activities, which may be routine and deliver comfort but are not business critical, needs to be redirected to other higher-risk priorities.

This approach to enterprise GRC goes beyond simplistic, incremental, budget-driven improvements to, and

convergence of, individual risk functions. Instead it balances risk coverage (those risks that matter most) with cost (by eliminating duplication, redundant or overlapping activities) and value (determined by ROI).

---

### Effective risk management isn't about spending more but rather about getting greater value from what is spent.

By effectively managing the right risks, management has a more timely and comprehensive understanding of risk. This in turn facilitates better decision-making and confidence to take on new ventures or even to accept higher levels of risk. The upshot of this investment includes a greater competitive advantage, reduced cost of capital and a steady share price. As well as focusing resources on priority areas, companies need to focus on enhancing the overall performance of their newly integrated GRC capabilities.

Currently many companies take a “check-the-box” approach to compliance with an over-emphasis on internal risk structures, committees and isolated risk assessments. By adopting a holistic and cohesive risk transformation approach, they can better align risk and strategic business processes.

Moving forward, an organization can expect its GRC capability to deliver value at four levels of performance:

- ▶ **Governance** – risk governance strategy is driven by and better aligned to key strategic risks and business objectives
- ▶ **Effective risk management** – deeper and more robust risk insight applied to enhance the design and effectiveness of the overall control environment. This optimises risk and control mechanisms to enhance decision-making and, potentially, facilitates greater risk-taking
- ▶ **Integration** – rather than stand-alone functions, risk is managed on a business-wide level to protect value and improve performance across the enterprise, delivering an appropriate ROI for the investment
- ▶ **Business performance** – an effective and agile GRC capability contributes to the protection and enhancement of overall business performance



# The human side of risk: protecting and creating value through culture

Risk taking, whether you love it or loath it, is the single cultural trait with the largest impact on organisational performance, according to research by the Corporate Leadership Council.

One of today's most challenging questions faced by business leaders is whether they have the confidence to leverage risk taking behaviours in order to create value. It is both the human and non-human elements of enterprise risk management that either create or erode value. At its most basic level, a human element is the behaviour of an individual which then combines into team behaviour, departmental behaviour and then organisational behaviour. Non-human elements are the parts of the business that human elements interact with to produce value, for example, processes, systems, rules and regulations. In effect, the combination of the two sets of elements results in "culture".

To optimise organisational value, you must strengthen the alignment between the human and non-human environments, and shape people's behaviour as you would shape organisational processes and systems. It is only when people really understand the risks they are taking through consistent and repeatable practices, moving away from just "ticking the box", that they can far better optimise the risk and reward equation for their business.

## **Understand and drive the right risk culture**

"The way we work around here", or the combined effect of the human and non-human environments, is what we define as the culture of a group and can be defined, changed, and monitored. A strong culture can constitute a powerful capability when addressing certain types of problems or seizing new market opportunities. However, it can also be a disability when not aligned to the strategy and risk appetite set by leadership.



In addition to what is required organisationally, behaviour is also the result of individual drivers, such as the need for achievement and need for affiliation (McClelland, 1961; Maslow, 1943). People, in any role they perform, do not come to work to fail. They are driven to achieve and grow in their work, to do the right thing and not actively make decisions that lead to adverse outcomes such as financial loss or unsafe practices. Equally, people need to feel they belong and are accepted by the various groups that they operate in. In the risk context these two needs, organisational and individual, can result in a level of tension between the way in which people would behave (to fulfil their need for achievement), and the behaviour required by the culture and norms of the groups in which they operate (to fulfil their need to belong).

Achieving your desired risk culture requires you to follow five stages.

**Stage one:** Identifying your risk culture. Meaningfully segment your organisation and define your risk culture vision.

**Stage two:** Diagnosing the health of your risk culture. Establish quantitatively and qualitatively whether your actual risk culture aligns with your vision.

**Stage three:** Designing the right behaviour change program. Create a behaviour change program that includes the interventions that you know, from diagnostic analysis, will work most effectively.

