INSURANCE
COUNCIL OF
AUSTRALIA

E-Commerce Crime and Vandalism –

Defence Plan for the General Insurance Industry

Contents

Purpose and Structure of this Document 1

1 Legal Issues on E-Commerce 2

2 E-Commerce Crime and Vandalism Exposures 6

3 Definitional Risk Management Framework 10

4 General Insurance Information – Privacy Code 18

5 General Insurance Code of Practice 21

6 Glossary of Terms 23

7 References and Annexures 28

Purpose and Structure of this Document

This document provides key points on a framework for an e-commerce crime and vandalism defence plan.

It is structured to:

- Raise awareness of e-commerce crime in the general insurance industry.
- Provide a general overview relating to e-commerce crime issues.
- Provide a general risk management model and to refer insurers to useful sources of information on security management.

Industry groups and individual insurance companies generally have risk management processes and operational contingency plans in place. The recommended approach for e-commerce crime and vandalism is to review and, where appropriate, strengthen these plans for specific issues related to e-commerce. Information in this document is relevant as at 3 July 2001.

1

Legal Issues on E-Commerce

Computer Crime: Law in Australia

The Commonwealth, State and Territories Attorneys-General have agreed to implement new laws in relation to Model Criminal Code Discussion Papers (Chapter 4). Legislation introduced, or to be introduced, will deal with crimes in relation to unlawful access, modification or impairment of data, including identity theft offences, and crimes in relation to the unauthorised impairment of electronic communication.

The agreed offences dove tail with the terminology of the Electronic Transactions Act 1999.

Legislation has been introduced into New South Wales and a Bill is before the Commonwealth Parliament. It can be expected that other States and Territories will follow with their legislation in coming months. The existing laws applicable in those States and Territories have been included in this report.

Commonwealth

The Cybercrime Bill 2001 was introduced into Parliament on 27 June 2001 and is proposed to complement State and Territory legislation.

New South Wales

On 19 June 2001 the Crimes Amendment (Computer Offences) Bill 2001 was assented and is part of proposed Australia-wide legislation. At the time of writing this report the Act had not been proclaimed.

Victoria

In 1988 the Summary Offences Act 1996 was amended to include the offence “Computer Trespass”. Section 9A provides a person must not gain access to, or enter, a computer system or part of a computer system without authority to do so.

Queensland

In 1997 section 408D entitled “Computer hacking and misuse” was inserted into the Criminal Code Act 1899

Western Australia

In 1990 the Criminal Code Act Compilation Act 1913 was amended to include an offence entitled “Unlawful operation of a computer system” (see section 440A of the Act).

South Australia

In 1989 the Summary Offences Act 1953 was amended to include the offence of “Unlawful operation of computer system” (see section 44 of the Act).

Tasmania

In 1990 the Criminal Code Act 1924 was amended to insert Chapter XXVIIIA entitled "Crimes Relating to Computers". In addition to Chapter XXVIIIA of the Crimes Act, Tasmania also has ss43A-43D of the Police Offences Act 1935, which appear to overlap considerably with the Crimes Act provisions.

Australian Capital Territory

In 1998 the Crimes Act 1900 was amended to insert a division entitled "Offences relating to computers" (see sections 135H to 135L of the Act).

Northern Territory

In 1984 Section 276(1) was inserted into the Northern Territory Criminal Code. This section covers computer related fraud and establishes the offence of making false data processing material. There is also Section 222 that makes it an offence to unlawfully extract confidential information from a computer with intent to cause harm to another person or to obtain an advantage.

The implementation of laws in Australia are of little consequence where the computer crime originates from outside Australia, for example, where a computer virus is created outside Australia but imported into Australian computers. In such cases Australia would have to rely on the adequacy of international laws or the laws governing the particular country where the perpetrator lives. In these circumstances there is a need for cooperation at an international level.

Gathering Evidence of Computer Crime

Laws in relation to computer crime are of no assistance unless adequate evidence is available which law enforcement agencies can rely upon to obtain a conviction where there is guilt on the part of the offender. From a business perspective it is important to be aware of potential evidence that must be collected, preserved and archived. It is also important to be aware of the form evidence must take in order to be admissible in the relevant court of law.

Each of the states, territories and the Commonwealth have their own rules of evidence which determine the admissibility of computer crime evidence in a court of law.

In each of these we have:

- The Commonwealth Evidence Act 1995.
- New South Wales has the Evidence Act 1995 which essentially mirrors the Commonwealth Act.
- Australian Capital Territory applies the Commonwealth Evidence Act 1995 in its courts.
- Victoria has the Evidence Act 1958.
- Queensland has the Evidence Act 1977.
- Western Australia has the Evidence Act 1906.
- South Australia has the Evidence Act 1929.
- Tasmania has the Evidence Act 1910.
- Northern Territory has the Evidence Act 1939.

Which rules of evidence apply and whether evidence is admissible will ultimately depend on the jurisdiction where the offence is prosecuted. In recent years there has been an attempt made to standardise the rules of evidence in Australia but to date there has not been complete standardisation.

Once a potential computer crime has been detected it is important to know when to hand the matter over to appropriate law enforcement agency and indeed which agency should be contacted.

The gathering of evidence could involve real evidence such as that produced by an audit function from a log and testimonial evidence provided by a witness. A system should never be shut down before evidence is collected.

The actual process of capturing the data and its storage is important as it can affect how the data is perceived. Establishing a clear chain of custody is crucial because electronic evidence can be altered.

Why is Evidence Collected

Evidence can be collected to stop someone else or the original party from doing the crime again. It can also bring the responsible party to justice.

The information gathered can also be used by others to prevent further attacks.

