ADVISEN
Productivity
& Insight
for Insurance
Professionals

THE GATHERING FRONT
NEW REALITIES OF TERRORISM RISK

March 2012

Sponsored by: CHARTIS®

THE GATHERING FRONT
NEW REALITIES OF TERRORISM RISK

For much of the last decade, the world focused on terrorist threats against government and corporate targets throughout the West. As U.S. military forces worked to corral and curtail these threats, leaders of business and politics steeled themselves against the possibility of repercussions and reprisals.

Recently, the world received a stark reminder that terrorism is not linked to one place in the world or one ideology. Norway, which had not been a target of terrorism and historically has experienced very little crime of any sort, was the scene of a one-day rampage that took nearly 80 lives. On July 22, 2011, Anders Behring Breivik first set off a car bomb in Oslo's government district that killed eight people. He then disguised himself as a police officer, went to an island summer youth camp and gunned down 69 people, mostly teenagers. It was textbook terrorism: Kill as many people as possible in the most dramatic way possible.

Recently, the world received a stark reminder that terrorism is not linked to one place in the world or one ideology.

Terrorism can occur anywhere in the world at any time; any person, business or country can be its target. It can occur on land, in the air or in the water, and in food supplies. It can be directed against physical structures and even against the largely unseen computer networks upon which so many companies have come to rely for their operations. Risk managers must secure businesses against some of the oldest forms of aggression, like piracy, as well as often imperceptible new threats, like cyber-attacks.

As terrorism evolves, so too must corporate risk managers and safety professionals. They must look for vulnerabilities in every facet of their operations, including their plants and offices, as well as supply and distribution chains. They should move toward the development of an enterprise-wide risk management system that protects employees, physical assets and data, wherever they may be around the world. Risk managers should work with their brokers to match their exposures with appropriate insurance coverages.

A Changing Front

According to the National Consortium for the Study of Terrorism and Responses to Terrorism (START), there were 4,640 terrorist incidents worldwide in 2010, up from 1,427 in 2001, although none of the attacks in 2010 claimed as many lives as the 9/11 attacks. The deadliest incident, in Midnapore, India, saw at least 115 people killed and more than 140 injured when unidentified assailants caused a train derailment[1].

Although causalities in 2010 were relatively small, virtually every corner of the world was affected, along with many aspects of daily life.

Although causalities in 2010 were relatively small, virtually every corner of the world was affected, along with many aspects of daily life. Government buildings were targeted, as well as law enforcement, transportation, telecommunications, military installations, private property and citizens, religious institutions and businesses. Some 542 attacks were directed against business interests worldwide in 2010. By contrast, there were just 128 attacks against business interests in 2001[2].

Other types of targets have shown an increased number of attacks as well. In 2001, there were just three attacks against food or water supplies and eight attacks on telecommunications facilities. In 2010, food or water supplies were targets six times and the number of terrorist incidents directed at telecommunications jumped to 54.

But to Brian Finlay, senior associate and program director at the Stimson Center, more worrisome than the number and nature of terrorist attacks, or the weapons that terrorists might choose, is the fact that, a decade after 9/11, the international community remains largely unprepared to address terrorism. "We learned the lessons of the first three aircraft and not the fourth," he says, referring to the planes hijacked on September 11, 2001. Finlay makes the point that it was the initiative of "brave and committed citizens" that kept the plane from reaching its target. Finlay believes that getting the public in the United States and around the world on guard against a subsequent terrorist incident is necessary to build the preventative capacity and preparedness we need.

That need for preparedness extends to businesses, says Finlay. While many corporations understand both the direct and indirect effects that a terrorist attack might have on their businesses, contraction in government spending around the world on counter-terrorism has increasingly left businesses to their own resources, which are often just as diminished.

More than 27 countries currently contribute naval forces towards piracy deterrence.

Piracy in the 21st Century

If there is anywhere that the business community bears a special burden for ensuring its own safety, it is on the high seas. While a handful of countries have decided they will not pay ransom and will retaliate against pirates who target vessels carrying their flag, the protection offered by most countries is simply not enough to cover the vast expanse of ocean that commerce now crosses. Eight percent of the world's cargo goes through the Gulf of Aden and the 22,000 ships[3] that carry it cross into a stretch of ocean as big as the entire European continent.

More than 27 countries currently contribute naval forces towards piracy deterrence. Most military and naval attention is devoted to the Horn of Africa, where "the big three" antipiracy missions are focused: Operation Atlanta, Operation Ocean Shield and Combined Task Force (CTF) 151. Operation Atlanta was launched in the end of 2008 by the European Union with the primary goal of protecting World Food Program vessels delivering aid to Somalia as well as other shipping in the region. Operation Ocean Shield is a NATO initiative to protect shipping in the region. CTF 151 is a multinational Task Force established in 2009 in the Gulf of Aden and the eastern coast of Somalia. Together, the three military efforts comprise about 45 warships operating off the Horn of Africa and the Indian Ocean. Together, they are able to create shipping lanes that are safer for transit and act when within range, but they are not able to protect each ship individually. There are rescue operations, but risk managers have come to know that such daring rescues are not something that they can rely on exclusively.

