



SMS

APPLICATION SOLUTIONS FOR THE ENTERPRISE

Managing Risk May Keep Emerging Tech Firms From Becoming a Statistic

BY LISA KRIST

CHUBB GROUP OF INSURANCE COMPANIES

One evening last May, thieves kicked in the door of a software company in the Northeast and stole most of its laptops, phone system, and servers—about \$130,000 worth of electronic equipment. That's a significant loss for a business of any size. But for an emerging technology company, even a relatively small loss due to theft, a fire or a burst boiler can be staggering, potentially threatening its ability to stay afloat.

Insurance can play an important role, allowing the business to replace lost property and revenue during a temporary shutdown. But a theft or fire can have repercussions that extend well beyond the value of the lost or

stolen property. Physical losses can cause delays that make it impossible to meet contractual deadlines, resulting in breach-of-contract lawsuits.

Technology companies are facing greater risks than ever—especially when it comes to product and service performance. Seventy-eight percent of IT organizations have been involved in a dispute that has ended in litigation, according to the Cutter Consortium. In more than half those situations, lawsuits stemmed from a failure to meet promised delivery dates. Given competitive pressures and technological complexities that surround technology undertakings, this upward trend in litigation is likely to continue.

RISK COMES IN DIFFERENT FORMS

In many respects, the risks that emerging technology firms face are not very different from those of other companies. Fires, floods, hurricanes and equipment failures can affect any type of business. Too often, however, fast-growing technology companies are living on the edge. Some may be so concerned with finishing one project and snagging the next that they may overlook the need to take common-sense steps to reduce their vulnerability to costly and potentially devastating mishaps.

One of the worst risks a young company faces is an interruption in business resulting from a physical event, such as a fire or a natural disaster.

An office fire can wipe out months of data in a matter of hours. Last year, a cleaning crew stole property from a small West Coast software company and other tenants in the same building. When the thieves realized security cameras had captured them on videotape, they set the building on fire. While insurance paid the technology company \$100,000 for the property that had been lost and covered a portion of its lost business income while it struggled to get the business going again, much of the firm's existing projects and intellectual property was lost and its reputation with customers was damaged.

Stolen hardware is another common risk technology companies face. The cost to replace stolen hardware costs technology companies almost \$250 million a year, according to a study conducted by RAND, the nonprofit research institution. When RAND calculated indirect costs—including subsequent increased security efforts and missed sales—losses swelled by another \$1 billion.

The RAND study found that 70 percent of reported hardware losses occurred while technology equipment was in transit. Manufacturers and assemblers of computers, computer peripherals and other communications equipment may be especially vulnerable to losses during shipping but, in fact, all emerging technology companies face this risk. Consider the example of a software firm in the Southwest that shipped a \$100,000 server to a third party to be upgraded. The server never made it; it was lost in transit.

Stolen laptop computers continue to

be a thriving trade. Today's thieves are just as interested in the information stored on the laptops as in the hardware itself. While laptops are often stolen one at a time, more devastating losses occur when multiple laptops are stolen right off the desks of employees. This carelessness translates to financial loss for firms: according to the 2002 Computer Security Institute/FBI Computer Crime and Security Survey, companies lost an average \$89,000 due to laptop theft. While the physical loss of computers and laptops can create a financial hardship, cyber crimes caused even greater financial losses. Companies reported losing on average \$283,000 as a result of attacks by computer viruses.

In addition to physical losses, emerging technology companies are vulnerable to claims of "technology malpractice." Frustrated with what they perceive as unmet promises, disgruntled customers of technology companies are increasingly turning to the legal system for compensation to cover financial losses incurred due to missed deadlines by their IT contractor and/or disappointing product performance. Such disputes, often resulting in lawsuits, typically claim negligence in maintaining acceptable professional standards or breach of contract for failing to perform services within the time frame and terms of the contract.

In one example last year, the customer of a small Internet service provider (ISP) claimed that it lost the right to its Internet domain name because the ISP failed to properly handle the transfer of its name and Web address. The customer sued for \$50,000, a stunning blow for an

ISP with annual revenues of only \$300,000.

Technology errors and omissions claims and litigation is a growing problem for companies large and small, but emerging technology companies seem particularly vulnerable to certain traps. Smaller companies hungry for a lucrative contract may oversell their capabilities or underestimate the complexity of the projects they are bidding on. On Web sites, in brochures and during sales presentations, a sales representative may overstate the firm's experience, capabilities or ability to complete projects better, faster and for less money than its competitors. Such puffery can come back to haunt a company when a project doesn't meet the client's expectations.

