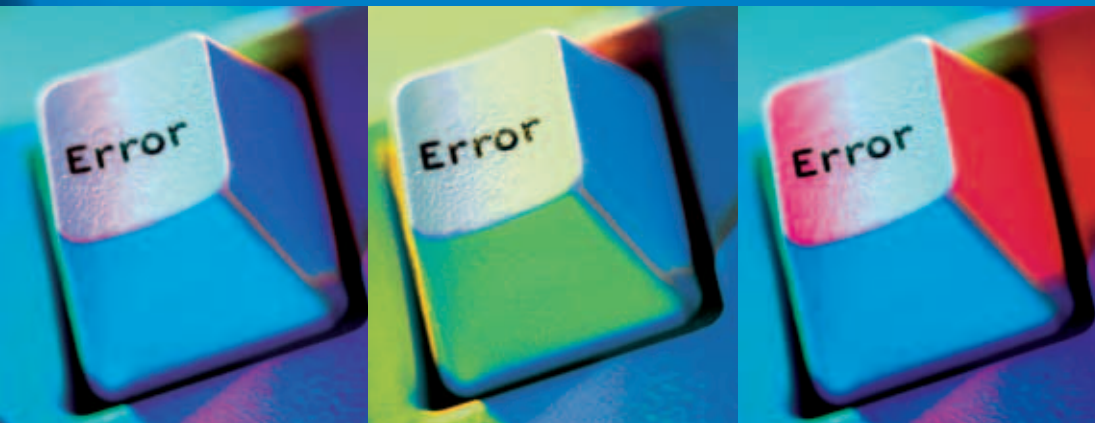




ERRORS & OMISSIONS RISK MANAGEMENT GUIDE

For Information and Network Technology Companies



0
1
2
3
4
5
6
7
8
9

ERRORS & OMISSIONS RISK MANAGEMENT GUIDE

For Information and Network Technology Companies

Both the number and cost of information and network technology errors and omissions (E&O) claims have been steadily rising. At the source of increasing E&O litigation are a number of factors, including the following:

- The trend toward using third parties for information and network technology solutions on a contract basis.
- An increase in business partner litigation, arising from customers' increased willingness to sue long established business partners for performance failures.
- Dramatic increases in average contract size, increasing the likelihood that a performance failure will be "worth the fight."
- An increase in average contract length, causing changes in contract specifications to be more likely and problems with delivery or bugs to more dramatically affect the ongoing business of the customer.
- Greater competitive pressure on the information technology "provider side," increasing the chances that marketing and sales pressure will invite over promising of provider capabilities.
- Greater dependence on information technology solutions, increasing the likelihood that software solutions will be core business solutions.
- An increase in the likelihood that customers will allege misrepresentation or fraudulent inducement and seek extra contractual remedies that can compromise the waiver of consequential loss (which has become the standard in software contracts).
- An increase in the number of companies "going global," resulting in a host of new exposures arising from foreign laws and regulations.
- Greater dependence on interconnected networks and the Internet resulting in new exposures.

WHY CHOOSE CHUBB?

Chubb is a leading insurer of electronics manufacturers, assemblers, software developers and networking companies as well as a growing number of emerging information technology companies. We know how to manage risk in an environment where innovation is a business imperative, not a lofty goal.

This guide, which is aimed at helping you avoid or mitigate exposure to E&O claims and litigation by gaining a better understanding of the risks associated with your business, will discuss in detail areas of potential E&O exposure for the information and network technology industry.

CONTRACTS AND AGREEMENTS

Legal review of contracts and agreements

Have legal counsel review all contracts, purchase orders, and license and service agreements, including those with subcontractors.

Customising contracts

Wherever possible, use standard contracts that set out risk positions you are comfortable with and that you are familiar with. If you must customise an agreement, ensure you understand all the implications of the changes and take every precaution possible to protect yourself from litigation. For example, use boilerplate amendments that become "standard exceptions," or make sure your legal counsel reviews all the deviations from standard.