**Stage four:** Delivering behavioural change. Focus on engineering the appropriate risk behaviours required within each meaningful sub-group and deploy targeted change interventions only in the areas that need them.

**Stage five:** Sustaining change and building on risk management capability. Continuously monitor the health of your risk culture and make adjustments early, before bad habits get ingrained.

Risk management is going through an exciting evolution. Its role to enable business performance is becoming increasingly appreciated and, with this, comes greater expectations of stakeholders as to what it can deliver. We believe that you can influence the right human behaviours to complement the existing non-human environment; it's just a matter of knowing how.

Behavioural change is a challenging feat and one which won't occur overnight, or by osmosis. It requires a methodical, analytical and planned approach that has strong leadership and typical program infrastructure. With these factors in place, the five stages of identify, diagnose, design, deliver and sustain are achievable. Be clear on your vision, diagnose the current state, design a change program for the areas that need it, deliver the targeted initiatives in a coordinated way and continue to sustain and evolve the risk capability that you have developed. The confidence to leverage risk taking behaviours will flow from there so you can protect the value you have and continue to create more.

---

People, in any role they perform, do not come to work to fail. They are driven to achieve and grow in their work, to do the right thing and not actively make decisions that lead to adverse outcomes such as financial loss or unsafe practices.



# Making risk appetite practical

Business leaders are under pressure as never before. Even though the global economy has slowed, there is always increased pressure from shareholders to deliver earnings growth through increasing investment in new products and services, by entering new markets, and through corporate development activity – in other words, by taking on more risk.

Furthermore, shareholder pressure has been supplemented by increased regulatory demands that have created an environment in which senior managers are required to take governance and oversight responsibilities much more seriously.

These simultaneous demands for faster growth and stronger governance are pushing companies to find an answer to the question “how much risk do we want to take?”

Perhaps surprisingly, many companies haven't fully considered this question before. While businesses must take risk to generate returns, the amount of risk taken is often set as a consequence of other strategy decisions, rather than as an input to those decisions.

More recently, some companies have started to quantify their 'risk appetites' more formally but, even then, they rarely link this effort to the evaluation of strategic options. More often than not, a firm's risk appetite is formed primarily on the basis of managerial instinct.

Some of the biggest challenges around defining risk appetite include the following:

- ▶ Determining risk appetite is a subjective and intuitive exercise
- ▶ Preferences for risk appetite vary and can result in inconsistencies across different groupings

- ▶ Operationalising risk appetite is tricky and risk appetite statements tend to be written at a high, strategic level and don't necessarily resonate with individuals at a business unit level
- ▶ Risk appetite decisions often involve choices across multiple risk classes
- ▶ Elements of risk appetite are intangible such as reputational risk
- ▶ Risk appetite statements tend to focus on the upper limit of acceptable, not on the required level of risk to be taken

One best practice technique used to define risk appetite and make it practical is leveraging a choice attribution model to understand how the key stakeholders of the company interpret events and how this relates to their thinking and behaviour around risk appetite.

Our choices are significantly driven by our emotional and motivational drives. This technique can be used to help understand the different risk appetites amongst board members and the C-suite, creating a more enlightened profile of the organisation's risk appetite.

Choice attribution technology can be used to survey board members and the C-suite in real time, against a series of risk management scenarios. The results are immediate and can be used to drive robust and insightful discussions around how the firm should proactively and reactively manage risk as a group, and as organisation.

The benefits of this type of approach are that it:

- ▶ Provides feedback of individual and group risk preferences and aversions
- ▶ Outlines individual and group alignment and misalignments
- ▶ Makes risk appetite and tolerance discussions more practical and relates to real business environment decision making
- ▶ Incorporates multiple risk classes across one overall assessment
- ▶ Allows for intangible risks to be weighed up against tangible risk classes
- ▶ Creates a frame of reference and principles that can steer future strategic and tactical decision making

Risk appetite is not fixed or finite. It is dynamic and varies over time in accordance with a wide range of factors such as market conditions, leadership style, internal pressures and opportunities to name just a few. Facilitating greater self awareness within leadership teams can lead to a better understanding of what is driving the organisation's decisions around risk and in turn better align risk appetite with overall business strategy.



