The top three business risks for 2018: Cyber, supply chain and regulatory compliance

Published: Feb. 13, 2018

The recently released Allianz Risk Barometer ranked the top business risks for 2018, based on the views of more than 1,900 risk management experts globally. Here, we look at the top three identified business risk for Australia and discuss how they can be effectively managed.

#1 Cyber incidents

It will come as no surprise that, in Australia, cyber risk is the top ranked risk and, globally, this is seen as the second biggest risk for companies.

Although the most publicised cyber incidents tend to involve the theft of personal data that hackers may then seek to sell (think of the theft of the data of 143 million consumers from Equifax) or publish (think of Ashley Madison's breach, where the data of 37 million users was stolen), cyber risk covers a broad range of activities other than data theft, including broader cyber crimes, data loss from employee error and system malfunctions. As an example of the other types of risk covered, Reuters reported the first safety system breach by hackers at an industrial plant in December 2017. Although few details are publicly available, it is reported that malware was used to take remote control of a workstation running the relevant safety shutdown system[i]. If that was not enough, in January 2018, vulnerabilities in Intel chips were discovered which allow the theft of data. Unfortunately, given that these vulnerabilities impact a broad range of hardware and software, it has been difficult to release patches that will provide protection from hackers seeking to exploit these vulnerabilities in all cases.

Although it may not be possible to eliminate cyber risks entirely, it is possible to take steps to minimise these. Companies should consider an overarching cyber management strategy, covering not only the implementation of IT protections, but also broader policies and procedures (including employee training), cyber insurance and protections in contractual arrangements. If an incident does occur, a well tested incident response plan is critical – given many companies suffer significant reputational damage if a cyber breach is not appropriately handled. For more information on the steps you may take, see here. Angela Flannery

#2 Business interruption (including supply chain disruption)

Business interruption was ranked as the number one global risk for the sixth consecutive year and the number two business risk in Australia.

Business interruption risk concerns are predominantly centred around infrastructure and supply chain disruption – both physical and electronic.

Traditional physical property damage to one's own supply chain infrastructure continues to be a risk. However, as supplier interdependence and supply chain integration takes on greater importance for business performance, businesses are forced more and more to consider the risk of third party supply chain infrastructure disruption as a critical risk to their own performance.

Also, business processes and information are becoming just as or more important than the end product or service, as product or service delivery, electronic supply chain integration and customer engagement increasingly become a primary means of marketplace differentiation. Systems disruption, communications protocol breakdown and data loss or corruption are now seen as key electronic supply chain risks.

Whilst natural disasters can't be controlled, other business interruption risks, or their consequences and mitigation, can be managed. Know-your-partner/supplier/contractor pre-engagement assurance processes should be seen as an investment in supply chain security and continuity.

Actively managing the performance of contracting parties is also essential to avoid supply chain disruption. Contracts should provide for performance measurement and management processes to encourage ongoing performance and/or provide for an orderly and timely transition to alternate providers if performance problems persist. Clear contracting is incredibly important in providing explicit performance standards and a clear exit plan. Any uncertainty on these fronts inevitably leads to disputes and delay, which can exacerbate the duration and impact of business disruption. Nathan Cecil

#3 Changes in legislation and regulation

Changes in law are ranked as the number three business risk in Australia and number 5 globally.

Globally, changes in protectionism and trade barriers are seen as significant. On the domestic front, changes in regulation and the burden of regulatory compliance represent an ever-growing business risk and cost. The costs of non-compliance extend far beyond business disruption and contract/project default, with significant corporate and Executive liability a recurring feature of the new compliance regimes introduced in a number of major sectors in Australia. Key changes taking effect this year include the following.

Data & Privacy

Final preparations are currently underway for the introduction of the Federal Government's new mandatory breach notification laws that are set to commence on 22 February. Read more from our team about how to prepare for the notifiable data breach scheme here. Another key privacy date this year will be the introduction of the General Data Protection Regulation (GDPR) on 25 May which requires many Australian businesses to reconsider the way they process, store and protect personal information. Read more about this here.

Transport

Significantly tougher Heavy Vehicle National Laws are due to be in place by mid-2018. These will feature a substantial increase in maximum penalties for Chain of Responsibility breaches to $3 million for corporations and $300,000 plus up to five years' imprisonment for individuals. Read our month-by-month guide to preparing for these new laws here.

Proposed critical infrastructure security laws have been tabled which will require owners and operators of such assets, including designated assets in the electricity, water and ports sectors, need to take proactive steps to ensure the security of those assets, including by implementing cybersecurity protections. See our summary here.

Further changes to Australia's coastal shipping regime have been tabled which are expected to liberalise the conduct of Australian coastal shipping, in particular for foreign shipping companies conducting such trade. Read more about this here.

Planning & Environment

This year will continue to see the roll-out of some recently introduced and reformed environmental legislation in NSW: the Biodiversity Conservation Act 2016 and the Environmental Planning and Assessment Amendment Act 2017. See our outline of the key changes, and at what stage they will be taking effect here.

Building & Construction

Following recent Australian and international building product failures and disasters, various Australian jurisdictions have introduced legislation aimed at unsafe or non-complying building products. These new laws introduce the concept of a shared chain of responsibility to ensure the safety of building products, which will be enforced against the domestic parties designing, importing, supplying or installing those products. More details can be found here and here.

This article was originally published on Holding Redlich Weekly Brief

https://metispd.com/blogs/news/the-top-three-business-risks-for-2018-cyber-supply-chain-and-regulatory-compliance?utm_source=MetisPD+Shopify+Subscribers&utm_campaign=6ddfd87741-EMAIL_CAMPAIGN_2018_02_15&utm_medium=email&utm_term=0_e6071e06fe-6ddfd87741-14044331&goal=0_e6071e06fe-6ddfd87741-14044331&mc_cid=6ddfd87741&mc_eid=645a486e8c

Submitted by:

Ruth Edge – Cardinia Shire Council