2

E-Commerce Crime and Vandalism Exposures

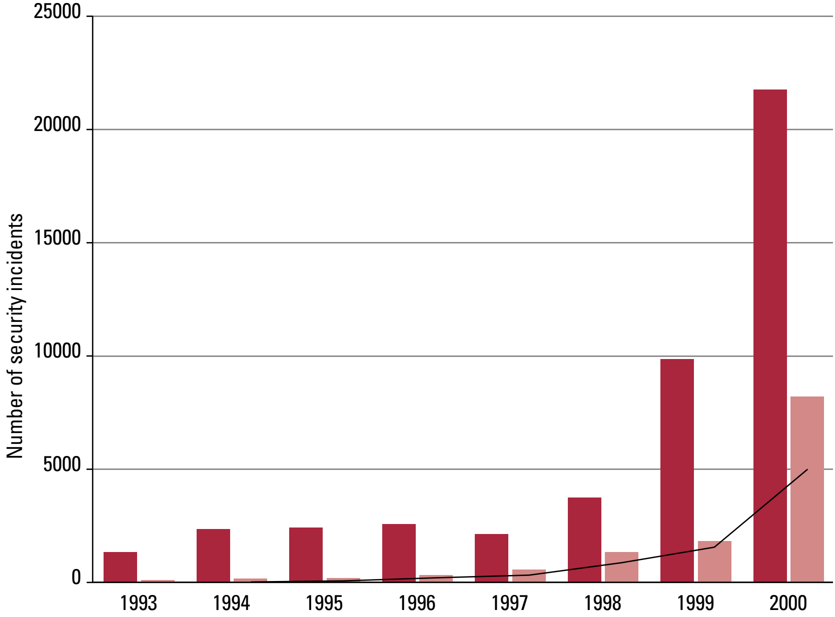
In Australia more than three million households and over one billion people worldwide are connected to the Internet. With the large growth in the Internet population and in electronic commerce over the last decade the integrity, security and reliability of computer data and electronic communication is becoming increasingly important.

Cybercrime activities, including hacking, virus propagation, "denial of service" attacks and web site vandalism, pose a significant threat to the integrity and security of computer data. The Commonwealth Attorney-General has quoted cybercrime as costing companies worldwide approximately $3 trillion dollars each year.

In the chart below is a comparison of Australian based security incidents which have been compared to the USA. It also indicates as a percentage the proportion of Australian to USA data. The chart highlights an increasing trend of severity incidents occurring in Australia which should be a concern to the general insurance industry.

Comparison of Australian Computer Security Incidents to USA

(Source: auscert.org.au & cert.org)



■ USA	1334	2340	2412	2573	2134	3734	9859	21756
■ AUS	110	171	191	309	572	1342	1816	8197
□ % AUS to USA	8%	7%	8%	12%	27%	36%	18%	38%

This line represents moving average

Whilst there is no specific definition for security incidents they would generally fall in to one of the following risk areas:

- Attempting to defraud business;
- Defrauding business;
- Dishonestly obtaining financial advantage from business;
- Dishonestly causing loss or damage to business;
- Extortion;
- Obtaining access to confidential information on business customers, including trade secrets and information of commercial value;
- Destroying, erasing or corrupting data; and
- Interfering with, interrupting and obstructing the lawful use of a computer or computers.

E-Commerce Security Risks and Threats

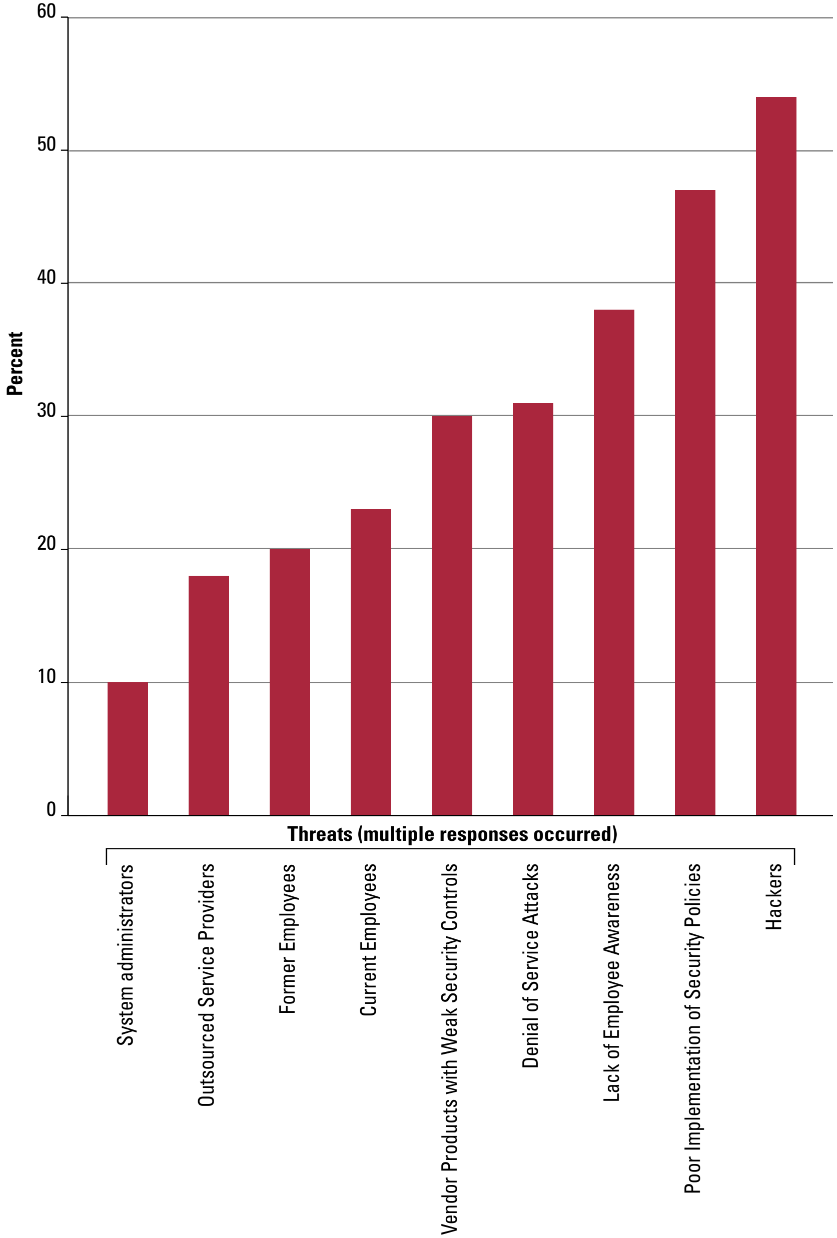
The chart below is based on survey responses from several countries. Survey participants were asked what they considered the greatest threats to their company's e-commerce system. Survey participants identified the greatest areas of threat to their e-commerce systems as:

- Hackers
- Poor implementation of security policies
- Lack of employee awareness

The survey responses were consistent for all participating countries – each country identified as their greatest threats a minimum of two of the three threats identified above.