Limitations of liability

Take advantage of all contract language measures that enable you to allocate risks and responsibilities, and to manage your liability risk. A good starting point is to consider what you want to totally exclude, and what liabilities you might be willing to accept on the basis of capped exposure (e.g. the value of the contract, or a multiple of that value). You should understand and manage your exposure to claims of loss of revenue, profits or savings, and indirect, consequential and similar damages by excluding or capping them. Exclusion and limitation of liability must conform to and be subject to the requirements and provisions of the Trade Practices Act.

Warranties

You should only give warranties that you understand and accept the performance risk on. Do not give warranties that are difficult to meet. Make the warranties appropriate and as specific as possible, avoiding the use of "general warranties" wherever possible. Include warranty disclaimers in your contracts. They help minimise your exposure to litigation by limiting the types of warranties that you are willing to offer. Warranty disclaimers, in relation to

exclusion and limitation of liability, must conform to and be subject to the requirements and provisions of the Trade Practices Act. There may also be other regulatory requirements that are relevant to the particular transaction and should be complied with.

Severability

Include an entire agreement clause in your contracts. Without it, your ability to rely on provisions in your contract that limit your liability may be jeopardised if a court finds another provision in your contract unenforceable.

Indemnities

If you are willing to give an indemnity, stipulate the indemnification procedures, terms and conditions that you want to follow if the indemnity is invoked by the customer. Protect the assets of your organisation by having indemnification wording that inures to your benefit and you should consider what indemnities you may wish the customer to give you. In many cases, asking for reciprocal indemnity is not unreasonable and will result in the customer withdrawing or moderating their request.

Arbitration

Consider including arbitration provisions in your contracts as a means to resolve customer disputes in lieu of litigation.

Force majeure

This wording is important for all information and network technology companies. It is especially critical if you operate in natural catastrophe-prone areas, particularly for online services or any business that relies on communications infrastructure to deliver services or products to its customers. Force majeure clauses limit your liability for losses or breaches resulting from external forces such as earthquakes, tornados, storms or other natural events, as well as events such as war. Specifically list the things you believe would be outside of your control rather than relying on a blanket clause stating "anything outside of your control."



Performance specifications

When negotiating contracts, ensure that all parties agree to and document ahead of time the specific expectations, promises and contingencies regarding the performance of the contract. Complete RFPs (Request for Proposal) and contract performance obligations should be included. Confirm whether or not critical employees are expected to be present throughout the course of the contract. If consultants, value-added resellers or other third parties are involved with a project, make sure that your customer knows exactly what you are (and are not) providing. Likewise, be sure you have confidence in whatever systems you are using, acquiring or recommending. Contracts should be specific regarding agreed-upon definitions, performance specifications, timetables, measures for dealing with contract and performance changes, and the processes and procedures to be used in dispute resolution.

Performance obligations

Be specific but brief with regard to performance obligations. This is not the place to be boastful about your abilities to achieve lofty performance standards.

Amendments and modifications

Specify the procedures for making amendments and modifications to your contracts. All such changes should be required to be made in writing. Where possible, standardise the documentation for requesting and agreeing to contract changes. Document any changes made to product and service specifications and deliverables.

Contract length

If possible, implement smaller, shorter-term projects under multiple short-term contracts. Longer contracts tend to be more complex and may change over time, presenting more opportunities for missed completion dates, which can result in the failure or non-delivery of a project, which in turn can lead to litigation. If shorter-term contracts are not an option, conduct a thorough risk assessment of the entire project. Consider such factors as the scope and inherent

feasibility of the project, the stability of customer requirements, the development and quality practices of the manufacturers, and how realistic the estimates are with regard to the time, money and other resources needed to successfully complete the project.

