

FOR CEO'S & BUSINESS LEADERS IN SYSTEMS ANALYSIS SERVICE





Usage Notice

The materials contained within this report constitute general information only and should be considered with personal financial advice from an Australian Financial Services license holder. It is highly recommended that you speak to an insurance professional when setting your insurance program as each policy should be tailored to your specific needs.

The information contained within the document is the property of The LMI Group and is intended for the addressee only. The contents of this document are not to be reproduced, modified or disclosed by its recipient without the express permission of the LMI Group. For a copy of our full terms of use, please visit our website:

www.lmigroup.com AFS License No: 283777.

1. ABOUT LMI GROUP

LMI Group is an independent company specialising in risk assessment for the general insurance and wider business communities. The LMI RiskCoach research team has over 1,000 years combined experience in assisting businesses following losses. Using this enormous bank of knowledge the team has developed RiskCoach to assist businesses and their insurance advisers understand the specific risks in up to 14 classes of general insurance for their industry / occupation before a claim occurs. LMI believe that insurance should be considered as protection and not a cost. The cost of insurance, called a premium, is the cost of transferring the risk from the shareholders and their families to an insurer.

Should you have any questions about this report please discuss them with your insurance adviser or email expert@LMIGroup.com enclosing a copy of your report. If you need claims assistance, please email claims@LMIGroup.com for expert assistance.

2. PURPOSE OF THIS REPORT

The Insurance Risk Report has been designed to assist you in identifying significant exposures to a business operating in your industry. Contained within this report is a Hazard Index graph which considers both the likelihood and severity of losses over 14 insurable classes of insurance for your industry and rates them accordingly. This graph is complemented with a number of explanations giving rise to the factors considered when providing the rating. If it is not already included in this report, you may request your Insurance Professional to provide you with a list of significant exposures relevant to your industry. These exposures are useful to highlight the most likely and severe risks to your industry and potentially your business and to get you thinking about other areas that may be at risk.

Please note: These ratings have been developed using historical claims and loss data for a general business operating in this field. It is recommended that additional factors specific to your business be taken into account when assessing this information such as location and crime rates.

3. HAZARD ASSESSMENT

Identifying hazards in the workplace involves finding things and situations that could potentially cause harm to the organisation. The following chart is a graphical representation of the likelihood and severity of a loss occurring within any of the classes of insurance listed in the chart.