Finally, emerging technology firms often work with clients who are many times larger than they are—giving the client the upper hand in negotiations. In such instances, some emerging technology companies may be willing to sign a customer's contract instead of their own standard contract. And, too often, they do so without first consulting their own lawyer to make sure their company's interests are adequately represented. In one example, an emerging technology company signed its customer's contract, which assigned all responsibility and liability for any problems to the small company—putting it in a compromising position.

MANAGING RISK

To protect their growing businesses and to avoid becoming a statistic, emerging technology companies need protocols for managing assets, both physical and intellectual:

Protect your hardware. Don't leave laptop computers on the back seat of the car or on top of a desk in the office, for that matter. Lock them up or take them home. One of the basic principals of insurance is to spread risk. If employees take their laptops home, they won't all be lost if someone breaks into the office.

Protect your data and your network. Any company connected to the Internet should have a formal security program that has been communicated to all employees. The program should include provisions for maintaining adequate backups offsite, including the backup of data every one to two days. Encryption, firewalls, virus protection and intrusion detection software are critical barriers to hackers, but are worthless if they are not updated regularly.

Develop a disaster recovery plan. Developing a comprehensive disaster recovery plan can help your company reduce the likelihood and impact of a disaster; enable it to respond quickly and effectively to an emergency to ensure the safety of employees and to contain losses; and establish contingencies to stay in business during a disaster and resume normal business operations as quickly as possible.

Use resources when engaging in a contract. Be wary of signing customers' contracts, and avoid customizing standard contracts. Take advantage of all contract language measures that enable you to limit your liability. Make sure that all parties agree to specific expectations, promises and contingencies regarding the performance of the contract, and specify procedures for modifying it. If possible, implement smaller, shorter-term contracts.

Longer contracts tend to be more complex and may change over time.

Manage quality and support of products and services. Implement quality control systems that, at a minimum, set standards for acceptable levels of reliability, performance, functionality, scalability and compatibility with integral systems.

Analyze performance complaints and contract disputes. An analysis of past claims and complaints from customers can provide a window on future litigation problems and should be used to help identify and eliminate potential problems. Determine if frequent contract delays arise because your company promises to meet unrealistic deadlines or agrees to unrealistic customer expectations.

Implement operational controls. Ask your lawyer to review advertising and marketing materials with regard to the promises explicitly made or implied to customers. Set realistic expectations and avoid boasts that are absolutes—claims of being “the best” or products that are “100 percent foolproof.” Your lawyer can also help develop sales and marketing training programs that prevent overselling. Any confusion between what a salesperson tells a customer and what the contract says may lead to a claim for misrepresentation or fraudulent inducement. Require subcontractors and vendors supplying or doing work for you to name you as an additional insured on their policies, and verify it by obtaining certificates of insurance.

FINANCIAL PROTECTION

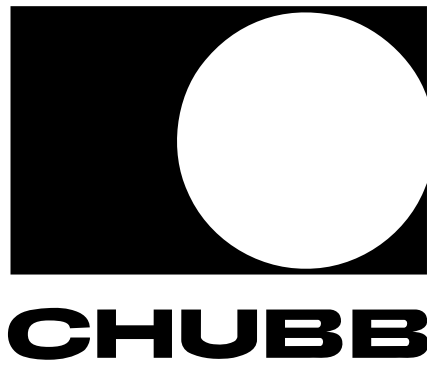
Although prudent risk management

may help contain losses and put a company back on its feet, it does not diminish the need for a comprehensive insurance portfolio. Examining the effectiveness of an emerging technology firm's insurance portfolio in light of its current, as well as its future, vulnerabilities is critical. A thorough evaluation can reveal, for example, that insurance might be needed to pay workers compensation costs for employees not otherwise covered while working on a project overseas. An emerging technology company might also want a policy that anticipates rapid growth by automatically increasing property limits over the course of a year. Any company that does business on the Web should look for global coverage.

Insurance agents, brokers and companies that specialize in this field can help emerging technology companies reduce the potential for financial ruin by helping them to accurately develop a risk management program combined with an insurance plan that accurately reflects the vulnerabilities they face. ■

Lisa Krist is assistant vice president and the Innovator product manager in Chubb & Son's Information & Network Technology underwriting segment (Whitehouse Station, NJ)

Reprinted by permission from the publisher of Storage Management Solutions®, Volume 8, Issue 2. ©2003 WestWorld Productions, Inc.



Chubb Group of Insurance Companies
15 Mountain View Road
Warren, New Jersey 07059

www.chubb.com

Form 36-10-0127