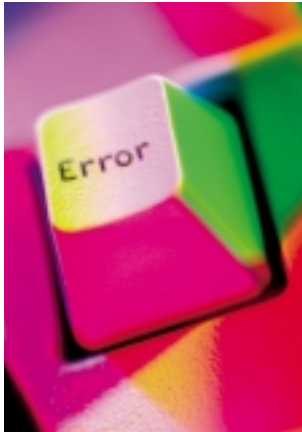# Errors & Omissions

**Risk Management Checklist
For Information and Network
Technology Companies**

Are you exposed to the often-unnecessary financial risk of an allegation of nonperformance? Errors and omissions (E&O) suits are occurring with increasing frequency throughout the information and network technology industry. Even if your products and services perform as they should, you could find yourself embroiled in costly and time-consuming litigation if you fail to adopt some simple but effective procedures.

Test your E&O risk management fitness — answer the following questions to find out if your company may be exposed to an E&O lawsuit. If your answer to any of these questions is "no," then you may need assistance in developing a risk management program or enhancing your current program to help better protect your company's assets. For help, turn to Chubb's technology underwriting specialists — they understand your business and can help identify areas where you can mitigate your company's exposure to E&O losses.

CONTRACTS AND AGREEMENTS	Yes	No
Does legal counsel review all contracts, orders, and license and service agreements?		
Do you always use a standard contract?		
Do you limit your liability in all contracts to avoid consequential loss, punitive damages, stipulated damages or liquidated damages?		
Do you include warranties and other disclaimers in your contracts and promotional material?		
Do all disclaimers and limitations of liability in your contracts conform to applicable legal requirements in terms of typeface and content?		
Are all warranties specific and realistic?		
Do your contracts include a severability clause, arbitration clause and "force majeure" wording?		
Do your contracts ensure that all parties agree to the specific expectations, promises and contingencies regarding the performance of the contract?		
Do you include RFPs and contract performance obligations?		
Do you confirm whether or not critical employees are expected to be present throughout the course of the contract?		
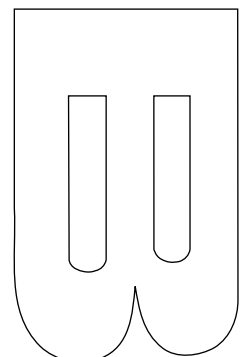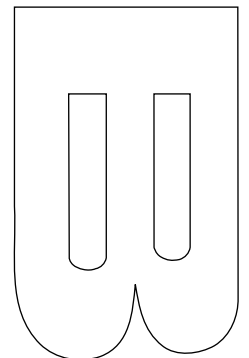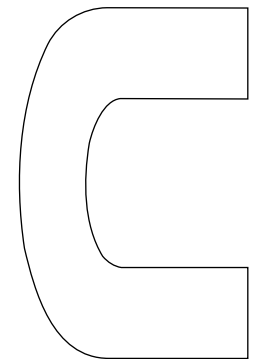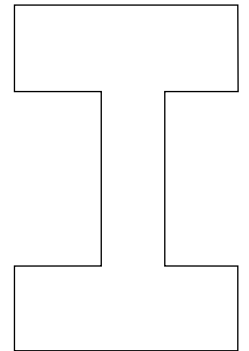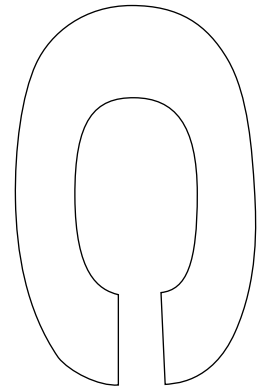
CONTRACTS AND AGREEMENTS *(continued)*	Yes	No
Are your contracts specific regarding agreed-upon definitions, performance specifications and obligations, timetables, dealing with changes and dispute resolution procedures?		
Do you document any changes made to product and service specifications and deliverables?		
Do you seek to implement longer-term projects under multiple short-term contracts?		
For longer-term contracts, do you conduct a thorough risk assessment of the entire project?		

QUALITY AND SUPPORT OF PRODUCTS AND SERVICES	Yes	No
Do your quality control procedures 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 and FDA)		
• Retention of critical contracts, documents and records for clearly defined time standards		
• Written and formally implemented quality control program		
Do you communicate plans to discontinue producing a product or to discontinue its service to all customers?		
Do your contracts limit your liability in the event one of your outsourced suppliers fails to deliver as promised?		
Do you carefully review the prior liabilities and loss experience generated by any organizations being considered for merger or acquisition?		

OPERATIONAL CONTROLS	Yes	No
Does legal counsel review all advertising and marketing materials with regard to the promises explicitly made or implied to customers?		
Are you cautious of changing your accounts receivable collection procedures?		
Do you seek legal counsel's assistance in developing sales and marketing training programs?		
Do you require subcontractors and vendors supplying or doing work for you to name you as an additional insured on their E&O policies?		
Do you obtain certificates of insurance from subcontractors and vendors?		

NETWORKING ISSUES	Yes	No
Do you have in place a formal security program that is regularly updated, documented and adhered to by your staff?		
Have you reviewed the encryption, firewalls, virus protection, security protocols and intrusion detection used to safeguard the data of others stored on your networks and servers?		
Has an individual or team been assigned ongoing responsibility for monitoring security threats?		
Do you invest in regular, frequent network vulnerability scanning by an outside vendor?		
Do you record and investigate all security threats and incidents?		
Do you have in place a formal disaster recovery plan?		
Do you have in place a crisis management plan?		
Have you established access authorization procedures for all of your systems that prevent former employees from accessing your systems?		
Do you conduct background checks of employees and potential employees?		
Do you provide all contractors and employees with security training commensurate with their level of access?		

NETWORK RELIABILITY, REDUNDANCY AND AVAILABILITY	Yes	No
Do you adhere to best practices with regard to architecture design?		
Have you designed your network in such a way that traffic cannot be lost or interrupted due to a break in the network?		
Are you capable of backing up or mirroring customer data on another part of the network?		
Does the design of your redundant network allow for load balancing in times of peak capacity?		

DISPUTES AND ALLEGATIONS OF NON-PERFORMANCE	Yes	No
Do you carefully analyze all non-performance losses, claims and litigation as well as their causes?		
If you have had product rollbacks or recalls in the past, have you documented why they occurred and the remedies used for resolving customer loss of use?		
Do you examine and respond to the causes of any contract delays?		
Do you have frequent and open discussions with your customers regarding the viability of any project as it progresses?		