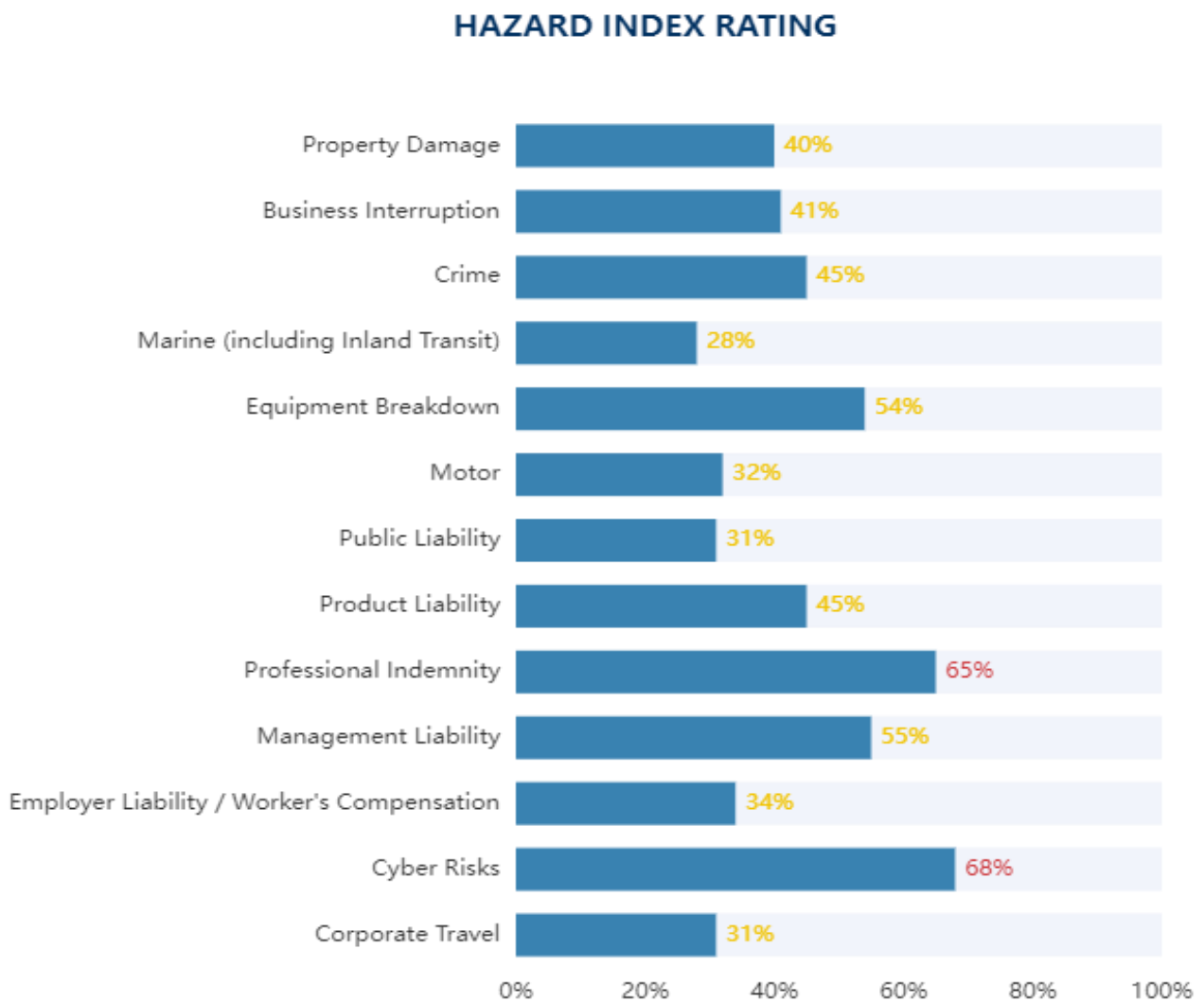


Fig 1: Hazard Index

Please note: These ratings have been developed using historical claims and loss data for a general business operating in this field. It is recommended that additional factors specific to your business be taken into account when assessing this information such as location and crime rates.

PROPERTY DAMAGE

40%

CLASSES OF INSURANCE

RISK SUMMARY

Accommodation needs will vary with type of operation. Software consultancy/development and web services will often be performed in office environments. Companies involved in hardware work will generally have greater space requirements and will need in house workshop space and also larger storage areas for computers being worked on, stock, parts and consumables etc. Risks associated with these firms from a property damage perspective are somewhat similar to those encountered in many other white collar occupations/office risks. The large quantity of computer and electronic equipment together with electrical equipment, personal portable heaters or desktop fans, faulty wiring and kitchen appliances creates large numbers of potential ignition sources. The presence of artwork, customer documents and existence of a library will also increase the fire load/hazard. Building construction and maintenance, as well as the presence, or otherwise, of automatic sprinkler protection and fire detection systems, will be the main concerns. Following a major loss the cost of reinstating records and data is a likely concern, though this should be addressed through good off site back-ups and mirroring. Firms working with hardware will have a higher fire hazard due to the presence of workshops where work on computers may be performed including soldering and use of power tools. They will also have greater space requirements and will have spare parts and computer stock at risk though volumes are unlikely to be substantial.

BUSINESS INTERRUPTION

41%

CLASSES OF INSURANCE

RISK SUMMARY

Business interruption exposure in this occupation can be considered as moderate. Most firms will lease rented office space and due to the non-specialised nature of the office space requirements, alternative premises are likely to be easily located. Large players have a multiple branch network (both local and overseas) and any loss or damage to one branch may be able to be mitigated by service from another branch as a temporary solution whilst service providers now have the ability carry out work on a computer system remotely from anywhere in the world. However, competition

in this industry (both locally and internationally) is high and the insured also faces competition from in house IT operations; this may delay the recovery process following a loss. Following a major loss, if the business is unable to retain its key staff (e.g. highly skilled computer programmers, software design engineers etc) that will have considerable effect on the business. Dependency on one or few large customers (banks, insurance company etc) for income creates vulnerability and may necessitate Named Customer cover.