QUALITY AND SUPPORT OF PRODUCTS AND SERVICES

Quality control

Implement quality control systems at every phase of production. At a minimum, set standards for acceptable levels of reliability, performance, functionality and scalability, compatibility with integral systems, product life span, the time it takes for deployment, and ongoing support and service. Your checklist for the development of a quality product or service should include the following:

- Alpha testing
- Beta testing
- Formal customer acceptance procedures
- Prototype development
- Statistical process control
- Vendor certification process
- Total quality management
- A formal product recall plan
- Products or services produced to nationally or internationally accepted standards (e.g. IEE, DOD, CMM, ISO and FDA)
- Retention of critical contracts, documents and records for clearly defined time standards
- Written and formally implemented quality control program

Discontinued products or services

Openly communicate to your customers any plans you may have to discontinue producing a product or to discontinue its service. Give them sufficient advance notice of the phase-outs and, if possible, a migration path to some other suitable product or service.

Outsourcing and resellers of services

Include in your contracts language that limits your liability in the event one of your outsourced suppliers fails to deliver as promised. If you are unable to fulfil your contractual obligations due to a failure of an outsourced vendor, you could have significant E&O exposure created by breach of contract.

Merger or acquisition activities

Carefully review the prior liabilities and loss experience generated by any organisations being considered for merger or acquisition. Only purchase the assets of an organisation that has a history of litigation problems or difficulty with managing or completing projects.

OPERATIONAL CONTROLS

Legal review of advertising materials and product brochures

Ensure that legal counsel reviews all advertising and marketing materials with regard to the promises explicitly made or implied to customers. Set realistic expectations and avoid absolutes (e.g. the best, the most comprehensive, 100% foolproof) in marketing materials. Product and promotional literature may develop expressed or implied warranties not contemplated in the contracts that are being used. A thorough legal review can reduce unintentional warranties from being enforced during litigation.

Accounts receivable collection procedures

Be cautious of changing your accounts receivable collection procedures. For example, if you have not been aggressively closing out accounts, be wary of doing so. Changing such practices often leads to counterclaims from customers who allege that your products or services are not performing as intended. Your customers could make these allegations in an effort to evade their payment obligations.

Sales and marketing training

Seek legal counsel's assistance in developing sales and marketing training programs that control product oversell and puffery. If any confusion exists between what a salesperson tells a customer and what the contract says, a claim may be made for misrepresentation or fraudulent inducement.

Certificates of insurance

Require suppliers, subcontractors and vendors supplying or doing work for you to carry suitable levels of liability insurance, including E&O, commensurate with the service or product provided. Obtain certificates of insurance from all suppliers, vendors and subcontractors as evidence that they have complied with your requirement. The certificates should specify effective dates, limits and coverage afforded.

NETWORKING ISSUES

Network security

Any company connected to the Internet should have in place a formal security program and communicate its specifics to all employees. Ensure that the program is updated, documented and adhered to by your staff. Closely review the encryption, firewalls, virus protection, security protocols and intrusion detection used to safeguard the data of others stored on your networks and servers. The following risk management recommendations apply to companies' external networks (if any) as well as internal networks. An external network is defined as any network or combination of network elements that lie outside of the network you use to manage your business and is used to provide services to your customers.