# Building the road to the 2012 Olympic Games

In July 2005, London won the bid to host the 2012 Olympic Games. The Olympic Delivery Authority (ODA) immediately faced an exciting but challenging journey to deliver the infrastructure and facilities.

Within a complex political and social stakeholder environment, David Law, Olympic Delivery Authority (ODA) Chief Risk Officer, shares his insight on how the ODA successfully established an integrated control framework to ensure there was appropriate focus on the key risks and issues to ensure the delivery of a successful Olympic Games.

## **What are the London 2012 Olympic Games headlines that best describe the scale, complexity and importance of the Olympic Games?**

The Games were won by the UK back in 2005, which was really a very big deal for London. Within the Olympic Park which is something like 250 hectares (around about 175 English football pitches), we're building 12 venues and our own power station, we've soil washed 1.3 million tons of soil to sift it and extract impurities, we've cleansed three and half miles of waterways, we're building around 20km of roads, we're building 40 bridges and in the course of our work we've found five unexploded bombs, one perfectly preserved World War II jeep, and 3500 shopping trolleys from Sainsbury and Tesco!

## **As Chief Risk Officer what was your vision for how you and your team would support the successful delivery of the London 2012 Olympics?**

You have to bear in mind that back in 2005/6 the ODA was a start up organisation so we had no history whatsoever and we were bringing in people from all walks of life, many of whom like myself had never previously worked in the public sector. We set ourselves up, in terms of the risk and audit function, to establish a control governance framework within which all of the projects would operate. In the course of our work over the next five to six years we've policed this framework to give people assurance that it is being adhered to.





We've found five unexploded bombs, one perfectly preserved World War II jeep and 3500 shopping trolleys from Sainsbury and Tesco!

A further complexity within the public sector in the UK was the sheer number of external bodies who were interested in the Games. Within Government alone there's something like 120 different elements of Government which have a key interest in the Games. A lot of these areas wanted to do their own assurance activities on different elements of the program. One thing that we were very keen to do in the early days was to say to them, "you can't come in and do what you want to do" because it would be overly intrusive and actually cause delay to the project. So what we offered to do was to incorporate into our own audit program the elements of assurance which they wanted to look at, so that they could rely on our work and we could share those elements. We've found that this approach has worked really well.

**What role did your team play in working with management to navigate the challenges that emerged as a result of the financial crisis?**

Two kinds of risk spring up in any due recession. The first is related to the likelihood of a supplier going bust. We have worked very closely with CLM (the Games delivery partner) to establish a monetary unit to look at the health of all the contractors in the park, be they the main tier one contractors or be they the tier five contractors. We received monthly data on all these companies and where difficulties were encountered we tried to help them out by making payments ahead of our contractual obligation dates. A lot of the firms really appreciated what we did for them.

The second risk that increases during recession is fraud. In the very early days the Olympic Delivery Authority (ODA) was keen to establish an awareness program and we've worked very closely with CLM and with the contractors to hold something like 40 fraud awareness workshops. There were about 12-15 people in each workshop who we've taken through the standards that we expect them to follow in terms of managing the potential risk of fraud within the projects that they are working on, and to date this has been remarkably successful.





**Based on your experiences of working on the London 2012 Games, what do you feel are the key learnings that could be applied to the delivery of major capital projects across other industries?**

What we tried to do within London 2012 was to manage time. So all the venues were aggressively managed and indeed the completion dates of all the venues were brought forward to 2011. This was good in one sense, however it did create another risk for the ODA which was that we had to manage the period between the completion of the venues and the Games themselves. We had to incur additional costs for this which we call park operations and park services. This was a brand new project which at the time of 2005 would not have been foreseen.