CRIME

45%

CLASSES OF INSURANCE

Theft, Money, Surety / Fidelity

RISK SUMMARY

The crime exposure under this occupation is moderate since:

- a. there will not be a large amount of cash on the premises;
- b. expensive computers, communications equipment, laptop computers, mobile phones etc can be a target for thieves but security measures at premises are generally superior due to data protection/privacy legislation requirements.

Employee fidelity issues could be a substantial risk for this occupation, depending on the level of control. Effective risk management involves minimising cash on premises, employee selection and monitoring, physical security and care with laptops.

MARINE (INCLUDING INLAND TRANSIT)

28%

CLASSES OF INSURANCE

Marine Cargo, Goods in Transit, Marine Consequential Loss, Commercial Hull, Carriers Insurance, Marine Liabilities

RISK SUMMARY

Marine exposures are usually limited to incoming shipments of office consumables, parts, computer stock and own computer equipment replacement or upgrades and occasionally office relocations or refits. Occasional office relocations will usually be handled under a single transit policy.

EQUIPMENT BREAKDOWN

54%

CLASSES OF INSURANCE

Machinery Breakdown, Engineering, Mobile Machinery, Computers, Electronic Equipment, Machinery Business Interruption

RISK SUMMARY

Computer system design and related service providers extensively use computers, communication and transmission equipment. The rapid pace of technological advances has meant that such equipment has become faster and more compact, requiring more power and generating more heat. Business interruption caused by failure of this important equipment is a major consideration for this industry; in the event of loss or damage, financial loss to the insured could be considerable. The non-specialised nature of the equipment will mean replacement or repair is straightforward, but a file server, for example, may be expensive. More importantly, the loss of data or records is a significant risk. There is a significant exposure for larger operations and an extension of the machinery policy to cover business interruption should be considered. This should include cover for interruption of public utilities. Additionally, there is a low to moderate exposure depending on ownership of or responsibility for building plant and equipment to consider.

MOTOR

32%

CLASSES OF INSURANCE

Commercial Motor, Earthmoving Equipment, Motor Fleet, Heavy Motor

RISK SUMMARY

The insured may have a small fleet of passenger vehicles/vans for sales calls and servicing. There may be either Management salary sacrifice vehicles or pool vehicles to consider. Good management of the pool cars is essential – see text for further details.

PUBLIC LIABILITY

31%

CLASSES OF INSURANCE

Public Liability, Advertising Liability, Environmental Liability, Liquor Liability

RISK SUMMARY

Other than the IT related risks, the public liability risk is generally low and usually limited to general office/occupiers liability. Work away from the premises, if any is low hazard, though the amount of work done at sites should be established; this could involve hardware maintenance work or repairs in some instances though often this is performed in the insured's own office for more complex work. The frequency with which functions or presentations are held involving large numbers of guests should be considered. Since the premises may be either owned or leased, the responsibility for common areas such as lobbies, lifts, stairwells etc, as well as any responsibility under tenancy agreements as owner or occupier must be clearly established in determining liability exposure. In addition to above most of the other risks for the insured are IT specific risks (refer to text - Nature of business operation). Some of these areas of liability are somewhat gray in terms of liability policy response and clarification should be sought from liability underwriters whether these aspects are to be covered under the general liability policy, product liability or professional indemnity/errors and omissions cover. Many IT risks are in the nature of professional risks exposures.

PRODUCT LIABILITY

45%

CLASSES OF INSURANCE

Product Liability, Product Recall, Product Guarantee, Extortion, Kidnap and Ransom

RISK SUMMARY

Computer system design and related service providers have a moderate product liability exposure arising out of bodily injury and property damage as a result of various computer hardware and software products supplied, developed and marketed by them (especially customised designs). It is important to mention that professional advice or service with regard to computer system design and related services provided by the insured is specifically excluded by the product liability policy. Product liability claims could arise as a result of faulty work conducted on hardware by the insured e.g. electric shocks to customers, fires originating in computers on which the insured has performed servicing, and could include claims for loss of data, business interruption and other consequential losses. It is advisable and prudent to write public, products and professional liability exposures either as a package or at least with one underwriter to minimise the potential for gaps in

cover. Other than the above product liability exposure is usually limited to the provision of corporate giftware or the responsibility for food and drink provided at functions.