Greatest Areas of Threat

(Taken from KPMG – 2001 global e.fraud survey.)



3

Definitional Risk Management Framework

This process can be applied to e-commerce by identifying threats or risks in relation to prevention, detection and response to e-crime and vandalism.

Some of the measures that may be adopted by general insurance companies in the "Risk Management Process" are outlined in this section.

Main elements of risk management:

The main elements to the risk management process include:

Establish the context (strategic, organisational and risk management context), identify risks, analyse risks, evaluate risks, treat risks, monitor and review, communicate and consult.

A risk assessment should be undertaken:

a. To determine effective security policy and controls.

b. When new systems or applications are introduced.

c. As part of change control procedures to determine if changes in configuration alter the agreed risk level, introduce new risk factors, and to reassess the risk associated with the change.

d. Periodically to ascertain if the risk environment has changed (emergence of new threats and vulnerabilities, changes in threat likelihood or changes in the asset value).

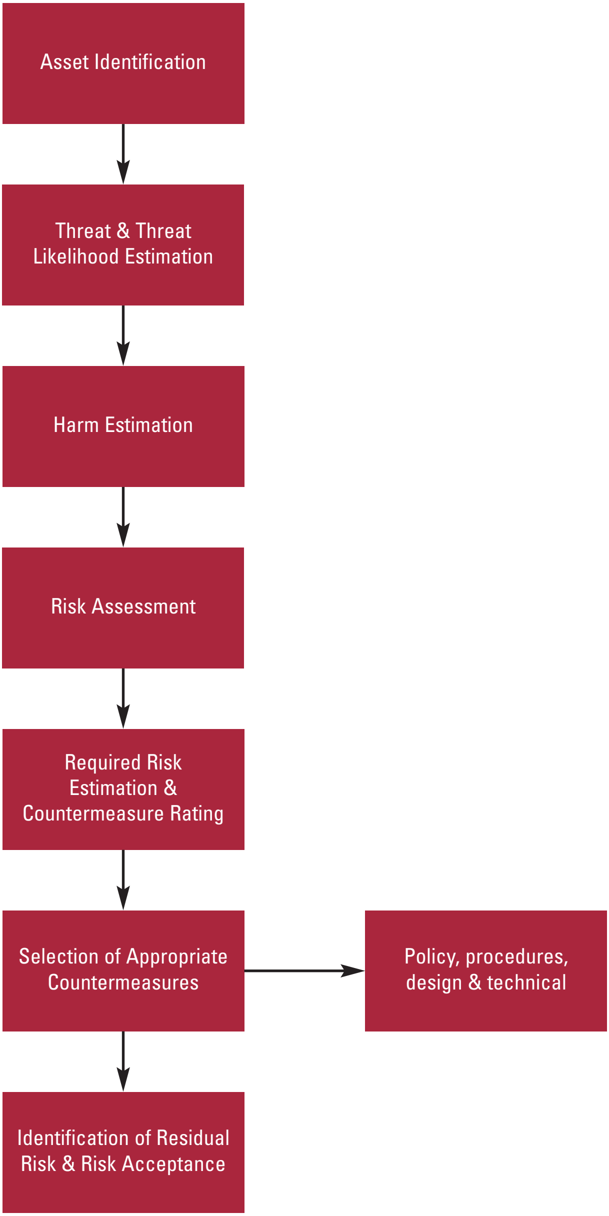
A risk assessment should have a flow through effect into policy objectives and identification of countermeasures.

A risk assessment is not a one-off process that is completed and forgotten. It is an ongoing process that should be reviewed regularly to take into account changes in the value of assets, nature of threat and changes in function, service or design, which may introduce new vulnerabilities.

Changes in the applied countermeasures may also alter the risk level.
Risk management is a tool used to balance business objectives and security requirements in order to achieve cost effective security measures.

The Security Risk Assessment Methodology chart on page 12 is designed to demonstrate the key features and the sequence that could be adopted to form a basis of an e-commerce defence plan.

Security Risk Assessment Methodology


Asset Identification
Threat & Threat Likelihood Estimation
Harm Estimation
Risk Assessment
Required Risk Estimation & Countermeasure Rating
Selection of Appropriate Countermeasures
Policy, procedures, design & technical
Identification of Residual Risk & Risk Acceptance

Asset Identification

An "asset" can be a tangible item, such as hardware, a grade or level of service, staff, or information.

- **Confidentiality of Information.** This could include all major databases or information storage centres.
- **Availability of Resources and Services**. This relates to those resources or services that require a degree of reliability, which has obvious implications on the infrastructure and system(s) configuration.
- **Integrity of Information.** Ensuring accuracy of information and the integrity of those processes required for creating or updating information is the third category of information assets that should be considered.
- **Equipment, including Software.** Includes those assets related to the effective operation of the systems, including PCs, mainframes, PABX systems, photocopiers and printers.
- **Staff.** This component may be included here, but more commonly forms part of a personnel or physical security risk assessment.

Threats and Estimation of Likelihood

There could be multiple threats associated with one asset, and this should be reflected in the risk assessment process. Threat estimation should include consideration of inherent vulnerabilities. Information on the probability of external threats can be derived in quantitative form from outside sources. The likelihood of internal threats can be estimated using previous experience of a company.

The source of the threat may be used in determining its probability (eg the likelihood of an attack by a highly skilled and motivated hacker may be different from that of teenagers using tools downloaded from the Internet). The threat probability is a measure of the likelihood of the threat being realised and the source is a consideration of estimating motive and capabilities.

Risk analysis methodologies include determining the threat by qualitative, semi-quantitative or fully quantitative methods.