Instead, shipping companies are increasingly adding private security forces to their crews. "Most of the industry was against the presence of armed guards, but this changed after the Maersk Alabama incident," says Captain Jorge Pecci Saavedra, executive vice president and chief operating officer of Chartis' Global Marine division. "Successful attacks dropped dramatically in 2011 because of the use of security forces on board. However, it potentially raises problems." If an improperly prepared security crew shoots and kills an innocent person, the repercussions could be enormous. Pecci Saavedra worked as a ship's captain until 1993 and knows first-hand the risks of steering a vessel around pirates: His ship was attacked off Nigeria by pirates looking for food.

That kind of piracy seems almost quaint now, when pirates are increasingly looking for crews to kidnap for ransom, and the monies received often going to terrorist organizations. Shipping companies paid $238 million in ransom in 2010 up from $177 million in 2009[4]; the average payout was $5.2 million.

If piracy is one of the oldest forms of terrorism, the Internet has become one of the newest opportunities for disruption.

But that figure doesn't begin to show the full costs of a piracy incident. After an attack, shippers on average need to factor in at least 50 percent more in additional costs to cover damage to the ship and the cost of the ship being out of service. Crews, who already are generally paid a double salary for working on ships in known trouble spots, must continue to be paid while the vessel is out of service. If crew members are injured during the attack, they have to be transported home. If the crew is kidnapped, a replacement crew must be provided while efforts to rescue the original crew are underway.

And then there is this to consider: "One of the most expensive things is to deliver the ransom money," says Pecci Saavedra."It is done by helicopter or fast boat, and under security to prevent the ransom from being hijacked."

The cost of guarding against an attack is steep as well. It can cost $100,000[5] to hire security to work in the Gulf of Aden for just the one week it takes to pass through that area. If the ship's captain seeks a safer route around trouble spots, there will be additional fuel and crew costs. And then there is insurance: War risk surcharges totaled $4 billion in 2010, while the cost of kidnap and ransom insurance premiums was $540 million. The total cost of piracy to the global shipping economy? Ten billion dollars in 2010 alone[6].

The Internet as a Weapon

If piracy is one of the oldest forms of terrorism, the Internet has become one of the newest opportunities for disruption. In an appearance before the Senate Armed Services Committee in June 2011, CIA Director Leon Panetta warned that a cyber attack could be "the next Pearl Harbor".

A cyber event might only be a "white hat" hacker seeking to demonstrate how vulnerable a company's computer network is, or it could be the work of so-called "hacktivists" seeking to make a point about a company policy. But terrorists—some of them state-sponsored—are increasingly targeting computer networks for the intellectual property and confidential information they contain. Once a network is compromised, the targeted company risks damage to its individual operations and repercussions that are both financial and legal. Beyond that lies the concern that, if terrorists take over a computer system used to control a critical piece of infrastructure, like an oil or gas drilling operation or transportation infrastructure, they could shut down segments of the broader economy.

Cyber crimes are on the rise. In an August 2011 study, the Ponemon Institute found a 44 percent increase in successful attacks against companies since its year-earlier study, and a

Cyber crimes are on the rise. In an August 2011 study, the Ponemon Institute found a 44 percent increase in successful attacks against companies since its year-earlier study.

56 percent increase in cost to affected companies. While the average time needed to resolve an external cyber attack is 18 days, the Ponemon Institute found that malicious insider attacks can take more than 45 days, on average, to contain[7]. Companies with Security Information and Event Management (SIEM) systems are better able to spot attacks and control the damage than those without.

Cyber-terrorism can be just as costly as terrorism caused by more traditional weapons. In a study released last year on payouts for data breaches, NetDiligence, a cyber-risk assessment service, put the cost per breach at $2.4 million, with most of that cost stemming from legal services[8]. But that cost does not include damage to a company's brand and reputation. The cost of a recent breach of a major corporation has been estimated at as much as $2 billion.

As the NetDiligence study indicates, a large part of the cost of responding to a cyber-terrorism incident stems from the laws that have been enacted in this area. Whether at the state, national or international level, companies are being required to quickly notify the parties whose data has been breached and provide remediation. If the company has failed to follow the applicable laws, it can be assessed regulatory fines and penalties.

In October 2011, the SEC issued new Disclosure Guidance related to cybersecurity risks. This guidance highlights the need for companies to increase their focus on cyber risk, underscores the severity of cyber exposures to directors and corporations, and advises companies to disclose their cyber exposures, including any relevant insurance coverage[9].

