

Anticipating the Worst, The P/C Industry Responds to Terrorist Threats

IT'S BEEN SAID MANY TIMES THAT SEPT. 11 was a paradigm shift for many of the world's industries. And it's equally important to contemplate how Sept. 11 changed the property/casualty (P/C) industry. In a flurry of meetings, conferences, and seminars in the past year, the P/C industry has struggled to cope with the new risks that Sept. 11 revealed.

It's also frustrating to see how some industries only react to new threats instead of working proactively. The airline industry did not make random passengers remove their shoes after detailed discussions with industry experts and academics at forums and seminars. Only near disaster on a flight last year prompted this response.

On the other hand, the P/C industry is looking ahead and trying to anticipate the needs of policyholders. Modeling firms have even developed models that contemplate the effect of suitcase nuclear bombs, even though there has never been such an attack. And although there have been no examples of a sovereign nation using cyber terrorism against an enemy (at least none we're aware of), large P/C insurers are already offering coverage despite data limitations and other constraints. The federal government is working with the P/C industry in an unprecedented mode of cooperation to build a "win-win" scenario for both parties.

Volatility

Losses from a major cyber-terrorist attack are potentially large and quite volatile. PricewaterhouseCoopers suggests that worldwide business losses from viruses planted by hackers totaled a stunning \$1.5 trillion in the year 2000 alone. Even the losses for a single attack could be staggering, though volatility of losses is a major concern. *E-Commerce*, an online magazine, notes that a "typical e-commerce concern" could produce losses of up to \$5 million for one company. And these scenarios consider the cyber attacker to be motivated either by profit or mischief; they don't address attacks against U.S. companies by a sovereign government or terrorist organization.

In addition, companies are generally unprepared for traditional 9/11-type terrorism risks, let alone a cyber attack. An FM Global survey of 200 chief financial officers, treasurers, and risk management professionals revealed that 50 percent of those firms are not very well prepared to recover from a major business disruption.

Data collection is a thorny issue as well. Although a few prominent insurers such as Chubb and Lloyd's are offering coverage, the various statistical and advisory agents in the United States don't offer data. To help offset this, the White House and the insurance industry have formed the Insurance Sector Working Group on Cyber Risk Modeling. One of the main goals of the working group is to identify rele-

vant data that will be needed and facilitate its collection. Government-contracted data banks have been gathering information on cyber incidents for years, and now this working group is tying this data to economic losses, giving insurers a better picture about the risks they face.

A Different Risk

Cyber terrorism is a whole new type of risk. Human behavior is difficult to predict even in controlled situations. While actuaries have been using models and other mechanisms to quantify insurance liabilities based on expected litigation behavior related to asbestos or environmental claims, one wonders if it would be possible to use these same models to predict terrorist behavior.

"You're dealing with an entirely different sort of risk," says John Purple, an actuary at the Connecticut Insurance Department and chair of the Academy's Committee on P/C Products, Pricing, and Market. "Most of these types of models deal with human behavior based around economic gain." Terrorist attacks, on the other hand, are scenarios where people spend money to generate chaos and destruction as opposed to spending money to generate economic gain.

GREG VASS IS SENIOR POLICY ANALYST, CASUALTY, AT THE AMERICAN ACADEMY OF ACTUARIES IN WASHINGTON.

Despite the fact that no cyber terrorism was involved, 9/11 was a wake-up call to the industry. Insurers began to prepare for contingencies that before September 2001 were mainly theories discussed by academics. But 9/11 allowed the industry and the U.S. economy to stay ahead of the curve on cyber terrorism.

One of the keys in this type of warfare is to first identify your enemy. To date, the White House has been aggressively attempting to identify what foreign powers are eyeing U.S. businesses for potential attack.

"There are terrorist groups that are interested," Richard Clarke, head of the Office of Cyberspace Security, told reporters. "We now know that al Qaeda was interested. But the real major threat is from the information-warfare brigade or squadron of five or six countries."

Modeling is another step, and current workers' compensation earthquake models are being adapted to address terror-

ism risk. Earthquake models work as a potential starting point because they contemplate a sudden, unforeseen calamity where people and businesses are unable to get out of harm's way. Cyber attacks resemble earthquake events in that they're also unforeseen. The cyber infrastructure will have to rely on its internal safeguards before the attack, just as workers in a earthquake can only rely on building safeguards that are in place well before the incident.

National Security

Perhaps the most compelling reason for the United States to upgrade its cyber attack safeguards is the need to protect national security in the face of a cyber attack from another country. The RAND Public Policy Institute conducted simulations even before 9/11 in which hostile governments wreak havoc, destroying not only economic assets but also lives.

RAND has simulated cyber attacks in

which misrouted aircraft and trains collide, killing and injuring many passengers. Cyber-engineered power blackouts and disruptions to control mechanisms could cause oil refinery explosions and fires. The RAND studies mainly concluded that "everyone can attack you, you cannot know what is real, and it is difficult to know you are under attack."

The cyber infrastructure of the United States is also greatly at risk. A study conducted by the Computer Security Institute reported that 85 percent of U.S. companies had some breach in their computer security in the year 2000. Large gaps in security are nearly an invitation for terrorists to attack not only individual entities but also the Internet infrastructure itself.

The White House/industry working group mentioned above is attempting to beef up the security of U.S. business in a roundabout manner through insurance. White House officials have stated that a primary goal is to improve security by fostering a healthy cyber terrorism insurance market. With a viable market in place, insurers will give discounts to insureds that strengthen their security. As insureds realize these discounts, they'll follow best practice standards determined by underwriters and others and the entire U.S. cyber economy will be less vulnerable to attack.

New Era

The hope is that this partnership of the federal government and the private insurance industry will facilitate the recognition and quantification of cyber terrorism risk that was not contemplated before 9/11. If best practice standards for computer security are promulgated, the security of the entire Internet will improve.

A secure information infrastructure is vital to all industries, and perhaps most vital to the financial services industry. Insurers willing to take risks in this potentially volatile market could yield significant economic gain. And insurers will find out that by working in concert with federal Homeland Defense officials, they will protect not only their bottom lines but our information technology infrastructure itself. ●

1/3
Chicago Consulting
Page 18