Another key element that we had to manage in the early days was “scope creep”, because I’m sure you can imagine that back in 2005 although budgets were drawn up, the precise obligations of the London Organising Committee at the Olympic Games (LOCOG) and the ODA were really not as black and white as everyone would have hoped for. There were a lot of grey areas and as time has gone by, within the ODA we had to make a conscious decision not to let arguments over the grey areas deflect us. What we did was to incorporate LOCOG’s scope changes as far as we possibly could and then we created what we called internally a “claims reserve” so we knew exactly how much we were building which we thought we shouldn’t have done, so we were able to keep tabs on it that way.

**For executives who are reliant on successful project delivery to achieve their strategic business objectives what is your advice with respect to project assurance?**

I think the first thing is to get the executives to believe and accept the audit program. I think there is a tendency for executives to believe that they understand their program better than anyone else. One of the strengths of internal audit is that we bring to any project we look at, not just an independent view but also an objective view. And I think if the executives have their minds sufficiently open to listen to that objective view then they will benefit greatly from it.



# Data leakage

Over the last five years, organisations have experienced a rise in the volume of intentional and unintentional data leakage.

Increasingly sophisticated malicious software (malware) is providing a channel for unknowingly releasing sensitive information outside the organisation. At the same time, organisation insiders or whistleblowers have embraced a new outlet for bringing questionable behaviour to light, publishing sensitive information on websites like WikiLeaks.ch (previously WikiLeaks.org).

Both The New York Times and the Guardian in the UK have announced intentions to develop similar portals, with many other publications sure to follow suit. The potential reputational harm caused by such data leakage cannot be underestimated.

Controlling confidential information within your organisation is challenging because of the intricate web of internal and external threats. Data leakage from the corporate network can occur deliberately, through the intentional action of an employee, an external hacker, or inadvertently, through an unsuspecting employee who has been compromised by malware or social engineering designed to entice users to violate recommended practices. Social engineering is a common avenue for attackers to collect information on or introduce malware into your organization by taking advantage of employees unaware of security risks and practices.

## Strengthening the security of your organisation

A strategic technical program is essential to strengthen the long-term security of your organisation. Such a program will address existing and emerging threats, reduce the cost of necessary security measures and facilitate the handling of security incidents.

The first step in building a strategic program is to identify sensitive and confidential information residing on your networks or with your business partners and to understand how that information is moving throughout your enterprise. A full data discovery and classification exercise will allow your company to implement the most efficient and targeted protection schemes possible. Performing a data loss prevention assessment helps identify risks and supports the development of an improvement plan that includes “quick wins” and long-term recommendations to reduce business risks.

Comprehensive attack and penetration assessments should be conducted regularly to identify a wide range of technical vulnerabilities that could be exploited by rogue employees. The assessments should include application and infrastructure testing, and source code and infrastructure reviews. Such full-scope assessments can help identify typical application and network exposures and “backdoors” in the environment.

Finally, take action against emerging threats posed by malware and social engineering. Performing regular and thorough malware detection is critical for combating attacks that target data over extended periods of time with a “low-and slow” approach. Malware surveillance can alert your organisation to ongoing attacks so you can shut them down quickly.

In addition to such technical controls it is also necessary to instil preventative and corrective behavioural controls within the company. Internal policies should be made available throughout the organisation ensuring employees are well informed of the company’s commitment to acting ethically and abiding by the law. The actions being taken to honour this commitment should be clearly conveyed, such as internal escalation procedures for disclosing and reporting suspected unlawful or unethical actions.





### Seven steps towards securing company data

Strategic changes are long-term fixes that take time and care to implement, and many companies seek guidance in initiating their strategic response. After more than 15 years of providing security advisory services, including attack and penetration assessments that employ the same tactics a hacker would use, Ernst & Young has determined that the following seven tactical measures provide the best foundation for an effective strategic program and offer the greatest return on investment:

#### 1. Identify and classify your data

A well-developed, granular information classification scheme will enable your company to design and implement the proper controls for different types of data. In addition, a clear and well understood policy will encourage proper behaviour by employees and data owners with respect to data handling, storage and transfer.

#### 2. Manage local administrators properly

Local users should not be granted local administrator privileges to corporate endpoints, such as laptops, PCs or mobile devices. Local administrator accounts should have strong passwords, and administrator passwords should not be shared across multiple machines.