PROFESSIONAL INDEMNITY

65%

CLASSES OF INSURANCE

RISK SUMMARY

Due to the nature of the work performed by the insured, various potential claims may arise which may fall under public liability, product liability or professional indemnity policies depending on the cause and circumstances of the losses/ incidents. Such claims may include and but not limited to:

- a. computer systems failures resulting in loss of data, business interruptions and so, which may result from faulty workmanship, design etc;
- b. incorrect recommendations regarding the selection of systems, software, hardware;
- c. breach of confidentiality, invasion of privacy and identity theft. Inadequate security could lead to personal identifying information being released and suffering unauthorised use;
- d. Intellectual Property Risks (copyright, trademark infringement, defamation, encryption, discovery, publishing and advertising risks;
- e. inadequate system testing, quality control, errors in judgement in design, failing to identify and resolve issues;
- f. transmission of virus, worm, spy-ware, trojan or similar destructive or damaging application which is inadvertently spread to customer systems or hardware; (f) destruction of or loss of integrity of data;
- g. financial loss arising from e-commerce transactions
- h. failing to adequately evaluate an organisation's computing environment for effective operational procedures, systems software/hardware, systems development and security procedures;
- i. not meeting time, cost and performance warranties in contracts;
- j. failure to continue or complete development of system/software in accordance with the contract specifications;
- k. loss of customers data due to insured's failure to carry out a backup of the information on the system and
- l. software developed by the insured not complying with agreed functionality etc.

As mentioned above some of these areas of liability are somewhat gray in terms of liability policy response and clarification should be sought from liability underwriters whether these aspects are to be covered under the general liability policy, product liability or professional indemnity/errors and omissions cover. Many IT risks outlined above are in the nature of professional indemnity exposures and generally it is preferable to write public, products and professional liability exposures either as a package or at least with one underwriter to minimise the potential for gaps in

cover. It is important to note that most broadform liability policies cannot accommodate many IT business risks which are excluded under the Treatment, Design and Professional risks exclusion. However, some insurers do offer tailored product for this occupation.

MANAGEMENT LIABILITY

CLASSES OF INSURANCE

55%

Directors and Officers Liability, Employment Practices Liability, Statutory Liability, Crime, Cyber / Internet Liability, Taxation, Trustees

RISK SUMMARY

Moderate exposure to directors and officers, cyber, statutory liability, employment practices, tax and similar corporate/operational risks, which increase with the size, complexity of the operation and number of employees. Examples of possible claims / exposures under each insurance class may include:

- Directors and officers - false, misleading and deceptive conduct, not acting in the best interest of shareholders, breach of trust, misappropriation of company funds / trade secrets, errors and omissions in financial reports, mixing personal and business assets, unfair treatment of shareholders, unfair trading activities, unfair competition, breach of intellectual property rights, insolvent trading, breach of contract, mismanagement of cyber risk exposure, failing to provide adequate training and supervision/ a safe environment for work, environmental breach/prosecution etc.
Increased regulations have heightened the operating risk for businesses of all sizes. Furthermore, with a fast-changing regulatory environment, directors are often unaware of their full legal responsibilities. Directors and officers have duties and obligations, for which they are personally responsible, some of which may carry unlimited personal liability.
- Cyber/Internet Liability - breach of privacy/security, inadvertent transmission of a computer virus, deleted or stolen data following hacking, damage to network, system or website, plagiarism, copyright infringement, cyber extortion / ransom demand. Inadequate privacy /security compliance through procedures and systems, poor management of large volumes of personal/corporate data are other common issues. These incidents can result in financial losses, reputational damage, and legal and regulatory consequences for the business.
- Statutory Liability - breaches of legislation and non-compliance - e.g., occupational health and safety laws, privacy/security laws, design laws, financial market misconduct etc. Non-existence of adequate compliance and control measures can be an issue (if applicable). Businesses are exposed to hundreds of pieces of legislation and the cost to a business of a simple regulatory breach /investigation can be considerable.
- Employment Practice Liability – allegations of unfair/wrongful dismissal, workplace harassment, bullying, sexual harassment, discrimination (e.g., age, racial, sexual, religious,