The scale below could be used for categorising threat probability:

Negligible	Unlikely to occur
Very Low	Likely to occur two/three times every five years
Low	Likely to occur once every year or less
Medium	Likely to occur once every six months or less
High	Likely to occur once per month or less
Very High	Likely to occur multiple times per month or less
Extreme	Likely to occur multiple times per day

Consequence or Harm Estimation

Harm is not related to threat likelihood. The threat likelihood of the loss of a proxy server due to an unstable operating system may be “high”, however the harm may be “minor” if the proxy server supporting the service of resource is not viewed by the data owner or management as critical.

The likelihood of accidental misconfiguration of a firewall may be “very low”, but its impact or harm could be “serious” to the security integrity of the system.

A guide to the consequence definitions that could be used in developing a security risk assessment:

Insignificant	Will have almost no impact if threat is realised.
Minor	Will have some minor effect on the asset value. Will not require any extra effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, only small but will require some expenditure.
Damaging	May cause damage to the reputation of system management, or notable loss of confidence in the system's resources or services. Will require significant expenditure to repair.
Serious	May cause extended system outage, loss of connected customers or business confidence.
Grave	May cause system to be permanently closed.

Risk Assessment

Risk can be expressed as *threat likelihood x consequence = risk*.

Using the definitions of *threat likelihood* and *consequence* the following table is an example of how it is expressed to show the degree of risk.

Risk Assessment Table

Asset Identification	**Threat to the Asset**	**Threat Likelihood**	**Harm, if threat is Realised**	**Resultant Risk**	**Required Risk**	**Counter-measure(s) Priority Rating**
Protection of sensitive internal e-mails	Inadvertent distribution of sensitive e-mail to outside addressee	Very high	Serious	Extreme	Nil	5
Reliability of e-commerce related web site	Accidental electrical power or equipment failure	Medium	Grave	Critical	Nil	4
Availability of external e-mail services	IP based "Denial of service" attack on the mail host	Extreme	Damaging	Critical	Low	3
	"Mail Bomb" attack on the mail host	Very High	Damaging	Critical	Low	3
Accuracy of Customer Information Database (CID)	Unauthorised access and tampering with information	Low	Serious	High	Nil	3
Secure disposal of redundant information media	Accidental compromise of sensitive information	Low	Serious	High	Nil	3
Secure access control to the electrical distribution panel/ system or any component of it (excluding UPS)	Inadvertent power outage due to accidental tampering with distribution system(s)	Low	Grave	High	Low	2
Accuracy of publicly available web information	Loss of confidence or goodwill due to "hacking" of web page	High	Minor	Medium	Low	1
Secure access to internal network services by authorised staff, from external networks	Loss of crypto token or keys required to access the secure channel(s)	Very low	Serious	Medium	Low	1

Countermeasure Priority Rating:

The countermeasure rating is the difference between required risk and resultant risk (expressed as a number).

Nil	0
Low	1
Medium	2
High	3
Critical	4
Extreme	5

The priority of the countermeasures should be reflected in the security policy and planning documents, which may relate to:

a. addition of security measures;

b. reduction of security measures;

c. risk avoidance through change of service and system specifications;

d. acceptance of residual risk; and

e. minimisation of harm through response mechanisms.

Insurance Areas of Exposure:

Some of the specific exposures for insurers are:

- Many insurers share information with intermediaries, loss adjusters and solicitors. It is important that they have secure systems and procedures.
- Insurers can rely on organisations for outsourced claims and it is important that they have adequate IT security in place.
- Insurers may be targeted by radical organisations. The aim may be to obtain information or disrupt the business.
- Insurers should consider their reputational risk which could be affected if they have not taken suitable action to minimise e-crime exposure. Other areas that could be affected are business continuity, security, misuse of products and services and with outsourcing Internet service provider, web designer and critical risk management support.

Vandalism to an insurer's information system hampers it from obtaining the full benefits of e-commerce and results in remedial costs. This leads to flow on costs to consumers in the form of increased premiums. Preventative measures in the form of appropriate defence strategy should limit the opportunity or affects of vandalism and as a consequence have a positive effect on the cost to consumers.

Incident Response Plan (IRT)

An IRT team within an organisation is extremely important and information on this can be obtained from the Auscert web site:
www.Auscert.org.au/Information/Auscert_info/Papers/Forming_an_Incident_Response_Team.html

Some areas to consider are; composition of the Incident Response Team, goals, scope of operation, staff training, operational manual, what technology will be dealt with, incident response and how it is handled, reporting and enforcement to name a few.

Risk Management Prudential Standard

The Australian Prudential Regulation Authority requires management to consider all risks and put in place strategies to mitigate and monitor the effectiveness of risk reduction measures. Further information on this can be obtained from the APRA web site (www.apra.gov.au) under "Insurance and Superannuation – General Insurance Discussion Paper – March 2001".

It may be prudent for insurers to discuss with external e-security specialists their specific needs. The risk management planning process may be beyond the internal resources of companies.

ICA acknowledges the assistance of the Defence Signals Directorate (Handbook 4 Security Management 33 (ACSI 33) dated 24 April 2001 and Standards Australia (AS4360) Risk Management published on 12 April 1999 in producing this section of the Defence Plan.

Commonwealth of Australia copyright reproduced by permission.

4

General Insurance Information – Privacy Code

An Information Privacy Code has been developed by the general insurance industry in response to the concern of consumers about the protection of personal information provided to insurers. There is a need for safeguards to be put in place to protect the personal information of customers. The Commonwealth Privacy Act is effective from 21 December 2001. Further information can be obtained on www.privacy.gov.au.

The Privacy Principles impose obligations and responsibilities on the insurer in its management of information for the protection of its customer. These include the protection of the information from misuse. The development of a management strategy to combat e-commerce crime and vandalism will provide this protection but it must be in line with the Privacy Principles. The operation of such strategy must take into account the principles that afford the customer's information protection and limit the circumstances in which their information might be disclosed to third parties.

There is an obligation on an insurer to protect the information under the Privacy Code. Principle 4.1 on Data Security provides in particular in relation to insurers that:

- "an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure".

