Counseling Risk Management in a World of Terror

BY DAVID GURNICK & TAL GRINBLAT


Gurnick

David Gurnick is Managing Partner and Tal Grinblat is an Associate in the Woodland Hills' office of Arter & Hadden. Gurnick and Grinblat practice in the area of Intellectual Property and Technology.


Grinblat

Terrorism is now a fact of life and another risk businesses must plan for. While risks have always been part of business, risk management today requires being prepared for a Pandora's box of new horrors. These now include bombs, bio-terror, chemical attacks, poisoning, computer sabotage, anonymous defamation ("cyber smearing"), and other previously unimaginable crimes. Fortunately, a range of tools are available for clients to reduce the impacts of both historic and new catastrophic threats. Here are steps clients can take to plan and address risks that everyone confronts today:

• *Planning.* Planning for risks starts with identifying threats to a business. It means thinking not only of Acts of God and accidents, but also crimes that were unimaginable before. It is not an overreaction to consider new forms of terror, new torts, and secondary impacts of attacks that happen elsewhere. (See e.g., Global Telemedia Int'l. v. Doe 132 F.Supp.2d 1261 (C.D.Cal. 2001) (internet libel action brought against anonymous defendants).

• *Prioritize.* A client's next logical step is to prioritize what they want their risk management program to accomplish. The choice and order of priorities impacts which options are selected and how they are implemented. Typical goals are reducing chances of an incident, providing physical safety beforehand, and first-aid afterward; protecting property, reducing stress to employees, customers and family; keeping the business running; avoiding lost income, avoiding liability to others, and providing resources to help others.

• *Safety.* Safety is first in most people's minds. This part of risk management focuses on physical and operational safety of a business. Safety first means examining premises, restricting access, improving lighting; video monitoring, and avoiding dangerous conditions like exposed chemicals, dangerous equipment and slip-and-fall hazards. Safety analysis may mean reviewing operating procedures that pose risks to customers, employees or visitors.

• *First Aid.* Hand-in-hand with safety-first, is first-aid after an incident. This reduces the impact of the incident. CPR and basic first aid training are widely available. Other preparedness steps include having emergency supplies on hand, like first aid kits, food and water, flashlights, blankets and other items based on which emergencies company management envisions.

• *Disaster Plan.* In a catastrophic incident at a business, how will the client respond? The answer can be in a step-by-step disaster plan, or different plans, for different emergencies. These can be in the company's operating manual or personnel handbook or stand alone plans. A company's plan will be tailored to its circumstances (geography, staff abilities, management priorities). The plan should tell each person what the company wants them to do, and who to call, in a catastrophic incident.

• *Practice.* Most people recall fire drills from their school days. The military, fire fighters and police train and drill to practice responding to emergencies. This familiarizes personnel with steps to take in an emergency, and uncovers weaknesses that need to be revised. A business's risk management plan may include practicing responses to incidents that could occur.

There are many ways to conduct drills. One is to construct a mock incident. This may mean telling personnel a drill will be conducted and scheduling accordingly. Or management could announce the drill but not identify the location or personnel who will participate. Each disaster plan should include a program to practice implementing the plan.

• *Alertness.* Personnel can be encouraged to be alert, and trained to spot indicators of an impending incident, to call police, to work in a safety conscious way, and to avoid

panic. An alert employee who identifies a potential danger and calls authorities, may prevent a tragedy.

Beyond physical facilities and training, there are a number of legal and contractual steps a business can take as part of a risk management program:

• *"Force Majeure" Clauses.* "Force Majeure" clauses state extraordinary circumstances beyond a party's control, that suspend or excuse contract performance. E.g. Interpol Bermuda Ltd. v. Kaiser Alum. Int'l. 19 F.2d 992; (9th Cir. 1983) (performance excused by force majeure disruption of product delivery to Persian Gulf). They allocate risk, provide predictability and alert parties when performance may be excused. A typical clause might read as follows:

> A party is not liable for failure or delay of performance caused by transportation shortage; unavailability of product supply; compliance with any law, regulation or order of a government official in a public emergency or disaster; Act of God; fire, strike or riot; embargo, war, or terrorism; hurricane, flood, tornado or earthquake, or other event beyond control of the party whose performance was disrupted. Delay resulting from any of these causes will extend the time for performance or excuse performance, as may be reasonable, but will not excuse payment of any amount owed to the other party. A party seeking relief under this provision shall immediately notify the other party in writing stating the cause, the obligation effected, and when performance will occur, which shall be as early as practicable.

The September 11 attacks may result in more attention to these provisions and more frequently including "terrorism" as a "force majeure."