U.S. companies must also be mindful of legislative changes abroad. In January 2012, the European Commission unveiled a proposal that would significantly increase data protection in Europe. Uniform standards could reduce the cost of complying with the patchwork of country-specific standards, but they are being paired with a requirement to notify authorities within 24 hours of a data breach and fines that could be as high as two percent of a company's worldwide sales. The rules will apply to both EU-based businesses as well as those that get access to personal data on European citizens. However, the rules still face debate within the European Parliament and the Council of the European Union, and, if approved, implementation is not likely until the latter part of this decade. But risk managers should keep their potential impact in mind as their companies move forward.

Preparedness and Protection

Mitigation is as complex as the threat itself. Insurance is available for many terrorism threats, but ensuring the appropriate coverages are in place can be challenging. Consider the steps needed to insure against cyber-terrorism alone. To protect itself against liability from a hack that causes computers to fail, a company would need cyber policy coverage. If the attack causes systems to malfunction and leads to physical property damage, a company would need property coverage. If a cyber event harms people, a company would need liability coverage that does not exclude such an event.

Insurance coverage must be coupled with readiness. Erik Nikodem, senior vice president and property division executive of Lexington Insurance Company, recommends that companies regularly run emergency preparedness drills that explore what would need to be done to respond to an attack on every facet of the operation, from building vulnerabilities to the risks that might face employees who travel for business. John J. Salinger, the president of Chartis' [Global] Trade and Political Risk division, cautions that while kidnappings were once used to make a political statement, they have become a central fundraising tool of terrorist organizations. Companies also must plan for redundancy within their supply chain by examining the preparedness of suppliers and being well versed in alternative supply sources.

American companies may take some comfort in the presence of the federal Terrorism Risk Insurance Act, which is a backstop to the insurance industry. But its reauthorization in 2007 put in place rising thresholds for the risk that companies and their insurers will have to bear. Losses from an event must now exceed $100 million for the act to be triggered, up from $50 million at TRIA's inception. And there is a $100 billion cap on coverage per year.[10]

American companies may take some comfort in the presence of the federal Terrorism Risk Insurance Act, which is a backstop to the insurance industry.

Watchfulness and Readiness

"The uprisings that are ending repressive regimes in many parts of the world may serve to diffuse some of the tensions that had played out as terrorist responses and elections may bring new leadership in other countries, contributing to a positive transformation," says Professor Marvin Zonis, professor emeritus at the Booth School of Business at the University of Chicago. "But weak economies could lead things back in a very opposite direction - we could face a vicious cycle of contraction that could slow economic growth around the globe," he adds.

The steep decline in the global economy has had more than just economic repercussions, however. It has undercut efforts by governments to fund counter-terrorism programs and by companies to protect corporate assets and key elements of infrastructure at home and

In the face of these uncertainties, risk managers must reassess every aspect of their operations.

abroad. The absence of another terrorist act on par with 9/11 has led to a relaxed mindset about terrorism in some circles of business and government.

The possibility of disruption has not abated however. Established political leaders remain vulnerable in many parts of the globe and the investment initiatives that they encouraged could vanish with them.

In the face of these uncertainties, risk managers must reassess every aspect of their operations. They must look for vulnerabilities in their plants and offices and in their supply and distribution networks. They must look to safeguard their employees and their data. And they must look to insurance strategies that match their exposures, in every corner of the globe.

"With governments around the world stretched thin by the global recession, a greater share of responsibility will fall on the private sector to protect their interests. When terrorists strike, the vast preponderance of future attacks will be on private sector targets," cautions Finlay. "Businesses need to prepare for that on a tactical level," he adds. But Finlay also advises businesses to remind their governments that terrorism remains an important issue that should demand their attention.

"A major incident," he adds, "is by no means out of the realm of possibility."

REFERENCES:
1. http://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=201005280005
2. http://www.start.umd.edu/gtd/search/Results.aspx?charttype=bar&chart=target&casualties_type=&casualties_max=&start_year=2010&start_month=1&start_day=1&end_year=2010&end_month=12&end_day=31
3. http://www.imo.org/About/Pages/FAQs.aspx
4. http://oceansbeyondpiracy.org/sites/default/files/documents_old/The_Economic_Cost_of_Piracy_Full_Report.pdf
5. http://www.marad.dot.gov/documents/Economic_Impact_of_Piracy_2010.pdf
6. http://oceansbeyondpiracy.org/sites/default/files/documents_old/The_Economic_Cost_of_Piracy_Presentation.pdf
7. http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf
8. http://www.netdiligence.com/files/CyberLiability-0711sh.pdf
9. http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
10. http://www.treasury.gov/resource-center/fin-mkts/Documents/tria-ea_finalrule_08252006.pdf