Thus a management plan that combats e-commerce crime and vandalism is clearly part of the insurer's opportunity to protect personal information. In meeting this responsibility, it is important the plan falls within the ambit of Principle 5.1 on openness, which provides:

- "an organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it".

An insurer should inform its customers in this context that it has a programme in place that will protect the personal information that it holds. The document should clearly inform the customer of the circumstances in which use and disclosure can be made of personal information to the parties and this would certainly be allowable in instances of e-commerce crime or vandalism under the principles.

There is a strong directive that the information be only used for a limited purpose with Principle 2.1 stating that in relation to the use and disclosure of information:

- "an organisation may only use or disclose personal information for the primary purpose for which it was collected".

There are circumstances in which the information can be provided to third parties.

For example, Principle 2.1(f) provides when:

"an organisation may use or disclose personal information for a secondary purpose if it suspects that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities".

A management strategy that combats e-commerce crime and vandalism is part of the insurer's responsibility to protect personal information from misuse. Provided consumers are informed that protection is in place and the circumstances in which third parties are to be provided with personal information it will conform to the Privacy Code.

5

General Insurance Code of Practice

There is a General Insurance Code of Practice for all general insurers. The aim of the Code is to raise the standards of practice and service in the industry.
The development of a management strategy by insurers to combat e-commerce crime and vandalism is in keeping with the aim and objectives of the Code of Practice.

A number of principles guide achieving the objectives of the Code and in particular Clause 1.3 of the Code states:

- "the objectives of this Code shall be achieved and the provisions of this Code shall be applied,

  (e) having regard to the need to protect consumers and insurers from the increased costs from fraud".

Further clause 7.1 provides the responsibility is on insurers to achieve such an objective as:

"an insurer shall ensure that it:

(a) implements appropriate systems and documentation to comply with the Code".

The development of a management strategy against e-commerce crime should be seen as a linkage to the Code. The extension of such a strategy to combat vandalism is a logical step and provides added benefits for consumers.

6 Glossary of Terms

Introduction

The list below sets out some of the key terms used in the e-commerce context (which are relevant to e-commerce crime and fraud) and there are others available addressing these definitions.

Electronic commerce:

"A general term applied to use of computer and telecommunications technologies, particularly on an inter-enterprise basis to support trading in goods and services. Electronic commerce uses a variety of technologies such as EDI, e-mail, facsimile transfer, electronic catalogues and directory systems."

Acceptable risk –(www.its.bldroc.gov/projects/t1glossary2000)
Is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.

Authorisation –(www.zdwebopedia.com)
The process of granting or denying access to a network resource. Most computer security systems are based on a two-step process. The first stage is *authentication*, which ensures that a user is who he or she claims to be. The second stage is authorisation, which allows the user access to various resources based on the user's identity.

Authentication –(www.zdwebopedia.com)
The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from *authorisation*, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Availability protection –(www.its.bldroc.gov/projects/t1glossary2000)
Requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical.

Certification –(www.its.bldroc.gov/projects/t1glossary2000)
Is synonymous with the term authorise processing. Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements. See also (Accreditation) and (Authorise Processing.)

Confidentiality protection –(www.its.bldroc.gov/projects/t1glossary2000)
Requires access controls such as user ID/passwords, terminal identifiers, restrictions on actions like read, write, delete, etc. Examples of confidentiality-protected information are personnel, financial, proprietary, trade secrets, internal agency, investigations, other federal agency, national resources, national security, and high or new technology under Executive Order or Act of Congress.

Computer crime –(www.its.bldroc.gov/projects/t1glossary2000)
A violation of law committed with the aid of, or directly involving, a data processing system or network. [2382-pt.8]

Denial of service –(www.its.bldroc.gov/projects/t1glossary2000)
The prevention of authorised access to resources or the delaying of time-critical operations. [2382-pt.8] 2. The result of any action or series of actions that prevents any part of an information system (IS) from functioning. [INFOSEC-99]

EDI –(www.zdwebopedia.com)
Short for Electronic Data Interchange, the transfer of data between different companies using networks, such as the Internet. As more and more companies get connected to the Internet, EDI is becoming increasingly important as an easy mechanism for companies to buy, sell, and trade information. ANSI has approved a set of EDI standards known as the X12 standards.

Encryption –(www.zdwebopedia.com)
The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text*; encrypted data is referred to as *cipher text*. There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.

Firewall –(www.its.bldroc.gov/projects/t1glossary2000)
[A] system designed to defend against unauthorised access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. [INFOSEC-99] Synonyms front-end security filter, proxy.

Hack –(www.its.bldroc.gov/projects/t1glossary2000)
To break into or use a computer network or use a system without authorisation, as a hacker might do. 2. Referring to a track used to bypass a flaw or a bug in an application program or application.

Hacker –(www.its.bldroc.gov/projects/t1glossary2000)
A person who breaks into, or attempts to break into, or use, a computer network or system without authorisation, often at random, for personal amusement or gratification, and not necessarily with malicious intent. 2. [An] unauthorised user who attempts to or gains access to an information system (IS). [INFOSEC-99] 3. A technically sophisticated computer expert who intentionally gains unauthorised access to targeted protected resources. [After ANSDIT] 4. Loosely, a computer enthusiast. [ANSDIT] 5. A person who uses a computer resource in a manner for which it is not intended or which is in conflict with the terms of an acceptable-use policy, but (unlike the work of a cracker) is not necessarily malicious in intent.

Identity authentication process
–(www.its.bldroc.gov/projects/t1glossary2000)
The performance of tests to enable a data processing system to recognise entities. Note: An example of identity authentication is the checking of a password or identity token. [2382-pt.8]

Identity authentication –(www.its.bldroc.gov/projects/t1glossary2000)
Is the process whereby some chosen attribute of a real-world entity (‘the distinguishing character or personality of an individual’) is demonstrated to belong to that entity.

Identity authentication is the process whereby some chosen attribute of a real-world entity (‘the distinguishing character or personality of an individual’) is demonstrated to belong to that entity. For example, if I am standing in front of you (provided that you are not visually impaired) the unique topography of my face is demonstrated to belong to me because you can see that it is attached to the rest of my body and that it displays all the subtleties of expression that you would expect in a human face. Thus, seeing my face permits identity authentication to take place. Note that I do not need to tell you my name.