disability, etc.), failure to maintain a safe workplace / working environment, breach of contract / employment contracts etc. Other issues may include - possible presence of part-time, casual or trainee personnel, long working hours, inadequate level of supervision etc. Employees are much more aware of their rights at work and are prepared to pursue claims against their employers. Hidden costs of employment practice liability related problems include – negative publicity, damage to reputation and goodwill, loss of productivity, stress for both the employer and employee etc.

- Crime - employee or third-party crime, including theft of money and property, fraud by internal collusion, employee fraud by collusion with suppliers, theft by contractors/consultants, fraudulent funds transfer, counterfeit fraud, forgery, credit card fraud, social engineering fraud etc. Higher exposure for businesses with inadequate controls in place.
- Taxation - non-compliance with taxation legislation / not meeting certain tax obligations, failure to keep records, poor accounting and monetary management, mistakes while filing tax returns of the business, asset misappropriation (physical and financial) etc. potential costs for such breach include e.g., taxation and government audit investigation costs, penalties for breaches of taxation legislation.
- Trustees - inappropriate investment strategy, failure to monitor fund performance, failure to prevent fraud, failure to insure trust property, conflict of interest, incorrect advice, incorrect payments etc. Other common issues may include - failure by trustees to discharge their obligations to the required standard, not acting in accordance with the trust deed and common law and legislation, lack of or no established governance & risk management framework etc.

The range of claims/lawsuits being pursued against business owners/operators by employees, shareholders, regulators, creditors or others are on the rise and the cost to a business for a simple regulatory investigation can be substantial. Claims costs and associated legal/other fees (investigation cost, defence cost, civil fines & pecuniary penalties, public relations expenses etc) that can arise when an incident occurs can be financially crippling for the business.

It should be emphasised that Management Liability insurance is designed to meet specific needs of small to medium sized companies and not for very large organisations. Further insurance coverage and limits offered under each policy will vary from insurer to insurer.

EMPLOYER LIABILITY / WORKER'S COMPENSATION

34%

CLASSES OF INSURANCE

RISK SUMMARY

Medium exposure. Possible claims mainly arise from:

- a. electrical shocks from malfunctioning computers or communications equipment;

- b. musculoskeletal injuries such as repetitive strain injuries, carpal tunnel syndrome etc due to frequent use of computer key boards, mouse, trackballs etc;
- c. injuries sustained during servicing and repair/build operations e.g. from soldering tools, cuts on casings etc;
- d. office risks including slips and falls, kitchen injuries and so on.

Mobile service/repairers and troubleshooters will be exposed to the hazards of the insured's operations whilst on site although mainly work will take place in office environments and the service staff will not be exposed to industrial/hazardous processes. Driving risks should be considered, particularly where there is a heavy workload. Employees in this industry may work long hours and suffer exposure to stress related sicknesses.

CYBER RISKS

68%

CLASSES OF INSURANCE

RISK SUMMARY

- Heavy dependency on digital technology/integrated IT systems;
- Security/privacy breach - presence of large volumes of sensitive personal and cooperate data;
- Data breach – laptops/data sticks being left on various places, emails sent in error, sensitive documents not being properly shredded, back-up hard drives being lost;
- External hacking attacks, internal negligence, deliberate acts, system glitches etc.;
- Electronic data/software loss and replacement cost following a cyber-attack;
- Electronic media liability - including invasion of privacy, libel or slander, infringement of copyright, title, slogan, trademark or service names including domain names, false advertising etc.;
- Business interruption/increased in cost of working following a cyber-attack;
- Businesses held to ransom before systems are released;
- Cyber-threat from interconnected supply chain business partners/outsourced services providers;
- Internal control and other issues – e.g. non-segregation of sensitive data, inadequate user access control/password protection, outdated POS software applications, absence of up to date antivirus software/firewalls, unencrypted data/information/lack of end-to-end encryption;
- Possible presence of older devices/computer systems with outdated operating systems and unsupported software;
- Inadequate training for employees on data security/privacy/cyber risk. No or inadequate background checks conducted on employees/various service providers/suppliers etc.;