• *Insurance.* A company should use insurance to address catastrophic risks. Some kinds of policies to consider are: (a) property and casualty, covering loss or damage to property of a business; (b) business interruption, to replace income lost in the disruption of an incident; and (c) general liability, errors and omissions, directors and officers liability, to provide coverage for accident claims made by others against a business. Various other kinds of liability insurance, tailored to the nature of the business, should also be considered. These are (d) workers compensation, covering many kinds of injuries to workers; and (e) health and medical insurance to make sure workers have coverage for their medical care.

A client and their broker may look not only at the scope and amounts of coverage, but also at policy definitions, exclusions and restrictions. For example, many policies exclude risks like crime, war or terrorism. Steps could be needed to get other insurance to cover the excluded matters.

• *Corporate Governance.* Corporation statutes in some states provide additional governance flexibility in emergencies. See, e.g., 8 Del. Code § 110; Va. Code Ann. § 13.1-628; Oh. Rev. Code Ann. §§ 1701.01 and 3901.27. Entity governance documents should be reviewed to add or update risk and succession provisions. The charter, bylaws or operating agreement may authorize executives to take charge until usual management can be assembled to make decisions and give directions. Temporary succession arrangements may be included in case key executives are unavailable. A company with several vice presidents should address which of them advances when the President is incapacitated. A procedure could be adopted to fill vacancies on a temporary or permanent basis if any significant part of company's management becomes unavailable.

Internal policies should also be updated with safety, security and succession in mind. For example, some companies prohibit more than two company executives or multiple board members from traveling together on the same plane. Other companies may wish to keep locations of upcoming board of director meetings confidential.

• *Suppliers.* Having multiple suppliers for key products and services is a well-known risk management tool. Increased supplier disruptions make this more important. For example, the main phone company switch for much of New York was at a single location near the World Trade Center. (Young, Trade Center Attack Shows Vulnerability of Telecom Network, WSJ, Oct. 19, 2001 at 1). Now companies are assessing having multiple sources for utilities. The Wall Street Journal reported that a brokerage plans to have a separate backup trading floor to avoid disruption if an incident occurs at its headquarters. (Smith, Morgan Stanley Plans Backup Trading Floor, Just in Case, WSJ Oct.30, 2001 at C1).

• *Data Protection.* Arrangements should be made to protect a company's internal and customer data. This means improving data backup procedures; duplicating computer and documentary data, and storing duplicates at remote sites. This risk management step also requires periodic tests to make sure stored data is recoverable when needed. In addition, backup copies of a company's key operating software should be arranged. It may even be worthwhile to have redundant computers off site for emergency use.

Arrangements should be made for access to source codes if a software provider becomes unavailable. This may include third party source code escrow or on-site source code lock-box arrangements. In a source code escrow, the source code is stored with a neutral escrow using an escrow agreement. In a lock-box arrangement, source code is stored at the licensee's facilities in a sealed container that can be opened in an emergency (akin to a fire-extinguisher stored behind glass, with a notice "in emergency, break glass").

• *Recruiting.* Job candidates may be screened for risks to security, espionage, theft of secrets, sabotage or the like. Care must be taken to assure that screening does not unlawfully discriminate. However, a number of organizations provide validated tests to evaluate dangerous propensities lawfully. Cf. Assoc. of Mexican-American Educators v. Calif. 231 F.3d 572 (9th Cir. 2000) (standardized preemployment screening test did not violate civil rights laws) Testing for dangerous predilections does not eliminate all threats, but in companies with a large workforces, it can reduce the overall incidence of higher risk persons.

• *Communication.* An emergency plan should have a contact list of law enforcement, health and safety officials, company personnel, and steps to reach them and communicate to company personnel. This can include a central phone with a recording to

continued on page 18

"Counseling Risk..." continued from page 7

disseminate emergency information; sharing information over the company's web site, or an email or phone tree. In some disasters electronic communication may not work. Plans may be needed for message trees or relays among personnel.

A company's risk management plan needs to be provided to company personnel, though distribution of some aspects of a plan may need to be limited. A routine memo that personnel do not read may be insufficient. To improve usage and dissemination, the plan may be repeated on the company's web site, in an area for employees. Some companies may put key portions of the emergency plan in wallet size cards to be carried by personnel at all times.

A company should consider telling personnel and possibly customers and the community about its emergency plan. This may be a memo, press release or letter to the public. A company leader may state frankly the range of incidents that can occur and that the company will be vigilant to prevent, or respond to. This instills confidence in others, enhances stability of relationships, and encourages others to adopt plans as well. With wider attention to risk planning the threats of catastrophic incidents may be reduced.

Today businesses must reexamine risk management. A range of options are available and each company's plan depends on how it prioritizes goals. Having a complete risk management plan helps a company protect health and safety, instill confidence, preserve the company after a disaster, and helps others in the community respond to catastrophic risks as well.