Information systems security (INFOSEC and/or ISS)
–(www.its.bldroc.gov/projects/t1glossary2000)
[The] protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorised users, including those measures necessary to detect, document, and counter such threats. [INFOSEC]

Public-key encryption –(www.zdwebopedia.com)
A cryptographic system that uses two keys – a public key known to everyone and a private or secret key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it.

Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman. For this reason, it is sometime called Diffie-Hellman encryption. It is also called asymmetric encryption because it uses two keys instead of one key (symmetric encryption).

Packet sniffer –(www.its.bldroc.gov/projects/t1glossary2000)
A dedicated device designed for the purpose of monitoring network traffic in order to recognise and decode certain packets of interest. 2. A software package that enables a general-purpose computer to recognise and decode certain packets of interest. [After 2382-pt.35] Note: The packet sniffer is normally used by system administrators for network management and diagnostics, but is occasionally used by hackers for illicit purposes such as stealing a user's password or credit-card number. [2382-pt.35] 3. In INFOSEC, synonym sniffer.

Privacy and authentication management
–(www.its.bldroc.gov/projects/t1glossary2000)
Functions to ensure the validity of both maintenance information and telecommunications network traffic key management, intrusion surveillance, and fraud control. [T1.Rpt34-1994]

Risk management –(www.its.bldroc.gov/projects/t1glossary2000)
Is the ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analysing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Virus –(www.its.bldroc.gov/projects/t1glossary2000)
An unwanted program which places itself into other programs, which are shared among computer systems, and replicates itself. Note: A virus is usually manifested by a destructive or disruptive effect on the executable program that it affects.
2. Self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence. [INFOSEC-99].

7

References and Annexures

The following are sources of information from various government and industry bodies on:

- e-commerce
- systems security
- information security management standards
- Management of electronic evidence
- risk management
- contingency planning
- the response process when an entity is dealing with a computer related crime of one form or another
- information services on up-to-date issues and risks relevant to information technology infrastructure.

These links or documents are by no means finite and are only an indication or a guide of the resources available for the research and development of your own specific guidelines.

Australian websites

1. Defence Signals Directorate

http://www.dsd.gov.au/infosec/

DSD's Information Security Group plays a key role in the protection of Australian official communications and information systems. DSD is the national authority for communications security (Comsec) and computer security (Compusec).
For information that is processed, stored or communicated by electronic or similar means. Papers of use written by the DSD cover the topics:

Title	Ver	Date
Introduction	1.0	20/12/00
Standards	1.0	20/12/00
Evaluated Products	1.0	20/12/00
Risk Management	1.0	20/12/00
Security Management	1.0	20/12/00
Emanations and Cabling Security	1.0	20/12/00
Media Security	1.0	20/12/00
System Access Control	1.0	20/12/00
Network Security	1.0	20/12/00
Cryptographic Systems	1.0	20/12/00
Web Security	1.0	20/12/00
Email Security	1.0	20/12/00
Malicious Software	1.0	20/12/00
Intrusion Detection	1.0	20/12/00
Physical Security	1.0	20/12/00

2. Internet Systems – Security and Authentication Issues

http://www.dsd.gov.au/infosec/publications/intsystems.html

The guide exposes Program Managers to some of the new or distinctive security issues that are likely to confront them in online service delivery projects. These may differ from some of the traditional security issues they may be more familiar with from experience with previous IT or physical service delivery projects.

3. Internet Security Checklist

http://www.govonline.gov.au/projects/standards/security_checklist.pdf

4. Standards Australia

AS/NZS 4360:1999 Risk Management

http://www.standards.com.au/Catalogue/Script/Details.asp?DocN=stds000023835

This Standard provides a generic guide for the establishment and implementation of the risk management process involving the identification, analysis, evaluation, treatment and ongoing monitoring of risks.

AS/NZS 17799:2001 Information Security Management – Code Of Practice For Information Security Management

http://www.standards.com.au/Catalogue/Script/Details.asp?DocN=stds000024858

This Standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organisation. It is intended to provide a common basis for developing organisational security standards and effective security management practice and to provide confidence in inter-organisational dealings.

AS/NZS 4444.2:2000 Information Security Management – Specification for Information Security Management Systems

http://www.standards.com.au/Catalogue/Script/Details

This Standard specifies requirements for establishing, implementing and documenting information security management systems (ISMSs). It specifies requirements for security controls to be implemented according to the needs of individual organisations.

5. The National Office of the Information Economy

http://www.noie.gov.au/

NOIE is the National Office for the Information Economy – Australia's leading Commonwealth agency for information economy issues. It was established in 1997. It publishes a number of relevant documents, some of these are below:

E-Commerce Across Australia

http://www.noie.gov.au/projects/information_economy/ecommerce_analysis/eCommAust/index.htm

This study involves the analysis of three seemingly imponderables: the impact of e-commerce on the economy at large; the impact of differing e-commerce preparedness and take up rates in regions; and the response of the underlying economy to such change and differences. It involves forecasting developments well into a future which remains uncertain.

The Phantom Menace: Setting the record straight about online credit card fraud for consumers.

http://www.noie.gov.au/publications/NOIE/consumer/creditcardfraud.pdf

NOIE and the Australian Computer Society explore how perception of high risk may be misplaced in, 'The Phantom Menace: Setting the Record Straight about Online Credit Card Fraud for Consumers'.

Legal Liability and E-Transactions

http://www.noie.gov.au/publications/NOIE/NEAC/publication_utz1508.pdf

This report brings much needed clarity to identifying and assessing liability issues in the use of electronic authentication systems. It also identifies various liability allocation models, and makes useful recommendations to NEAC.

E-Commerce Security: The integration of Business E-Commerce Systems

http://www.noie.gov.au/publications/NOIE/NEAC/publication_csir0608.pdf

This scoping study for NEAC provides advice and information on the technological solutions and standards available to Australian enterprises. It provides an update on the current standards for authentication technologies, including public key technologies, and provides advice on their integration into business e-commerce systems.