- **Security manager**
Assign an individual or team ongoing responsibility for monitoring security threats such as virus infestations, DOS attacks and password theft.
 - **Testing and validation**
Invest in regular, frequent network vulnerability scanning by an outside vendor to validate that your security program is being adhered to. If holes or weaknesses are found in the network, take immediate steps to fix the problems.
 - **Incident logging and investigation**
Record and investigate all security threats and incidents. Without quick and proper investigation, problems can spread throughout a company's network. If your entire external network is affected, you may be at risk for a multiple litigant, class action lawsuit.
 - **Formalised disaster recovery program**
Develop a formal disaster recovery plan. The absence of such a program may be construed as gross negligence by the courts.
 - **Crisis management**
Have in place a crisis management plan. Be prepared to quickly convey accurate information regarding security threats and incidents to all appropriate parties.
 - **Access authorisation/revocation**
Establish access authorisation procedures for all of your systems. Prevent former employees from accessing your systems by revoking their access or authorisation codes.
 - **Background checks of employees**
Conduct background checks of employees and potential employees. Avoid hiring or retaining those with the potential to be security risks or those who create potential litigation problems.
 - **Security training**
Provide all contractors and employees with security training commensurate with their level of access. Companies are using more and more contract labour when developing products and services. This could lead to serious security ramifications if the contractor does not receive the proper security training and adhere to the agreed-upon security procedures.
- Network reliability, redundancy and availability**
- Additional areas of concern for network service providers are their customers' expectations with regard to network reliability, redundancy and availability. These issues, in addition to security, should be covered under your service level agreements.
- **Ensuring reliability**
Adhere to best practices with regard to architecture design. Use high-quality software, hardware and outsourced service vendors. Perform ongoing maintenance and upgrades.
 - **Ensuring redundancy**
Design your network in such a way that traffic cannot be lost or interrupted due to a break in the network. Be capable of backing up or mirroring customer data on another part of the network to minimise or eliminate downtime in the event of an interruption to service.
 - **Ensuring availability**
In addition to building a redundant network, ensure that its design allows for load balancing in times of peak capacity.

DISPUTES AND ALLEGATIONS OF NON-PERFORMANCE

Loss history

Carefully analyse all non-performance losses, claims and litigation as well as their causes. Include in your review all suits, potential suits, complaint letters, disputes or any other circumstances alleging non-performance of your product or services. A thorough loss history can be a window on future litigation problems and should be used to help identify and eliminate potential sources of loss, claims and litigation.

Product rollbacks or recalls

If you have had product rollbacks or recalls in the past, document why they occurred and the remedies used for resolving customer loss of use.

Contract delays

Examine the causes of any contract delays you have experienced. If the delays arose from promising unrealistic deadlines or agreeing to unrealistic customer expectations, address the issue with your sales force and customers and negotiate more reasonable contract terms.

Contract disputes/non-payment

Once a contract is in dispute or a customer is withholding payment, you should strive to work with that customer to resolve the dispute and avoid litigation. Aggressive attempts to get paid for a project that remains in dispute tend to invite breach of contract claims. Instead, positive dialogue and frequent, open discussion concerning the viability of any project as it progresses enables both parties to resolve disputes before they get out of hand and take action when a project hits a snag. Projects can proceed, be cancelled or be redirected by scaling them back or changing the requirements, thereby resulting in a win-win for both parties.

Important Notice: This guide is advisory in nature. It is offered as a resource in developing or maintaining a loss prevention/risk management program. The guide is necessarily general in content and intended to give an overview of certain aspects of information and network technology errors & omissions liability. It should not be relied on as legal advice or a definitive statement of the law in any jurisdiction. For such advice, readers should consult their own legal counsel. No liability is assumed by reason of the information this document contains.



Chubb Insurance Company of Australia Ltd

ABN 69 003 710 647 AFS Licence Number 239778

Sydney Level 36, Tower Bldg, Australia Square, 264-278 George Street, Sydney NSW 2000
Melbourne Level 14, 330 Collins Street Street, Melbourne VIC 3000
Perth Level 22, Exchange Plaza, 2 The Esplanade, Perth WA 6000
Brisbane Level 11, 12 Creek Street, Brisbane QLD 4000

Tel (02) 9273 0100
Tel (03) 9242 5111
Tel (08) 6211 7777
Tel (07) 3229 4488

Fax (02) 9273 0101
Fax (03) 9642 0909
Fax (08) 9325 7730
Fax (07) 3221 1677

<http://www.chubb.com>

Disclaimer: For promotional purposes, Chubb and Chubb Insurance refers to member insurers of the Chubb Group of Insurance Companies. Coverage is underwritten by the Chubb Insurance Company of Australia Ltd, AFS Licence Number 239778. This information is descriptive only. The precise coverage afforded is subject to the terms and conditions of the insurance policy when issued. Chubb recommends considering our policy wording in deciding whether to acquire or to continue to hold Chubb insurance products.

RMG/12/04