#### 3. Do not allow unauthorised machines on your network

The attempt of non-corporate assets to access the corporate infrastructure signals one of two undesirable conditions: an unauthorised party has entered the company's premises and plugged into the network, or an employee has brought a personal device into the office and connected to it. Personal devices will not have corporate utilities like updated antivirus and host-based firewalls; consequently, infected machines could propagate malware throughout the enterprise.

Network access control devices will prevent non-corporate assets from joining the network and will notify the appropriate security personnel should such an attempt occur.

#### 4. Do not permit easy exfiltration via removable media

Endpoints should be configured to disable all removable devices such as CDs and USBs. Mobile devices like laptops and mobile smartphones or PDAs should have full disk encryption, and your company should have the ability to erase them remotely if they are lost or stolen.

#### 5. Fail safe by default

Data loss prevention (DLP) tools should be implemented and configured to "fail safe." In this mode, if the DLP tool cannot verify the contents of a communication (for example, an encrypted email that is not readable), the tool should be able to block the communication and log the event.

#### 6. Implement strong password management practices

Company security policies must include enforcement of strong passwords and account lockout for repeated log-in failures. Attributes of strong passwords include high minimum character length, avoidance of real words and a mixture of upper and lowercase letters, numbers and special characters (e.g., symbols or punctuation). Passwords should be protected by strong, non-reversible cryptographic algorithms.

#### 7. Review and tighten data access controls and usage triggers

When identity and access management systems are initially deployed, user roles and user access are typically broadly defined. Now is the time to review those roles and access to make sure employees have access only to the information required to fulfil their responsibilities successfully and nothing more. Access restrictions should be augmented by monitoring to identify unusual or suspicious activity by those with access to sensitive data.



---

Controlling confidential information within your organisation is challenging because of the intricate web of internal and external threats.

#### **Gain the confidence of whistleblowers**

Data theft by corporate insiders is a real threat with long-term ramifications, such as business interruption and lasting reputational damage. Perpetrators may be motivated by a variety of factors, including social conscience or desire for personal gain. Preventive measures must take into account this range of motives in order to be truly effective.

The problem of responsible parties bypassing the corporate hierarchy to reveal embarrassing information about unethical or unlawful activity must not be met with hostility or disdain. Such individuals should be encouraged to come forward and to work within approved company channels designed specifically for this purpose. Employees must be convinced that your organisation is dedicated to eradicating unethical behaviour, and that must be recognized and appreciated by the public as well.

Once you have gained the confidence of whistleblowers, they will feel comfortable and confident about working within the organisation, and you will have prevented the negative publicity that accompanies a leak.

On the other hand, determined adversaries pose a distinct and dangerous ongoing threat to your organisation. Data loss prevention, attack and penetration and malware detection all contribute to locating, understanding, classifying and protecting sensitive data. Educating employees on leading practices in cybersecurity will heighten security awareness and arm them against social engineering.

A robust incident response program will enable a rapid and correct reaction when unanticipated events or individuals threaten your business operations.



# Contacts

## Craig Jackson

Risk Retreat Network Leader  
craig.m.jackson@au.ey.com  
Tel: +61 2 8295 6551

## Rob Perry

Asia-Pacific Risk Leader  
rob.perry@au.ey.com  
Tel: +61 3 9288 8639



Ernst & Young

Assurance | Tax | Transactions | Advisory

**About Ernst & Young**

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organisation of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organisation, please visit [www.ey.com](http://www.ey.com)

© 2011 Ernst & Young, Australia.

All Rights Reserved.

SCORE No. AU00001120

This communication provides general information which is current as at the time of production. The information contained in this communication does not constitute advice and should not be relied on as such. Professional advice should be sought prior to any action being taken in reliance on any of the information. Ernst & Young disclaims all responsibility and liability (including, without limitation, for any direct or indirect or consequential costs, loss or damage or loss of profits) arising from anything done or omitted to be done by any party in reliance, whether wholly or partially, on any of the information. Any party that relies on the information does so at its own risk.

Liability limited by a scheme approved under Professional Standards Legislation.