6. AusCERT

http://www.auscert.org.au

AusCERT provides a single, trusted point of contact in Australia for the Internet community to deal with computer security incidents and their prevention. AusCERT's aims are to reduce the probability of successful attack, to reduce the direct costs of security to organisations and lower the risk of consequential damage. AusCERT provides Incident Response 24 hours a day 7 days a week. Incidents are accepted by e-mail, fax or telephone. AusCERT provides information and expertise to help members to detect, interpret and respond to attacks. AusCERT facilitates communication between affected parties, gives suggestions based on experience and disseminates information to other parties who may be at risk while protecting privacy and confidentiality as much as possible. Although AusCERT accepts security incident reports from anyone, priority is always given to those sites that are registered and those reports that affect registered clients.

7. Government Online

http://www.govonline.gov.au/projects/publickey/index.asp

An Australian Government resource covering a wide range of issues. This particular link provides information on the governments strategy on the Commonwealth’s strategy on ‘Gatekeeper’. Gatekeeper is the Commonwealth strategy for the use of PKI and a key enabler for the delivery of Government online. Gatekeeper also leads by example to encourage the uptake of e-commerce in the private sector.

8. The Australian Privacy Commissioners Website

http://www.privacy.gov.au/issues/index.html

As the name suggests this is the Australian site dedicated to privacy issues and addresses the issue of information systems and the use of technology in protecting details of persons in Australia. The development of information technology and the Internet has dramatically increased the quantity of information available in digital form. This has resulted in a proliferation of uses of personal information. Some of these have major implications for the privacy of individuals.

9. Austrac

Evidence and the Internet
http://www.austrac.gov.au/text/publications/agec/index.htm

It is also often assumed that it is more difficult to present a criminal case in court if the relevant offences were committed by electronic means rather than on paper. The purpose of this Paper is to consider whether the latter assumption is correct and, if it is, to determine what changes should be made to the rules of evidence.

Research Group into the Law Enforcement Implications of Electronic Commerce Issues Paper (volume 2)
http://www.austrac.gov.au/text/publications/rgec/2/html/index.html

The business community and consumers continue to seek the same levels of legal and commercial certainty that govern conventional business dealings. But how do these assurances and a framework of legal and commercial certainty continue in the virtual world?

Implications of Electronic Commerce (volume 3)
http://www.austrac.gov.au/text/publications/rgec/rgec3/index.htm

10. Department of Industry, Sciences and Resources

http://www.isr.gov.au/industry/ecommerceinfo/Law/law.html

This is an Australian government website that covers:

- ➢ E-Commerce and the Law
- ➢ Encompasses privacy, copyright and a legal framework.

11. Australian Bureau of Criminal Intelligence

http://www.afp.gov.au/publica/platypus/mar00/frddesk.htm

The National Fraud Desk (NFD) is an initiative by Police Commissioners' to facilitate the exchange of fraud and e-crime intelligence between law enforcement agencies to all jurisdictions. The NFD monitors developing trends in many areas of fraud and e-crime and shares this intelligence on a secure intranet site.

To enhance the quality and quantity of fraud and e-crime intelligence, the NFD is strengthening its strategic relationship with the private sector. The NFD has already formed a close liaison with many financial institutions and forensic accounting firms, to facilitate the exchange of intelligence.

Anyone wishing to contract the NFD and/or contribute intelligence to the NFD, please contact Jeff Pope, Coordinator National Fraud Desk on (02) 6243-5640 or e-mail jeff.pope@abci.gov.au or Ross McCrone, Intelligence Officer on (02) 6243-5614 or e-mail ross.mccrone@abci.gov.au.

12. Parliament of Australia Senate

http://www.aph.gov.au/senate/committee/it_ctte/e_privacy/Contents.htm

This is a report by the Australian Senate Select Committee on Information Technologies relating to the Privacy in the Information Society. It has important awareness issues in the context of any information security plans or preventative measures an organisation may be considering as there are recommendations in this paper to protect the privacy of users that may undertake electronic transactions, privacy and disclosure obligations of organisations that have access to consumer databases and the access by consumers to personal information held in consumer databases.

13. Australian Prudential Regulation Authority (APRA)

www.apra.gov.au

APRA is the prudential regulator of banks, insurance companies and superannuation funds, credit unions, building societies and friendly societies.

14. Australian Securities and Investment Commission (ASIC)

www.asic.gov.au

ASIC is one of three Commonwealth government bodies that regulate financial services. It protects policyholders, regulates and enforces laws, underpins the reputation of Australia's financial markets, maintains a public database of companies and works with other financial, consumer and law enforcement bodies in Australia and internationally.

15. BIS Shrapnel

www.bis.com.au

BIS Shrapnel is an economic forecaster who research and analyse companies. They have on their web site under Basel Committee papers on risk management principles in electronic banking and risks in computer and the telecommunication systems.

16. Law enforcement agencies

The following list of law enforcement agencies in Australia provide a port of call if you need to confer with local authorities over a particular incident relating to an information security intrusion, e-fraud or any type of crime.

Australian Federal Police
http://www.afp.gov.au/ecrime/index.htm

Provides daily cybercrime reports, electronic crime strategy report, e-crime link source and documentation about on-line security.

NSW Police Service
http://www.police.nsw.gov.au/main/default.cfm

Queensland Police Service
http://www.police.qld.gov.au/

Victorian Police Service
http://www.police.vic.gov.au/

Tasmanian Police Service
http://www.police.tas.gov.au/

South Australian Police Service
http://www.sapolice.sa.gov.au/

West Australian Police Service
http://www.wapol.gov.au/

Northern Territory Police Service
http://www.nt.gov.au/pfes/

Interpol
http://www.interpol.int/

This is the International Criminal Police Organisation. Like the Australian websites, this website provides a means of conferring with an agency where there are international concerns and you are not sure who to report a problem to.

17. Federal Treasury Department

www.ecommerce.treasury.gov.au

Treasury has information available on their web site on the E-Commerce Best Practice Model which is designed to assist business in meeting their legal and consumer obligations.