- Compliance and control issues - possible lapses on policies, procedures and protocols on cyber security and related matters (if applicable);
- Cyber threat relating to - Bring your own devices (BYOD), download and install personal, or unauthorised software, use of USB or other media devices etc;
- Extra expenses following a cyber incident including forensic investigation costs, crisis management expenses, notification and monitoring expenses, remediation/other extra expenses;
- Brand and reputational damage following a cyber-attack/data breach;
- Security lapses in company web-sites – cyber threat to own hardware and software; cyber threat to visitors of the website;
- Lack of security measures including a combination of technology (e.g. IT security) and physical security at the premises;

CORPORATE TRAVEL

31%

CLASSES OF INSURANCE

RISK SUMMARY

Exposure will vary considerably depending on the various factors including - number of persons travelling in any given year, the frequency of travel, staff designations, the numbers travelling together (accumulation), destinations (local/overseas), reasons for travel / nature of work undertaken, issues/risks/hazards, that can affect an employee's health, safety and security whilst travelling, transport mode, staff's fitness to travel /work abroad, previous travel experience, specific health risks at the destination, availability of reliable emergency services etc. Therefore, given hazard rating to be further assessed, considering the above factors in mind. Other main risks for this industry category may include:

- Some travel staff may perform hazardous activities (sometimes remote locations/unsafe worksite/s) which may require a high level of physicality and use of heavy equipment.
- Other travel staff are unlikely to be involved in worksite activity and will usually be visiting offices or attending conferences, training or trade events etc.
- Increase risk due to political, social and economic volatility/instability in many parts of the world
- Developing countries/remote locations - non-availability of appropriate medical services, transport challenges with access during a medical emergency / evacuation difficulty / reduced access to adequate infrastructure for medical attention.
- Security related issues/concerns in some locations/countries – terrorist attacks, civil unrest/war, kidnap and ransom, harassment etc.
- Traveller falling ill while abroad, delayed flights, losing passport, accommodation mix-ups, local language barriers, as well as exposure to disease, natural disasters and technology failings

- Travelling with company owned equipment; risk to data carrying equipment/loss of baggage /passport
- Legal Risks/Risks to reputation/Illegal activity by travellers - Breaching local laws and customs, misbehaviour by travelling employees/ unethical conduct by employees, non-compliance with regulation.
- Transport and related issues / concerns – flight/tour cancellation, flight delay, miss of a connecting flight, traffic accidents, poor safety standards of transport/public transport / self-driving immediately after long-haul flights
- Business travellers usually stand out from the local population as different, making them a target for criminals and terrorists
- Also refer to Employer Liability/Worker's compensation.

4. WANT MORE CERTAINTY AROUND YOUR BUSINESS RISK...REACH OUT

4Sight Risk Partners was built on a singular truth – that no two clients' business are the same, yet all should feel confident in managing their business with knowledge and certainty around risk.

Our clients secure a strategic advantage from their qualified risk profiles and quantified risk appetite. They leverage our 75 years of global risk and insurance expertise, navigating uncertainties and opportunities with confidence. Operating within our 4Sight Risk Partners 'IQ-ARTA' framework, our clients implement effective tailored risk management solutions.

4Sight Risk Partners collective strength, choice, and value, along with Insurance Advisernet's network, constitutes our greatest asset. 4Sight Risk Partners give our clients confidence and greater clarity around risk and insurance, despite its complexity. We provide trusted advice and advocate for our clients as their valued business partner.

To find out more go to www.4sightrisk.com.au or reach out.



4Sight Risk Partners Pty Ltd


☎ 0499 988 980

☎ +61(0) 499 988 980

✉ gareth@4sightrisk.com.au

📍 Level 31, 100 Miller Street
North Sydney NSW 2060, Australia

4Sight Risk Partners Pty Ltd is a Corporate Authorised Representative, Number: 1251287, of Insurance Advisernet Australia. Australian Financial Services License Number: 240549.

www.lmiriskcoach.com 
riskcoach@lmigroup.com 