International websites

• National Infrastructure Protection Center (NIPC)

http://www.nipc.gov/

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The mission of the NIPC is to:

- ➢ detect, deter, assess, warn, respond, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target our critical infrastructures;
- ➢ manage computer intrusion investigations;
- ➢ support law enforcement, counter-terrorism, and foreign counterintelligence missions related to cyber crimes and intrusion;
- ➢ support national security authorities when unlawful acts go beyond crime and are foreign-sponsored attacks on United States interests; and
- ➢ coordinate training for cyber investigators and infrastructure protectors in government and the private sector.

The NIPC publishes a document called ‘cybernotes’ every two weeks since 1999 for security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices. CyberNotes seeks to provide computer security professionals with a summary of security-related topics and issues and does not provide exhaustive details regarding any issue. CyberNotes does provide references to the respective sources used in compilation of the report in order to allow follow up on the part of the security professional.

There is another useful publication called 'highlights' that is published on a monthly basis by the National Infrastructure Protection Center (NIPC). Its mission is to apprise policy and/or decision makers of current events, incidents, developments, and trends related to Critical Infrastructure Protection (CIP). Highlights seeks to provide policy and/or decision makers with value-added insight by synthesising all source information to provide the most detailed, accurate, and timely reporting on potentially actionable CIP matters.

• Federal Bureau of Investigation National Computer Crime Squad

http://www.emergency.com/fbi-nccs.htm

USA based site that briefly outlines some guidelines in prevention and contingency management

The FBI's National Computer Crime Squad (NCCS) investigates violations of the Federal Computer Fraud and Abuse Act of 1986. These crimes cross multiple state or international boundaries. Violations of the Computer Fraud and Abuse Act include intrusions into government, financial, most medical, and Federal interest computers. Federal interest computers are defined by law as two or more computers involved in a criminal offence, which are located in different states. Therefore, a commercial computer which is the victim of an intrusion coming from another state is a “Federal interest” computer.

• The Internet Engineering Task Force

http://www.ietf.org/html.charters/wg-dir.html#Security_Area
http://www.ietf.org/internet-drafts/draft-ietf-grip-prot-evidence-01.txt

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. It covers such topics as security and electronic evidence collection

• Computer Incident Advisory Capability

http://www.ciac.org/ciac/CIACHome.html

This is a USA based site for the Department of Energy and provides realtime listing of current risks and threats to computer networks.

CIAC provides on-call technical assistance and information to Department of Energy (DOE) sites faced with computer security incidents. This central incident handling capability is one component of all encompassing service provided to the DOE community. The other services CIAC provides are: awareness, training, and education; trend, threat, vulnerability data collection and analysis; and technology watch. This comprehensive service is made possible by a motivated staff with outstanding technical skills and a customer service orientation. CIAC is an element of the Computer Security Technology Centre (CSTC) which supports the Lawrence Livermore National Laboratory (LLNL).

• CERT

http://www.cert.org/

This is the USA based organisation of the Australian AUSCERT. They are not directly related other than serve the same purpose of each other in their respective countries and all belong to the same 'community'

At the CERT®/CC, we study Internet security vulnerabilities, provide incident response services to sites that have been the victims of attack, publish a variety of security alerts, do research in wide-area-networked computing, and develop information and training to help you improve security at your site.

• EuroCERT

http://www.eurocert.net/

This is a European based website.

EuroCERT provided an information and co-ordination service as part of the SIRCE (Security Incident Response Co-ordination for Europe) pilot sponsored by TERENA to provide support for computer Incident Response Teams (IRTs) in Europe.

• Forum of Incident Response and Security Teams

http://first.org/

USA based website.

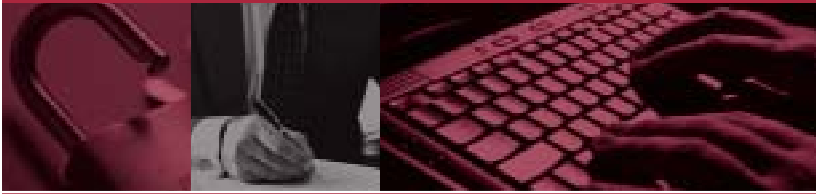
The Forum of Incident Response and Security Teams (FIRST), brings together a variety of computer security incident response teams from government, commercial, and academic organisations. FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large.

ICA acknowledges the support provided by the Undernoted in the preparation of this document

Name	Company
Andrew Lennon	Allianz Australia Limited
Iain Cottrell	AMP General Insurance Limited
Tim Gove	CGU Insurance Limited
Kym Bennetts	EIG-Ansvar Limited
Michael Arnold	General Insurance Enquiries & Complaints Scheme
Colin Dickings	Insurance Council of Australia Limited
Brian Hollis	Insurance Council of Australia Limited
Ragini Rajadurai	Insurance Enquiries & Complaints Limited
Andrew Yeend	NRMA Insurance Limited
David Phillips	QBE Insurance (Australia) Limited
Geoff Bown	QBE Mercantile Mutual Limited

Disclaimer

The information contained in this document is provided "as is". All warranties and representations of any kind with regard to such information are hereby disclaimed, including any implied warranties of merchantability and fitness for a particular purpose or warranties as to any results to be obtained from the use of such information or derived from such information. The Insurance Council of Australia Limited (ICA) its participant firms, and all other parties that provided information for the purpose of creating this document shall not have any liability for any losses (in contract, tort, warranty or otherwise) incurred in connection with (i) any decision made, or any action or inaction taken by any party in reliance upon the information contained in this document; or (ii) any inaccuracies, errors in, or omissions of the information contained in this document. Under no circumstances will ICA in itself be liable for any ordinary, direct, consequential, incidental, special, punitive, or exemplary damages arising out of any of the foregoing.



www.ica.com.au

INSURANCE
COUNCIL OF
AUSTRALIA

Insurance Council of Australia Limited ABN 50 005 617 318
Level 3 56 Pitt Street Sydney NSW 2000 Australia
Telephone: 61 2 9253 5100 or 1300 728 228 Facsimile: 61 2 9253 5111

www.ica.com.au